

Three Essays of Consumer Inference Making and Metacognitive Experience  
in Perceived Information Security

Yong Wan Park

Dissertation Paper submitted to the faculty of the Virginia Polytechnic  
Institute and State University in partial fulfillment of the requirements for the  
degree of

Doctor of Philosophy

In

Business, Marketing

Paul M. Herr

Rajesh Bagchi

Frank R. Kardes

Byung Cho Kim

04.17.2013

Blacksburg, Virginia

Keywords: Information Security, Perceived Security, Inference Making,  
Metacognitive Experience, Fluency, Debias

# Three Essays of Consumer Inference Making and Metacognitive Experience in Perceived Information Security

Yong Wan Park

## ABSTRACT

The internet has served as the virtual world since the beginning of the digital era, and it has provided consumers the valuable source of information and become a fundamental basis of e-commerce by passing the limit of time and distance of offline stores. It is hard to imagine our life without the internet. Because consumers store and access their private and financial information on the internet, information security is even more important than ever. Although many studies demonstrate the importance of information security to consumers, researchers have paid little attention to consumers' inference processing underlying their perceptions of information security. We investigate how consumers infer and evaluate online information security based on consumer inference making process and metacognitive experience. We argue that consumers' perceived security could be enhanced by simply increasing complexity, even if that increased complexity is meaningless. It is because consumers have a belief that security is achieved by sacrificing convenience or increasing complexity. We demonstrated that consumers evaluated a website more secure when asked to enter redundant information in Chapter 1. Chapter 2 suggested that disfluency and difficulty of retrieval could increase perceived security because metacognitive experience makes consumers misattribute their feeling of difficulty to technical difficulty. We found that the positive effect of disfluency was held when a product was not security-related. In Chapter 3, we focused on how to improve the accuracy of security judgments. We found that perceived security enhanced by meaningless complexity would be adjusted by asking specific dimensions of security (Confidentiality, Integrity, and Availability), and the positive impact of a disfluency effect could be debiased by providing participants the true source of their subjective difficulty. Furthermore, we demonstrated that consumers' interpretation about accessibility experience varied depending on what kind of naïve theory was activated. Through a series of experiments, we demonstrated our arguments were valid and these results provided useful insights and implications about consumers' inference processing and perception of information security.

## Acknowledgements

I would like to express my very great appreciation to my advisor, Paul M. Herr, for his valuable and constructive suggestions and guidance during the planning and developing of this research works. I would also like to thank Eloise Coupey and Jane Machin for their help and support to me. My grateful thanks are also extended to all committee members, Frank R. Kardes, Rajesh Bagchi, and Byung Cho Kim for their valuable comments and suggestions.

I would like to extend special thanks to Yong-Won Ha, who stimulated my academic curiosity and interests in marketing and consumer research.

Finally, I am deeply indebted and thankful to my parent and Hyun-A for their emotional support.

Thank you.

# Contents

<b>Introduction</b> .....	1
<b>I Consumer Inference Making about Information Security</b> .....	3
<b>I.1 Introduction</b> .....	3
<b>I.2 Literature Review and Hypotheses</b> .....	4
<b>I.2.A Information Security</b> .....	4
<b>I.2.B Inference Making</b> .....	7
<b>I.2.C Omission Neglect Theory and Consumer Knowledge</b> .....	11
<b>I.2.D Security Inference Making</b> .....	14
<b>I.3 Results of Experiment 1-1(A)</b> .....	21
<b>I.4 Discussion of Experiment 1-1(A)</b> .....	27
<b>I.5 Results of Experiment 1-1 (B)</b> .....	29
<b>I.6 Discussion of Experiment 1-1(B)</b> .....	34
<b>I.7 Results of Experiment 1-2</b> .....	36
<b>I.8 Discussion of Experiment 1-2</b> .....	39
<b>I.9 Results of Experiment 1-3</b> .....	40
<b>I.10 Discussion of Experiment 1-3</b> .....	43
<b>I.11 Results of Experiment 1-4</b> .....	44
<b>I.12 Conclusion and Summary</b> .....	45
<b>II Metacognitive Experience in Information Security</b> .....	48
<b>II.1 Introduction</b> .....	48
<b>II.2 Literature Review and Hypotheses</b> .....	49

II.2.A	Metacognitive Experience .....	49
II.2.B	Metacognitive Experience and Information Security .....	55
II.3	Results of Experiment 2-1.....	58
II.4	Discussion of Experiment 2-1 .....	62
II.5	Results of Experiment 2-2.....	63
II.6	Discussion of Experiment 2-2 .....	65
II.7	Results of Experiment 2-3.....	66
II.8	Discussion of Experiment 2-3 .....	69
II.9	Results of Experiment 2-4.....	70
II.10	Conclusion and Summary .....	72
III	Improving Consumers' Information Security Estimation.....	75
III.1	Introduction .....	75
III.2	Literature Review and Hypotheses .....	76
III.2.A	Debiasing Metacognitive Experience and Omission Neglect .....	76
III.2.B	Debiasing Overestimated Information Security.....	79
III.3	Results of Experiment 3-1.....	81
III.4	Results of Experiment 3-2.....	83
III.5	Results of Experiment 3-3.....	84
III.6	Discussion of Experiment 3-3 .....	87
III.7	Conclusion and Summary .....	88
	Conclusion of Dissertation .....	89
IV	Reference .....	91

<b>V</b>	<b>Appendixes</b> .....	97
	Appendix A. Stimuli in Experiment 1-1.....	97
	Appendix B. Objective Security Knowledge Measures.....	100
	Appendix C. Measures for C-I-A Triad.....	102
	Appendix D. Priming Security Awareness .....	103
	Appendix E. Stimuli of Experiment 1-4.....	105
	Appendix F. Stimuli for Experiment 2-1.....	107
	Appendix G. Raw Data Set .....	109

## The List of Figures

Figure 1 Perceived Convenience and Perceived Security .....	25
Figure 2 Histogram of Subjective and Objective Knowledge.....	26
Figure 3 Confidence of Subjective and Objective Knowledge.....	26
Figure 4 Convenience, Security, and Preference in Control-Twice condition .....	31
Figure 5 The Interaction Effect on Perceived Security.....	32
Figure 6 Convenience, Security, and Preference in Control-Pop-Up condition .....	33
Figure 7 Confidence of Objective and Subjective Knowledge.....	34
Figure 8 The Interaction effect between Priming and Complexity .....	42
Figure 9 The Interaction effect between Fluency and Description .....	61
Figure 10 Preference, Perceived Convenience, and Perceived Security.....	69
Figure 11 The Interaction effect between Naive Theory and Retrieval Ease .....	87

## The List of Tables

Table 1 Parameter estimates of Logistic Regression .....	39
--	----

## **Introduction**

The internet has become an important part of everyday life, and consumers know that their personal information could easily be hacked by even the tiniest mistake on their part. Thus, information security is more important than ever. Many studies investigate information security, but most have focused on technical issues and firm's perspectives. Many studies also demonstrate the importance of information security to consumers, but researchers have paid scant attention to the inferential processes underlying consumers' perceptions of information security. Therefore, we investigate how consumers infer and evaluate online information security using a research paradigm drawing from marketing, social psychology, and consumer psychology principles and frameworks. If consumers do not appreciate security features or know how to accurately estimate security aspects of a product, secure products or websites may lose their competitive edge and the cost to build and offer security may be largely wasted. Hence, it is important to know how consumers evaluate and infer security.

Most theories of human judgment assume that people judge and form an attitude toward a target object based on attributes or features of a target object. In other words, consumers would form a favorable attitude toward the product that has more positive attributes than other products. However, some researchers argue that human judgment is influenced by not only the content of information but also their subjective experience processing information, such as how easily information is retrieved from memory, how easily thoughts are generated, and how fluently information is processed. These subjective experiences are known as metacognitive experience (Schwarz 2004). In this study, we investigate how consumers evaluate or estimate information security based on both the content of information and their metacognitive experience. Specifically, we argue that consumers estimate or infer

information security based on the inconvenience that comes from using attributes or features of a product. This inference making process based on the correlated relationship between inconvenience and perceived security is examined in Chapter 1. We examine the effect of metacognitive experience on perceived security in Chapter 2. Finally, we investigate how to reduce or alleviate consumers' biased security perception in Chapter 3.

# **I Consumer Inference Making about Information Security**

## **I.1 Introduction**

In the movie ‘Mission Impossible,’ Ethan Hunt (Tom Cruise) aimed to stealthily enter a base that was protected by many security devices such as eye scanner, temperature sensor, motion sensor, etc. Since the 911 terror attack, the US Department of Homeland Security has added strict regulations, such as limiting the number of bags and types of items that passengers may carry on aircraft and screening procedures for passengers. Although some people complained about the full body scanning device due to the potential risk of privacy, the government insists that these security-screening systems are necessary for national security, even if increasing inconvenience and slowing down the boarding process. These examples demonstrate that enhancing physical security often comes with installing more security devices, so consumers may have a general belief that complexity is positively correlated with security. When consumers have little product knowledge, they may use their prior knowledge of similar or related product categories to better understand or make an inference about it (Moreau, Markman, and Lehmann 2001; Sujana and Dekleva 1987). Therefore, consumers may extend their general belief, that physical security is enhanced by installing additional devices, to related product or service categories such as information security. In the past, the belief that security is highly correlated with complexity (or inconvenience) had been true not only in the physical world but also in the IT world. However, consumers still hold this belief even though the advancement of science and technology enables companies to develop a product to achieve security without sacrificing convenience (Kim and Park 2012). Consumers may rely on a correlated relationship between security and complexity, and infer security from the complexity of security features. If so, we

suggest that consumers' security evaluations may be enhanced by simply increasing complexity, even if that increased complexity is in fact irrelevant to actual security.

Physical security aims to prevent unauthorized access by unauthorized individuals to specific areas such as facilities and buildings. Information security also intends to protect information from unauthorized access, use, modification and destruction by unauthorized parties, so both physical and information security appear similar. However, there are some differences as well. To this end, we examine the information security literature to understand how information security differs from physical security. Then, the literatures of inference making, omission neglect theory, and consumer knowledge are explored to understand how consumers may evaluate information security based on given product information. We expect inference-making about information security will be similar to the price-quality inference-making because of consumers' general belief that the correlation between security and complexity is highly positive. Based on these literatures, we propose a conceptual model of the information security inference process. Specifically, we argue that consumers' perceived security is enhanced by increasing complexity, even if the complexity is redundant and meaningless. The experiments and results are presented, followed by a discussion of theoretical and managerial implications.

## **I.2 Literature Review and Hypotheses**

### **I.2.A Information Security**

In general, security is defined as the degree of protection against danger, damage, loss, and crime. Security also applies to structures and processes that provide or improve security as a condition ("Security" 2004). Specific meanings of security can differ depending on the context, such as physical, political, financial area, and IT (Information Technology). For

example, physical security means a denial of unauthorized person's physical access to a building or facility, and designing structures or devices to prevent or resist hostile acts. On the other hand, political security, such as homeland security and national security, refers to security efforts to protect the states from terrorist activities and maintain the survival of states by using economic, diplomacy, political and military power. Security in this study, however, is limited to information security. It refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, recording, or destruction ("Information Security" 2004). The fundamental elements of information security are described as the C-I-A triad or information security triad (Chellappa and Pavlou 2002; Chirillo and Danielyan 2005; Flavian and Guinaliu 2006; Gerber and von Solms 2001; Parker 1998; Posthumus and von Solms 2004). The C-I-A triad consists of confidentiality, integrity, and availability. First, confidentiality means to prevent the leak of information to unauthorized people or systems. If, for example, someone looks over your shoulder at your computer screen where critical or important data are displayed, confidentiality is violated. If your password for email accounts is disclosed, people can access your account without your permission. Second, integrity refers to data not being modified undetectably. If unauthorized parties intentionally modify information during information storage, processing, and transmitting, the integrity principle is breached. Even if information modification happens accidentally, integrity is breached. Finally, availability intends that all information should be accessible to authorized users at the right time. Even if confidentiality and integrity are well-kept but authorized users cannot access the information they need, both confidentiality and integrity will be meaningless. Therefore, all three elements of security are equally important.

Information is a valuable asset in most organizations today, so considerable effort is placed on its protection and on enhancing security (Posthumus and von Solms 2004). For

example, the success of e-commerce depends on controlling security threats and increasing consumers' perceived security (Casalo, Flavian, and Guinaliu 2007; Chellappa and Pavlou 2002; Friedman, Kahn, and Howe 2000; Salisbury et al. 2001; Shneiderman 2000). In the last decade, e-commerce has grown dramatically, but consumers' concerns about the security of their private and sensitive information have the potential to limit future growth. Chellappa and Pavlou (2002) argue that perceived information security, distinct from objective security level, is critical in consumer trust in e-commerce transactions. Perceived information security is defined as "the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations" (Chellappa and Pavlou 2002). Salisbury and his colleagues (2001) demonstrate that consumers' purchase intentions from the World-Wide-Web are influenced by not only the ease of navigation but also perceived security. Flavian and Guialiu (2006) also show that consumers' loyalty to a website is closely related to consumer trust, which is also affected by perceived security. Consumer trust plays an important role in purchase intention and behavior, so it affects directly the level of profitability of the website (Flavian and Guinaliu 2006). Similarly, website security directly affects consumer trust in the online banking system, and consumer trust is the key mediating factor for commitment to the online banking system (Casalo et al. 2007). Chellappa and Pavlou (2002) propose antecedents of perceived security, which are *Encryption* (translating information from its original form into incomprehensible form), *Protection* (processing that the information is safeguarded by the organization managing the information), *Verification* (verifying the identity of the online company such as a domain name), and *Authentication* (a trusted third party that guarantees an online retailer). Their results show that encryption, protection, and authentication have significantly positive effects

on perceived security (Chellappa and Pavlou 2002). Although previous studies of information security show how important it is, researchers in computer science and information systems have focused on the technical aspects and the impact of security on the usage of websites, rather than the underlying process of how consumers form perceptions of security.

In sum, information security is different from physical security because of the nature of the objects – information versus more tangible facilities. Specifically, confidentiality, integrity, and availability are not as applicable to physical security. Moreover, consumers may have more difficulty understanding the mechanism of protecting information, compare to physical security. On the other hand, psychologists and marketing researchers pay little attention to how consumers form security perceptions even though principles of marketing and psychology are necessary to understand consumers' formation of security perception. Hence, the inference making literature is examined in the next section.

### **I.2.B Inference Making**

Consumers frequently make judgments and decisions based on incomplete information, so they must infer missing product properties and characteristics by going beyond the given information (Kardes et al. 2008). One of the most common types of inference-making processes is the correlation-based or covariation-based inference. Correlation-based inference is characterized as a memory-based and inductive inference (Kardes, Posavac, and Cronley 2004b). Memory-based inference means that consumers' prior beliefs about the relation between two attributes guide consumers' inference process, while inductive inference suggests that consumers derive a conclusion about a property from a specific attribute or cue. Consumers hold implicit theories – a prior belief that two variables are strongly correlated- so given information about one variable helps them infer an estimate of the other. However,

their inferred value of the missing information varies depending on what kind of inference strategies consumers use. If consumers use the consistency strategy, they infer that the brand that is superior on one dimension is also superior on the unknown dimension (Broniarczyk and Alba 1994a; Dick, Chakravarti, and Biehal 1990). For example, consumers who want to purchase a car may infer unknown attributes (e.g., reliability) from brand reputation. As a result, a highly reputed brand may be inferred to also be highly reliable. Another covariation-based inference is to figure out an intuitive relation from the decision situation or context. For instance, compensatory inference refers to consumers' belief that all alternatives in the market have equal values if the market is efficient. Consequently, consumers infer unknown information in favor of equalizing the overall value by making a comparison with competitors' products (Chernev and Carpenter 2001). Similarly, Chernev (2007) proposes the zero-sum heuristic, which refers to any advantage of one alternative is counterbalanced by its disadvantage. When consumers compare a product specialized in one attribute (called a specialized product) to a product combining all attributes (called an all-in-one product), they may estimate unknown information based on the belief that the overall value of a specialized product is equal to that of an all-in-one product. Therefore, consumers believe that a specialized product is better than an all-in-one product on the specialized dimension, whereas an all-in-one product is better than a specialized product on other dimensions (Chernev 2007). However, the most typical case of correlation-based inference is price-quality inference-making (Kardes et al. 2004b). We suggest that a process similar to price-quality inference-making may be involved in how consumers infer security feature from known complexity. To that end, we examine the price-quality inference-making literature.

Many researchers have demonstrated that consumers largely rely on price information when they estimate quality of a target product (Broniarczyk and Alba 1994a; Kardes et al.

2004a; Rao and Monroe 1989). For example, Rao and Monroe (1989) conducted a meta-analysis to investigate the impact of price, brand name, and store name on consumers' evaluations of product quality, and found that price and brand name are positively and significantly related to perceived product quality, but not store name. An interesting test in their study was to compare multi-cue studies to single-cue studies. Because a product has a variety of features or attributes, consumers might use numerous cues to infer product quality. As a result, single-cue studies (price-quality) may reveal larger effects than multi-cue studies because subjects were forced to show a positive price-quality relationship in the absence of any other information about a product. However, the results indicated that there was no statistical difference between single-cue studies and multi-cue studies, so the price-quality effect examined from multi-cue studies is no smaller than that detected in single-cue studies (Rao and Monroe 1989). Broniarczyk and Alba (1994) also investigated how consumers estimated or predicted quality of product when their prior belief conflicts with data. Specifically, researchers presented subjects information about price, quality, and advertising budget. In the study phase, subjects examined data about 3 variables, and then estimated quality based on price and advertising in the test phase. The correlations between quality and ads were manipulated from zero to 1.00, whereas price was not correlated with quality. Results showed that subjects relied on the prior belief (price-quality) even though the correlation between quality and ads was 0.87. When it was 1.0, they used ads as a predictor for quality. In their study 3, they fixed the correlation between quality and ads (= 0.87), and then used different ways to present information to subjects. *Free inspection* presented three columns of data- price, quality, and ads- on the same page. *Predictor* presented data separately (price-quality was on one page, and ads-quality was on another page). *Brand* presented a brand with three corresponding variables. *Prediction* was identical to *Brand* but

required a prediction for quality. Then, true values appeared on the screen. *Paragraph* presented a summary description of the data (rated above or below average), rather than the data themselves. *Paragraph* participants responded differently than others who were presented data with various formats. Specifically, their estimation relied on their prior belief and they ignored the summary of data. Thus, data have impact only when presented case by case, not summarized. These findings suggest that consumers may dramatically overestimate and mainly rely on the price-quality relationship when inferring product quality. Kardes and his colleagues (2004a) also investigated under which condition consumers' overestimation for the price-quality relationship becomes more severe. Specifically, consumers process information easily when it is consistent with their prior belief, but they have difficulty processing belief-inconsistent information, since more effort is needed to resolve the conflict between their prior belief and belief-inconsistent information. Therefore, consumers largely rely on price-quality relationship when information load is high. Similarly, when information is presented in a rank-ordered format rather than random-ordered, consumers process belief-consistent information more easily than belief-inconsistent information. The need for closure refers to an individual's desire to hold a firm/definite opinion or solution as opposed to confusion or ambiguity (Cronley et al. 2005; Kardes et al. 2004a). When need for closure is high, consumers want to reach judgment or decision as quickly as possible. Thus, the degree to which price is used as a basis for inferring quality is increased when need for closure is high (vs. low), provided that information load is high (vs. low) and information is presented in a rank-ordered format. The authors suggest these conditions make consumers employ a selective information processing (Cronley et al. 2005; Kardes et al. 2004a). Consumers focus selectively on belief-consistent information and neglect belief-inconsistent information, so their estimates of product quality are heavily based on price information.

In sum, this inference-making is guided by consumers' prior beliefs (expectations or implicit theories) about the correlation between price and quality, so it is memory-based, rather than stimulus-based. It is also inductive, rather than deductive, because consumers draw a conclusion about a dimension or property from a specific attribute or cue (Kardes et al. 2004b). Kim and Park (2012) demonstrate that consumers perceive an inconvenient option as more secure than a convenient option, even though a convenient option is technically more secure than an inconvenient option. This result indicates that consumers infer a property (e.g., security) from a specific cue (e.g., convenience) and this inference process is guided by their prior belief (e.g., the relationship between security and convenience), so it implies that security inference is inductive and memory-based, rather than deductive and stimulus-based. Therefore, we expect that the underlying process of price-quality inference may directly apply to security inference-making.

### **I.2.C Omission Neglect Theory and Consumer Knowledge**

Essentially, inference-making is a process to estimate missing or unknown information, so it is worthwhile to examine omission neglect theory. Omission neglect theory analyzes how consumers respond to missing or unknown information (Bechkoff et al. 2009; Kardes et al. 2006; Sanbonmatsu, Kardes, and Herr 1992; Sanbonmatsu et al. 2003; Sanbonmatsu et al. 1997; Silvera et al. 2005). Consumers use given or available information at the time of judgment or evaluation, and tend to ignore missing information, since consumers overestimate the importance of given, known, or available information. As a result, they confidently form extreme judgments even though based on limited or weak information. This phenomenon occurs because consumers tend to overestimate the diagnosticity of presented information, even when it may be limited or incomplete. Under certain conditions, however,

consumers become more sensitive to missing information and adjust their judgments, accordingly. Kardes and his colleagues (2006), for example, investigate how to debias omission neglect, and suggest two ways to reduce it; considering judgment criteria before exposure to product information and rating presented and missing information before making the overall product evaluation (Kardes et al. 2006). Specifically, participants in criteria-consideration condition were asked to rank order nine attributes in terms of the importance before receiving product information. Product information provided to them included price and three other attributes. Compared to participants in a control condition, those in the criteria condition showed less extreme judgments and less confidence in their evaluations. In their experiment 2, half of participants rated five presented attributes and three missing attributes after seeing an advertisement of a target product, and then gave an overall product evaluation. The remaining participants provided the overall product evaluation, and then rated attributes. As expected, participants who rated attributes first were less extreme and less confident in their judgments, compared to those who did the overall evaluation first (Kardes et al. 2006). Sanbonmatsu and his colleagues (1992) also showed that consumers' sensitivity toward missing information increases and they form more moderate judgments when they are informed that there is missing information and when they have well-defined knowledge about the domain (Sanbonmatsu et al. 1992). Because highly knowledgeable consumers can detect the existence of missing information automatically or spontaneously, the impact of omission neglect is relatively less in highly knowledgeable consumers than in low and moderately knowledgeable consumers. Thus, omission neglect theory suggests that consumer knowledge or expertise plays an important role in the inference making process. The degree of prior knowledge consumers have also influences the inference making based in the price-quality relationship (Rao and Monroe 1988). Novice consumers are more likely to use price

information to assess product quality because they do not have intrinsic product information in their memory and their knowledge schema is less developed. On the other hand, experts may use a variety of information cues retrieved from their knowledge schema to infer product quality, and are more likely to use price information only if they believe that the price-quality relationship is accurate in that product category (Rao and Monroe 1988). Moreover, experts' information processing differs from novices.' Because experts have well-defined knowledge structures, they may match given information to their prior knowledge, and then retrieve information from the matched category and make an evaluation – a category-based process. Novices, however, follow a piecemeal-based process, in which each attribute is processed in isolation in order to evaluate the overall value of the product (Sujan 1985). Wood and Lynch (2002) demonstrate that consumers with greater prior knowledge learn less about a new product, compared to those with lower prior knowledge, stemming from their low motivation, rather than ability to learn. Specifically, those with higher prior knowledge incorrectly generalize from knowledge of existing products and assume that they already know how to use the new product properly. Therefore, they learn less than those with low prior knowledge. If, however, consumers with higher prior knowledge are exposed to a cue that prior knowledge is useless, this effect is reversed (Wood and Lynch 2002). The results of Wood and Lynch (2002) imply that experts might be biased when a new product is incompatible with prior knowledge. Highly knowledgeable consumers use information that is retrieved from their knowledge structures in memory. The retrieved information may, however, be outdated and incompatible with newer technology, especially if technology is developed rapidly. In the present case, information security technology is indeed changing rapidly. As a result, the impact of knowledge on perceived security might be weak, irrespective of

expertise. The confidence of consumers in their judgment, however, may differ depending upon expertise.

Consumer knowledge is an important topic in consumers research because it is closely interrelated with cognitive effort, cognitive structure, analysis, elaboration, and memory (Alba and Hutchinson 1987). Researchers usually distinguish between actual knowledge and self-assessed (subjective) knowledge. Actual knowledge refers to objective knowledge, with accurate stored information reflecting what consumers know, while self-assessed knowledge refers to self-beliefs about their own knowledge, reflecting what they think they know (Alba and Hutchinson 2000; Carlson et al. 2009). The relationship between objective knowledge and subjective knowledge varies across domains and context. For example, some studies report positive correlations between objective knowledge and subjective knowledge (.76 for knowledge of bicycles, .88 for knowledge of statistics, and .74 for knowledge of cars), while other studies found weak or no correlation (-.09 for knowledge of nutrition and .08 for ecological behavior, (Carlson et al. 2009). Alba and Hutchinson (2000) argue that the gap between objective and subjective knowledge indicates some degree of miscalibration, and it can affect the decision making process. If the correlation between objective and subjective knowledge is weak or nonexistent, the effect of knowledge on consumers' choices and judgments will vary depending on whether it is objective or subjective. If the correlation is highly positive, the effect of knowledge will be identical or similar, regardless of type of knowledge.

#### **I.2.D Security Inference Making**

In the previous section, we examined consumers' inference-making processes and the impact of consumer knowledge. Grounded in these theories, we now extend it to consumers'

security perceptions. Specifically, we focus on how consumers' perceptions of security might increase by examining their perceptions of a correlated relationship between security and complexity. A central characteristic of information security is that it is often difficult for consumers of information goods (e.g., software) to observe the quality of security directly. Therefore, consumers must infer security from something they know, and the typical inference they implement is based on the belief that security is correlated with complexity (Kim and Park 2012). To enhance physical security (e.g., home), people install devices such as a keypad lock. A conventional lock-and-key system may not be enough for some people, so companies develop more complex devices. In the physical world, people may easily see how it works, so the inference about security performance of devices for enhancing physical security is less necessary. In the online context, however, operation processes of security are usually hidden, so consumers have to infer security based on their knowledge or given specific belief cues. As a result, they appear to rely on the relationship between security and complexity. Kim and Park (2012) demonstrate that the consumers perceive a correlated relationship between security and complexity and use it when inferring security of a product. In their study, consumers evaluate security of a dominated product as more secure than that of a dominant one because the dominant appears less complex than the dominated. Specifically, participants were exposed to information of one of two alternatives – WLAN and WLSS. WLAN is a wireless internet service that verifies users with the conventional ID & Password system, whereas WLSS is also a wireless internet service that provides an automatic login process by verifying users with a digital certificate. Thus, WLAN is clearly less convenient than WLSS, but technically WLSS is more secure than WLAN. It means that WLSS is dominating WLAN. However, participants perceived WLAN as a more secure option than WLSS in their study. This result directly demonstrates that consumers' inference-

making is not accurate and relies on a simple rule – the relationship between security and complexity. This phenomenon can be explained as follows. Consumers do not have well-defined knowledge about information security. Information security consists of three major elements – confidentiality, integrity, and availability (Chellappa and Pavlou 2002; Chirillo and Danielyan 2005; Flavian and Guinaliu 2006; Gerber and von Solms 2001; Parker 1998; Posthumus and von Solms 2004). Studies in computer science and information systems use specific items to measure confidentiality, integrity, and availability, but consumers may not know what these are. They may form a broad and rough impression about information security based on their intuition and general beliefs that come from knowledge of physical security. Thus, this suggests that companies or marketers can increase consumers' perceived security by increasing complexity. Generally consumers believe that an expensive product is a quality item, even if they are exposed to evidence that the correlation between price and quality is none or low (Broniarczyk and Alba 1994b), largely because they focus on information that is consistent with their prior beliefs (Cronley et al. 2005; Kardes et al. 2004a). In the same manner, consumers may believe that a complex option is more secure than a less complex one, even if complexity is not correlated with security. Also, prior research shows that consumers tend to give more value to a brand with an irrelevant attribute (Broniarczyk and Gershoff 1997; Carpenter, Glazer, and Nakamoto 1994). A brand differentiated by a unique but irrelevant attribute can be evaluated favorably, compared to a competitor that does not have it. Adding an irrelevant and unique attribute can create meaningful differentiation to consumers by making them think the unique attribute is valuable, even though they may know it is irrelevant (Carpenter et al. 1994). This suggests that perceived information security may increase by simply adding a procedure, even if it is meaningless. For example, the most typical method of confirming consumers' identities is the

ID & Password system. It is a critical part of integrity that information should not be modified by unauthorized parties during data storage and transmitting. What if a website requires consumers to input the same password twice? Typing the same password is redundant because it is identical information to confirm the consumer identity, but complexity (or inconvenience) increases. When consumers infer product quality, they use the price information because they believe there is a positive correlation between price and quality. The most interesting aspect of price-quality inference making is that consumers tend to ignore other information and focus on price (Broniarczyk and Alba 1994b; Cronley et al. 2005; Kardes et al. 2004a; Rao and Monroe 1989). We expect the consumer inference process for information security is similar to that for product quality based on price. Therefore, consumers may use complexity as an implicit theory to infer security. These arguments lead to the following hypothesis.

H1-1: Consumers evaluate a website, which seems complex and inconvenient, more secure than a website, which seems relatively easy and uncomplicated.

We also consider additional factors that may affect the consumer inference process. First, inference processes may differ depending upon expertise. Experts usually engage in category-based processing rather than piecemeal processing (Sujan 1985), so they may judge security features based on their knowledge. Specifically, they may try to retrieve product information from memory to fit given information, and then make a judgment about the security feature based on the retrieved product information. If, however, 'retrieved' information is dated or irrelevant, even experts may rely on implicit theories (complexity and

newness) when estimating security. On the other hand, novice consumers do not have well-developed categorical knowledge structures, so they may need to examine all information given to them. However, novice consumers may rely on an implicit theory in order to infer security, because they do not have sufficient knowledge to figure out which information is valid for a security inference. Although both experts and novices may use implicit theories in order to infer security, experts' inference processing may differ from novices.' Experts may use a top-down process (categorical or schema-driven) in which knowledge and prior experience guide their inferences. This process may be relatively less effortful than novices', who may use a bottom-up process (piecemeal or data-driven process) in which basic elements are examined and process upward until arriving at a super-ordinate or abstract principle. The response time when consumers infer missing attributes or unknown information can provide useful insight about the inference processes (Kardes et al. 2008). If consumers use a relatively more effortful process, they need time to perform cognitive tasks. On the contrary, if their processing is relatively less effortful, their response time for the questionnaire may be relatively shorter. Thus, the response time of high knowledge consumers may be quicker than that of low knowledge consumers because low knowledge consumers need to perform a more effortful process than high knowledge consumers. The impact of consumer knowledge can affect not only the response time but also consumers' confidence in their judgment.

Following omission neglect theory, consumers are more likely to form moderated judgments and make inference corrections when they are highly knowledgeable (Kardes et al. 2006; Sanbonmatsu et al. 1992; Sanbonmatsu et al. 2003). Because it is almost impossible that consumers have all the information about a product and process it completely in evaluating or making product decisions, consumer judgments and decisions are generally made using limited information. However, high-knowledgeable consumers are more likely to know how

many attributes a certain product has, what kind of information is important, and which information is unknown or missing. As a result, their judgments tend to be relatively moderate, compared to low- knowledgeable consumers.’ However, what if consumers’ subjective knowledge differs from their objective knowledge? When Sanbonmatsu and his colleagues (1992) examined omission neglect, they examined the bicycle product category, in which the correlation between subjective and objective knowledge is strongly positive. Although many studies suggest that subjective and objective knowledge are positively correlated, others show no or weak relationship between subjective and objective knowledge (Carlson et al. 2009). If subjective knowledge and objective knowledge in the information security domain are positively correlated, perhaps more knowledgeable consumers are less confident about their security judgments. If, however, the correlation between subjective and objective knowledge is weak or nonexistent, the degree of confidence about security judgment may differ depending on the specific type of knowledge. Consumers with high objective knowledge may express more moderate judgments than those who have low objective knowledge about information security, per the omission neglect theory. On the other hand, consumers who have high subjective knowledge may be more confident about their judgment than those who have low subjective knowledge about information security. Wood and Lynch (2002) demonstrate that consumers with high prior knowledge learn less about a new product than those with low prior knowledge because of the lack of the motivation, rather than their inability. When, therefore, the correlation between subjective and objective knowledge is low or none, consumers with higher subjective knowledge express more confidence about their judgments, unlike the omission neglect theory. These arguments lead to the following hypotheses:

H1-2: Low knowledge consumers use more effortful processes than high knowledge consumers, so the more knowledgeable consumers are, the shorter is their response time to make security inferences.

H1-3(a): If objective knowledge is highly correlated with subjective knowledge, high-knowledgeable consumers are less confident in their security inferences than low-knowledgeable consumers.

H1-3(b): If the correlation between subjective and objective knowledge is weak or none, consumers who have high objective knowledge are less confident in their security judgments than those who have low objective knowledge, while consumers who have high subjective knowledge are more confident in their security judgments than those who have low subjective knowledge.

The sensitivity for security is another factor to consider. Consumers' security motivation or involvement will likely vary depending upon the context or the information requiring protection. For example, consumers may be more sensitive for security of their bank accounts than security of their twitter accounts. Specifically, their involvement and motivation to increase security may increase as the importance of accounts or information increases. As a result, consumers may want to select more secure websites, so they may use more effortful and deliberative inference making to infer security for important accounts or information, compared to less important accounts. However, the only available cue may be the relation between security and complexity, so they still may use the correlation-based inference, even if they exert cognitive effort in inference making. Similarly, if consumers

have experienced security problems or troubles in the past, they are likely to have heightened sensitivity about security, so they may use effortful and deliberate inference making. Also, they likely have relatively more knowledge about security, compared to novice consumers with no experience with security problems. These arguments lead to the following hypotheses.

H1-4: Consumers enlist a more effortful process when inferring security of important websites than when inferring security of relatively less important websites

### **I.3 Results of Experiment 1-1(A)**

The main objective of Experiment 1-1(A) is to confirm whether consumers use complexity (or convenience) to infer perceived security. Based on our arguments that consumers infer security based on the correlated relationship between security and complexity, we predict that consumers perceive websites with inconvenient log-in procedures as more secure than websites with relatively simple and convenient log-in procedures.

#### *Method*

*Participants and Stimuli.* One-hundred-seventy-two participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation for participating. This study employs a 3 (complexity of log-in procedure: control vs. typing passwords twice vs. typing passwords twice but in a separated window) by 2 (contexts: email account vs. bank account) between-subject experiment design. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). Participants were randomly assigned to one of six conditions. A log-in procedure is an important step to examine whether an individual is an

authorized user or not, and is a part of confidentiality in the C-I-A triad. A log-in system with ID & Password is the most typical procedure to check consumers' identities, and most consumers are familiar with it. Therefore, the *control* condition is a conventional log-in procedure (ID & Password). If a website requires typing a password twice in the log-in process, it is meaningless and redundant because the website just receives the same information again from consumers. Typing the same password twice also may annoy consumers, increasing perceptions of inconvenience and complexity, compared with the conventional ID & Password system. Thus, complexity of log-in procedure is manipulated by asking for password entry one twice when logging on to the website. We chose the log-in pages of *Google gmail* and *Wells Fargo*, and captured the pictures of these websites. Then, we removed their brand names and logos on these pictures to avoid any effect from exposure to real brands (see Appendix 1).

*Procedure.* Participants, randomly assigned to one of the six conditions, read a study introduction and then saw a picture of the website log-in page with instructions. For example, participants in the bank account condition read, "Imagine the following situation. Recently you opened a new bank account, so you create an online account connected to your new bank account. Here is the first page of the website of the bank, and it shows how to log into the website. Please look at the picture and answer the questions carefully." Participants in the email account condition read, "Imagine the following situation. Recently you needed to create another free email account, so you looked for several websites to provide a free email account. Finally, you decided on one of them, and here is the picture to show how to log-in to the website. Please look at the picture and answer the questions carefully." The rest of the instructions were identical across conditions. After participants saw a picture of the website log-in page, which varied depending on conditions to which they were assigned, they were

asked to report their opinion about the website with three items (1 = Bad, 7 = Good; 1 = Unfavorable, 7 = Favorable; 1 = Dislike, 7 = Like). Then, they were asked to rate how easy, how convenient, how complex, how secure, how safe, and how much your information is protected with 7 point Likert scales (1 = not easy at all, 7 = very easy; 1 = not convenient at all, 7 = very convenient; 1 = not complex at all, 7 = very complex; 1 = not secure at all, 7 = very secure; 1 = not safe at all, 7 = very safe; 1 = not protected at all, 7 = well protected). We also measured the confidence of the security judgment (“How confident are you that your estimation for security of this website is similar to the actual security level of the website?”). To measure their subjective knowledge, we asked participants how familiar, how much expertise, how knowledgeable, and how interested they are in computers and software with 7 point Likert scale. To measure objective security knowledge, 10 questions were selected from an Information Security Quiz (see Appendix 2 for details of objective knowledge measures). In addition, the total time participants spent to answer the questionnaire was recorded.

### *Results*

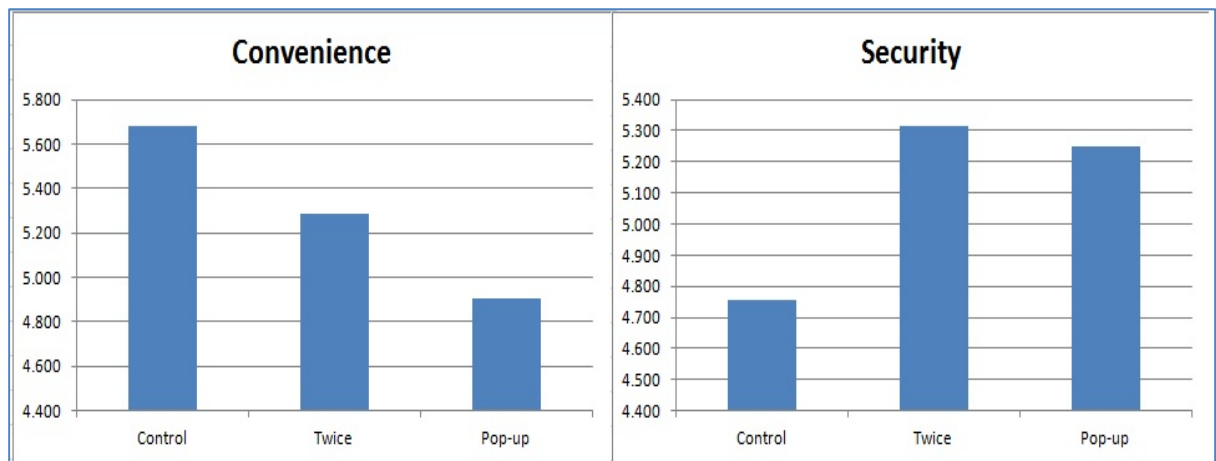
*Security, Convenience, and Preference.* We predicted that consumers would infer security based on complexity (or inconvenience), even if complexity is increased by adding a meaningless procedure. In detail, a website which requires typing a password twice would be perceived more secure than a website which requires typing a password only once. To test our arguments, we present pictures of websites with log-in processes that vary depending on conditions and measure participants’ overall opinion (preference), perceived convenience, and perceived security. A two-way ANOVA was conducted with context (bank vs. email) and complexity of log-in procedure (control vs. typing a password twice vs. typing a password twice with a pop-up window) as the independent factors and preference, perceived

convenience, and perceived security as the dependent variables. An analysis of variance (ANOVA) for perceived security revealed the predicted effect for complexity of log-in procedure ( $F_{\text{perceived security}}(2, 166) = 2.90, p = .06$ ). Specifically, participants evaluated the conventional log-in procedure (control condition;  $M = 4.75$ ) as a less secure option than both typing a password twice (stated as ‘Twice’;  $M = 5.32, p < .05$ ) and typing a password twice with a pop-up window (stated as ‘Pop-up’;  $M = 5.25, p < .05$ ). However, the main effect of context (bank vs. email account;  $F_{\text{perceived security}}(1, 166) = .13, p > .10$ ) and the interaction effect of context and complexity ( $F_{\text{perceived security}}(2, 166) = .38, p > .10$ ) were not significant. We also conducted an ANCOVA with two covariates, subjective and objective knowledge. Both subjective ( $F_{\text{perceived security}}(1, 164) = 5.50, p < .05$ ) and objective knowledge ( $F_{\text{perceived security}}(1, 164) = 9.03, p < .01$ ) were significant. Although the  $p$ -value slightly increased, complexity of log-in procedure was still marginally significant ( $F_{\text{perceived security}}(2, 166) = 2.784, p = .07$ ), and neither the main effect of context nor the interaction were significant ( $p > .10$ ). These results indicate that the impact of knowledge on security inference-making is circumscribed, and consumer inference of security relies on complexity.

An ANOVA for perceived convenience showed that the main effect of complexity was significant ( $F_{\text{perceived convenience}}(2, 166) = 5.39, p = .005$ ), but the main effect of context ( $F_{\text{perceived convenience}}(1, 166) = .04, p > .10$ ) and the interaction effect of complexity and context ( $F_{\text{perceived convenience}}(2, 166) = .23, p > .10$ ) were not significant. Specifically, participants’ perceived convenience in the control condition ( $M = 5.68$ ) was higher than that in ‘Pop-up’ condition ( $M = 4.91; p = .001$ ). Although there was no significant difference between the control condition ( $M = 5.68$ ) and ‘Twice’ condition ( $M = 5.29; p = .10$ ), the direction was as expected. Subjective ( $F_{\text{perceived convenience}}(1, 164) = .87, p > .10$ ) and objective knowledge ( $F_{\text{perceived convenience}}(1, 164) = 1.02, p > .10$ ) were not significant covariates in the ANCOVA. On

the other hand, when the dependent variable is preference, the main effects of context ( $F_{\text{preference}}(2, 166) = .05, p > .10$ ) and complexity ( $F_{\text{preference}}(2, 166) = 1.74, p > .10$ ) and the interaction effect ( $F_{\text{preference}}(2, 166) = .08, p > .10$ ) were not significant. Although the ANCOVA revealed that only objective knowledge ( $F_{\text{preference}}(1, 164) = 10.10, p < .01$ ) was significant as a covariate, the main effects of context and complexity and the interaction effect remained non-significant ( $ps > .10$ ).

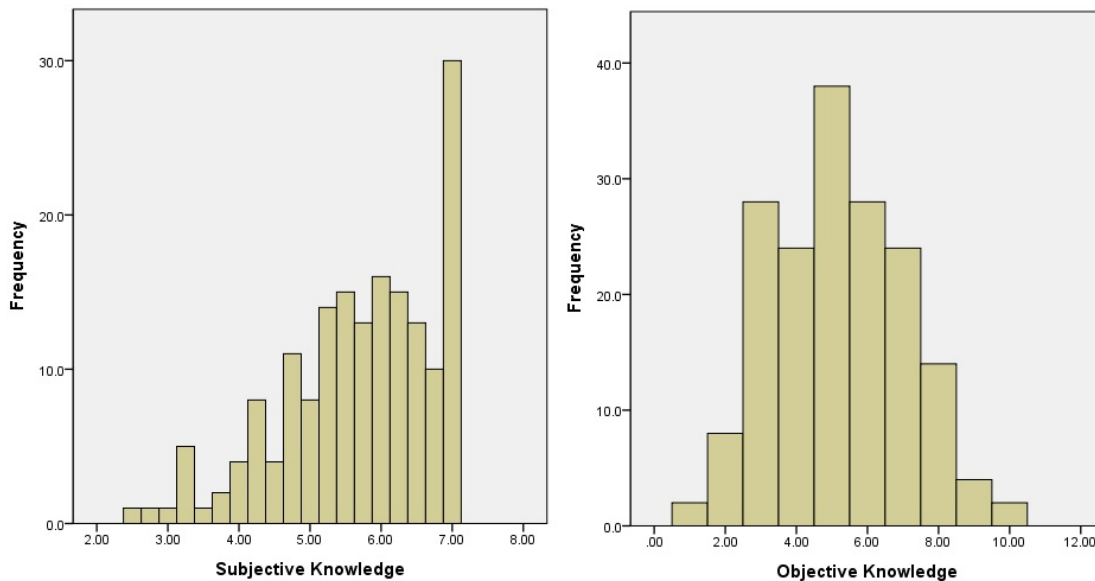
**Figure 1 Perceived Convenience and Perceived Security**



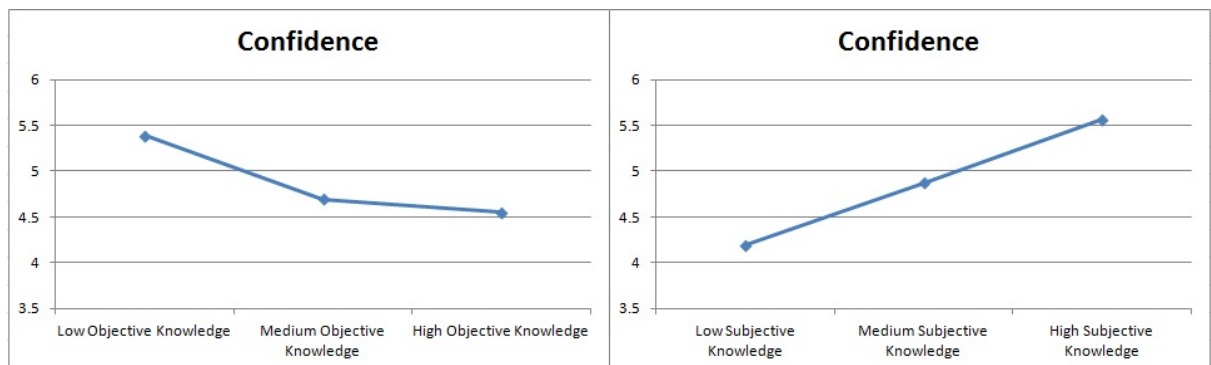
*Confidence and Response Time.* We predicted that consumers' confidence in their security judgment would vary depending on the knowledge type when the relation between subjective and objective knowledge is weak. To examine this possibility, participants were split into low, medium, and high knowledge groups. For objective knowledge group assignment, participants who correctly answered from 7 to 10 questions are grouped as high knowledge consumers, while those with 4 to 6 correct answers are grouped as medium knowledge consumers. The rest were grouped as low knowledgeable consumers. The mean of subjective knowledge is 5.69. Participants whose subjective knowledge is more than 6.5 were grouped as high knowledge consumers, while those whose subjective knowledge was more

than 4.6 and less than 6.5 were grouped as medium knowledgeable consumers. The rest are low knowledgeable consumers. The correlation between subjective and objective knowledge is .17 ( $p < .05$ ). Although significant, the correlation value is quite low.

**Figure 2 Histogram of Subjective and Objective Knowledge**



**Figure 3 Confidence of Subjective and Objective Knowledge**



A two-way ANOVA was conducted with subjective (high vs. medium vs. low) and objective knowledge (high vs. medium vs. low) as the independent factors and confidence as the dependent variable. As expected, the main effects of subjective and objective knowledge

are found for confidence ( $F_{\text{subjective knowledge}}(2, 169) = 9.95, p < .001$ ;  $F_{\text{objective knowledge}}(2, 169) = 3.04, p = .051$ ). Participants with high subjective knowledge ( $M = 5.48$ ) were more confident than those with medium subjective knowledge ( $M = 4.91, p < .05$ ), who were in turn more confident than low subjective knowledge participants ( $M = 3.93, p = .001$ ). Although there was no difference between high ( $M = 4.5$ ) and medium objective knowledge consumers ( $M = 4.91, p > .10$ ), high objective knowledge consumers were more confident than low objective knowledge consumers ( $M = 5.29, p < .05$ ). To examine whether high knowledge consumers use less effortful processes than low knowledge consumers, we conducted a three-way ANOVA with context, complexity of log-in procedure, and knowledge type as the independent factors and response time as the dependent variable. No significant effect was found, regardless of the type of knowledge. The main effects of subjective and objective knowledge, context, and complexity were not significant ( $ps > .10$ ), and all interaction effects were also not significant ( $ps > .10$ ).

#### **I.4 Discussion of Experiment 1-1(A)**

Experiment 1-1(A) demonstrate that consumers use perceived convenience for inferring information security. As expected, participants evaluated websites with complex log-in procedures as more secure than websites having the typical and conventional log-in procedures. In Experiment 1-1(A), complexity of log-in procedure marginally influences perceived security. Although the perceived convenience of ‘Twice’ condition is not significantly different from the control condition, the direction of the perceived convenience is consistent with our prediction. Hence, H1-1 is partially supported. Based on omission neglect theory and consumer knowledge, we predicted that high-knowledgeable consumers are less confident than low-knowledgeable consumers when objective knowledge is highly

correlated with subjective knowledge (H1-4(a)). If the correlation between subjective and objective knowledge is weak or none, consumers with high objective knowledge are expected to be less confident than those with low objective knowledge, while consumers having high subjective knowledge are expected to be more confident than those with low subjective knowledge (H1-4(b)). Although the correlation between subjective and objective knowledge is significant, the correlation is quite low. As expected, the pattern of subjective knowledge is opposite that of objective knowledge in the confidence of judgment, supporting H1-4(b). We expected that the response time of low knowledge consumers to be longer than highly knowledgeable consumers (H1-3), and that context (e.g., importance of websites) also would lead to a similar effect on response time (H1-5). For example, consumers' involvement with a bank account should be higher than that with an email account, so they may engage in a more effortful process when inferring security features of a bank website than of an email account. However, these effects were not significant, failing to support H1-3 and H1-5.

There are two issues we still need to address. First, perceived convenience of the 'Twice' condition did not differ from the control condition, even though the direction of the means was as predicted. One potential reason may be that there is no common reference point for determining whether the website login is (in)convenient. We used the conventional log-in procedure in the control condition. Although consumers are familiar with the conventional log-in procedure, they may be annoyed to type ID & Password when they log in to a website. Thus, if they are exposed to both the conventional log-in procedure and the log-in procedure of 'Twice' condition, perceived convenience of control condition may be highlighted and clearly distinguished from that of 'Twice' condition. Second, we did not find a difference in response time, expected to vary by knowledge and context. We argue that the more knowledgeable consumers are, the less effortful is their information processing. Therefore,

we predict that knowledgeable consumers would respond faster than less knowledgeable consumers. There was, however, no significant difference among low, medium, and high knowledgeable consumers. One possible explanation is that the given information may be insufficient to motivate participants to engage in a more effortful inference process. In this experiment, we simply showed the pictures of websites, rather than descriptions about technology adopted in the websites. The limited amount of information may constrain participants' inference process, so they may rely on only a simple correlation-based inference process. If so, their response time may vary depending on the amount of information given. In addition, their inference process may be affected by motivation. For example, highly motivated novices may follow the piecemeal (bottom-up) process as we expected, but less motivated novices may use a heuristic or rule of thumb (security-convenience trade-off) without examining available information given to them. Therefore, novice consumers may use a more effortful process under high than low motivation. However, experts may stick to the top-down (categorical) process, regardless of the degree of motivation. Another possible explanation is that there simply may be no difference depending on knowledge and context. Rao and Monroe (1989) show that there is no difference between single-cue studies and multi-cue studies in the price-quality inference. If consumers believe in the relationship between two attributes (e.g., price and quality), they tend to focus and rely on it when inferring the other attribute. If this holds true in an information security context, consumers' inference processing may not be influenced by knowledge and context.

## **I.5 Results of Experiment 1-1 (B)**

The main objective of Experiment 1-1(B) is to replicate the results of Experiment 1-1(A) with a within-subject design. Although Experiment 1-1(A) supports some of our predictions,

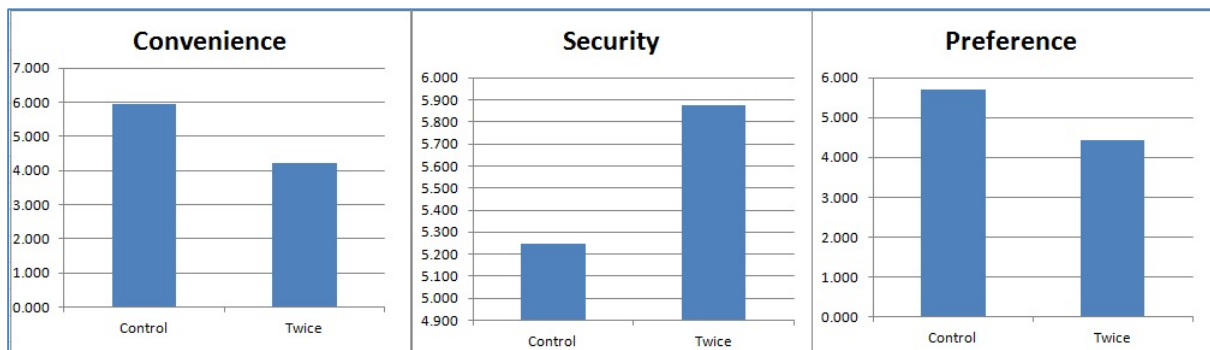
not all are fully supported. One plausible reason may be participants' point of reference. In Experiment 1-1(A), we present only one option to participants, and ask them to infer security based on the given information. If they face several options, they may make inferences through a comparison between two options, revealing the inference process more clearly. Stimuli and procedures are identical to Experiment 1-1(A) except the experimental design. We use a 2 (Context (between-factor): bank vs. email) by 2 (Complexity of Log-in procedure (within-factor): Control vs. Twice) mixed design. Although both 'Twice' and 'Pop-up' conditions require typing a password twice, 'Twice' condition is different from 'Pop-up' condition because 'Pop-up' condition is consisted of two stages. Thus, we analyze Control-'Twice' condition, separated from Control-'Pop-up' condition. Specifically, participants in 'bank & Control-Twice' condition saw the pictures of two websites at the same time; one with the conventional ID & Password log-in system, and the other requiring participants to type the password twice. Then they were asked to respond to questions about their preference, perceived convenience, perceived security, confidence in judgments, and their subjective and objective knowledge. One-hundred-thirteen individuals recruited through Amazon Mechanical Turk for nominal monetary compensation participated in Experiment 1-1(B).

### *Results*

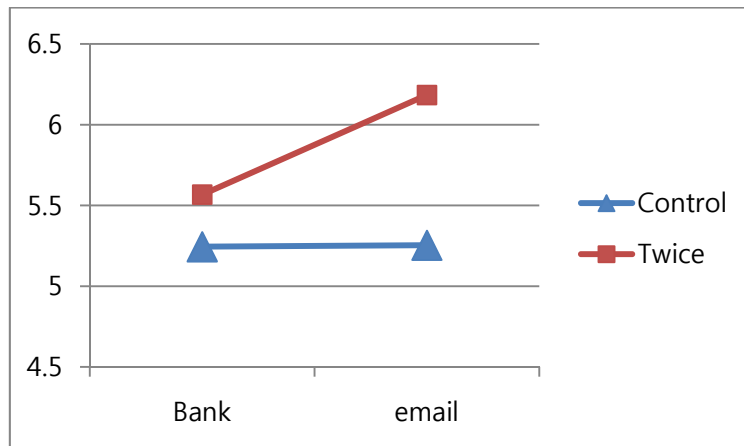
*Security, Convenience, and Preference.* A two-way ANOVA with repeated measures was conducted with context (between-factor: bank vs. email) and complexity of log-in procedure (within-factor: control vs. Twice) as the independent factors and preference, perceived convenience, and perceived security as the dependent variables. The main effects of complexity of log-in procedure are significant ( $ps < .001$ ), but the main effects of context are not significant ( $ps > .10$ ) when dependent variables are security, convenience, and

preference. Specifically, perceived security of Control ( $M = 5.25$ ) is significantly lower than that of Twice ( $M = 5.88$ ;  $F_{\text{perceived security}}(1, 57) = 18.81, p < .001$ ), while perceived convenience of Control ( $M = 5.95$ ) is significantly higher than that of Twice ( $M = 4.23$ ;  $F_{\text{perceived convenience}}(1, 57) = 77.03, p < .001$ ). Interestingly, participants form more favorable opinions toward Control ( $M = 5.69$ ) than Twice ( $M = 4.44$ ;  $F_{\text{preference}}(1, 57) = 20.51, p < .001$ ; see Figure 5). When the dependent variable is perceived security, the interaction between complexity of log-in procedure and context is significant ( $F(1, 57) = 2.73, p < .05$ ). In detail, perceived security of Control condition in the bank account ( $M = 5.25$ ) is not different from that of Twice condition in the bank account ( $M = 5.57$ ;  $p > .10$ ), while perceived security of Control condition in the email account ( $M = 5.25$ ) is significantly lower than that of Twice condition in the email account ( $M = 6.18$ ;  $p < .001$ ; see Figure 5).

**Figure 4 Convenience, Security, and Preference in Control-Twice condition**

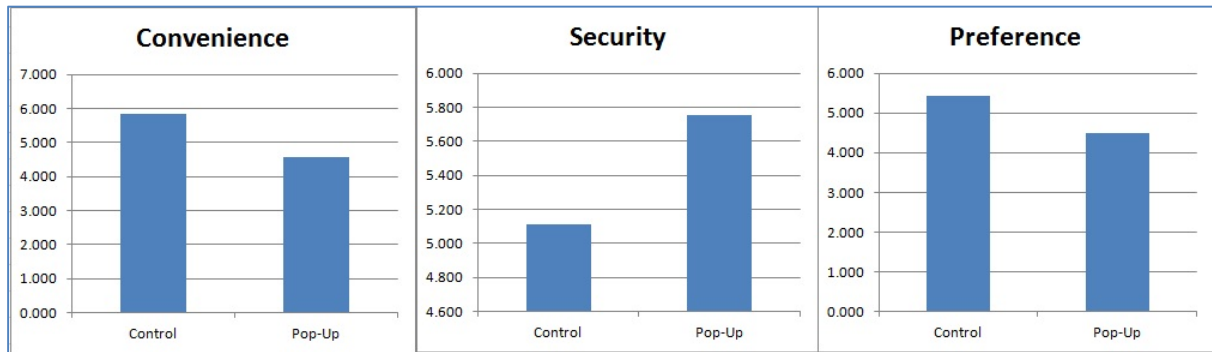


**Figure 5 The Interaction Effect on Perceived Security**



Similarly, a two-way ANOVA with repeated measures was conducted with context (between-factor: bank vs. email) and complexity of log-in procedure (within-factor: control vs. Pop-up) as the independent factors and preference, perceived convenience, and perceived security as the dependent variables. The main effects of complexity of log-in procedure were significant ( $ps < .001$ ), but the main effects of context and the interaction effects between complexity of log-in procedure and context were not significant ( $ps > .10$ ) when dependent variables are security, convenience, and preference. Specifically, perceived security of Control ( $M = 5.11$ ) was significantly lower than that of Pop-Up ( $M = 5.76$ ;  $F_{\text{perceived security}}(1, 52) = 8.24, p < .01$ ), while perceived convenience of Control ( $M = 5.85$ ) was significantly higher than that of Pop-Up ( $M = 4.59$ ;  $F_{\text{perceived convenience}}(1, 52) = 33.71, p < .001$ ). Participants formed more favorable opinions toward Control ( $M = 5.43$ ) than Pop-Up ( $M = 4.48$ ;  $F_{\text{preference}}(1, 52) = 8.42, p < .01$ ; see Figure 6).

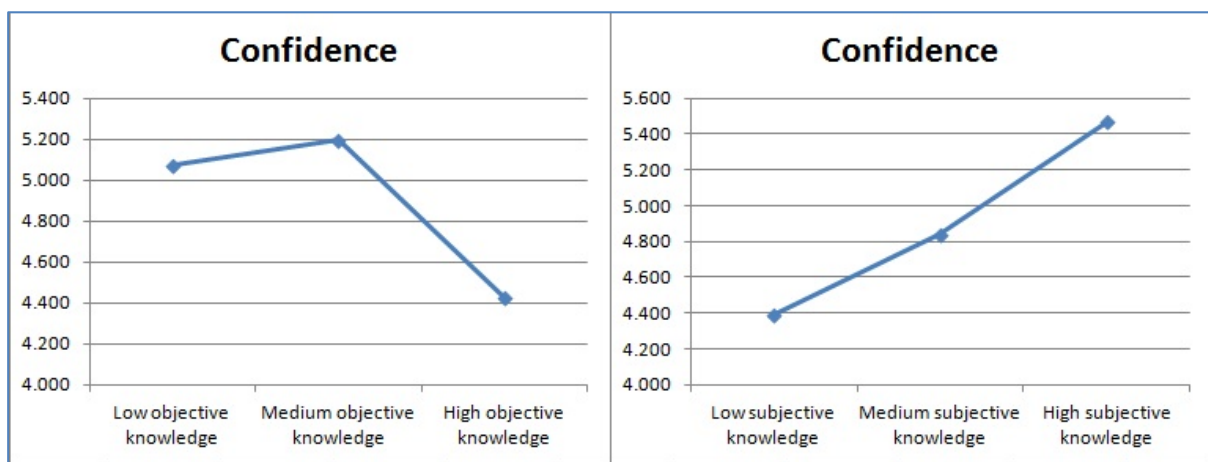
**Figure 6 Convenience, Security, and Preference in Control-Pop-Up condition**



*Confidence and Response Time.* Response time and confidence of judgment are not affected by complexity of login-procedure, so we pooled the data of Control-Twice and Control-Pop-up to examine the effect of subjective and objective knowledge. We split participants into three groups - low, medium, and high knowledge groups. In objective knowledge, participants answering 7 to 10 questions correctly are grouped as high knowledge consumers, while those answering 4 to 6 questions correctly are grouped as medium knowledge consumers. The rest are low knowledge consumers. The mean of subjective knowledge is 5.51 and the standard deviation is 1.13. Participant whose subjective knowledge was more than 6.5 are grouped as high knowledgeable consumers, while those whose subjective knowledge was more than 4.5 and less than 6.5 are grouped as medium knowledgeable consumers. The rest were grouped low knowledgeable consumers. The correlation between subjective and objective knowledge is .15 ( $p > .10$ , ns), indicating no relation between subjective and objective knowledge. A two-way ANOVA was conducted with subjective (high vs. medium vs. low) and objective knowledge (high vs. medium vs. low) as the independent factors and confidence as the dependent variable. Main effects of subjective and objective knowledge were significant ( $F_{\text{subjective knowledge}}(2, 104) = 3.63, p < .05$ ;  $F_{\text{objective knowledge}}(2, 104) = 2.83, p = .06$ ), but the interaction between subjective and

objective knowledge was not ( $F(4, 104) = 1.79, p > .10$ ). Specifically, participants who had high objective knowledge ( $M = 4.43$ ) showed less confidence than those who had low ( $M = 5.07$ ) and medium objective knowledge ( $M = 5.20$ ). On the contrary, participants who had high subjective knowledge ( $M = 5.47$ ) showed more confidence than those who had low ( $M = 4.39$ ) and medium subjective knowledge ( $M = 4.84$ ; see Figure 7). However, the response time did not significantly vary depending on subjective and objective knowledge ( $ps > .10, ns$ ).

**Figure 7 Confidence of Objective and Subjective Knowledge**



## I.6 Discussion of Experiment 1-1(B)

Experiment 1-1(B) also demonstrates that consumers evaluated websites with complex log-in procedures as more secure than websites having the conventional log-in procedures, replicating H1-1 in Experiment 1-1(B). Also, we argued that the failure to find a difference between perceived convenience of the Control condition and Twice condition in Experiment 1-1(A) was due to an absence of a relevant reference point. As expected, we found the significant difference between perceived convenience of Control condition and Twice condition in Experiment 1-1(B). Moreover, the impact of knowledge in the confidence of judgment was replicated. The correlation between subjective and objective knowledge was

quite low and not significant, and high objective knowledge participants were less confident than medium and low objective knowledge, whereas high subjective knowledge participants were more confident than medium and low subjective knowledge, supporting H1-4(b). However, there was no difference in response time based on subjective and objective knowledge and the context, so H1-3 and H1-5 were not supported.

Thus, there are two issues we need to address. First, we found the interaction between complexity of login procedure and context in Control-Twice condition in Experiment 1-1(B), while it was not observed in the Control-Pop-up condition in Experiment 1-1(B) with the dependent variable perceived security. Participants evaluated that security of Control was similar to that of Twice, but that security of Pop-up was better than that of Control. If this result is due to the difference between Twice and Pop-up, we should have observed the same pattern in the email context. One possible explanation is the characteristics of the context. Consumers may be more sensitive to security of financial websites such as online banking than of others. Because of this belief, they may expect that banks have already built more secure websites than other companies. This may underlie the mixed results. Second, we found that the preference of Control was higher than Twice and Pop-up in Experiment 1-1(B) but not in Experiment 1-1(A). It may be quite critical for companies to produce IT products. If consumers prefer convenient and insecure products to inconvenient and secure ones, there is neither need nor motivation to enhance security. However, this may be different in a choice setting. Specifically, comparable attributes such as price tend to receive more weight in rating tasks, while enriched attributes such as brand name tend to be more meaningful and informative in choice tasks (Nowlis and Simonson 1997). Perceived security may be a relatively enriched attribute, rather than a strictly comparable one. Hence, it may be worth examining preference in a choice setting.

## **I.7 Results of Experiment 1-2**

Experiment 1-2 investigates consumer preference elicited by choice task, rather than rating task. It is well-known that consumer preference can be reversed or affected depending on what kind of method researchers use to measure preference (e.g., Nowlis and Simonson 1997). In Experiment 1-1(A), we found there was no difference among conditions on consumer preference, and thought that it might cause from attribute-task compatibility. Nowlis and Simonson (1997) argued that comparable attributes (e.g., price) were likely to receive more weight on comparison-based tasks (e.g., rating), while enriched attributes (e.g., brand) were likely to receive more weight on separate evaluation based tasks (e.g., choice). Information security is directly unobservable for consumers, so it may be difficult to compare one product to the other on a security attribute. On the other hand, convenience/complexity is obvious and clear, so it is relatively easily compared. Thus, a security attribute may be more of an enriched attribute than a comparable attribute. We expect that consumers would prefer a website with a complex/inconvenient procedure to a website with a simple/convenient procedure when we use choice task to elicit consumer preference. We present only one of two websites (single vs. twice password) to examine how consumers choose under a separate evaluation in Experiment 1-2(A), whereas we present two websites at that same time to examine consumer choice under a joint evaluation in Experiment 1-2(B).

### *Method of Experiment 1-2(A)*

Three hundred twenty three participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation for participating. It was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). Participants were randomly assigned to condition (website with single password or website with twice passwords), and were required

to evaluate perceived convenience and perceived security of the website. They then chose whether to create their own account in the website or not. Stimuli and measurement items were identical to Experiment 1-1.

#### *Results of Experiment 1-2(A)*

We predicted that perceived security would increase when consumers experienced inconvenience or complexity, and this argument was validated in the previous experiments. In this experiment, we examine how consumer preference is affected by complexity/inconvenience in choice task, rather than rating, and whether our argument replicates. To the end, a one-way ANOVA was conducted with complexity (single vs. twice passwords login procedure) as the independent variable, and perceived convenience and perceived security as the dependent variables. Significant differences emerged between single password and twice passwords websites ( $F_{\text{perceived convenience}}(1, 321) = 7.955, p = .005$ ;  $F_{\text{perceived security}}(1, 321) = 8.894, p = .003$ ). Specifically, participants evaluated the conventional single password login procedure (control condition;  $M = 5.82$ ) as more convenient option than twice password login procedure ( $M = 5.49$ ). They also evaluated the conventional single password login procedure (control condition;  $M = 4.96$ ) as less secure option than twice password login procedure ( $M = 5.34$ ). We asked participants to make a choice whether they registered on the website or not. A Chi-square test revealed no difference between choice ratios of single and twice passwords ( $\chi^2 = 818, df = 1, p > .10$ ). 75.9% of participants (120 / 158) chose to create their account in the single password condition, whereas 71.5% of participant (118 / 165) chose to do so in the twice password condition.

#### *Method of Experiment 1-2(B)*

One hundred seventy three participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation for participating. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)), and individuals who took part in Experiment 1-2(A) were excluded from participating in this experiment. The procedure, stimuli and measurement items were identical to Experiment 1-2(A), except participants made a choice between two websites.

### *Results of Experiment 1-2(B)*

We predicted that consumers would choose the website with twice passwords login over that with single password because security would be regarded as an enriched attribute, rather than a comparable attribute. Before testing this argument, we examined whether H1-1 was replicated or not. Because we presented two websites to participants at the same time, we conducted an ANOVA with repeated measures. The results showed that participants evaluated the website with single password ( $M = 5.88$ ) more convenient than that with twice password ( $M = 4.05$ ;  $F_{\text{perceived convenience}}(1, 172) = 183.93, p < .001$ ), while they evaluated that with a single password ( $M = 4.71$ ) less secure than that with twice password ( $M = 5.64$ ;  $F_{\text{perceived security}}(1, 172) = 68.53, p < .001$ ). Thus, we successfully replicated H1-1 in this experiment. A chi-square test showed that consumers preferred the convenient option to the secured options ( $\chi^2 = 3.61, df = 1, p = .06$ ). Specifically, 57.2% of participants (99 / 173) chose the single password over twice passwords website (42.8%; 74 / 173). Although the choice ratio of single password was slightly higher than that of twice passwords, a considerable number of consumers still chose the secure option. Logistic regression also demonstrated that both convenience and security significantly affected consumers' choice of websites. To examine the impact of perceived security and perceived convenience on

consumer choice, we ran the logistic regression with two covariates (perceived security and perceived convenience). Perceived convenience was calculated by subtracting perceived convenience of website with twice passwords from that of website with single password, whereas perceived security was calculated by subtracting perceived security of website with single passwords from that of website with twice password<sup>1</sup>. The result clearly indicated that both convenience and security significantly influenced consumer choice. The negative coefficient of convenience indicated that the choice of the conventional single password website were driven by convenience (Wald = 20.62;  $p < .001$ ), while the positive coefficient of security indicated that the choice of the twice password website were driven by security (Wald = 27.89;  $p < .001$ ; see Table 1).

**Table 1 Parameter estimates of Logistic Regression**

		Parameter Estimates							
choice2 <sup>a</sup>		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
Twice	Intercept	-.350	.276	1.604	1	.205			
	convenience	-.677	.149	20.620	1	.000	.508	.380	.681
	security	1.198	.227	27.886	1	.000	3.315	2.125	5.172

a. The reference category is: Single.

## **I.8 Discussion of Experiment 1-2**

Experiment 1-2(A) and 1-2(B) examined if one alternative, perceived more secure, would be chosen over another, perceived less inconvenient and complex because security is an enriched rather than comparable, attribute. Convenience is relatively easy to observe and compare, while security is hard to detect, since consumers may determine security only after

---

<sup>1</sup> Convenience = convenience of Single – convenience of Twice; Security = security of Twice – security of Single

experiencing the website for a long time. Therefore, we expected that the Twice passwords website would be preferred when preference was elicited by a choice task, rather than rating. Although both convenience and security significantly played a role in consumer choice, the results showed that consumers slightly preferred a convenient option to a secure option when choosing between two options. However, there was no difference between the choice ratios of a convenient option and a secure option when consumers were asked to decide whether to create their own account or not (separate evaluation). It may be effective for a sales person to encourage consumers to focus on a target product in order to engage consumers in separate evaluation. Moreover, some companies may be tempted to be negligent to develop or enhance security feature because convenience could be enough to attract consumers. Thus, a government may need to consider a policy or regulation about security for consumer welfare.

## **I.9 Results of Experiment 1-3**

Experiment 1-3 examines how consumers' sensitivity to security may affect their preference, perceived security, and inference processing. In Experiment 1-1, we failed to find a significant difference in response time depending on the category of websites. We predicted that consumers would engage in more thoughtful processing when they examine relatively more important websites, compared to less important websites. However, there was no difference in their response time. This may be due to the product category. Because each product category has its own price range, different features and characteristics, consumption behavior, and etc, it may be inappropriate to examine our argument with a product category as one of the independent variables. Thus, we manipulate consumers' security awareness by priming within a single product category, and examine influences on consumer preference, perceived security, and inference processing.

## *Method*

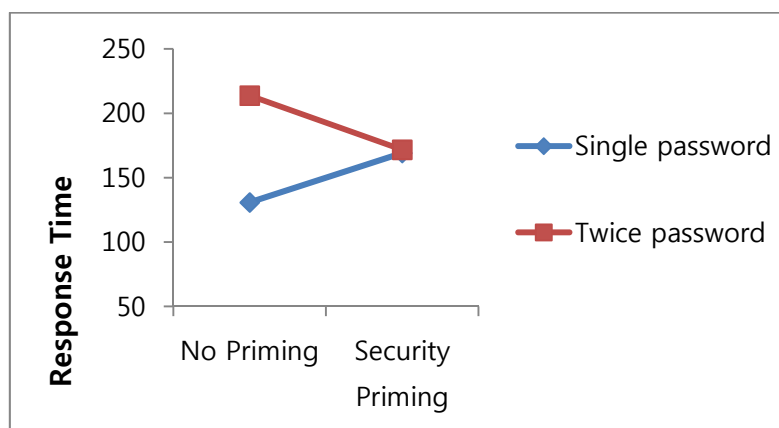
Two hundred twenty participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. A 2 (security priming: no priming vs. security priming) by 2 (complexity: conventional single password login vs. twice password login) between-subject experimental design was employed to examine our arguments, and the experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). Dependent variables and stimuli for complexity of websites were identical to those used in Experiment 1-1. In order to manipulate security awareness, we asked participant to read one page of a newspaper. This newspaper contained four articles, which were about ‘Disney and Lukas Arts,’ ‘Apple’s new iPad,’ ‘Audi’s new vehicle – Allroad Quattro,’ and ‘internet security.’ The security-related article (for priming) was located in right-bottom corner. In the no-priming condition, a security related article was replaced with a travel article (see Appendix 4). Participants were randomly assigned to one of four conditions, and asked to read one page of a newspaper. We asked participants to evaluate products, including our target product (website) and two filler products (home theatre and running shoes) to reduce demand artifacts. Then, security awareness was measured for a manipulation check with filler questions about Apple and Audi.

## *Results*

*Manipulation Check and Response Time.* We manipulated security awareness by presenting one page of a newspaper containing a security-related article and asked participants to read it. To confirm whether they were primed or not, we measured three items (important, sensitive, and concerned) on a 7-point-likart scale. Surprisingly there was no difference between priming condition and no-priming condition ( $p > .10$ ). When, however,

we analyzed it with response time as the dependent variable, we found the significant main effect of login procedure ( $F(1, 216) = 3.38, p = .07$ ) and the significant interaction effect between priming and login procedure ( $F(1, 216) = 3.00, p = .09$ ). Specifically, participants responded more slowly when they evaluated the Twice password login website ( $M = 192.69$  ms) than the conventional single password login website ( $M = 149.97$  (ms)). The interaction effect showed that participants spent more time to evaluate the twice password login website ( $M = 213.72$ ) than single password website ( $M = 130.76$ ) under no-priming condition, whereas there was no difference between the conventional single password ( $M = 169.17$ ) and the twice password ( $M = 171.67$ ) under security-priming condition (see Figure 8). Response time clearly showed that priming had the significant impact on their inference processing, even though three items for security awareness failed to capture it. These results indicated that consumers were engaged in deeper processing to infer security feature of the website when they were aware about security.

**Figure 8 The Interaction effect between Priming and Complexity**



*Convenience, Security, and Preference.* When the dependent variable was perceived convenience, the results of ANOVA showed that no significant effect (the main effects of priming and login procedure and the interaction effect;  $ps > .10$ ). When the dependent

variable was perceived security, the main effect of login procedure was marginally significant ( $F(1, 224) = 2.76, p = .10$ ). Specifically, participants evaluated the twice password login website ( $M = 5.24$ ) as more secure than the conventional single password login website ( $M = 4.96$ ). Thus, we successfully replicated H1-1 in this experiment, but the main effect of priming and the interaction effect were not significant ( $ps > .10$ ). When, surprisingly, the dependent variable was preference, the main effect of login procedure was marginally significant ( $F(1, 224) = 2.93, p = .09$ ). Participants evaluated the twice password login website ( $M = 5.57$ ) more favorably than the conventional single password login website ( $M = 5.31$ ), while the main effect of priming and the interaction effect were not significant ( $ps > .10$ ). Consumers expressed preference for a secure option over a convenient option.

### **I.10 Discussion of Experiment 1-3**

In Experiment 1-2(B), we found that participants slightly preferred convenient option to secure option, but surprisingly the result was reversed in this experiment. This may be caused by the following reasons. First, consumers might be easily swayed when choosing between secure and convenient options. When we asked participants to choose one of two options in Experiment 1-2(B), they selected a convenient option over a secure option, and we also observed this pattern in Experiment 1-1(B) with a rating task. However, it was reversed in this experiment, and there was no difference in Experiment 1-1(A). These mixed results may suggest that consumer preference is unstable, so the success of a security-focused product could depend on marketing strategy. On the other hand, one major difference between this experiment and previous experiments is the presence of priming. The convenient option was preferred in previous experiments, while the secure option was preferred in this experiment. Priming might influence consumers' preference judgment.

We found that consumers engaged in deeper inference processing when evaluating complex/inconvenient websites than convenient websites under no-priming condition. However, there was no difference under security priming condition. This result partially and indirectly supports our expectation (H1-5) that consumer would enlist more effortful process when inferring security feature of important websites than that of relatively less important websites. Although the importance of websites is conceptually different from security awareness, consumers may care about security more when accessing important websites. In addition, the manipulation check failed to capture the success of priming suggesting that explicit measures may be insufficient, compared to implicit measures.

### **I.11 Results of Experiment 1-4**

Experiment 1-4 examines H1-1 with another manipulation of complexity/inconvenience in order to increase the generalizability of our arguments. Previous experiments used the login procedure to increase meaningless complexity/inconvenience, but we now increase complexity/inconvenience by adding redundant actions in a product description, such as a pop-up warning window, registering safe site and application, compared to a control condition. Then, we measure perceived convenience, perceived security, and their preference.

#### *Method*

Sixty-four participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. A one-way ANOVA was employed to examine our hypotheses, and the experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). One independent variable was complexity/inconvenience, and the dependent variables were identical to that used in Experiment 1-1. In order to manipulate

complexity/inconvenience, we added meaningless features or properties of a target product. The product category was personal firewall software, providing protection from threats and controlling network traffic to and from a computer, and the product description in the control condition was taken directly from the real-world product – Online Amor Premium, while the product description in inconvenience/complexity condition included the following meaningless features: manual activation of Banking Mode, manual registration of trusted websites and applications, and pop-up window for warning (see Appendix 5). Then, we measured perceived convenience, perceived security, preference, and how technically advanced was the product.

### *Results and discussion*

Neither perceived convenience nor preference, differed between control and inconvenience condition ( $ps > .10$ ). Perceived security, however, was marginally ( $F(1, 62) = 2.95, p = .09$ ) greater in the inconvenient description ( $M = 5.36$ ) than the control condition ( $M = 4.97$ ). We also asked how technologically the product was. . Participants evaluated the inconvenient product ( $M = 5.48$ ) as technologically more advanced than the control condition ( $M = 4.88$ ),  $F(1, 62) = 5.09, p = .03$ ). Although marginally significant, H1-1 was replicated with different stimuli in this experiment.

## **I.12 Conclusion and Summary**

In sum, Experiment 1-1 showed that perceived security could increase by asking consumers to enter redundant information. Entering redundant information (e.g., typing a password twice) increased complexity (or inconvenience), and it resulted in enhancing perceived security because consumers believed that security could be achieved by sacrificing convenience. Although this belief might be true in physical security, it is not always true in

information security. Consumers nonetheless appear to have applied their knowledge about physical security in order to estimate information security. Furthermore, we found that subjective knowledge was weakly correlated with objective knowledge, so consumers' confidence about their inference varied depending on their knowledge. Specifically, consumers with high objective knowledge were less confident in their security judgments than those possessing low objective knowledge, while consumers who with subjective knowledge were more confident in their security judgments than those with low subjective knowledge. Objective knowledge apparently made consumers judge moderately, whereas subjective knowledge made them overestimate their judgment abilities. Although consumer knowledge affected judgment confidence, we failed to find a significant impact of consumer knowledge on the inference process response time. Experiment 1-2 was purposed to investigate the impact of perceived security on consumer preference formation. We argued that security might be a relatively enriched attribute, compared to convenience, so an option perceived secure would be preferred when preference was elicited by a choice task, rather than by a rating task. In the separate evaluation, there was no difference between the securely-perceived and conveniently-perceived option, but consumers slightly preferred the conveniently-perceived option to securely-perceived option in the joint evaluation. In Experiment 1-3, we demonstrated that security awareness manipulated by priming could affect consumer inference processing. Although priming did not influence perceived security, perceived convenience, and preference, consumers' response times varied depending on priming and complexity (or inconvenience). We examined another manipulation of complexity in order to examine the generalizability of our arguments in Experiment 1-4. Perceived security could be enhanced by adding redundant actions (e.g., manual registration of safe websites, pop-up warning windows, and manual activation of 'banking mode').

This study aimed to investigate consumer inference processing based on the relationship between complexity (or inconvenience) and security. The internet has become an important part of our daily life, so it is hard to imagine our life without it. As important as the internet is, security issues have risen because consumers frequently access and store their private and financial information on the internet. However, they are unfamiliar and not knowledgeable about security features, so we argued that they might use their knowledge about physical security to infer information security, and this inference process would be similar to a covariation-based inference such as price-quality inference. Through a series of experiments, we demonstrated that consumers make inferences about security based on complexity or inconvenience, apparently because consumers hold a general belief that convenience must be sacrificed in order to increase security. This study provides theoretical ground about how consumers infer unobservable security feature with observable complexity (or inconvenience). Although the mixed results about consumer preference indicate that further investigation is needed, we explained information security inference process based on the theory of price-quality inference making and provide better understanding about the role of consumer subjective and objective knowledge.

## **II Metacognitive Experience in Information Security**

### **II.1 Introduction**

A core assumption in most theories of human judgment is that people judge an object based on declarative information that comes to mind at the time of judgment. For example, we would form a favorable attitude toward the product that has more positive attributes, compared to other products that have relatively fewer positive attributes. However, some researchers argue that human judgment is influenced not only by declarative information but also by metacognitive experience, such as the ease of information retrieval or information processing fluency (Alter and Oppenheimer 2009; Schwarz 2004). The impact of metacognitive experience has been examined in a variety of domains and contexts such as truth judgment (Reber and Schwarz 1999; Unkelbach 2006), preference formation (Labroo, Dhar, and Schwarz 2008; Winkielman and Cacioppo 2001), confidence (Finn 2008; Kelley and Lindsay 1993; Ulkumen, Thomas, and Morwitz 2008), and typicality (Rhodes, Halberstadt, and Brajkovich 2001; Winkielman et al. 2006). The basic underlying mechanism of metacognitive experience is a misattribution of the difficulty experienced coming from one's unfavorable attitude toward an object. Numerous studies have demonstrated how critical metacognitive experience is in consumer judgment and decision making. While we examined how consumers infer information security, what kind of naïve theory they use in order to infer information security, and what their inference processes are depending on their knowledge and context in Chapter 1, Chapter 2 mainly focuses on how metacognitive experience influences perceived security. In other words, we covered the impact of declarative information (e.g., inconvenience of log-in procedure and newness of website) in Chapter 1, but we now investigate how consumers use their subjective experience of

processing, generating, or retrieving information in order to evaluate or estimate information security. To this end, we explore the metacognitive experience literature to understand how metacognitive experience affects consumers' judgment and decision making under a variety of contexts and domains. Although many metacognitive studies have focused on the negative effect of low fluency or difficult retrieval, some studies also investigate the positive effect of low fluency or difficult retrieval under certain conditions (Labroo and Kim 2009; Nielsen and Escalas 2010; Pocheptsova, Labroo, and Dhar 2010; Tamir et al. 2004). Based on these results, we expect that low fluency or difficult retrieval may lead to increased perceived security. In the next section, we examine the metacognitive literature, and propose how metacognitive experience can influence security estimation or evaluation.

## **II.2 Literature Review and Hypotheses**

### **II.2.A Metacognitive Experience**

The main argument of metacognitive experience is that consumers' subjective experience of generating or retrieving thoughts and processing information is informative in itself, rather than just the content of thoughts or information. Schwarz (2004) suggests that there are two distinctive meta-cognitive experiences; one is accessibility experience (the ease or difficulty of retrieval or generating thoughts) and the other is processing fluency (the ease or difficulty of processing presented information). If, for example, consumers can generate ten reasons to buy a product, they might predict they would like it because their favorable attitudes are supported by many reasons, compared to a case where only one reason is generated. However, recent work on metacognitive experience demonstrates that consumer preference can be influenced by how easy or difficult is the experience of retrieving or generating information, not the number of generated reasons. Because generating ten reasons is difficult, consumers

interpret this difficult experience as a less favorable attitude toward an object. On the contrary, generating one reason is simple and easy, so consumers interpret it as indicative of a more favorable attitude. The experience of retrieving or recalling information is informative by itself, regardless of the content of information (Hertwig et al. 2008; Kelley and Lindsay 1993; Menon and Raghurir 2003; Novemsky et al. 2007; Schwarz 1998; Tormala et al. 2007; Tybout et al. 2005; Wanke, Bohner, and Jurkowitsch 1997). On the other hand, processing fluency refers to the ease or difficulty of processing new and external information. For example, Labroo and colleagues (2008) demonstrate that consumers exposed to the word “Frog” prefer the prime-compatible product (a bottle of wine with a frog picture on the label) to another product (a wine without a frog on the label) because consumers process the prime-compatible product more fluently than other products. There are two different kinds of processing fluency – perceptual fluency and conceptual fluency. Perceptual fluency refers to how easily consumers perceive and identify the physical characteristics of a stimulus, whereas conceptual fluency refers to how easily the meaning of a stimulus is activated (Lee and Labroo 2004). Thus, whether accessibility or processing fluency is occurring depends on where information comes from – internal vs. external, but some researchers refer to all meta-cognitive experience as fluency, including accessibility and processing fluency, as a more general and broad term (Alter and Oppenheimer 2009).

Many researchers have demonstrated the impact of metacognitive experience in a variety of contexts and domains. Fluent statements seem truer than disfluent statements (Begg, Anas, and Farinacci 1992; Reber and Schwarz 1999). For example, Reber and Schwarz (1999) manipulated perceptual fluency by using the contrast of colors against a white background, and found the probability that statements were perceived as true was greater when presented in highly visible color, whereas the probability did not differ from chance when presented in

a moderately visible color. Consumers' confidence in their judgments also is affected by metacognitive experience (Alter et al. 2007; Finn 2008; Kelley and Lindsay 1993; Ulkumen et al. 2008). Ulkumen and colleagues (2008) argued that a feeling of difficulty was interpreted as an indication of inaccuracy, so participants showed less confidence when asked to estimate budgets for the next year than for the next month, since previous year's expenses require generation of a large number of expense categories, compared to next month. Alter and colleagues (2007) found that participants under low fluency (frowning their brows) indicated less confidence in their judgment than those under high fluency (puffing their cheeks). Metacognitive experience also influences preference and choice (Ferraro, Bettman, and Chartrand 2009; Labroo et al. 2008; Labroo and Lee 2006; Lee and Labroo 2004; Novemsky et al. 2007; Tamir et al. 2004; Wanke et al. 1997; Winkielman and Cacioppo 2001). For example, Winkielman and Cacioppo (2001) presented 20 black-and-white pictures to participants, and then measured their facial expression with an electromyography (EMG) device. Before presenting pictures, the targets were preceded by a prime with visual contour, made by deleting the inside detail of target pictures. Easy-to-process photos led to higher activity of zygomaticus muscle, indicating positive emotion, and self-reports of positive response were also consistent with the result of EMG. Ferraro and colleagues (2009) demonstrated that consumers who were exposed to the target brand incidentally, preferred the target brand even though they were not aware of the brand exposure. Specifically, participants were instructed that they would see twenty photos, and then be asked about the photos. They were asked to focus on the facial expression of people in the photos. In the fluent condition, there was a bottle of Dasani at the corner of the photo, whereas there was no Dasani in the disfluent condition. After finishing decoy tasks, they were asked to choose a bottle of water as a reward for their participation from four different brands (Dasani, Deer

Park, Aquafina, Poland Spring). More Dasani was chosen in the fluent condition than in the disfluent condition (Ferraro et al. 2009). Thus, metacognitive experience appears quite robust and accompanies many cognitive processes such as attitude formation (Fang, Singh, and Ahluwalia 2007; Labroo et al. 2008; Winkielman and Cacioppo 2001), choice (Ferraro et al. 2009; Novemsky et al. 2007; Tamir et al. 2004), confidence (Alter et al. 2007; Rhodes and Castel 2008), distance (Alter and Oppenheimer 2008), categorization judgment (Oppenheimer and Frank 2008), and numeric differences (Thomas and Morwitz 2009).

The key factor in the meta-cognitive experience is the naïve theory held by consumers (Alter and Oppenheimer 2009; Schwarz 2004). The impact of meta-cognitive experience comes from how experience is interpreted, rather than the intrinsic characteristics of the experience itself (Unkelbach 2006). The naïve theory is a kind of guideline for how to apply or interpret meta-cognitive experience into specific domains or judgments. For example, one naïve theory may interpret low fluency or difficult retrieving experience as clumsy and awkward, whereas another naïve theory may interpret it as novel and interesting. Unkelbach (2006) demonstrate how people interpret fluency depends on their naïve theory; consumers' interpretation for the fluency was influenced by the training session. Specifically, participants were asked to indicate whether presented names were perceived as new or old. Before starting the main study, they took a training session. In the training session, there were three conditions – classic, reverse, and control. During the training session, old names were paired with high fluency (and new names were paired with low fluency) in the classic condition, so participants judged names presented in high fluency as old (and names presented in low fluency as new) in the main study. On the contrary, participants' judgments in the main study were reversed when they experienced the reverse condition during the training session - old names were paired with low fluency (and new names were paired with high fluency).

Similarly, Winkielman and Schwarz (2001) asked participants to recall four versus twelve childhood events. In one condition, they told participants that unpleasant events might be poorly represented in memory because people did not like to think about bad events. In another condition, they told participants that pleasant events might be poorly represented in memory because people do not consider good events deeply. As a result, participants who recalled twelve events indicated their childhood as less happy when informed that negative events were difficult to recall than when informed that positive events were difficult to recall. Thus, these results indicate the naïve theory plays an important role in the meta-cognitive experience (Winkielman and Schwarz 2001). Schwarz (2004) proposes that selection of a naïve theory from a large number of possible naïve theories and its application to the context is affected by characteristics of the stimuli and presentation, judgment tasks, and consumers' own knowledge in a domain.

Although most research has focused on the positive effect of fluency and the negative effect of low fluency, several studies demonstrate the positive effect of low fluency. Interpretation of fluency depends on the naive theory people apply, and is affected by various factors. For example, Tamir and colleagues (2004) found that fluency could result in opposite outcomes depending upon the context. In Study 1, they used a 2 (task difficulty) by 2 (fluency: facial expression) experimental design. Choice between two similar posters represented a difficult task, whereas choice between two distinct posters was regarded as an easy task. They argued that brow tension (low fluency) would signal effort, and participants would interpret it as performing adequate problem solving and decisive judgment in the difficult task. Low fluency (the sign of effort) would be interpreted as confusion and indecisiveness in the easy task (Tamir et al. 2004). Alter and colleagues (2007) demonstrate that people use System 1 (intuitive and effortless processing) when information is processed

fluently, whereas they use System 2 (analytic and deliberate processing) when information is processed disfluently. In their Study 2, participants in the disfluent condition rated reviewer's competence more favorably when information about important features was presented than when information about unimportant features was presented (Alter et al. 2007). Similarly, Thompson and Chandon (2013) showed that low fluency enhanced judgments of a real estate agent's competence, and it resulted in increasing the intention for hiring. This result was replicated in another judgment context of an online course advisor who helped students to search, prepare, and apply to graduate schools. Participants in the disfluent condition evaluated a target service as more competitive and interpreted low fluency as a sign of effort (Thompson and Chandon 2013). Labroo and Kim (2009) propose that the goal and the means to accomplish the goal would influence the interpretation of low fluency. When people pursue a goal, they choose a means to achieve their goal, and the means is usually associated with effort. Therefore, consumers trying to reach a goal may perceive low fluency as effort, resulting in a favorable evaluation of the object. In Study 1, goals were primed (feel-good vs. goal-unrelated vs. self-control) and an object (chocolate) was presented in an easy- or difficult-to-read font. Chocolate can be a means to feel-good, so under feel-good instructions consumers evaluated it more favorably when exposed to a difficult-to-read font than an easy-to-read font. Under the good-unrelated priming condition, however, the effect is reversed. Similarly, they tested it in a donation context with a 2 (Be-Kind goal: high vs. low) by 2 (easy- vs. difficult-to-read font)(Labroo and Kim 2009). Nielsen and Escalas (2010) also demonstrated that difficult metacognitive experience could increase preference of a product when an advertisement encouraged narrative processing, rather than analytical processing. They asserted that consumers interpreted difficult metacognitive experience as a signal that the advertising story was complex, so they were transported by the story. As a result,

persuasion increased. Pocheptsova and colleagues (2010) also argue that consumption domains activate the relationship between product familiarity and value. Low fluency in the domain of everyday products should make consumers believe that the product is unfamiliar, resulting in low evaluations. In the domain of special occasion products, low fluency makes consumers believe that the product is rare, resulting in high evaluation (in Study 1, everyday cheese vs. special gourmet cheese; in Study 2, casual everyday restaurant vs. special upscale restaurant; in Study 4, priming everyday vs. special). As a result, the fluency makes everyday goods seem more attractive, whereas low fluency makes special-occasion products more attractive (Pocheptsova et al. 2010). In sum, the effect of low fluency can be positive depending on the selection of naïve theories and it is affected by various factors such as the characteristics of the task (Tamir et al. 2004), the characteristics of attributes (Thompson and Chandon 2013), the goal and the means (Labroo and Kim 2009), and the product category (Pocheptsova et al. 2010). Based on these findings, we propose consumers' perceived security may be influenced by their metacognitive experience.

## **II.2.B Metacognitive Experience and Information Security**

Metacognitive experience plays a critical role in consumer judgment and decision making. Especially, metacognitive experience can lead to positive or negative impact depending on what kind of naïve theories consumers use or adopt, and the selection of naïve theories is affected by a variety of factors such as situation, context, experience, and knowledge. We argue that low fluency and difficulty of retrieval can increase perceived security. Thompson and Chandon (2013) showed that low fluency made people believe that a real estate agent was competitive though the interpersonal liking decreased. Similarly, consumers perceived that a cooking recipe would take more time and require more skill in

disfluent condition than fluent condition (Song and Schwarz 2008). These results may be applied to the estimation or evaluation of information security. When evaluating perceived security for IT products, consumers may make inferences based on the trade-off relationship between security and convenience (Kim and Park 2012). We expect that high fluency increases perceived convenience, whereas low fluency may increase perceived security of a target product. In fact, companies develop advanced technology to enhance both convenience and security of IT products. However, consumers may think that convenience comes from creativity and product design, whereas security comes more from technology. Song and Schwarz (2008) demonstrated that low fluency made people believe that a cooking recipe required more skill. Similarly, we expect that consumers may evaluate IT products as technically more advanced in low fluent condition than in high fluent condition. As a result, perceived security may increase when consumers experience low fluency. On the other hand, Pocheptsova and colleagues (2010) demonstrated that low fluency in everyday products resulted in a negative effect, whereas low fluency in special products resulted in a positive effect on the product evaluation. Because consumers interpret low fluency as exclusivity, uniqueness, and unusualness, consumers under low fluency indicate a favorable attitude toward a product when it is categorized as a special product, rather than an everyday product. Consumers use different naïve theories to interpret their metacognitive experience depending on the product description – e.g., special gourmet cheese vs. everyday cheese. Thus, we expect consumers to form more favorable attitude toward a target product under low fluency than high fluency when its description is security-oriented, but it would be reversed when it is convenience-oriented. These arguments lead to the following hypotheses.

H2-1: Low fluency increases perceived security of a target product, while high fluency increases perceived convenience of a target product.

H2-2: Low fluency increases perceived security of a target product when the description of a target product is focused on security, compared to convenience.

We assert that consumers infer security based on inconvenience because they believe a trade-off relationship between convenience and security exists, so in Chapter 1 we demonstrated that perceived security was enhanced by increasing inconvenience, even though actual security was constant. This argument may interrelate with metacognitive experience, especially the perceived ease of retrieval. The typical way to manipulate the ease of retrieval is the number of thoughts retrieved or generated from memory. The more thoughts consumers are asked to generate or retrieve, the more inconvenience they feel. When, for example, consumers join a website, they usually input their personal information such as name, address, email address, phone number, and so on. Then, the website asks them to set up security questions, anticipating a situation in which they forget their ID or password. These security questions are selected by consumers themselves, and are private and personalized, such as their pet's name, mother's maiden name, or name of their best friend. However, it is quite rare to need to answer these security questions. Also, some companies just send a temporary password to customers' email accounts, rather than asking these questions. Because the main purpose of these security questions is the verification of their identification, email is an alternative method to verify their identification and is also easy and simple. This suggests that the number of security questions does not affect the level of security, but may influence consumers' perceived security. Moreover, consumers' interpretation of the difficult

experience of retrieval may be similar to that of low fluency, so consumers may indicate higher perceived security in difficult experience of retrieval than in easy experience of retrieval. This argument leads to the following hypothesis:

H2-3: Perceived security increases when consumers experience the difficulty of retrieval, compared to when they experience the ease of retrieval.

### **II.3 Results of Experiment 2-1**

Experiment 2-1 examines how processing fluency influences consumers' perceived security and product evaluation depending on product description within a product category. We showed that perceived security of and preference for a target product were affected by perceived complexity/inconvenience because of a general belief that security could be achieved by sacrificing convenience. In this experiment, we examined our argument with a traditional font manipulation. We expect that consumers will misattribute their subjective difficulty to advanced technology because consumers are usually unfamiliar and feel difficulty understanding technology. Moreover, perceived security might be influenced by product characteristics. If, however, we used product category as an independent variable, it may confound various factors. Thus, we would like to examine our argument in a single product category, with the product description either security-oriented or convenience-oriented, depending on condition. We expect low fluency will have more impact under security-oriented descriptions than convenience-oriented descriptions. Specifically, we predict that low fluency (e.g., difficult-to-read font) will increase perceived security of a target product when a product description is security-oriented than when it is convenience-oriented. On the other hand, it is expected that high fluency (e.g., easy-to-read font) results in

increasing perceived convenience when a product description is convenience-oriented, compared to a security-oriented description. Therefore, consumers will prefer a security-oriented described product to a convenience-oriented described product when printed in a difficult-to-read font, while they will prefer a convenience-oriented described product to a security-oriented described product when printed in an easy-to-read font.

### *Method*

One hundred thirty two participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. A 2 (fluency: easy-to-read font vs. difficult-to-read font) by 2 (product description: security- vs. convenience-oriented) between-subject design was employed to test our arguments. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). Participants were randomly assigned to one of four conditions, and the manipulation of fluency was identical to Song and Schwarz (2008) except the font size (easy-to-read font (Arial, 14 point) vs. difficult-to-read font (Mistral, 14 point); Song and Schwarz (2008) used 12 point, rather than 14 point). A data backup software was selected as a target product, and the description was directly borrowed from the actual description of Norton Ghost, one of the most popular data backup softwares. The description was split into two descriptions as follows. The security-oriented description was ‘*our data backup software provides professional grade backup and recovery. It safeguards your photos, videos, and other files, and takes periodic snapshots of your entire computer hard drive to be able to completely restore your computer system to a specific backup version in the case of hard drive failure. It compresses and encrypts your backups, and our advanced encryption helps keep sensitive data safe from prying eyes. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system,*’ whereas the

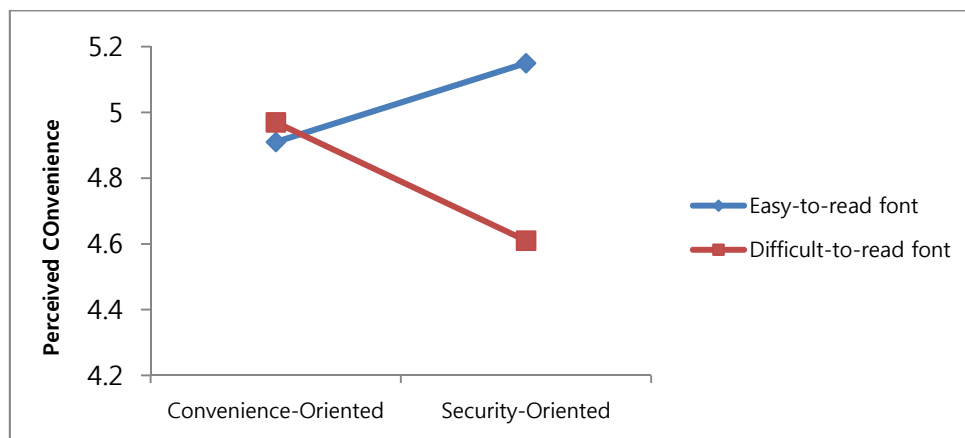
convenience-oriented description was ‘*our data backup software provides professional grade backup and recovery. It provides easy recovery of your data files, or your entire hard drive or a mapped drive to a previous backup image. Moreover, it allows you to quickly restore your system without needing a bootable CD. You can backup and recover your files from any type of devices such as a CD, DVD, Blue-ray disc, external drive, or network-attached storage device. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system* (see Appendix 6).’ Participants were asked to read the description of product, and then answer questionnaire about their preference, perceived security, perceived complexity, and technical advanced.

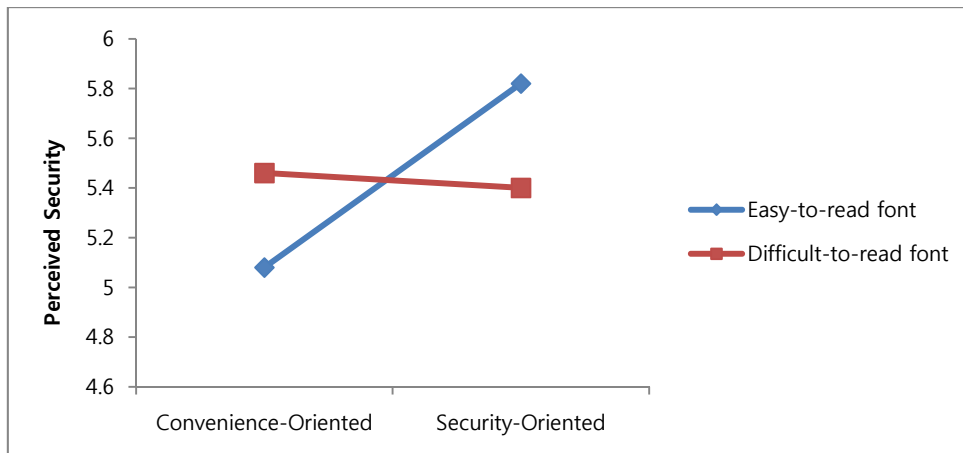
### *Results*

When the dependent variable was perceived convenience, we found that the interaction between fluency and product description was marginally significant ( $F(1, 128) = 3.32, p = .07$ ). Participants evaluated the security-oriented description with high fluency (easy-to-read font;  $M = 5.15$ ) more convenient than that with low fluency (difficult-to-read font;  $M = 4.61; p = .03$ ), but there was no difference between high fluency ( $M = 4.91$ ) and low fluency ( $M = 4.97$ ) when the description was convenience-oriented ( $p > .10$ ). Thus, this result indicates that high fluency effectively increased perceived convenience when a target product was described as security-oriented, rather than convenience-oriented. When the dependent variable was perceived security, the main effect of description was significant ( $F(1, 128) = 4.38, p = .04$ ), and we also found the significant interaction effect between product description and fluency ( $F(1, 128) = 6.06, p = .02$ ). It was natural that participants perceived the security-orientedly described data-backup software ( $M = 5.62$ ) more secure than the convenience-orientedly described one ( $M = 5.27$ ). The interaction effect was quite interesting.

Specifically, the pair-wise comparison test revealed that low fluency (difficult-to-read font;  $M = 5.46$ ) was perceived more secure than high fluency (easy-to-read font;  $M = 5.08$ ) when the target product was described as convenience-oriented ( $p = .09$ ). When, however, the target product was described as security-oriented, the result was reversed. The security-oriented described product with high fluency (easy-to-read font;  $M = 5.82$ ) was perceived more secure than that with low fluency (difficult-to-read font;  $M = 5.40$ ;  $p = .08$ ). Therefore, H2-1 was partially supported but H2-2 was not. When the dependent variable was ‘technically advanced,’ the main effect of the description was significant ( $F(1, 128) = 7.23, p = .008$ ). The security-oriented description ( $M = 5.90$ ) was evaluated more technically advanced than the convenience-oriented one ( $M = 5.41$ ). When, however, the dependent variable was preference, there was no significant effect ( $ps > .10$ ).

**Figure 9 The Interaction effect between Fluency and Description**





## II.4 Discussion of Experiment 2-1

Many studies of fluency demonstrate that high fluency leads to favorable evaluation, compared to low fluency (e.g., Alter and Oppenheimer 2009; Schwarz 2004), even though low fluency brings positive impact to consumer evaluation depending on context, product category, etc. (e.g., Pocheptsova et al. 2010). In this experiment, however, we failed to demonstrate that fluency would affect consumer preference. On the other hand, we found that high fluency led to increasing perceived convenience when the description was security-oriented. Because participants processed information smoothly and easily, they misinterpreted their experience of processing information as convenience of the target product, but it was effective in the security-oriented description. Interestingly we observed a different pattern on perceived security. Specifically, low fluency had a positive effect when the target product was described in terms of convenience, while it was reversed when the target product was described in terms of security. In other words, high fluency had positive effect in the security-oriented description, and it was opposite to our prediction. This might be due to consumers' unfamiliarity with security information creating difficulty in processing security information, especially when the description is in a difficult-to-read font. As a result,

their experienced difficulty was amplified, so they might fully understand information when printed in easy-to-read font, compared to difficult-to-read font. Therefore, perceived security in high fluency condition was higher than that in low fluency condition when the description was security-oriented. When, on the other hand, the description was convenience-oriented, low fluency had a positive impact on perceived security. Because there was little information about security in the convenience-oriented description, metacognitive experience, caused from difficult-to-read font, was the only one source from which to infer or estimate security of the target product. As a result, they interpret difficulty of processing information as high performance of security, a result of trade-off with convenience. Although we failed to find a significant effect of fluency on preference, these results provided interesting and useful insight about security inference making.

## **II.5 Results of Experiment 2-2**

Experiment 2-2 examines how processing fluency influences consumers' perceived security and product evaluation. Numerous studies about fluency have demonstrated that high fluency elicits favorable evaluation, while low fluency elicits less favorable product evaluation. However, some studies argue that low fluency can lead to favorable evaluation depending on context or product category, so we argue that low fluency may make consumers think a target product is more technically advanced. Because consumers might believe that security was closely related to technology, low fluency would result in increasing perceived security, while high fluency would increase perceived convenience. We manipulated fluency with the font (easy- vs. difficult-to-read font) in Experiment 2-1, but we tried an alternative method – the use of technical terms. Oppenheimer (2006) examined the impact of fluency by manipulating vocabulary difficulty and two different translations of the

first paragraph of Rene Decartes *Meditation IV*. We invoke a similar approach. It might be a more realistic examination of our arguments.

### *Method*

Sixty seven participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. One way ANOVA was employed to examine hypotheses. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). The independent variable was fluency, and was manipulated by using technical terms, rather than traditional font or color-contrast. The target product category was a web-browser, and the description came from the actual description of Google Chrome. Of course, we did not disclose information of Brand name (Google Chrome) to participants. The description of fluency condition was *'this web browser is designed to be fast in every possible way on HTTP, FTP, and HTTPS. It's quick to start up from your desktop, loads web pages in a snap, and runs complex web applications lightning fast with our own technology. This browser is streamlined, clean and simple, and has features that are designed for efficiency and ease of use based on HTML, XML, and Javascript. The auto-updates makes sure you have all the latest update & fixes with our own technology. Our web browser has many useful features built in, including automatic full-page translation and access to thousands of apps, extensions, and themes from our app store.'* In low fluency condition, we wrote down the full names of technical terms, rather than abbreviations. For example, *HTTP* was replaced with *Hypertext Transfer Protocol*, and *HTTPS* was replaced with *Hypertext Transfer Protocol on the top of Transport Layer Security/Secure Socket Layer*. Participants were randomly assigned to one of two conditions (high fluency vs. low fluency). Participants were asked to read the description of the product, and then answer questions about their

preference, perceived security, perceived convenience, and how technically advanced is the product.

### *Results and Discussion*

As predicted, main effects of fluency on perceived security ( $F(1, 65) = 4.36, p = .04$ ) and technical advanced ( $F(1, 65) = 3.66, p = .06$ ) emerged. Perceived security was higher when the target product was described with unfamiliar and technical terms ( $M = 5.57$ ) than when it was described with easy and familiar terms ( $M = 5.09$ ). Similarly, participants evaluated the target product described with unfamiliar and technical terms ( $M = 5.91$ ) more technically advanced than that described with easy and familiar terms ( $M = 5.31$ ). Thus, H2-1 was successfully supported. However, there was no statistical difference between the two fluency conditions when the dependent variables were preference and perceived convenience ( $ps > .10$ ).

## **II.6 Discussion of Experiment 2-2**

Our failure to obtain differences in preference and perceived convenience might be due to the manipulation of fluency. When fluency was manipulated by the font in the previous experiment, we found that perceived convenience was higher in high fluency than low fluency when the description was security-oriented. Consumers believed that their subjective difficulty came from low convenience and high security, even though it actually came from the font. In this experiment, however, participant clearly figured out where it came from – the technical terms. These technical terms made participants believe that the target product was technically advanced and resulted in increasing perceived security. Although consumers knew the true source of their difficulty, this experiment provided useful insight about

metacognitive experience because it could be applicable to the real world situation. When, on the other hand, Oppenheimer (2006) manipulated fluency with the difficulty of vocabulary and complexity of translations, he found that low fluency decreased the author's intelligence because of complexity of the essay, but we found that complexity of the product description increased perceived security. The nature of the target product differs in the two experiments. Specifically, the main goal of the essay was to deliver the content or message and the difficulty of vocabulary interrupted it. As a result, complexity of the essay has a negative impact on the author's intelligence. However, in our experiment consumers believed that complexity of IT products came from the technical advance, so it had a positive impact on perceived security. Fluency may have a different impact depending on product characteristics and dependent variables.

## **II.7 Results of Experiment 2-3**

The main objective of Experiment 2-3 is to investigate whether the ease-of-retrieval can affect consumers' security judgment. Based on our arguments that consumers infer security based on metacognitive experience and the correlated relationship between security and complexity, we predict that consumers' perceived security for websites can be enhanced by increasing the difficulty-of-retrieval. We demonstrated that increased complexity (or inconvenience) could enhance perceived security in Experiment 1-1, and low fluency could lead to increasing perceived security and preference in Experiment 2-1 and 2-2. The number of thoughts generated or retrieved has been widely adopted for manipulating accessibility experience, because participants experience difficulty generating or retrieving thoughts from memory and misattribute this difficulty to their unfavorable attitude toward a target product. At the same time, however, this difficulty might be recognized or perceived as

complexity/inconvenience to consumers, so the number of retrieval or thought generation could be processed as both accessibility experience and perceived complexity to consumers. Therefore, we expect that perceived security and preference could be affected, depending on accessibility experience.

### *Method*

*Participants and Stimuli.* One-hundred-fifteen participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. Perceived security should be higher when consumers experience difficulty of retrieval than when they experience ease of retrieval (H2-3). As stated above, the number of security questions will be related to both metacognitive experience and the correlated relationship between security and complexity. If, for example, consumers are required to set up 7 customized security questions, they should find the task inconvenient and complex. At the same time, they would experience difficulty generating 7 private and personalized questions. That is, not only is the experience inconvenient, it is hard as well. This may lead to increased perceived security, compared with 2 or zero questions. Therefore, we manipulated the ease of retrieval – accessibility experience with the number of security questions. We conduct a one-way ANOVA to test the difference among zero vs. two vs. seven questions.

*Procedure* This study employs a between-subject experimental design, conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). Participants were randomly assigned to one of three conditions (zero vs. two security questions vs. seven security questions). In the beginning of the experiment, participants were asked to imagine the following situation – ‘*Recently you find a website that is interesting and somewhat relevant to you, so you decide to create your account of the website. As usual, you decide your ID and password for this website and enter*

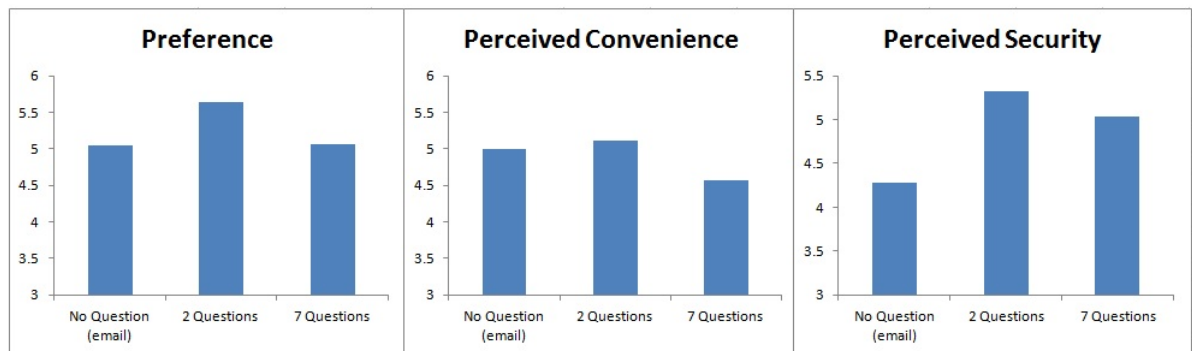
*your personal information (name, gender, and date of birth). Then, the following message shows up.* The message was about security question setup, and it varied depending on the condition participants were assigned. For example, the ‘zero’ condition in the number of security questions was presented as follows; *‘In the case that you forget your ID or passwords, we will send your ID or temporary passwords to you by email, rather than asking private and personalized security questions such as your mother’s maiden name.’* The other conditions will be presented as follows; *‘In the case that you forget your ID or passwords, we ask you to set up 2 (or 7) security questions such as your mother’s maiden name. Please write down your own 2 (or 7) security questions.’* The main purpose of security question setup was to check and confirm customers’ identities, and even if sending a new password to customer’s email account, the website could check their identity. Therefore, actually there was no difference among three conditions. Then, they were asked to report their preference, perceived convenience, and perceived security about the website.

### *Results*

We predicted that perceived security would be higher when consumers experienced the difficulty of retrieval than when they experienced the ease of retrieval. In detail, a website would be perceived more secure as consumers were asked to generate many (versus few or no) security questions. To test our arguments, a one-way ANOVA was conducted with the number of security questions (zero vs. two vs. seven questions) as the independent factor, and preference, perceived convenience, and perceived security as the dependent variables. An analysis of variance (ANOVA) showed that there was a significant difference among the three conditions (zero vs. two questions vs. seven questions;  $F_{\text{preference}}(2, 112) = 3.81, p = .03$ ;  $F_{\text{perceived convenience}}(2, 112) = 2.88, p = .06$ ;  $F_{\text{perceived security}}(2, 112) = 8.92, p < .001$ ). When, specifically, the dependent variable was preference, participants significantly preferred ‘two

security questions' condition ( $M = 5.64$ ) to both zero ( $M = 5.04$ ) and 7 security questions conditions ( $M = 5.06$ ;  $p < .05$ ), but there was no difference between zero and 7 security condition ( $p > .10$ ). In other words, the website requiring two-security-question setup was evaluated more favorably than others (no-question and seven-question). When the dependent variable was perceived convenience, 'seven security questions' condition ( $M = 4.57$ ) was significantly lower than both zero ( $M = 5.00$ ) and 'two security questions' conditions ( $M = 5.12$ ;  $p < .10$ ), but there was no difference between zero and 2 security condition ( $p > .10$ ). When the dependent variable was perceived security, both 'two' ( $M = 5.32$ ) and 'seven security questions' conditions ( $M = 5.03$ ) were significantly higher than both zero conditions ( $M = 4.28$ ;  $p < .01$ ), but there was no difference between 2 and 7 security condition ( $p > .10$ ; see figure 10).

**Figure 10 Preference, Perceived Convenience, and Perceived Security**



## II.8 Discussion of Experiment 2-3

Although the result that the website with seven security questions was less convenient than that with two security questions was exactly identical to our prediction, it was surprising that there was no difference between the website with no-question and the website with two questions. It might be due to the fact that both 'no-question with email account' and 'two

*security questions*’ are the most common way to check customers’ identities when they lost or forgot their ID and passwords. Therefore, participants might not feel any inconvenience in setting up two security questions, compared to ‘*no-question with email account*,’ even though it is actually much easier and simpler. This surprising result was illuminated by the dependent variable perceived security. Participants clearly evaluated ‘*no-question with email account*’ as less secure than the other two conditions (two and seven security questions), but the level of security of two security questions did not differ from that of seven security questions. Although we predicted consumers would perceive ‘*seven security questions*’ more secure than ‘*two security questions*,’ this result might be caused by participants simply imagining the situation, rather than actually generating security questions by retrieving their personal and private memory. That is, participants may not have experienced any difficulty at all owing to their “miscalibration” of the accessibility experience of generating security questions. Hence, a critical element of the theoretical driver of the anticipated effect may be absent. Because ‘*two security questions*’ was superior or equal to both ‘*no-question with email account*’ and ‘*seven security questions*,’ it was obvious that it was preferred over other two conditions. Although we failed to obtain precisely what was predicted, our argument receive some support from participants evaluating ‘*two security questions*’ more secure than ‘*no-question with email account*.’ To confirm this, and to ensure that participants are inferring from experience we conduct Experiment 2-4, in which participants generate security questions based on their personal and private memory.

## **II.9 Results of Experiment 2-4**

Experiment 2-4 examined the impact of accessibility experience on perceived security and preference by asking participants to actually generate security questions. This experiment

is identical to Experiment 2-3 except participants generate security questions and the ‘*no question with email*’ condition is eliminated. This condition was dropped because our focus is on the difference between ‘*two security questions*’ and ‘*seven security questions*’ when questions are generated, and we already observed that ‘*no question with email*’ condition was dominated by both ‘*two security questions*’ and ‘*seven security questions*’ in perceived security in Experiment 2-3.

### *Method*

Sixty five participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. Subjects who participated in Experiment 2-3 were excluded from this experiment. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). We expected that perceived security would be higher when consumers were asked to actually experience the difficulty by listing seven security questions than two security questions. Participants were randomly assigned to one of two conditions (two security questions vs. seven security questions). The procedure was identical to Experiment 3-A except actual generation. Then, participants’ preference, perceived convenience, and perceived security about the website were measured.

### *Results and Discussion*

When the dependent variables were perceived convenience and preference, we surprisingly failed to find any significant difference between ‘*two security questions*’ and ‘*seven security questions*’ ( $ps > .10$ ). However, participants evaluated ‘*seven security questions*’ ( $M = 5.29$ ) more secure than ‘*two security questions*’ ( $M = 4.82$ ;  $F(1, 63) = 5.08, p = .03$ ). This result is exactly as predicted, supporting H2-3, that perceived security increases when consumers experience difficult retrieval, compared to when they experience relatively

easy retrieval. However, we did not find any difference in perceived convenience and preference, even though these differed in Experiment 2-3 with identical stimuli. Perhaps participants' preference for and their perceived convenience of the website with two security questions was diluted or weakened by their experience. Actually generating even two questions (versus imagining generating questions) may be sufficiently effortful to overwhelm any notions of convenience and preference participants in experiment 2-3 may have held. Further investigation of these differences is needed. Despite this limitation, the results of this experiment clearly showed that increasing the difficulty of retrieval could enhance perceived security.

## **II.10 Conclusion and Summary**

In sum, a series of experiments demonstrated that low fluency could increase perceived security. Because prior studies showed that low fluency made consumers believe that their subjective experienced difficulty came from competence (Thompson and Chandon 2013) and more skills required (Song and Schwarz 2008), we argued that low fluency might make consumers misattribute their experienced difficulty into technical complexity for achieving security, rather than convenience, and it might be amplified when a product was security-related. In Experiment 2-1, we described a target product in two different ways – security-oriented vs. convenience-oriented, and tested our predictions. The results provided partial supports for our predictions. High fluency led to increased perceived convenience in security-oriented description, while it had no effect in convenience-oriented description. We found that high fluency effectively increased perceived security when the description was security-oriented, but the positive effect of low fluency was observed when the description was convenience-oriented. Experiment 2-2 examined an alternative manipulation of fluency. As

Oppenheimer (2006) manipulated fluency by vocabulary difficulty, we did it with technical terms, unfamiliar to consumers. As predicted, low fluency resulted in increasing perceived security (H2-1 supported) even though there was no difference between low and high fluency in preference and perceived convenience. Experiment 2-3 & 2-4 showed that accessibility experience (retrieval ease) could also lead to affecting perceived security. Although we failed to support our arguments in Experiment 2-3 (imagination), we found the significant difference of perceived security between the ease of retrieval and the difficulty of retrieval when actually asking to write down the security questions.

This study demonstrated that metacognitive experience could lead to increasing perceived security even if the actual level of security was constant. One of interesting findings was that low fluency brought the positive impact on perceived security only when it was not a security-related product. Although this study contributes to research about metacognitive experience, there are some limitations. First, we failed to find a significant difference between high fluency and low fluency when the dependent variable was ‘technically advanced’ in Experiment 1, even though we argued the reason why low fluency enhanced perceived security was the misattribution that consumers’ experienced difficulty came from the technology, which was hard for them to understand. Because consumers believed that security was enhanced by technical advances, the main effect of the description (security- vs. convenience-oriented) was significant when the dependent variable was ‘technically advanced.’ However, we found the significant difference in Experiment 2-2. Specifically, consumers evaluated the low fluency condition more technically advanced than the high fluency condition. These mixed results might be due to the manipulation of fluency (technical terms) in Experiment 2-2. When fluency was manipulated by the font, consumers’ experienced difficulty was unconsciously misattributed to their attitude, preference, or other

features. If they knew why they felt difficulty, they adjusted their misattribution. Compared to traditional or conventional manipulation methods of fluency (e.g., color contrast and font), consumers easily and consciously figured out why they felt difficulty because they were clearly unfamiliar with the technical terms. This may explain the mixed results. Second, we failed to find a significant difference between the ease of retrieval and the difficulty of retrieval on perceived security in Experiment 2-3 even though we observed what we predicted in Experiment 2-4. Wanke and her colleagues (2007) found a significant effect, regardless of whether they were asked to actually generate reasons or just imagine the situation, but our argument was effective only when actually generating questions. In spite of these limitations, this study provided interesting findings and insights to consumer researchers and companies.

## **III Improving Consumers' Information Security Estimation**

### **III.1 Introduction**

The notion that consumer preference is constructive rather than inherent is broadly accepted by most consumer researchers even though some argue that inherent preference is often meaningful and useful (Bettman, Luce, and Payne 1998; Simonson 2008; Simonson et al. 2001). Systematic errors or biases in judgment and decision making originate from not only constructive preference processes but also bounded rationality, so behavioral decision theory (BDT) has focused on identifying and demonstrating what kinds of biases exist and why these biases happen (Bettman et al. 1998; Kahneman 2003). Although biases in judgment and decision making are hard to avoid, many researchers have suggested ways to attenuate or eliminate them (Kahn, Luce, and Nowlis 2006). Kahn and her colleagues (2006) defined a bias as decision inconsistencies or a deviation from a prescriptive norm. Enhanced perceived security emanating from metacognitive experience and inference making based on the trade-off relation between security and convenience represent a kind of bias because perceived security is enhanced by increasing inconvenience with a meaningless procedure and subjective experience of processing information, rather than a technical improvement. Chapter 3 aims to investigate how to improve consumers' precise estimation of information security. Based on prior work on metacognitive and omission neglect theory, we argue that information security estimation may be made more accurate and precise by asking missing information questions or altering true sources of difficult experience and low fluency. To this end, we examine prior studies on debiasing omission neglect and metacognitive experience. Then, we suggest an experimental design to demonstrate the effectiveness of debiasing strategies, followed by a discussion of theoretical and managerial implications.

## III.2 Literature Review and Hypotheses

### III.2.A Debiasing Metacognitive Experience and Omission Neglect

When consumers are asked to list 10 reasons why they should buy a BMW, they feel difficulty generating many reasons, and then believe that this difficulty may be due to their low preference toward BMW. When, however, they are asked to list one reason, they feel it is easy, and then believe that they may love BMW (Wanke et al. 1997). Consumers primed with a frog indicate higher preference toward a product with a frog on the label than those not primed (Labroo et al. 2008). These phenomena are just a few examples of numerous metacognitive experiences, derived from consumers' misattribution of their subjective experience. Although a recognition heuristic and availability heuristic driven by metacognitive experience (Hertwig et al. 2008) can be efficient and effective as a judgmental cue because it is fast and frugal (Gigerenzer and Goldstein 1996), metacognitive experience may cause irrational and inconsistent behaviors – biases. Many studies have demonstrated not only the impact of metacognitive experience but also the debiasing strategy for eliminating or attenuating it. The impact of metacognitive experience may be reduced by discrediting the informational value of subjective experience or encouraging another naïve theory to interpret subjective experience differently. For example, informing and providing a true source of low fluency (e.g., 'this information may be difficult to read because of the font') are effective because consumers attribute their subjective experience to the font, rather than their preference or attitude (Pocheptsova et al. 2010). Changing naïve theories is another approach to reverse the effect of metacognitive experience. When, for instance, participants were asked to recall their childhood events, their rating of the happiness for their childhood varied depending on the instruction; '*pleasant childhood is difficult to remember*' versus '*unpleasant childhood is difficult to remember*' (Winkielman and Schwarz 2001). These

approaches are judgmental correction, which happens at a later stage of information processing, but interestingly Topolinski and Strack (2010) showed that attenuating the effect of fluency is possible without judgmental correction. Specifically, they asked participants to rate the fame of Bollywood actors based on their names. Half of names were shown to participants in the study phase, and then all names were presented in the test phase. Participants were randomly assigned to one of two conditions – kneading a ball vs. eating popcorn. Eating popcorn was directly related to their oral system, so the metacognitive experience, which came from reading or pronouncing names, was interfered with at an early stage of information processing (Topolinski and Strack 2010). On the other hand, Oppenheimer (2006) provided an alternative source of low fluency to participants and found the effect of fluency was reversed. When participants evaluated the intelligence of writers, low fluency (difficult-to-read font) resulted in lower estimation, whereas high fluency (easy-to-read font) resulted in high estimation of intelligence. When, however, low fluency was manipulated by a bad print condition due to the lack of the print toner, intelligence estimation in low fluency condition was higher than that in high fluency condition (Oppenheimer 2006). This is surprising because providing alternative sources for low fluency leads to reversing the effect of fluency, rather than attenuating or eliminating.

When consumers infer missing or unknown information, they may use implicit theories regarding a relationship between product attributes and features, and the typical example of an implicit theory is most likely the positive relationship between price and quality. A variety of implicit theories provide useful tools for maximizing accuracy and minimizing cost. However, implicit theories may be wrong or stochastic depending on variables such as context and time. For example, Broniarczyk and Alba (1994) showed that consumers overly relied on price information in order to infer product quality even though they were exposed to

the evidence that price was not an indicator for product quality. Vanhouche and van Osselaer (2009) argued that some attributes are likely to bias quality judgments, and are called ‘initially biased attributes.’ These biased attributes can increase the accuracy of judgments in later purchase situation if they provide quality feedback to consumers (Vanhouche and van Osselaer 2009). However, this finding focuses on the positive effect of biased belief about the relationship between attributes and benefits, and is limited to a subsequent purchase or trial. Omission neglect theory provides pertinent and relevant insight about consumers’ responses to missing or unknown information (Kardes et al. 2004b). Omission neglect theory asserts that consumers’ judgments and attitudes tend to be extreme and highly confident even though made on the basis of limited or incomplete information (Kardes et al. 2004b; Kardes et al. 2006; Sanbonmatsu et al. 1992; Sanbonmatsu et al. 2003; Sanbonmatsu et al. 1997). Consumers become sensitive to omissions and form moderate attitudes when informed that information is missing or unknown (Kardes et al. 2004b; Sanbonmatsu et al. 1992), when consumers are highly knowledgeable (Kardes et al. 2004b; Sanbonmatsu et al. 1992), and when comparison processes clearly show that some choices are described with a lot of information while others with relatively little information (Kardes et al. 2004b; Sanbonmatsu et al. 2003; Sanbonmatsu et al. 1997). Kardes and his colleagues (2006) also demonstrated that omission neglect could be de-biased when asking consumers to consider judgment criteria before receiving product information and when asking consumers to rate presented and missing product attribute information before making the overall product evaluation. By increasing the salience of missing or unknown information, omission neglect could be debiased.

### **III.2.B Debiasing Overestimated Information Security**

In Chapters 1 and 2, we demonstrated that perceived information security increased by adding inconvenience and difficult subjective experience. Typing a password twice, for example, increases inconvenience without enhancing security. The server system of a website receives the identical information from a user, so it is redundant and a waste of the system resource. Our results, however, show that consumers perceived it as more secure than a conventional single-password log-in procedure. This bias is driven by consumers' implicit theory that security is enhanced by sacrificing convenience. On the other hand, information security consists of three elements - confidentiality, integrity, and availability (Gerber and von Solms 2001; Parker 1998; Posthumus and von Solms 2004). Confidentiality refers to limiting information access and disclosure to authorized users or parties and preventing access by or disclosure to unauthorized users and parties. Integrity refers to the trustworthiness of information that data or information should not be changed or modified inappropriately. Availability refers to that information should be available when it is need or requested by authorized users and parties. If we ask consumers to evaluate confidentiality, integrity, and availability of a website separately, rather than overall security, they may figure out how much complexity can enhance overall security, or the impact of complexity in security inference may be minimized because the log-in procedure is just a part of confidentiality. Kardes and his colleagues (2006) demonstrated that asking consumers to rate presented and missing information before overall product evaluation was effective to debias omission neglect. Similarly, if we make consumers realize that information security comes from not only confidentiality but also integrity and availability, perceived security enhanced by biased inference making may decrease. This argument leads to the following hypothesis:

H3-1: There is no difference in overall perceived security between a complex/inconvenience website and a simple/convenient website when consumers are asked to evaluate confidentiality and integrity of a website before evaluating the overall security.

We argue that both low fluency and the difficulty of retrieval make consumers believe that information security is enhanced, compared to high fluency and the ease of retrieval. If metacognitive experience comes from misattribution, the effect may be eliminated or attenuated if a reason explaining the difficult experience is presented. When a product description is presented with a difficult-to-read font, consumers' preference may decrease but perceived security may increase. If a statement that information is difficult to read because of the font is added, consumers may understand why they experience the difficulty and then attribute it to the right source – the font, rather than security or technology. Similarly, we argue that asking to set up seven security questions may increase consumers' perceived security, compared to two questions. If we state that generating seven personal and private questions may be difficult because they should think carefully and effortfully to exclude information other people may know, consumers may think the difficulty they feel is reasonable, so the impact of the retrieval difficulty may decrease. If we state that generating five personal and private questions may be easy because they have lots of information about themselves that other people do not know, consumers may not find the true source of difficulty, and the difficulty they experience may be misattributed to the technical advance and security. As a result, the retrieval difficulty may increase perceived security. These arguments lead to the following hypotheses:

H3-2: Perceived security, enhanced by low fluency, is attenuated when the true source of a difficult experience is provided.

H3-3: Perceived security, enhanced by retrieval difficulty, is attenuated when another naïve theory to interpret difficult experience is provided.

### **III.3 Results of Experiment 3-1**

Experiment 3-1 examines the debiasing strategy to enhance consumers' judgment accuracy. We demonstrated that consumers overestimated security of websites when perceived complexity/inconvenience was high because of a general belief that security is obtained by sacrificing convenience or increasing complexity. Although it might be true in physical security, it is not always true in information security or the IT world. The reason why consumers tend to overestimate security is that they are unfamiliar to information security and make inference about information security based on their knowledge about physical security. Therefore, if they know and realize the difference between information security and physical security, increased perceived security by complexity/inconvenience would be eliminated. To that end, we ask participants to respond to specific questions about dimensions of information security (Confidentiality, Integrity, Availability). As a result, we expect participants will realize that the login procedure is just a part of information security and then adjust their security inference.

#### *Method*

Seventy three participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. The experiment was

conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). A one-way ANOVA was conducted with the independent variable complexity of websites, manipulated by login procedure. The dependent variables and stimuli were identical to those used in Experiment 1-1. Participants were randomly assigned to one of two conditions. After looking at a picture of the website login procedure, participants were asked to evaluate perceived convenience and perceived security of the website and their preference. However, participants in ‘twice password login’ condition were be asked to answer specific questions about confidentiality and integrity of information security (see Appendix 3) before they were asked to rate perceived convenience, perceived security, and preference.

### *Results and Discussion*

When the dependent variable was perceived convenience, the results of the ANOVA indicated that participants evaluated ‘conventional single password login website’ ( $M = 5.75$ ) more convenient than ‘twice password login website’ ( $M = 5.21$ ;  $F(1, 71) = 4.33$ ,  $p = .04$ ), but there was no significant difference between the two conditions when the dependent variables were preference and perceived security ( $ps > .10$ ). The mean of perceived security of ‘twice password login website’ ( $M = 5.34$ ) was directionally higher than that of ‘conventional single password login website’ ( $M = 5.05$ ), but not statistically significant. Also, the mean of preference of ‘twice password login website’ ( $M = 5.62$ ) was not different from that of ‘conventional single password login website’ ( $M = 5.55$ ). Convenience of websites was clearly distinctive by the login procedure, as expected. Perceived security, enhanced by complexity/inconvenience, can be adjusted or corrected by asking specific questions about confidentiality and integrity (dimensions of information security). As we argued, consumers realized that information security could not be guaranteed by only the

login procedure because the login procedure was just a step for checking their identity and a part of whole security. As a result, there was no difference between two conditions, so H3-1 was supported.

### **III.4 Results of Experiment 3-2**

Experiment 3-2 examines how to debias the effects of processing fluency on perceived security and product evaluation. In the previous experiment (Experiment 1-1), we demonstrated that disfluency increased perceived security when the product description was convenience-oriented, rather than security-oriented. Many prior studies demonstrated that fluency effect could be eliminated by letting consumers know the source of their experienced difficulty (e.g., Pocheptsova et al. 2010). Knowing the source of their subjective difficulty, they could adjust their attitude or evaluation about a target product. Thus, we examined whether the impact of fluency on perceived security could be eliminated by adding a statement that they might feel difficulty reading information because of the font.

#### *Method*

One hundred thirty five participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). A 2 (fluency: easy-to-read font vs. difficult-to-read font with the debiasing statement) by 2 (product description: security- vs. convenience-oriented) between-subject design was employed to test our arguments. Participants were randomly assigned to one of four conditions, and the procedure and stimuli were identical to Experiment 2-1 except the statement in disfluency condition, which was ‘*you may feel difficulty to read information because of the font.*’ Participants were asked to read the

description of the product, and then answer questions about their preference, perceived security, perceived complexity, and how technically advanced was the product.

### *Results and Discussion*

The main effects of fluency and description and the interaction effects were not significant ( $ps > .10$ ), regardless of what the dependent variables were except perceived security. The interaction effect between description and fluency was marginally significant when the dependent variable was perceived security ( $F(1, 131) = 3.29, p = .07$ ), but this effect was driven by the difference between the convenience-oriented and the security-oriented description when printed in easy-to-read font ( $p = .095$ ). There was no statistical difference between high fluency (easy-to-read font;  $M = 5.32$ ) and low fluency (difficult-to-read font;  $M = 4.98; p > .10$ ) in the security-oriented description. Similarly, there was no statistical difference between high fluency (easy-to-read font;  $M = 4.89$ ) and low fluency (difficult-to-read font;  $M = 5.21; p > .10$ ) in the convenience-oriented description. The pattern of the interaction plots is quite similar to what we observed in Experiment 2-1. Participants adjusted their judgment about security features of the target product. As a result, the variance of low fluency conditions increased, and these were not statistically different from high fluency conditions. Thus, we confirmed that the biasing effects of disfluency could be eliminated by adding the statement, supporting H3-2. Providing the true source of subjective difficulty prevented participants from misattribute their experienced difficulty to their preference or the security of a target product.

### **III.5 Results of Experiment 3-3**

Experiment 3-3 examines how to debias the impact of accessibility experience on perceived security and preference. Experiment 2-3 and 2-4 demonstrated that perceived security could be influenced by consumers' subjective experience, caused by the number of security questions. The key factor of metacognitive experience was what naïve theory consumers selected and applied to contexts (e.g., Alter and Oppenheimer 2009; Schwarz 2004). For example, Winkielman and Schwarz (2001) demonstrated that consumers interpreted their experience differently depending on what kind of instruction they received from researchers. In this experiment, we provided participants two different naïve theories about their upcoming experience in the experiment, and examined how it could improve the accuracy of their security judgment.

#### *Method*

One hundred fifty four participants were recruited from Amazon Mechanical Turk ([www.mturk.com](http://www.mturk.com)), and received nominal monetary compensation for participating. Subjects who participated in Experiment 2-3 and 2-4 were excluded in this experiment. The experiment was conducted via Qualtrics ([www.qualtrics.com](http://www.qualtrics.com)). A 2 (security questions: two vs. seven) by 2 (naïve theory: easy vs. difficult) between-subject experiment design was employed. Participants were randomly assigned to one of four conditions. The procedure was identical to Experiment 2-3 with the exception of providing naïve theories to participants. In the easy naïve theory, we provided an instruction to participants as follows; '*generating personal and private questions may be easy because you have lots of information about yourself that other people do not know.*' The instruction in the difficult naïve theory condition was '*generating personal and private questions may be difficult because you should think carefully and effortfully to exclude information other people may know.*' Then, we measured

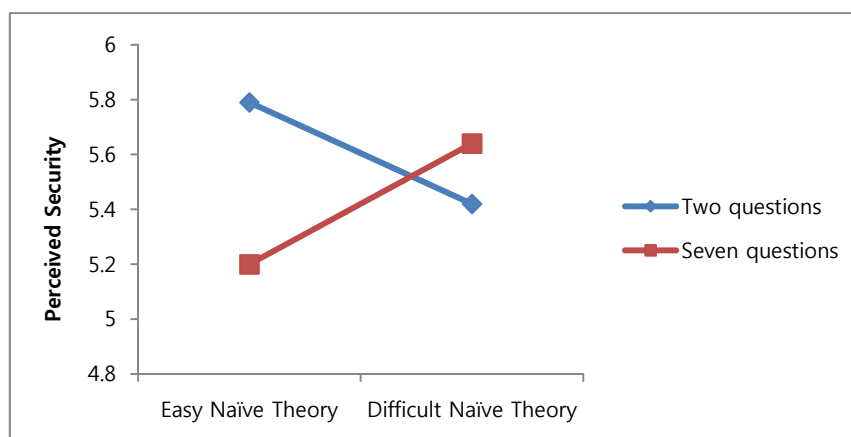
their preference, perceived convenience, and perceived security of the website. In addition, we asked participants whether they actually tried or made an attempt to generate security questions.

### *Results and Discussion*

We found that the main effects of accessibility experience (the number of security questions) were significant when the dependent variables were preference ( $F(1, 148) = 5.56, p = .02$ ) and perceived convenience ( $F(1, 148) = 4.21, p = .04$ ), but the main effect of naïve theory and the interaction effect were not significant ( $ps > .10$ ). Specifically, participant preferred ‘two security questions’ condition ( $M = 5.54$ ) to ‘seven security questions’ condition ( $M = 5.04$ ), and they perceived ‘two security questions’ condition ( $M = 5.03$ ) more convenient than ‘seven security questions’ condition ( $M = 4.64$ ). When, however, the dependent variable was perceived security, we did not find any significant effect ( $ps > .10$ ). These results were typical patterns we could observe in metacognitive experience researches, and we failed to find any difference of perceived security between two security questions and seven security questions, which was consistent with what was observed in Experiment 2-3. We suspect this is because participants were not required to actually generate security questions. We next analyzed only responses from participants who actually tried to generate security questions, resulting in responses of twenty nine participants being eliminated from the data set. An interaction obtained ( $F(1, 119) = 4.16, p = .044$ ), with no significant main effects ( $ps > .10$ ) for perceived security. Specifically, there was no difference between ‘two security questions’ ( $M = 5.42$ ) and ‘seven security questions’ condition ( $M = 5.64$ ) when naïve theory was difficult ( $p > .10$ ), but ‘two security questions’ condition ( $M = 5.79$ ) was perceived more secure than ‘seven security questions’ condition ( $M = 5.20; p = .037$ ). This

suggests that having an ‘easy’ naïve theory amplified the positive impact of the retrieval ease, while a ‘difficult’ naïve theory attenuated it. When, on the other hand, the dependent variables were perceived convenience and preference, no significant effect emerged ( $p > .10$ ).

**Figure 11 The Interaction effect between Naive Theory and Retrieval Ease**



### III.6 Discussion of Experiment 3-3

When focusing on the ‘easy’ naïve theory condition, the result was opposite to that found in Experiment 2-4. Specifically, perceived security in the seven security question condition was higher than that in two security question condition in Experiment 2-4, but it was reversed when participants were instructed that they might feel easy to generate security questions – ‘easy’ naïve theory condition. Moreover, there was no difference in the ‘difficult’ naïve theory condition. These mixed results might be caused from the following possible reasons. First, the experience of actually generating security questions is likely different from the experience of only imagining doing so. Participants who imagined generating questions might think about plausible questions but not generate all questions completely, and hence underestimate the difficulty. Second, providing a specific naïve theory might interfere with the information process of interpreting the actual experience. For instance, some participants

might disagree with the instruction even though other might agree with it. Thus, it could foster resistance about difficulty or easiness. Examining only participants who self-reported attempts at generating security questions, results partially supporting H3-3 were found. Although mixed results are found, it provides useful insights about metacognitive experience and naïve theory. Instructing a specific naïve theory may make consumers interpret their experience in completely different ways. The specific naïve theory applied may be the key factor in alleviating or eliminating completely the impact of an accessibility experience.

### **III.7 Conclusion and Summary**

This chapter investigates how to enhance consumer judgment about information security. Prior studies about metacognitive and omission neglect theory showed that consumers could adjust their judgments and improve the accuracy by asking missing information questions or providing altering true sources of difficult experience and low fluency. To this end, we conducted three experiments. As we predicted, there was no difference in overall perceived security between a complex/inconvenience website and a simple/convenient website when consumers were asked to evaluate confidentiality and integrity of a website before evaluating the overall security. Furthermore, perceived security which was enhanced by low fluency could be attenuated by providing the true source of a difficult experience, and perceived security which was enhanced by retrieval difficulty could also be attenuated by providing a naïve theory to interpret their subjective experience. Although the results of Experiment 3-3 were different from our expectation, the overall results suggest that consumer judgment may be made more accurate and precise by eliminating biases, which come from metacognitive experience and inference making based on consumers' theories about the relationship between security and complexity.

## **Conclusion of Dissertation**

Although many studies demonstrate the importance of information security to consumers, researchers have paid scant attention to the inferential processes underlying consumers' perceptions of information security. If consumers do not appreciate security features or know how to accurately estimate security aspects of a product, secure products or websites may lose their competitive edge and the cost to build and offer security may be largely wasted. Hence, it is important to know how consumers evaluate and infer security. We investigate how consumers infer and evaluate online information security based on consumer inference making process and metacognitive experience.

Chapter 1 argued that consumers would rely on a correlated relationship between security and complexity in order to infer security. As a result, consumers' security evaluations could be enhanced by simply increasing complexity, even if that increased complexity is in fact irrelevant to actual security. Throughout the series of experiments, we demonstrated that consumers evaluated a website more secure when asked to enter redundant information in Experiment 1-1. Experiment 1-2 revealed that perceived security played an important role when consumers chose a website. Experiment 1-3 showed that no-primed consumers were engaged in deeper inference process when inferring complex websites than conventional websites, whereas the response time of security-primed consumers did not differ regardless of the complexity of websites. We successfully replicated that complexity/inconvenience could increase perceived security with a different manipulation in Experiment 1-4. Thus, we clearly verified our arguments that complexity/inconvenience reinforced by a meaningless procedure could increase perceived security because of the relationship between security and complexity.

Chapter 2 suggested that disfluency and difficulty of retrieval could increase perceived security because metacognitive experience makes consumers misattribute their feeling of difficulty to their favorable or unfavorable attitude toward an object, depending on context and product category. Experiment 2-1 showed that perceived security was higher under low fluency (difficult-to-read font) than high fluency (easy-to-read font) when a product description was convenience-oriented, but it was reversed when a product description was security-oriented. In Experiment 2-2, we manipulated disfluency with technical terms, rather than traditional font or color-contrast, and showed that the product description with unfamiliar technical terms was perceived more secure than one with easy and familiar terms. Experiments 2-3 and 2-4 demonstrated that perceived security was also enhanced by difficulty of retrieval – the number of security questions generated.

Chapter 3 focused on how to improve the accuracy of security judgments. We expected that perceived security enhanced by meaningless complexity would be adjusted by asking specific dimensions of security (Confidentiality, Integrity, and Availability), and Experiment 3-1 demonstrated support for this argument. Experiment 3-2 showed that the positive impact of a disfluency effect could be debiased by providing participants the true source of their subjective difficulty, which came from difficult-to-read font, rather than their attitude or perception. In Experiment 3-3, we demonstrated that consumers' interpretation about accessibility experience varied depending on what kind of naïve theory was activated.

## IV Reference

- "Information Security" (2004), "Wikipedia: The Free Encyclopedia," in *Wikipedia: The free encyclopedia*, FL: Wikimedia Foundation, Inc., [http://en.wikipedia.org/wiki/Information\\_security](http://en.wikipedia.org/wiki/Information_security).
- "Security" (2004), "Wikipedia: The Free Encyclopedia," in *Wikipedia: The free encyclopedia*, FL: Wikimedia Foundation, Inc., <http://en.wikipedia.org/wiki/Security>.
- Alba, J. W. and J. W. Hutchinson (1987), "Dimensions of Consumer Expertise," *Journal of Consumer Research*, 13 (4), 411-54.
- (2000), "Knowledge Calibration: What Consumers Know and What They Think They Know," *Journal of Consumer Research*, 27 (2), 123-56.
- Alter, A. L. and D. M. Oppenheimer (2008), "Effects of Fluency on Psychological Distance and Mental Construal (or Why New York Is a Large City, but New York Is a Civilized Jungle)," *Psychological Science*, 19 (2), 161-67.
- (2009), "Uniting the Tribes of Fluency to Form a Metacognitive Nation," *Personality and Social Psychology Review*, 13 (3), 219-35.
- Alter, A. L., D. M. Oppenheimer, N. Epley, and R. N. Eyre (2007), "Overcoming Intuition: Metacognitive Difficulty Activates Analytic Reasoning," *Journal of Experimental Psychology-General*, 136 (4), 569-76.
- Beckhoff, J., V. Krishnan, M. Niculescu, M. L. Kohne, R. W. Palmatier, and F. R. Kardes (2009), "The Role of Omission Neglect in Response to Non-Gains and Non-Losses in Gasoline Price Fluctuations," *Journal of Applied Social Psychology*, 39 (5), 1191-200.
- Begg, Ian M., Ann Anas, and Suzanne Farinacci (1992), "Dissociation of Processes in Belief: Source Recollection, Statement Familiarity, and the Illusion of Truth," *Journal of Experimental Psychology: General*, 121 (4), 446-58.
- Bettman, James R., Mary Frances Luce, and John W. Payne (1998), "Constructive Consumer Choice Processes," *Journal of Consumer Research*, 25 (3), 187-217.
- Broniarczyk, S. M. and J. W. Alba (1994a), "The Role of Consumers Intuitions in Inference Making," *Journal of Consumer Research*, 21 (3), 393-407.
- (1994b), "Theory Versus Data in Prediction and Correlation Tasks," *Organizational Behavior and Human Decision Processes*, 57 (1), 117-39.
- Broniarczyk, S. M. and A. D. Gershoff (1997), "Meaningless Differentiation Revisited," *Advances in Consumer Research*, Vol Xxiv, 24, 223-28.
- Carlson, J. P., L. H. Vincent, D. M. Hardesty, and W. O. Bearden (2009), "Objective and Subjective Knowledge Relationships: A Quantitative Analysis of Consumer Research Findings," *Journal of Consumer Research*, 35 (5), 864-76.

Carpenter, G. S., R. Glazer, and K. Nakamoto (1994), "Meaningful Brands from Meaningless Differentiation - the Dependence on Irrelevant Attributes," *Journal of Marketing Research*, 31 (3), 339-50.

Casalo, L. V., C. Flavian, and M. Guinaliu (2007), "The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking," *Online Information Review*, 31 (5), 583-603.

Chellappa, Ramnath K. and Paul A. Pavlou (2002), "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions," *Logistics Information Management*, 15 (5/6), 358-68.

Chernev, A. (2007), "Jack of All Trades or Master of One? Product Differentiation and Compensatory Reasoning in Consumer Choice," *Journal of Consumer Research*, 33 (4), 430-44.

Chernev, A. and G. S. Carpenter (2001), "The Role of Market Efficiency Intuitions in Consumer Choice: A Case of Compensatory Inferences," *Journal of Marketing Research*, 38 (3), 349-61.

Chirillo, John and Edgar Danielyan (2005), "Fundamental Security Concepts," in *Sun Certified Security Administrator for Solaris 9 & 10 Study Guide*, United States: McGraw-Hill, 3-34.

Cronley, M. L., S. S. Posavac, T. Meyer, F. R. Kardes, and J. J. Kellaris (2005), "A Selective Hypothesis Testing Perspective on Price-Quality Inference and Inference-Based Choice," *Journal of Consumer Psychology*, 15 (2), 159-69.

Dick, A., D. Chakravarti, and G. Biehal (1990), "Memory-Based Inferences During Consumer Choice," *Journal of Consumer Research*, 17 (1), 82-93.

Fang, X., S. Singh, and R. Ahluwalia (2007), "An Examination of Different Explanations for the Mere Exposure Effect," *Journal of Consumer Research*, 34 (1), 97-103.

Ferraro, R., J. R. Bettman, and T. L. Chartrand (2009), "The Power of Strangers: The Effect of Incidental Consumer Brand Encounters on Brand Choice," *Journal of Consumer Research*, 35 (5), 729-41.

Finn, B. (2008), "Framing Effects on Metacognitive Monitoring and Control," *Memory & Cognition*, 36 (4), 813-21.

Flavian, C. and M. Guinaliu (2006), "Consumer Trust, Perceived Security and Privacy Policy - Three Basic Elements of Loyalty to a Web Site," *Industrial Management & Data Systems*, 106 (5-6), 601-20.

Friedman, B., P. H. Kahn, and D. C. Howe (2000), "Trust Online," *Communications of the Acm*, 43 (12), 34-40.

Gerber, M. and R. von Solms (2001), "From Risk Analysis to Security Requirements," *Computers & Security*, 20 (7), 577-84.

Gigerenzer, Gerd and Daniel G. Goldstein (1996), "Reasoning the Fast and Frugal Way: Models of Bounded Rationality," *Psychological Review*, 103 (4), 650-69.

Hertwig, R., S. M. Herzog, L. J. Schooler, and T. Reimer (2008), "Fluency Heuristic: A Model of How the Mind Exploits a by-Product of Information Retrieval," *Journal of Experimental Psychology-Learning Memory and Cognition*, 34 (5), 1191-206.

- Kahn, B. E., M. F. Luce, and S. M. Nowlis (2006), "Debiasing Insights from Process Tests," *Journal of Consumer Research*, 33 (1), 131-38.
- Kahneman, Daniel (2003), "Maps of Bounded Rationality: psychology for Behavioral Economics " *The American Economic Review*, 93 (5), 1449-75.
- Kardes, F. R., M. L. Cronley, J. J. Kellaris, and S. S. Posavac (2004a), "The Role of Selective Information Processing in Price-Quality Inference," *Journal of Consumer Research*, 31 (2), 368-74.
- Kardes, F. R., S. S. Posavac, and M. L. Cronley (2004b), "Consumer Inference: A Review of Processes, Bases, and Judgment Contexts," *Journal of Consumer Psychology*, 14 (3), 230-56.
- Kardes, F. R., S. S. Posavac, D. Silvera, M. L. Cronley, D. M. Sanbonmatsu, S. Schertzer, F. Miller, P. M. Herr, and M. Chandrashekar (2006), "Debiasing Omission Neglect," *Journal of Business Research*, 59 (6), 786-92.
- Kardes, Frank R., Steven S. Posavac, Maria L. Cronley, and Paul M. Herr (2008), "Consumer Inference," in *The Handbook of Consumer Psychology*, ed. Curtis P. Haugtvedt, Paul M. Herr and Frank R. Kardes, *Mahwah, NJ: Lawrence Erlbaum Associates*, 165-92.
- Kelley, C. M. and D. S. Lindsay (1993), "Remembering Mistaken for Knowing - Ease of Retrieval as a Basis for Confidence in Answers to General Knowledge Questions," *Journal of Memory and Language*, 32 (1), 1-24.
- Kim, Byung Cho and Yong Wan Park (2012), "Security Versus Convenience? An Experimental Study of User Misperceptions of Wireless Internet Service Quality," *Decision Support Systems*, 53 (1), 1-11.
- Labroo, A. A., R. Dhar, and N. Schwarz (2008), "Of Frog Wines and Frowning Watches: Semantic Priming, Perceptual Fluency, and Brand Evaluation," *Journal of Consumer Research*, 34 (6), 819-31.
- Labroo, A. A. and S. Kim (2009), "The "Instrumentality" Heuristic: Why Metacognitive Difficulty Is Desirable During Goal Pursuit," *Psychological Science*, 20 (1), 127-34.
- Labroo, A. A. and A. Y. Lee (2006), "Between Two Brands: A Goal Fluency Account of Brand Evaluation," *Journal of Marketing Research*, 43 (3), 374-85.
- Lee, A. Y. and A. A. Labroo (2004), "The Effect of Conceptual and Perceptual Fluency on Brand Evaluation," *Journal of Marketing Research*, 41 (2), 151-65.
- Menon, G. and P. Raghuram (2003), "Ease-of-Retrieval as an Automatic Input in Judgments: A Mere-Accessibility Framework?," *Journal of Consumer Research*, 30 (2), 230-43.
- Moreau, C. P., A. B. Markman, and D. R. Lehmann (2001), "'What Is It?' Categorization Flexibility and Consumers' Responses to Really New Products," *Journal of Consumer Research*, 27 (4), 489-98.
- Nielsen, J. H. and J. E. Escalas (2010), "Easier Is Not Always Better: The Moderating Role of Processing Type on Preference Fluency," *Journal of Consumer Psychology*, 20 (3), 295-305.
- Novemsky, N., R. Dhar, N. Schwarz, and T. Simonson (2007), "Preference Fluency in Choice," *Journal of Marketing Research*, 44 (3), 347-56.
- Nowlis, Stephen M. and Itamar Simonson (1997), "Attribute-Task Compatibility as a Determinant of Consumer Preference Reversals," *Journal of Marketing Research*, 34 (2), 205-18.

Oppenheimer, DANIEL M. (2006), "Consequences of Erudite Vernacular Utilized Irrespective of Necessity: Problems with Using Long Words Needlessly," *APPLIED COGNITIVE PSYCHOLOGY*, 20, 139-56.

Oppenheimer, Daniel M. and Michael C. Frank (2008), "A Rose in Any Other Font Would Not Smell as Sweet: effects of Perceptual Fluency on Categorization " *Cognition*, 106, 1178-94.

Parker, Donn B. (1998), *Fighting Computer Crime: A New Framework for Protecting Information*, USA: Wiley Computer Publishing.

Pocheptsova, A., A. A. Labroo, and R. Dhar (2010), "Making Products Feel Special: When Metacognitive Difficulty Enhances Evaluation," *Journal of Marketing Research*, 47 (6), 1059-69.

Posthumus, S. and R. von Solms (2004), "A Framework for the Governance of Information Security," *Computers & Security*, 23 (8), 638-46.

Rao, A. R. and K. B. Monroe (1988), "The Moderating Effect of Prior Knowledge on Cue Utilization in Product Evaluations," *Journal of Consumer Research*, 15 (2), 253-64.

--- (1989), "The Effect of Price, Brand Name, and Store Name on Buyers Perceptions of Product Quality - an Integrative Review," *Journal of Marketing Research*, 26 (3), 351-57.

Reber, R. and N. Schwarz (1999), "Effects of Perceptual Fluency on Judgments of Truth," *Consciousness and Cognition*, 8 (3), 338-42.

Rhodes, G., J. Halberstadt, and G. Brajkovich (2001), "Generalization of Mere Exposure Effects to Averaged Composite Faces," *Social Cognition*, 19 (1), 57-70.

Rhodes, M. G. and A. D. Castel (2008), "Memory Predictions Are Influenced by Perceptual Information: Evidence for Metacognitive Illusions," *Journal of Experimental Psychology-General*, 137 (4), 615-25.

Salisbury, W. David, Rodney A. Pearson, Allison W. Pearson, and David W. Miller (2001), "Perceived Security and World Wide Web Purchase Intention," *Industrial Management & Data Systems*, 101 (4), 165-77.

Sanbonmatsu, D. M., F. R. Kardes, and P. M. Herr (1992), "The Role of Prior Knowledge and Missing Information in Multiattribute Evaluation," *Organizational Behavior and Human Decision Processes*, 51 (1), 76-91.

Sanbonmatsu, D. M., F. R. Kardes, D. C. Houghton, E. A. Ho, and S. S. Posavac (2003), "Overestimating the Importance of the Given Information in Multiattribute Consumer Judgment," *Journal of Consumer Psychology*, 13 (3), 289-300.

Sanbonmatsu, D. M., F. R. Kardes, S. S. Posavac, and D. C. Houghton (1997), "Contextual Influences on Judgment Based on Limited Information," *Organizational Behavior and Human Decision Processes*, 69 (3), 251-64.

Schwarz, N. (2004), "Metacognitive Experiences in Consumer Judgment and Decision Making," *Journal of Consumer Psychology*, 14 (4), 332-48.

Schwarz, Norbert (1998), "Accessible Content and Accessibility Experiences: The interplay of Declarative and Experiential Information in Judgment " *Personality and Social Psychology Review* 2, 87-99.

Shneiderman, B. (2000), "Designing Trust into Online Experiences," *Communications of the Acm*, 43 (12), 57-59.

Silvera, D. H., F. R. Kardes, N. Harvey, M. L. Cronley, and D. C. Houghton (2005), "Contextual Influences on Omission Neglect in the Fault Tree Paradigm," *Journal of Consumer Psychology*, 15 (2), 117-26.

Simonson, Itamar (2008), "Will I Like a "Medium" Pillow? Another Look at Constructed and Inherent Preferences " *Journal of Consumer Psychology*, 18, 155-69.

Simonson, Itamar, Ziv Carmon, Ravi Dhar, Aimee Drolet , and Stephen M. Nowlis (2001), "Consumer Research: In Search of Identity," *Annual Review of Psychology*, 52, 249-75.

Song, H. J. and N. Schwarz (2008), "If It's Hard to Read, It's Hard to Do: Processing Fluency Affects Effort Prediction and Motivation," *Psychological Science*, 19 (10), 986-88.

Sujan, M. (1985), "Consumer Knowledge - Effects on Evaluation Strategies Mediating Consumer Judgments," *Journal of Consumer Research*, 12 (1), 31-46.

Sujan, M. and C. Dekleva (1987), "Product Categorization and Inference Making - Some Implications for Comparative Advertising," *Journal of Consumer Research*, 14 (3), 372-78.

Tamir, Maya, Micheal D. Robinson, Gerald L. Clore, Leonard L. Martin, and Daniel J. Whitaker (2004), "Are We Puppets on a String? The Contextual Meaning of Unconscious Expressive Cues," *Personality and social psychology Bulletin*, 30, **237-49**.

Thomas, M. and V. G. Morwitz (2009), "The Ease-of-Computation Effect: The Interplay of Metacognitive Experiences and Naive Theories in Judgments of Price Differences," *Journal of Marketing Research*, 46 (1), 81-91.

Thompson, Debora Viana and Elise Chandon (2013), "When Disfluency Signals Competence: The Effect of Processing Difficulty on Perceptions of Service Agents," *Journal of Marketing Research*.

Topolinski, Sascha and Fritz Strack (2010), "False Fame Prevented: Avoiding Fluency Effects without Judgmental Correction," *Journal of Personality and Social Psychology*, 98 (5), 721-33.

Tormala, Z. L., C. Falces, P. Brinol, and R. E. Petty (2007), "Ease of Retrieval Effects in Social Judgment: The Role of Unrequested Cognitions," *Journal of Personality and Social Psychology*, 93 (2), 143-57.

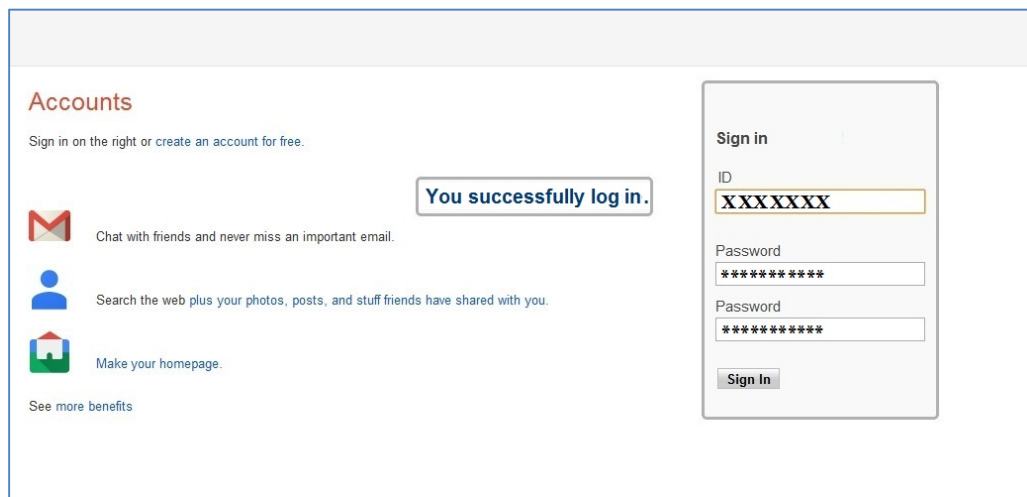
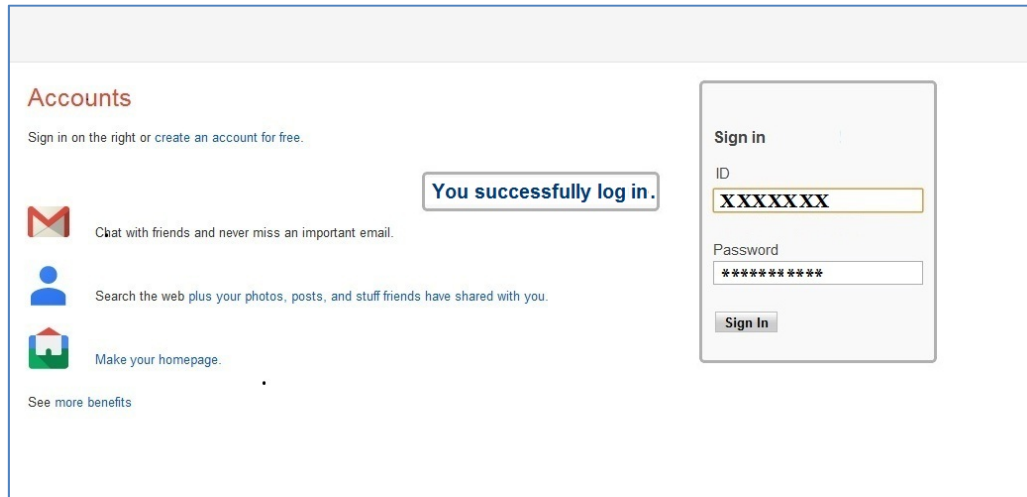
Tybout, A. M., B. Sternthal, P. Malaviya, G. A. Bakamitsos, and S. B. Park (2005), "Information Accessibility as a Moderator of Judgments: The Role of Content Versus Retrieval Ease," *Journal of Consumer Research*, 32 (1), 76-85.

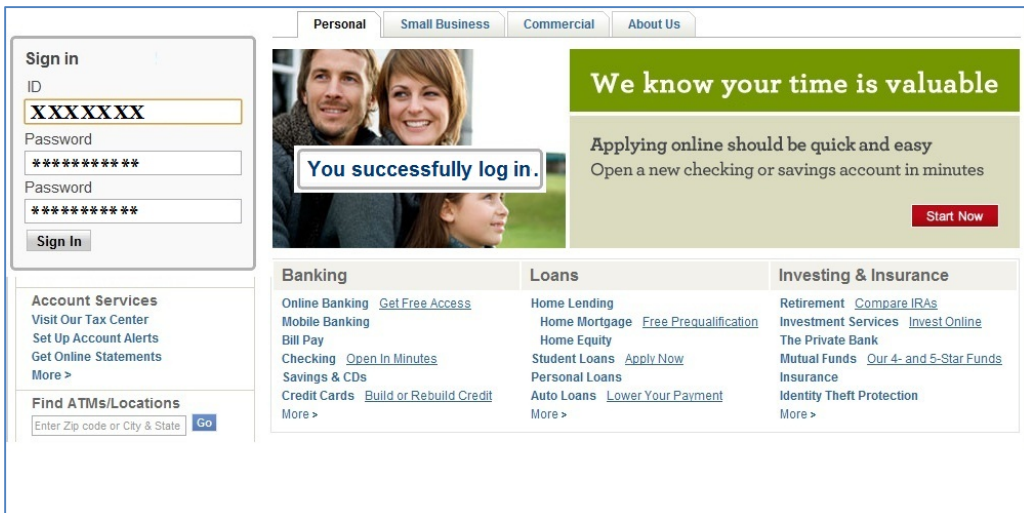
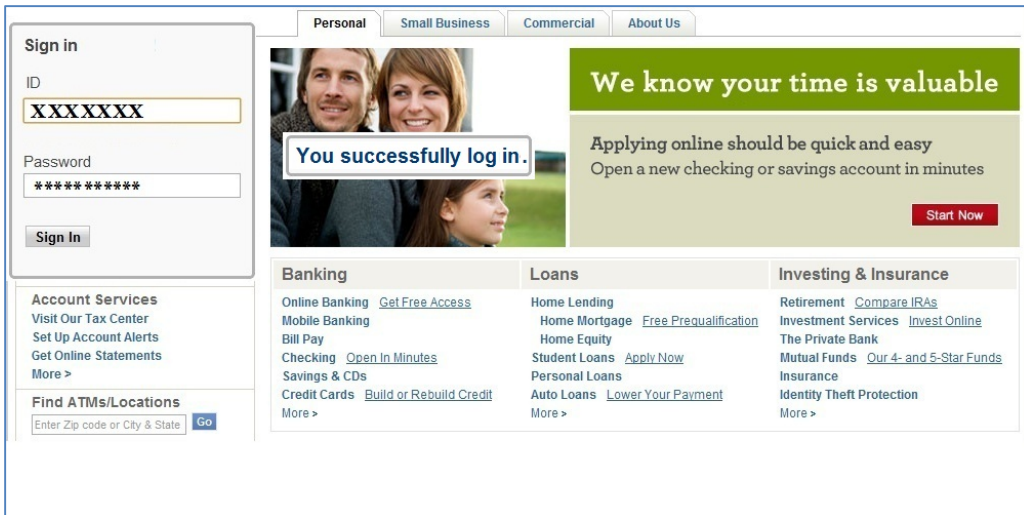
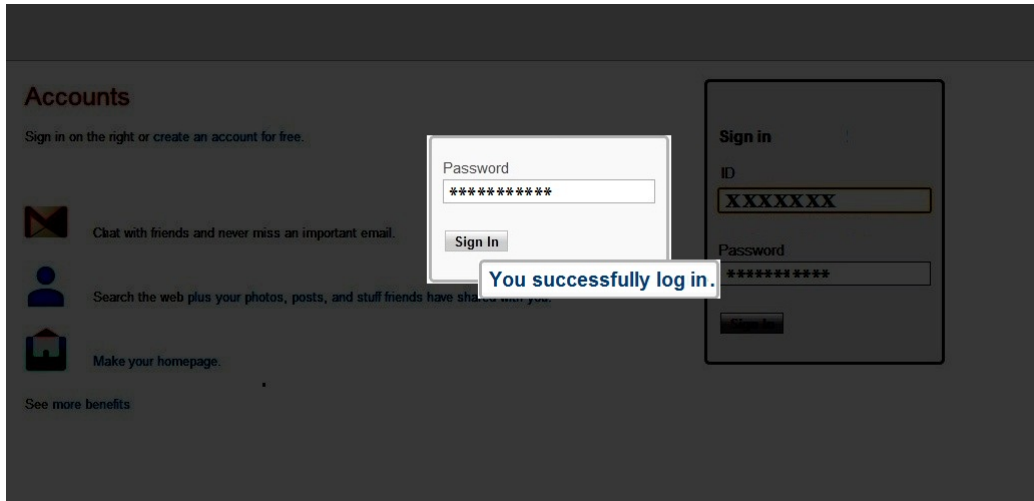
Ulkumen, G., M. Thomas, and V. G. Morwitz (2008), "Will I Spend More in 12 Months or a Year? The Effect of Ease of Estimation and Confidence on Budget Estimates," *Journal of Consumer Research*, 35 (2), 245-56.

- Unkelbach, C. (2006), "The Learned Interpretation of Cognitive Fluency," *Psychological Science*, 17 (4), 339-45.
- Vanhouche, Wouter and Stijn M. J. van Osselaer (2009), "The Accuracy-Enhancing Effect Of biasing Cues " *Journal of Consumer Research*, 36 (2), 317-27.
- Wanke, M., G. Bohner, and A. Jurkowitsch (1997), "There Are Many Reasons to Drive a Bmw: Does Imagined Ease of Argument Generation Influence Attitudes?," *Journal of Consumer Research*, 24 (2), 170-77.
- Winkielman, P. and J. T. Cacioppo (2001), "Mind at Ease Puts a Smile on the Face: Psychophysiological Evidence That Processing Facilitation Elicits Positive Affect," *Journal of Personality and Social Psychology*, 81 (6), 989-1000.
- Winkielman, P., J. Halberstadt, T. Fazendeiro, and S. Catty (2006), "Prototypes Are Attractive Because They Are Easy on the Mind," *Psychological Science*, 17 (9), 799-806.
- Winkielman, P. and N. Schwarz (2001), "How Pleasant Was Your Childhood? Beliefs About Memory Shape Inferences from Experienced Difficulty of Recall," *Psychological Science*, 12 (2), 176-79.
- Wood, S. L. and J. G. Lynch (2002), "Prior Knowledge and Complacency in New Product Learning," *Journal of Consumer Research*, 29 (3), 416-26.

# V Appendixes

## Appendix A. Stimuli in Experiment 1-1





Personal Small Business Commercial About Us

**Sign in**

ID  
XXXXXXX

Password  
\*\*\*\*\*

**You successfully log in.**

**We know your time is valuable**

online should be quick and easy  
w checking or savings account in minutes

**Account Services**  
Visit Our Tax Center  
Set Up Account Alerts  
Get Online Statements  
More >

**Find ATMs/Locations**  
Enter Zip code or City & State

**Banking**  
Online Banking [Get Free Access](#)  
Mobile Banking  
Bill Pay  
Checking [Open in Minutes](#)  
Savings & CDs  
Credit Cards [Build or Rebuild Credit](#)  
More >

**Loans**  
Home Lending  
Home Mortgage [Free Prequalification](#)  
Home Equity  
Student Loans [Apply Now](#)  
Personal Loans  
Auto Loans [Lower Your Payment](#)  
More >

**Investing & Insurance**  
Retirement [Compare IRAs](#)  
Investment Services [Invest Online](#)  
The Private Bank  
Mutual Funds [Our 4- and 5-Star Funds](#)  
Insurance  
Identity Theft Protection  
More >

## Appendix B. Objective Security Knowledge Measures

1. As information security increases, performance decreases.

True / False

2. A properly configured firewall will provide complete information security from external attacks.

True / False

3. A user ID and password prevents unfriendly network connections.

True / False

4. Encryption should be considered for internal network traffic as well as external network traffic.

True / False

5. A fully patched computer is safe from a hacker.

True / False

6. What does DDoS stand for?

Dangerous DOS open Security / Digital Default of Servers / **Distributed Denial of Service**

7. Which kind of malware typically resides in a larger, innocent computer program?

Worm / **Computer virus** / Trojan horse

8. \_\_\_\_\_ will scan your system and let you know not only what patches you may be missing, but also other security issues like accounts with no passwords or having the Guest account enabled

Scandisk / Defrag / **MBSA** / Disk Cleanup

9. Most antivirus software also has the ability to perform \_\_\_\_\_ scanning which uses known signs or patterns of malware to try and detect viruses or worms that aren't yet known and for which your software doesn't have a signature to match it against.

Proactive / **Heuristic** / Predictive / Holistic

10. A(n) \_\_\_\_\_ application monitors all incoming and outgoing network traffic and blocks unauthorized packets from getting through

Antivirus / Intrusion Detection System (IDS) / **Personal Firewall** / Network Monitor

## **Appendix C. Measures for C-I-A Triad**

### Confidentiality

I think this website has mechanisms to ensure the safe transmission of its users' information

I think this website shows great concern for the security of any transactions

I believe this website will not expose the information I provide during my transaction to inappropriate parties

I believe inappropriate parties may deliberately view the information I provide during my activity in this website ®

### Integrity

When I send data to this website, I am sure that they will not be intercepted by unauthorized third parties

I think this website has sufficient technical capacity to ensure that the data I send will not be intercepted or modified by a third party

I am confident that the private information I provide during my activity in this website will only reach this store.

# The ○○○○ Times

Wednesday, October 24, 2012 Last Update: 10:38 AM ET

## Disney buys Lucasfilm for \$4 billion



Luke Skywalker and Han Solo are joining Mickey Mouse, Buzz Lightyear and Iron Man in Disney's roster of heroes.

Disney is buying Lucasfilm for \$4 billion, adding the legendary *Star Wars* franchise to the entertainment giant's stable of characters. Lucasfilm is 100% owned by founder George Lucas. The purchase culminates a one and a half

year pursuit of the Lucas empire, Disney's CEO said. Lucas, who receives 40 million Disney shares from the deal, will be the second-largest non-institutional shareholder of Disney, Bloomberg News says, behind the trust of deceased Apple co-founder Steve Jobs.

The 68-year-old Lucas will serve as a creative consultant but plans to retire. "For the past 35 years, one of my greatest pleasures has been to see *Star Wars* passed from one generation to the next," said Lucas, chairman and CEO of Lucasfilm, in a statement. "It's now time for me to pass *Star Wars* on to a new generation of filmmakers."

Said Disney CEO Robert Iger: "This is one of the great entertainment properties of all time, one of the best branded and one of the most valuable, and it's just fantastic for us to have the opportunity to both buy it, run it and grow it." (continues to page 2)

## Move to the Cloud in the Least Expensive iPad Mini



Now that the Apple iPad Mini is here, I'm fielding one particular

question from friends, family and readers: Which model should I buy? This could be a potentially expensive decision. The iPad Mini starts at \$330 for the 16-gigabyte Wi-Fi version and goes all the way to a high-altitude \$670 for the 64-gigabyte version with 3G data.

So what do all the extra Benjamin Franklins get you? Not much, really. Each rung higher on the iPad Mini ladder will cost you \$100 for a slight memory increase. It's obvious that Apple is making hefty margins from these upgrades. (continues to page 3)

## Review: 2013 Audi Allroad steers toward active yuppies



The Allroad, a rugged cousin of Audi's A4 station wagon, blends style and smooth driving. It will appeal to outdoorsy yuppies, or those

projecting such an image.

If anecdotal evidence gleaned from trips through L.A.'s moneyed coastal enclaves like Malibu, Pacific Palisades and Manhattan Beach is any indication, there's a new automotive trend for the outdoorsy yuppie. It's a station wagon.

Too culturally sensitive to be caught in an SUV, yet ever mindful of the curbside erratum that is the minivan, those with an active lifestyle or projection thereof clearly seem to be finding solace in the 2013 Audi Allroad. (Continue to page 5)

## Researcher says 100,000 passwords exposed on IEEE site

A computer scientist says he discovered that a server of the IEEE (Institute of Electrical and Electronics Engineers) had about 100,000 usernames and passwords stored in plaintext and publicly accessible.

The data was publicly available on the IEEE FTP (File Transfer Protocol) server for at least a month, potentially exposing usernames and passwords of people who work at Apple, Google, IBM, Oracle, Samsung, NASA, Stanford, and other organizations and firms, he said. The glitch exposed all the actions the users performed on the ieee.org site, as well as spectrum.ieee.org, he added.

The IEEE provided CNET with a statement late this afternoon. "IEEE has become aware of an incident regarding inadvertent access to unencrypted log files containing user IDs and passwords. We have conducted a thorough investigation and the issue has been addressed and resolved. We are in the process of notifying those who may have been affected," the organization said. "IEEE takes safeguarding the private information of our members and customers very seriously. We regret the occurrence of this incident and any inconvenience it may have caused." (Continues to page 3)

# The ○○○○ Times

Wednesday, October 24, 2012 Last Update: 10:38 AM ET

## Disney buys Lucasfilm for \$4 billion



Luke Skywalker and Han Solo are joining Mickey Mouse, Buzz Lightyear and Iron Man in Disney's roster of heroes.

Disney is buying Lucasfilm for \$4 billion, adding the legendary *Star Wars* franchise to the entertainment giant's stable of characters. Lucasfilm is 100% owned by founder George Lucas. The purchase culminates a one and a half

year pursuit of the Lucas empire, Disney's CEO said. Lucas, who receives 40 million Disney shares from the deal, will be the second-largest non-institutional shareholder of Disney, Bloomberg News says, behind the trust of deceased Apple co-founder Steve Jobs.

The 68-year-old Lucas will serve as a creative consultant but plans to retire. "For the past 35 years, one of my greatest pleasures has been to see *Star Wars* passed from one generation to the next," said Lucas, chairman and CEO of Lucasfilm, in a statement. "It's now time for me to pass *Star Wars* on to a new generation of filmmakers."

Said Disney CEO Robert Iger: "This is one of the great entertainment properties of all time, one of the best branded and one of the most valuable, and it's just fantastic for us to have the opportunity to both buy it, run it and grow it." (continues to page 2)

## Move to the Cloud in the Least Expensive iPad Mini



Now that the Apple iPad Mini is here, I'm fielding one particular

question from friends, family and readers: Which model should I buy? This could be a potentially expensive decision. The iPad Mini starts at \$330 for the 16-gigabyte Wi-Fi version and goes all the way to a high-altitude \$670 for the 64-gigabyte version with 3G data.

So what do all the extra Benjamin Franklins get you? Not much, really. Each rung higher on the iPad Mini ladder will cost you \$100 for a slight memory increase. It's obvious that Apple is making hefty margins from these upgrades. (continues to page 3)

## Review: 2013 Audi Allroad steers toward active yuppies



The Allroad, a rugged cousin of Audi's A4 station wagon, blends style and smooth driving. It will appeal to outdoorsy yuppies, or those

projecting such an image.

If anecdotal evidence gleaned from trips through L.A.'s moneyed coastal enclaves like Malibu, Pacific Palisades and Manhattan Beach is any indication, there's a new automotive trend for the outdoorsy yuppie. It's a station wagon.

Too culturally sensitive to be caught in an SUV, yet ever mindful of the curbside erratum that is the minivan, those with an active lifestyle or projection thereof clearly seem to be finding solace in the 2013 Audi Allroad. (Continue to page 5)

## Finding Zen in a Patch of Nature



SEWANEE, Tenn. — It is afternoon in a hardwood forest on the edge of the Cumberland Plateau, and the cicadas are singing. David Haskell, an ecologist and evolutionary biologist at the University of the South, is taking me through part of the 13,000 acres owned by the university, to a small circle of

forest floor a bit over a yard in diameter. He visited this randomly chosen forest "mandala," as he calls it, many times over the course of a year and recorded his observations in "The Forest Unseen: A Year's Watch in Nature."

He is pointing out flowers, salamanders, insects, trees, as we follow a well-worn hiking path, and stops for a moment to listen. These are swamp cicadas, he says, not the kind that hatch all at once after years underground and hammer the ear mercilessly.

"Was it last year or the year before we had the 13-year cicadas?" he says. "I took my sound pressure meter down to a place where they were really loud, and it came to over 90 decibels. At 85 OSHA says you need hearing protection in your workplace.

"Everybody else hates them." (Continues to page 3)

## Online Armor Premium



If you use online banking, buy things online, send and receive emails or just browse the internet then you're open to serious threats that your Antivirus Software just wasn't designed to stop. That's where Online Armor's Personal Firewall comes in.

Online Armor's new personal firewall provides awesome protection from inbound threats and complete control of data leaving your computer for the internet.

Never worry about banking online again. An online banking safety feature called "Banking Mode" blocks users from being able to fall for scams to divert them to phishing sites. **In "Banking Mode," the firewall will only permit connections to safe websites.**

Probably the number one threat online; identity theft ruins lives. Online Armor protects you from phishing and keylogging techniques that these criminals use. **Only trust applications can send out information to outside from your computer.**

Malicious programs are getting tougher and tougher and often attack other programs (including security programs) to do their nasty deeds. Online Armor's Program Guard guards not only itself against tampering, but protection other programs from malicious code.

Online Armor protects your passwords and private information from being stolen by blocking the keylogger as it tries to activate. Online Armor's behavior detection ensures that even specially created or new keyloggers are detected and prevented.

## Online Armor Premium



**If you use online banking, buy things online, send and receive emails or just browse the internet then you're open to serious threats that your Antivirus Software just wasn't designed to stop. That's where Online Armor's Personal Firewall comes in.**

Online Armor's new personal firewall provides awesome protection from inbound threats and complete control of data leaving your computer for the internet.

Never worry about banking online again. An online banking safety feature called "Banking Mode" blocks users from being able to fall for scams to divert them to phishing sites. **After a user opens Online Amor and activates "Banking Mode," the firewall will only permit connections to websites that you register on safe site list.**

Probably the number one threat online; identity theft ruins lives. Online Armor protects you from phishing and keylogging techniques that these criminals use. **By registering trust applications on the safe list, a user prevents malicious hidden application sending out information to hackers.**

Malicious programs are getting tougher and tougher and often attack other programs (including security programs) to do their nasty deeds. Online Armor's Program Guard guards not only itself against tampering, but protection other programs from malicious code. Also, **pop-ups will warn a user if suspicious attempts may happen.**

Online Armor protects your passwords and private information from being stolen by blocking the keylogger as it tries to activate. Online Armor's behavior detection ensures that even specially created or new keyloggers are detected and prevented.

## Appendix F. Stimuli for Experiment 2-1

Convenience-Oriented Description printed in easy-to-read font (Arial)

Our data backup software provides professional grade backup and recovery. It provides easy recovery of your data files, or your entire hard drive or a mapped drive to a previous backup image. Moreover, it allows you to quickly restore your system without needing a bootable CD. You can backup and recover your files from any type of devices such as a CD, DVD, Blue-ray disc, external drive, or network-attached storage device. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system.↵

Convenience-Oriented Description printed in difficult-to-read font (Mistral)

*Our data backup software provides professional grade backup and recovery. It provides easy recovery of your data files, or your entire hard drive or a mapped drive to a previous backup image. Moreover, it allows you to quickly restore your system without needing a bootable CD. You can backup and recover your files from any type of devices such as a CD, DVD, Blue-ray disc, external drive, or network-attached storage device. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system.↵*

Security-Oriented Description printed in easy-to-read font (Arial)

Our data backup software provides professional grade backup and recovery. It safeguards your photos, videos, and other files, and takes periodic snapshots of your entire computer hard drive to be able to completely restore your computer system to a specific backup version in the case of hard drive failure. It compresses and encrypts your backups, and our advanced encryption helps keep sensitive data safe from prying eyes. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system.

Security-Oriented Description printed in difficult-to-read font (Mistral)

*Our data backup software provides professional grade backup and recovery. It safeguards your photos, videos, and other files, and takes periodic snapshots of your entire computer hard drive to be able to completely restore your computer system to a specific backup version in the case of hard drive failure. It compresses and encrypts your backups, and our advanced encryption helps keep sensitive data safe from prying eyes. Also, it automatically backs up when online threats raise an increased need to save the latest version of your system.*

**Appendix G. Raw Data Set**

**Raw Data of Experiment 1-1(A)**

No	product	Condition	good	favor	like	time1	easy	convenient	complex	Time2	secure	safe	protect	Time3	confident	familiar	expertise	knowledgeable	interest	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10
1	Bank	single	7	7	7	20.608	7	7	1	13.728	6	6	6	36.863	7	5	5	5	6	2	2	1	1	2	2	3	3	4	1
2	Bank	single	4	4	3	1.952	5	4	4	8.49	3	3	3	19.348	5	6	6	6	7	2	1	1	1	1	3	2	3	4	3
3	Bank	single	5	5	5	26.953	7	6	2	13.787	7	7	7	9.839	6	7	6	6	7	2	1	2	1	2	3	3	3	1	3
4	Bank	single	7	6	7	80.763	6	7	2	383.333	7	7	7	62.358	5	6	6	6	7	2	1	1	1	2	3	2	1	3	3
5	Bank	single	7	7	7	162.365	7	7	1	14.104	7	7	7	94.874	7	7	7	7	7	2	1	1	1	1	2	3	4	1	4
6	Bank	single	5	5	4	77.356	5	5	2	9.998	5	4	5	18.831	2	6	5	5	6	1	2	1	1	2	3	3	3	3	1
7	Bank	single	5	4	6	56.3	6	5	2	25.105	3	4	3	20.977	6	7	6	7	6	2	2	1	1	2	3	3	3	2	3
8	Bank	single	5	5	5	24.22	5	5	3	11.122	6	5	5	13.417	6	5	4	5	5	2	2	2	1	2	3	3	1	4	1
9	Bank	single	6	6	7	17.421	5	5	4	7.396	5	5	6	6.714	6	5	5	5	6	2	1	1	1	2	1	1	3	1	3
10	Bank	single	5	5	5	10.606	6	6	3	6.748	5	5	5	5.53	6	7	7	7	7	2	2	2	1	2	3	1	3	2	3
11	Bank	single	3	2	4	36.195	3	4	1	17.398	1	2	1	23.772	5	7	6	6	7	1	1	2	1	2	3	3	3	2	3
12	Bank	single	4	5	5	18.911	5	6	4	9.137	4	4	5	9.636	5	7	7	6	6	2	1	2	1	2	3	1	1	2	2
13	Bank	single	5	5	6	28.831	7	7	6	19.049	5	4	5	17.912	5	5	5	5	7	2	1	1	1	1	3	2	3	1	3
14	Bank	single	5	5	5		6	7	2	9.145	6	5	5	10.88	6	7	6	6	5	2	2	1	1	2	3	1	3	3	4
15	Bank	single	6	6	7	8.317	7	6	2	17.151	6	5	3	11.094	5	6	6	5	7	2	1	1	1	1	2	2	1	1	3
16	Bank	single	2	2	2	23.216	3	3	1	18.116	1	1	1	7.14	5	7	7	7	7	1	1	2	2	1	3	3	3	2	3
17	Bank	single	5	5	4	10.354	4	5	3	29.801	5	5	5	4.664	5	5	5	5	5	2	2	2	1	2	2	3	1	1	3
18	Bank	single	7	7	7	27.466	7	7	1	14.018	5	5	4	18.252	7	7	7	7	7	1	1	2	1	2	2	2	4	4	3
19	Bank	single	5	5	5	29.096	6	6	3	11.02	5	5	5	13.231	5	7	6	6	6	1	2	2	1	2	3	2	3	2	3

20	Bank	single	7	7	7	14.855	7	7	1	8.77	7	7	7	4.793	4	6	5	5	7	2	1	2	1	2	3	3	1	2	4
21	Bank	single	5	4	6	56.31	5	6	3	20.18	4	5	5	20.349	2	7	6	7	7	1	2	1	2	2	3	3	3	3	4
22	Bank	single	6	7	7	58.753	6	7	4	11.555	7	6	6	8.573	7	5	4	5	6	2	2	2	1	2	1	2	3	3	2
23	Bank	single	6	5	5	24.061	7	7	1	8.362	4	4	4	9.733	1	7	3	3	5	1	2	2	1	2	3	3	1	1	4
24	Bank	single	3	3	4	24.496	6	6	3	13.178	2	2	2	8.099	5	6	5	5	7	2	2	2	1	2	2	2	1	3	2
25	Bank	single	7	6	6	32.312	6	6	2	10.926	3	4	3	15.947	2	6	5	5	5	2	2	2	1	2	3	1	1	3	3
26	Bank	single	5	5	5	18.233	6	5	3	12.188	4	4	4	11.724	4	6	6	6	6	2	2	2	1	2	3	3	3	3	3
27	Bank	single	5	5	5	15.699	6	5	3	11.669	5	5	5	6.259	6	7	6	6	6	2	1	2	1	2	3	3	1	3	3
28	Bank	single	7	7	7	45.647	7	7	1	35.396	6	6	6	21.511	6	7	7	7	7	2	2	2	1	2	3	3	3	1	4
29	Bank	single	5	5	5	29.457	5	6	4	8.688	6	6	5	8.078	5	4	4	4	5	2	1	1	1	2	2	2	4	3	2
30	Bank	Twice	6	5	6	48.15	6	7	1	7.139	6	6	6	9.351	6	6	5	5	6	2	1	1	1	2	3	3	1	2	1
31	Bank	Twice	5	5	5	17.905	5	5	6	13.263	5	5	5	8.311	6	7	7	7	7	2	1	1	1	1	3	3	1	3	1
32	Bank	Twice	6	6	6		6	6	2	16.21	6	6	6	15.357	5	7	6	6	6	2	1	1	1	2	2	3	3	3	2
33	Bank	Twice	4	4	3	14.891	5	6	2	7.072	3	3	2	8.98	3	7	7	7	7	2	1	1	1	1	3	2	3	1	3
34	Bank	Twice	6	7	6	51.177	6	7	2	17.488	5	6	5	18.271	6	7	7	7	7	1	1	1	1	1	3	2	1	1	1
35	Bank	Twice	6	7	5	37.8	5	6	3	23.392	6	4	5	12.327	5	7	6	7	7	2	1	1	2	2	3	2	1	2	4
36	Bank	Twice	6	7	7	52.045	7	6	1	12.449	6	6	7	8.873	6	7	6	7	7	2	1	2	1	1	3	1	1	3	2
37	Bank	Twice	7	7	7	4.346	7	7	1	12.648	5	6	5	9.065	2	7	7	7	7	2	2	2	1	2	3	1	3	3	3
38	Bank	Twice	2	2	2	26.386	3	2	6	16.43	4	4	4	22.375	5	7	6	6	7	2	1	1	1	1	3	3	3	3	4
39	Bank	Twice	6	6	5	15.031	6	6	2	7.609	5	6	5	7.513	6	6	5	5	6	2	1	1	1	1	2	3	1	1	4
40	Bank	Twice	5	5	5	139.838	6	6	2	10.248	6	6	6	54.448	3	7	7	7	7	1	2	2	1	2	3	2	3	2	3
41	Bank	Twice	5	5	5	37.842	6	6	3	30.359	6	6	6	13.709	5	7	6	6	6	1	1	1	1	2	3	3	3	2	3
42	Bank	Twice	6	6	6	18.618	5	5	5	5.909	3	4	3	7.73	7	6	5	5	5	2	2	1	1	2	3	3	1	2	3
43	Bank	Twice	3	3	3	0	7	6	1	0	2	2	3	0	3	4	3	3	4	1	1	1	1	1	3	2	3	1	3

44	Bank	Twice	5	4	4	18.898	2	2	5	10.428	7	7	7	11.23	6	6	6	7	6	1	1	2	1	2	3	2	1	3	4	
45	Bank	Twice	7	7	7		7	6	7	13.064	7	7	7	7.827	7	7	7	7	7	1	1	1	1	1	2	2	1	2	2	
46	Bank	Twice	5	5	5	21.826	7	6	1	9.905	5	5	5	12.279	3	7	7	7	7	1	2	2	1	2	3	3	3	3	3	
47	Bank	Twice	4	3	3	39.882	6	5	2	12.884	5	4	4	12.404	5	7	6	6	7	1	2	1	1	2	3	2	4	1	3	
48	Bank	Twice	5	4	5	24.885	7	6	5	24.606	5	6	5	7.66	6	7	7	7	7	2	2	1	1	2	3	3	3	2	3	
49	Bank	Twice	7	7	7	19.022	7	7	4	55.313	6	5	4	19.171	5	6	5	5	6	2	2	1	1	1	2	2	1	1	3	
50	Bank	Twice	5	4	4	37.493	7	7	1	9.585	5	5	5	10.318	4	4	2	2	2	2	2	2	2	1	2	2	1	1	1	3
51	Bank	Twice	4	3	3	26.156	3	3	5	11.851	6	6	6	11.075	5	7	7	7	7	1	2	2	1	2	3	3	1	2	4	
52	Bank	Twice	5	5	5	30.991	5	5	2	10.463	5	5	5	30.556	4	7	6	6	6	2	2	1	1	2	3	3	3	4	3	
53	Bank	Twice	4	4	4	22.154	4	3	4	17.646	5	5	5	12.721	5	4	4	4	5	1	2	2	1	2	1	3	3	1	3	
54	Bank	Twice	6	5	6	63.969	7	7	4	22.671	6	5	6	21.838	5	6	5	5	7	1	2	1	1	2	3	3	1	3	1	
55	Bank	Twice	7	7	7	27.428	4	4	5	11.851	7	7	7	7.554	7	5	5	5	6	1	2	1	2	2	3	1	3	3	3	
56	Bank	popup	7	7	7	19.146	7	7	7	6.119	7	7	7	6.904	7	7	7	7	7	1	1	1	1	1	1	3	4	3	3	
57	Bank	popup	5	5	5	202.689	6	6	6	11.688	6	6	6	3.621	7	7	7	7	7	1	1	1	1	2	3	1	3	2	2	
58	Bank	popup	7	7	6		6	7	6	4.774	6	7	7	3.613	6	7	7	7	7	1	1	1	1	1	3	1	4	2	3	
59	Bank	popup	6	5	5	32.23	5	5	2	14.929	6	4	5	15.603	5	7	6	6	7	2	1	1	1	2	3	3	3	2	3	
60	Bank	popup	6	6	6	132.227	5	6	5	25.364	6	7	6	20.153	5	6	5	6	6	1	1	1	1	2	3	2	1	4	1	
61	Bank	popup	6	6	6	50.587	6	6	6	11.724	6	6	6	7.988	6	6	4	6	6	2	1	1	1	1	1	3	1	3	3	
62	Bank	popup	5	6	6	36.346	5	4	4	2168.94	5	6	6	51.364	6	4	5	5	5	2	2	1	1	1	2	2	3	1	3	
63	Bank	popup	5	6	4	7.029	4	3	4	4.298	4	3	3	3.387	4	4	4	3	4	2	2	1	2	2	2	2	2	3	3	
64	Bank	popup	6	6	6	29.916	7	7	2	8.435	6	6	6	7.164	4	6	5	5	4	2	2	2	1	2	2	3	2	1	3	
65	Bank	popup	3	2	2		5	4	2	21.832	2	1	2	15.538	6	7	6	7	7	2	1	1	1	1	3	2	3	1	3	
66	Bank	popup	7	7	7	6.843	7	6	7	5.686	7	7	7	9.633	7	7	7	7	7	1	1	1	1	1	2	2	3	3	3	
67	Bank	popup	6	6	6	30.674	6	6	3	9.722	5	6	6	7.632	2	6	6	6	7	2	2	1	1	2	3	3	3	2	3	

68	Bank	popup	4	4	3	44.76	6	5	2	13.797	4	4	4	14.715	3	7	5	7	7	2	2	2	1	2	3	3	3	1	3	
69	Bank	popup	4	5	4	13.84	7	5	2	6.615	4	4	4	6.943	2	3	5	4	4	1	2	1	2	2	2	3	1	3	1	
70	Bank	popup	1	1	1	50.806	3	1	6	11.58	4	4	4	8.869	4	6	6	6	6	2	2	2	1	2	3	3	3	2	3	
71	Bank	popup	5	5	5	70.937	5	6	4	11.859	5	6	6	15.187	5	4	4	4	4	1	2	1	1	2	2	1	2	1	1	
72	Bank	popup	5	6	5	45.125	6	6	3	23.337	6	6	6	9.108	7	7	7	7	7	1	2	1	1	2	3	3	3	3	3	
73	Bank	popup	6	2	6	36.576	6	5	5	8.339	4	4	4	11.261	3	4	5	3	3	2	2	1	1	1	1	1	2	1	2	1
74	Bank	popup	6	6	6	26.576	6	5	5	14.382	7	7	7	10.45	7	5	4	4	4	2	2	2	1	2	3	1	3	2	3	
75	Bank	popup	1	1	1	551.017	3	1	4	9.188	6	6	7	13.91	6	7	7	7	7	2	1	1	1	1	3	3	1	3	3	
76	Bank	popup	3	3	3	41.435	3	3	5	9.208	5	5	5	8.472	3	6	6	6	5	2	2	2	1	2	2	3	3	2	3	
77	Bank	popup	6	6	6	71.871	6	6	3	12.791	7	7	7	35.519	6	5	5	5	6	2	1	1	1	2	3	3	4	1	3	
78	Bank	popup	6	6	5	17.939	7	7	1	6.377	6	6	6	6.421	5	7	7	6	7	2	1	2	1	2	3	3	1	4	3	
79	Bank	popup	4	4	4	58.288	6	6	3	18.929	3	3	3	15.847	4	5	5	6	6	2	2	2	1	2	3	3	3	2	2	
80	Bank	popup	4	4	4	31.047	5	5	3	10.235	2	2	3	14.969	4	7	6	6	6	2	1	2	1	1	2	1	1	1	2	
81	Bank	popup	4	1	1	25.848	1	1	5	4.566	7	7	7	12.461	5	3	2	2	6	2	1	2	1	2	2	3	1	4	1	
82	Bank	popup	4	3	3	27.121	6	5	3	8.422	6	6	6	7.722	6	6	6	6	6	1	2	1	1	2	3	3	3	2	3	
83	Bank	popup	6	6	6	135.88	7	7	1	10.531	7	7	7	315.74	5	6	5	5	6	2	1	1	1	1	3	2	1	1	3	
84	Bank	popup	5	5	5	28.69	5	6	6	4.806	6	6	6	4.698	6	6	6	6	6	2	1	1	1	2	2	2	2	4	1	
85	Bank	popup	5	5	4	60.984	7	6	1	49.891	6	4	4	36.266	4	6	5	6	7	2	2	2	1	2	3	3	3	2	3	
86	email	single	6	7	6	20.095	7	7	1	7.289	4	4	4	8.247	3	7	7	7	7	2	2	2	1	2	3	3	1	3	4	
87	email	single	7	7	7	53.491	7	7	1	17.15	7	7	7	18.488	7	3	1	2	6	2	2	1	1	1	2	2	1	1	1	
88	email	single	7	6	6	41.793	6	6	1	9.912	6	5	4	6.267	6	7	6	6	6	2	1	1	1	2	3	3	1	3	1	
89	email	single	4	5	4	58.686	6	4	5	15.698	4	4	5	20.5	5	6	5	5	7	2	1	2	1	2	1	2	1	1	1	
90	email	single	6	7	7	25.794	7	7	2	8.276	7	6	6	7.47	7	7	7	7	7	2	1	1	1	1	2	2	1	3	1	
91	email	single	5	6	4	0	6	6	6	0	3	5	6	0	7	6	6	6	6	1	2	2	1	2	3	2	1	2	1	

92	email	single	4	5	5	23.929	5	7	1	15.115	3	4	5	20.792	5	6	3	6	6	1	2	1	2	1	1	3	1	1	4
93	email	single	6	2	2	19.768	6	6	3	6.788	6	6	6	6.53	5	5	5	5	7	2	2	2	1	2	3	1	1	1	2
94	email	single	6	6	6	19.746	6	6	2	6.106	6	5	6	5.942	5	6	6	5	6	1	1	1	1	2	3	1	3	3	3
95	email	single	5	5	6	34.218	5	5	6	9.266	5	5	5	8.266	6	5	5	4	6	2	2	1	1	2	2	3	1	3	3
96	email	single	5	4	4	85.666	6	6	2	16.37	4	4	5	14.97	4	7	7	7	6	2	2	2	1	2	3	3	3	3	3
97	email	single	5	7	6	24.115	6	7	4	8.667	7	7	2	7.507	7	7	7	7	7	2	2	1	1	2	3	3	3	1	3
98	email	single	3	3	3	36.902	2	2	2	8.822	1	1	1	5.457	2	3	3	3	4	2	2	2	1	2	3	3	3	2	3
99	email	single	5	4	4	32.743	6	5	3	11.359	6	5	6	13.137	6	5	6	6	5	1	1	1	2	2	2	3	1	3	3
100	email	single	7	7	7	20.579	7	7	1	7.386	4	5	5	10.877	6	6	5	6	6	2	2	1	1	1	3	3	1	2	3
101	email	single	6	6	6	37.73	6	6	2	7.794	4	4	5	8.049	3	6	3	5	7	2	2	2	1	2	3	3	3	2	3
102	email	single	6	6	5	36.021	6	6	3	42.776	6	5	6	13.68	4	6	4	4	5	1	1	1	1	1	3	2	2	2	2
103	email	single	6	6	6	29.671	6	5	3	23.022	6	6	6	21.976	6	7	6	6	7	1	2	2	1	1	3	3	3	2	3
104	email	single	6	6	5	29.833	7	7	1	6.107	4	4	4	9.483	1	5	4	4	4	2	2	2	1	2	2	1	3	1	3
105	email	single	3	3	3	104.47	3	3	5	44.908	3	3	3	21.156	5	6	6	6	6	2	2	2	1	2	3	3	1	2	4
106	email	single	5	5	6	50.328	6	5	2	20.127	4	4	4	25.894	5	6	6	6	6	1	2	2	1	2	3	3	3	1	3
107	email	single	6	5	2	11.195	6	5	6	15.04	4	5	5	5.997	5	6	7	6	7	1	1	1	2	1	2	2	3	4	3
108	email	single	7	7	7	53.403	7	7	1	13.975	4	4	4	9.896	4	5	5	5	6	1	2	1	2	2	3	1	3	3	3
109	email	single	4	4	4	36.863	5	5	4	13.114	4	4	4	7.569	5	6	5	5	6	2	1	2	1	2	2	1	4	3	3
110	email	single	7	7	7	23.535	7	7	1	12.511	7	6	6	9.692	6	5	5	5	4	2	2	2	1	2	3	2	1	3	3
111	email	twice	7	7	7	40.969	7	7	1	11.112	7	6	6	8.374	5	5	5	5	4	2	2	2	1	2	2	2	1	3	3
112	email	twice	6	6	6	57.009	7	6	1	41.619	6	6	6	15.503	4	6	5	5	5	2	2	1	1	2	2	2	1	1	3
113	email	twice	5	6	6	26.611	7	6	3	16.183	6	6	6	11.559	5	7	7	7	7	1	1	1	1	1	3	1	3	2	2
114	email	twice	4	6	4	16.346	7	4	1	41.865	6	6	4	22.474	4	4	4	4	6	2	1	1	1	1	3	2	3	2	2
115	email	twice	6	6	5	55.819	7	3	2	35.164	7	7	6	13.025	4	7	6	6	7	2	1	1	1	1	3	3	1	1	3

116	email	twice	7	6	7	28.113	7	7	7	8.979	7	7	7	7.466	7	7	7	7	7	1	1	1	1	1	1	2	1	1	2	
117	email	twice	6	7	6	53.681	6	6	1	14.605	6	6	6	25.738	6	7	6	6	7	1	1	1	1	2	3	1	1	1	1	
118	email	twice	7	7	7	57.424	7	7	1	13.393	7	7	6	14.588	7	7	7	7	7	2	1	2	1	2	3	2	1	1	4	
119	email	twice	6	6	6	24.38	6	6	2	60.826	3	3	3	8.832	3	5	4	4	4	2	2	1	1	2	2	1	1	1	4	
120	email	twice	5	5	4	15.466	4	4	5	18.067	5	4	5	86.59	5	5	4	5	4	2	1	2	1	1	3	3	4	1	4	
121	email	twice	6	3	3	40.236	3	3	3	9.398	7	5	5	14.293	5	4	4	4	4	5	2	1	1	1	1	3	3	3	1	3
122	email	twice	3	3	3	56.035	3	2	1	18.965	5	5	6	80.351	6	7	6	7	7	1	1	2	1	2	2	1	3	1	3	
123	email	twice	6	6	6	30.493	6	6	3	11.49	6	6	6	10.243	4	5	4	5	5	1	1	1	1	1	3	2	3	1	1	
124	email	twice	6	6	6	14.541	5	5	3	7.132	7	7	7	7.719	7	4	3	3	3	2	1	2	1	2	2	2	1	3	1	
125	email	twice	2	2	2	19.378	3	3	5	5.469	3	3	3	7.122	5	6	5	5	6	1	2	2	1	2	3	3	4	3	3	
126	email	twice	7	6	6	46.352	7	6	2	7.342	5	5	5	37.89	3	3	2	3	5	1	1	1	1	2	3	3	1	1	3	
127	email	twice	3	3	3	53.987	7	2	1	24.588	5	5	5	12.338	3	5	2	5	7	2	2	2	1	2	3	3	3	1	3	
128	email	twice	7	7	7	10.5	4	5	5	11.061	7	7	7	6.005	7	7	7	7	7	2	1	2	1	1	2	2	1	4	2	
129	email	twice	6	7	6	42.132	7	6	2	14.921	6	6	5	9.645	6	7	6	6	6	1	1	1	2	1	3	2	4	1	1	
130	email	twice	6	6	5	56.415	5	6	6	13.076	6	6	6	7.455	6	6	6	5	6	1	1	2	1	1	1	2	1	1	3	
131	email	twice	4	5	5	4.985	4	5	5	3.887	4	3	4	4.091	4	2	2	3	4	1	2	1	1	1	3	1	1	4	2	
132	email	twice	6	6	7	48.965	7	5	1	15.281	7	7	7	10.779	6	7	5	6	7	2	2	2	1	2	3	1	3	2	3	
133	email	twice	4	4	4	79.94	6	6	1	15.203	6	6	6	9.354	4	4	4	4	5	2	1	1	1	2	1	3	1	1	1	
134	email	twice	5	4	4	58.899	6	5	2	12.169	6	5	4	18.686	6	6	5	6	7	2	1	2	2	2	3	3	3	3	3	
135	email	twice	6	5	4	417.368	6	4	3	10.743	6	6	6	8.974	4	6	6	6	6	2	2	2	1	2	3	3	3	3	3	
136	email	twice	5	5	5	44.476	7	7	1	11.855	4	4	4	8.295	6	7	6	6	5	2	2	1	1	2	3	3	1	1	3	
137	email	twice	2	2	2	32.358	2	2	4	7.485	5	5	5	9.658	4	5	5	5	5	2	2	2	1	2	3	3	3	1	3	
138	email	twice	5	5	6	39.693	7	5	2	495.116	5	5	5	55.076	5	6	5	6	6	1	2	1	1	2	3	1	4	3	3	
139	email	twice	3	3	3	34.161	4	5	2	12.264	3	3	3	13.919	4	6	6	6	6	1	2	2	2	2	3	3	3	1	2	

140	email	twice	4	4	4	21.251	3	3	4	10.545	4	4	4	8.421	4	6	5	6	4	2	1	1	1	2	3	3	1	3	4
141	email	popup	7	7	7	28.129	6	6	2	33.269	7	7	7	9.769	7	6	5	6	7	2	1	2	1	1	2	3	1	2	4
142	email	popup	6	7	6	12.247	5	6	5	10.707	7	7	5	6.475	5	6	5	6	5	1	2	1	2	1	2	2	3	2	2
143	email	popup	4	5	4	44.512	5	4	5	11.868	5	4	5	9.615	4	6	6	5	6	1	1	2	1	2	3	2	2	4	3
144	email	popup	6	5	4	141.289	7	6	2	6.818	2	5	3	1182.367	5	5	5	5	6	2	2	1	1	1	2	2	1	3	1
145	email	popup	6	6	6	70.561	5	6	5	19.714	6	6	6	17.861	6	6	5	5	7	2	1	1	1	1	2	1	2	1	3
146	email	popup	5	6	3	24.531	7	5	5	64.812	3	6	5	16.25	5	7	6	7	7	2	1	1	2	2	3	2	4	2	4
147	email	popup	7	7	7	25.329	7	7	1	5.742	7	7	7	4.233	7	7	7	7	7	2	1	1	1	1	3	3	4	1	4
148	email	popup	5	5	5	54.83	7	6	3	15.354	6	6	6	20.465	3	5	5	5	6	2	2	1	2	2	3	1	1	1	1
149	email	popup	7	7	7	39.192	5	7	6	18.605	7	7	7	9.225	6	5	4	4	5	2	1	2	1	2	2	1	1	3	1
150	email	popup	5	5	6	25.832	6	6	3	8.92	6	6	6	4.043	5	5	5	5	5	1	1	1	1	2	3	3	3	1	3
151	email	popup	3	5	4	3.321	3	4	5	8.149	3	3	3	6.293	3	3	3	3	4	1	2	1	2	2	2	1	1	3	1
152	email	popup	6	6	6	13.114	6	5	5	4.753	6	5	5	4.137	5	6	6	6	5	2	1	1	1	2	3	3	3	1	3
153	email	popup	2	6	5		4	2	7	2.073	1	4	6	3.273	1	2	5	5	7	1	2	1	2	1	1	3	2	2	2
154	email	popup	2	1	2	50.46	1	1	2	11.26	5	6	5	11.313	4	7	6	7	7	1	1	1	1	2	3	3	3	2	3
155	email	popup	6	6	6	51.45	7	7	1	13.085	5	4	4	77.162	6	7	6	6	5	1	2	2	1	2	3	3	3	2	3
156	email	popup	4	4	3	58.154	3	3	5	11.359	4	4	4	10.375	1	5	5	5	4	1	2	2	2	2	3	3	1	2	4
157	email	popup	7	7	7	20.98	7	6	3	12.429	6	6	5	9.214	4	7	6	6	7	1	2	2	1	2	3	3	3	2	3
158	email	popup	6	6	6	39.409	6	6	3	11.991	5	5	6	12.524	4	5	5	5	6	2	2	2	1	2	3	1	1	3	2
159	email	popup	5	5	4	60.77	5	2	3	28.924	6	4	4	20.095	4	5	4	4	4	2	1	2	1	2	3	3	3	1	3
160	email	popup	5	5	5	28.301	7	7	1	11.118	4	4	4	8.646	1	4	4	4	4	1	2	1	2	2	2	3	1	3	3
161	email	popup	3	4	1	68.906	2	1	4	11.499	5	4	4	14.894	4	7	7	7	7	1	2	2	1	2	3	3	3	2	3
162	email	popup	5	3	3	17.619	5	3	4	12.234	2	2	2	8.807	4	7	6	6	6	2	2	2	1	2	3	2	3	2	3
163	email	popup	6	4	5	53.078	7	5	1	14.875	6	6	7	20.438	3	7	6	5	4	2	1	1	1	2	3	2	3	2	3

164	email	popup	6	4	2	24.797	7	7	1	9.674	7	7	7	8.131	4	7	6	5	7	2	1	2	2	2	3	3	1	1	4
165	email	popup	3	1	3	76.611	4	2	2	18.425	5	5	5	22.31	3	5	3	3	5	1	1	2	1	2	3	1	1	3	3
166	email	popup	4	3	3	51.521	4	2	3	15.832	5	6	6	9.007	5	6	4	6	6	2	2	2	1	2	2	3	1	1	3
167	email	popup	7	7	7	21.968	6	7	2	8.748	6	6	6	9.496	5	7	7	7	7	1	2	1	1	2	3	1	3	2	3
168	email	popup	6	6	6	0	6	6	6	0	6	6	6	0	7	5	5	5	5	1	1	1	1	1	2	1	1	1	3
169	email	popup	6	6	6	33.143	6	6	2	13.005	4	4	5	7.363	5	5	5	5	5	2	2	2	1	2	2	1	1	1	4
170	email	popup	4	4	4	56.441	5	5	2	13.971	4	4	4	15.206	4	5	5	5	4	2	2	2	1	2	3	3	3	3	3
171	email	popup	5	5	5	28.297	6	6	3	5.723	6	6	6	4.634	6	5	5	5	4	2	1	1	1	2	3	3	4	3	3
172	email	popup	3	2	2	29.015	2	2	5	6.947	4	4	4	5.766	5	7	7	7	6	1	2	2	1	2	3	3	2	3	3

Raw Data of Experiment 1-1(B)

No	Product	Condition	good1	favor1	like1	good2	favor2	like2	Time1	easy1	convenient1	complex1	easy2	convenient2	complex2	Time2	secure1	safe1	protected1	secure2	safe2	protected2	Time3	confidence	familiar	expert	knowledgeable	interest	O K1	O K2	O K3	O K4	O K5	O K6	O K7	O K8	O K9	OK10
1	Bank	Control-Twice	5	5	5	6	7	6	131.421	6	6	3	4	4	2	38.386	4	4	5	6	6	6	34.62	6	5	5	5	6	2	1	1	1	2	2	1	1	3	3
2	Bank	Control-Twice	6	5	6	3	2	2	0	6	5	3	4	2	2	0	5	6	6	5	5	6	0	5	6	5	6	2	1	2	1	2	3	3	3	1	1	
3	Bank	Control-Twice	7	7	7	7	4	4	45.918	7	7	7	7	4	7	17.392	7	7	7	7	7	7	11.39	5	7	7	7	7	1	2	2	1	2	1	3	1	1	2
4	Bank	Control-Twice	7	7	7	7	7	7	57.618	6	6	6	6	6	6	34.938	6	6	6	6	6	6	23.17	7	6	6	6	6	2	1	2	1	1	2	2	4	3	2
5	Bank	Control-Twice	6	6	6	6	5	5	6.564	6	7	5	5	5	6	13.816	6	6	6	6	6	6	10.48	4	4	3	4	4	1	2	2	1	2	3	1	1	3	3
6	Bank	Control-Twice	3	2	3	5	6	5	148.991	5	6	6	5	3	5	69.193	6	6	7	6	6	7	58.62	5	6	6	6	7	1	2	2	1	2	3	2	3	2	3
7	Bank	Control-Twice	5	5	5	6	7	6	26.72	5	5	6	5	5	6	12.817	5	5	5	6	6	6	15.15	3	6	5	5	5	2	1	1	1	2	1	1	1	4	4
8	Bank	Control-Twice	5	5	5	5	5	5	102.422	5	5	6	5	5	6	363.656	4	4	4	4	4	4	169.7	4	4	1	3	3	1	2	2	1	2	3	1	1	1	4
9	Bank	Control-Twice	5	6	5	4	3	3	96.68	6	7	7	3	3	3	45.067	3	4	4	3	4	4	44.11	5	7	7	7	7	2	1	1	1	1	3	3	3	3	2
10	Bank	Control-Twice	5	5	5	5	5	5	0	5	5	5	5	5	5	0	3	3	3	3	3	3	0	6	7	7	7	7	2	2	2	1	2	3	2	3	2	3
11	Bank	Control-Twice	5	5	5	3	3	3	37.023	5	6	6	6	2	6	16.97	6	6	6	6	6	6	29.24	6	7	7	7	7	2	2	2	1	2	3	3	1	3	4
12	Bank	Control-Twice	7	7	7	2	2	2	68.759	6	7	6	2	1	2	18.254	5	5	5	6	6	6	16.76	4	6	6	6	7	1	2	2	1	2	3	3	3	2	3
13	Bank	Control-Twice	6	6	6	4	4	4	43.492	6	6	5	4	4	4	14.701	5	5	5	6	6	6	13.9	3	7	7	7	7	1	2	1	1	2	3	3	3	1	4



28	Bank	Cont rol- Twic e	4	4	4	7	7	7	15.4 61	5	5	7	5	5	6	15.1 22	4	4	5	6	6	6	15. 28	6	4	3	3	5	1	1	1	1	1	3	2	1	4	1	
29	Bank	Cont rol- Twic e	5	3	4	6	6	7	36.0 3	5	5	6	5	5	5	15.5 21	4	4	3	6	6	6	15. 71	4	4	2	2	5	1	1	1	1	1	3	2	2	3	1	
30	Bank	Cont rol- Twic e	4	4	4	5	5	5	34.3 67	6	6	6	5	5	5	28.8 18	5	5	5	6	6	6	23. 69	4	4	4	4	5	1	2	1	1	1	2	1	3	3	1	3
31	Bank	Cont rol- Twic e	7	7	7	2	2	2	39.1 52	7	7	1	1	2	6	47.9 74	5	5	5	6	6	6	18. 03	6	5	5	5	6	2	1	1	1	1	3	3	3	3	3	
32	Bank	Cont rol- Twic e	6	5	2	5	5	3	51.7 55	6	6	7	5	5	6	23.7 94	6	6	6	7	7	7	26. 93	4	3	1	1	2	2	2	1	1	1	2	1	1	3	3	
33	Bank	Cont rol- Twic e	6	6	6	5	5	5	0	6	5	2	6	5	3	0	6	6	6	6	6	6	0	5	7	7	7	7	2	1	1	2	2	3	3	1	1	1	
34	Bank	Cont rol- Twic e	5	5	5	4	4	4	113. 858	5	5	5	4	4	3	38.2 96	3	3	3	5	5	5	33	2	4	4	4	5	2	2	2	1	2	3	1	3	2	3	
35	Bank	Cont rol- Twic e	6	6	6	4	4	4	39.4 16	7	7	7	5	5	4	22.1 31	5	6	6	7	6	6	27. 68	5	6	6	6	7	2	2	2	1	2	2	1	1	3	4	
36	Bank	Cont rol- Twic e	4	5	6	5	5	6	28.0 12	6	6	6	6	5	6	16.2 49	6	6	5	6	6	5	14. 19	6	7	6	6	6	2	1	1	1	1	2	3	1	1	1	
37	Bank	Cont rol- Twic e	6	5	5	3	2	3	40.8 96	6	6	6	4	3	4	15.5 07	4	4	4	6	6	6	13. 89	4	6	5	6	5	2	2	2	1	2	2	3	4	1	3	
38	Bank	Cont rol- Twic e	5	5	5	5	5	4	45.8 34	6	6	4	5	4	4	18.8 12	5	5	5	6	6	6	14. 55	4	5	4	5	5	1	2	1	1	2	1	3	1	1	4	
39	Bank	Cont rol- Twic e	4	4	4	7	7	7	100. 301	7	7	7	5	4	2	38.7 61	4	4	4	7	7	7	29. 65	4	7	4	5	5	1	2	2	1	1	3	2	3	2	2	
40	Bank	Cont rol- Twic e	7	7	7	7	1	1	71.7 1	7	7	7	1	1	1	26.7 85	7	7	7	7	7	7	19. 7	7	4	4	4	7	2	1	1	1	1	3	1	2	1	4	
41	Bank	Cont rol- Twic e	6	6	6	4	4	4	100. 672	7	7	1	5	5	3	11.9 85	6	6	6	7	7	7	21. 89	5	5	4	4	4	2	2	2	1	2	2	3	1	2	2	
42	Bank	Cont rol- Twic e	5	5	5	7	7	7	98.9 81	7	7	7	6	7	6	40.0 83	4	5	4	7	7	7	23. 68	6	7	7	7	7	2	2	1	1	2	3	3	3	1	3	

43	Bank	Cont rol- Twic e	6	6	6	2	2	2	62.9 82	5	6	6	3	2	3	31.1 49	4	4	4	5	4	5	30. 87	6	6	6	6	6	2	2	2	1	2	3	3	3	1	3
44	Bank	Cont rol- Twic e	5	6	6	7	7	6	42.5 23	7	6	7	5	5	4	17.9 12	5	5	5	6	7	6	21. 61	5	6	6	7	4	2	2	2	1	2	3	3	1	1	3
45	Bank	Cont rol- Twic e	6	6	6	2	2	2	51.2 28	7	7	7	1	1	1	20.7 16	7	7	7	7	7	7	16. 66	6	6	6	6	6	2	2	2	1	2	3	1	3	1	3
46	Bank	Cont rol- Twic e	7	7	7	5	6	6	36.7 76	7	7	7	6	6	7	11.1 01	6	6	6	7	7	7	11. 56	5	6	6	6	7	2	2	2	1	2	3	1	1	3	2
47	Bank	Cont rol- Twic e	6	6	6	3	3	3	60.7 6	6	6	6	3	2	3	16.1 64	6	6	6	6	6	6	19. 76	6	7	7	7	7	2	2	2	2	2	3	3	3	2	3
48	Bank	Cont rol- Twic e	7	7	5	5	5	5	313. 346	7	7	6	6	2	1	77.4 84	6	6	6	7	7	7	56. 9	6	6	5	5	6	1	1	1	1	1	3	1	3	2	2
49	Bank	Cont rol- Twic e	4	5	5	4	3	3	5.86 3	5	4	3	6	6	3	8.36 6	4	5	4	3	4	4	7.9 7	5	5	4	4	5	1	2	1	1	2	3	1	3	1	3
50	Bank	Cont rol- Twic e	7	7	7	5	6	4	26.9 56	7	7	7	2	3	4	18.0 95	5	4	5	7	7	7	23. 12	5	7	7	7	7	1	1	1	2	1	3	3	3	2	3
51	Bank	Cont rol- Twic e	5	6	6	3	3	1	44.6 12	6	5	6	5	3	6	23.1 75	5	5	5	5	5	5	19. 95	5	7	7	7	7	2	2	2	1	2	3	3	3	2	3
52	Bank	Cont rol- Twic e	6	5	5	6	6	6	23.4 54	6	7	6	7	6	5	24.9 76	5	5	5	6	6	5	14. 1	4	6	6	7	6	2	1	1	1	2	3	2	3	2	3
53	Bank	Cont rol- Twic e	6	6	6	3	3	3	26.3 81	6	6	2	4	4	4	21.8 63	6	6	6	5	5	5	14. 08	5	5	5	5	4	2	2	2	1	2	2	3	3	3	3
54	Bank	Cont rol- Twic e	7	7	7	4	4	4	67.9 29	7	7	7	3	3	3	21.9 26	7	7	7	7	7	7	19. 3	4	5	5	5	4	2	1	1	1	1	2	2	4	1	1
55	Bank	Cont rol- Twic e	6	6	6	3	2	2	44.7 06	6	6	6	4	4	3	29.4 65	5	6	6	6	6	6	21. 49	6	5	3	3	4	2	2	2	1	2	3	1	2	3	4
56	Bank	Cont rol- Twic e	7	7	7	1	1	1	42.1 45	7	7	4	4	4	1	34.7 73	5	5	5	7	7	7	10. 44	4	7	7	7	4	1	2	2	1	2	2	1	2	3	3
57	Bank	Cont rol- Twic e	5	5	5	5	7	7	34.1 47	6	6	7	6	6	5	17.0 79	4	4	4	6	6	6	33. 82	6	5	4	4	7	2	1	1	1	1	3	2	1	1	1

58	Bank	Cont rol-Twic e	7	7	7	5	4	5	38.054	7	7	5	6	5	3	22.324	5	5	5	7	7	7	10.08	4	7	7	7	7	1	1	2	1	2	3	3	3	3	3	3
59	Bank	Cont rol-Twic e	5	6	6	5	5	5	67.475	7	7	7	5	5	4	17.641	5	5	5	6	6	6	15.51	6	7	6	6	5	2	1	1	1	2	2	3	1	3	4	
60	Bank	Cont rol-Popu p	3	3	3	6	6	6	65.972	3	3	3	6	6	5	16.007	5	5	5	6	6	6	16.75	4	7	6	6	6	2	1	2	1	2	2	3	3	3	4	
61	Bank	Cont rol-Popu p	4	4	4	7	7	7	75.219	7	7	7	6	4	5	27.981	2	3	3	7	7	7	23.49	4	5	4	4	4	2	2	2	1	2	3	1	3	1	3	
62	Bank	Cont rol-Popu p	6	7	7	3	3	2	104.155	6	7	6	4	4	4	190.204	6	6	6	6	6	6	14.22	6	6	5	5	5	2	2	1	1	1	3	3	1	1	1	
63	Bank	Cont rol-Popu p	5	6	4	4	3	3	62.197	4	4	4	3	3	5	33.821	6	6	6	6	6	6	17.52	2	5	5	5	6	2	2	2	1	2	3	3	3	3	3	
64	Bank	Cont rol-Popu p	5	5	5	6	6	6	404.457	6	2	6	6	6	6	8.338	5	5	5	6	6	6	5.98	5	5	5	5	6	2	2	1	1	1	2	2	1	1	2	
65	Bank	Cont rol-Popu p	6	6	6	4	4	3	104.36	6	6	7	6	6	5	152.069	7	7	7	7	7	7	14.87	6	4	4	4	4	2	2	2	1	2	2	3	3	2	1	
66	Bank	Cont rol-Popu p	5	5	5	6	6	6	61.288	6	5	6	5	5	6	24.122	6	6	6	7	7	7	16.07	3	4	4	3	3	2	2	2	1	2	2	3	1	3	3	
67	Bank	Cont rol-Popu p	6	6	6	1	1	2	16.623	6	5	5	2	2	3	6.803	6	6	6	5	5	4	5.94	4	6	6	6	6	2	2	1	1	2	3	3	3	2	3	
68	Bank	Cont rol-Popu p	4	4	4	7	7	7	49.288	7	5	6	6	5	5	26.332	1	1	1	7	7	7	15.71	1	5	5	5	7	2	2	2	1	2	3	3	3	2	3	
69	Bank	Cont rol-Popu p	6	5	5	4	3	4	53.891	6	6	2	6	5	6	7.706	5	5	5	4	4	5	13.87	5	4	4	4	5	2	2	2	1	2	3	3	1	4	1	
70	Bank	Cont rol-Popu p	5	5	5	4	4	4	45.982	6	6	6	4	4	3	18.32	7	7	7	7	7	7	14.29	7	5	4	4	4	1	2	1	1	2	3	3	1	2	2	
71	Bank	Cont rol-Popu p	7	7	7	6	5	5	70.309	7	7	6	7	5	4	49.639	6	6	6	7	7	7	34.45	6	7	7	7	7	1	2	2	1	2	3	3	3	2	3	
72	Bank	Cont rol-Popu p	6	6	6	5	4	4	88.43	6	6	4	6	6	4	128.454	6	6	6	6	6	6	10.43	7	6	4	5	5	2	2	1	1	2	2	3	3	3	4	

73	Bank	Cont rol-Popu p	5	6	5	6	6	6	30.5 18	5	4	3	5	6	4	32.0 1	4	4	5	4	5	6	29. 47	6	7	6	7	7	2	1	2	1	2	3	3	3	1	4
74	Bank	Cont rol-Popu p	6	6	6	6	5	5	38.4 98	7	7	5	5	5	3	22.7 18	6	6	6	6	6	6	27. 14	6	7	7	6	6	1	1	1	1	2	3	3	3	2	2
75	Bank	Cont rol-Popu p	4	4	4	5	6	5	150. 321	5	5	3	5	4	4	58.8 06	3	3	3	5	5	5	19. 22	5	4	4	4	5	1	1	1	1	2	3	3	3	3	3
76	Bank	Cont rol-Popu p	4	3	4	4	4	5	23.6 94	5	6	7	6	5	3	23.0 63	5	3	6	7	5	4	20. 2	5	7	7	7	7	2	1	1	1	2	3	3	1	2	2
77	Bank	Cont rol-Popu p	6	6	6	4	5	4	80.3 17	7	7	7	7	5	7	22.4 42	3	3	4	7	7	7	29. 49	4	5	5	4	5	1	2	2	1	2	3	3	3	2	3
78	Bank	Cont rol-Popu p	6	6	6	7	7	7	23.9 98	7	7	7	6	6	7	26.0 77	6	6	6	7	7	7	52. 91	7	6	5	5	5	2	1	1	1	2	2	2	1	3	3
79	Bank	Cont rol-Popu p	7	7	7	1	1	1	39.7 68	7	7	7	1	1	3	36.0 16	5	5	5	5	5	5	22. 03	7	7	7	7	4	2	2	2	1	2	3	3	3	2	3
80	Bank	Cont rol-Popu p	5	5	4	5	4	4	65.1 81	5	5	6	5	5	6	31.1 13	4	4	4	4	4	4	20. 07	2	4	3	4	3	2	2	1	1	2	3	1	1	2	2
81	Bank	Cont rol-Popu p	5	5	5	5	6	5	37.4 23	5	5	3	5	5	4	18.7 46	6	5	7	6	6	7	10. 59	5	5	7	6	6	1	1	2	1	2	1	2	4	3	2
82	Bank	Cont rol-Popu p	5	6	5	4	3	3	72.3 43	7	6	7	5	4	3	22.5 5	6	6	7	6	6	7	42. 15	7	7	7	7	7	1	2	1	1	2	3	3	3	2	3
83	Bank	Cont rol-Popu p	6	6	5	2	3	1	27.2 23	7	6	6	2	2	5	32.1 6	2	6	5	7	4	5	25. 48	4	6	5	6	3	1	2	1	2	1	2	2	3	2	3
84	Bank	Cont rol-Popu p	4	3	4	6	6	6	75.1 23	5	5	5	4	4	3	23.1 47	4	5	5	6	6	6	21. 24	6	6	6	6	7	2	1	1	1	1	3	2	1	3	2
85	email	Cont rol-Popu p	6	6	6	4	4	4	65.1 42	5	5	3	4	4	5	17.9 27	6	6	6	4	4	4	6.0 1	4	5	5	5	6	2	1	2	1	2	2	1	2	3	2
86	email	Cont rol-Popu p	6	6	6	3	3	2	135. 355	7	7	7	4	2	6	27.2 4	4	4	4	5	5	5	36. 51	4	5	4	5	6	2	1	1	1	2	2	1	3	4	4
87	email	Cont rol-Popu p	6	2	2	4	2	2	80.1 7	7	7	6	5	5	5	38.5 97	5	4	4	6	6	6	30. 71	5	6	6	6	6	2	1	2	1	2	3	2	1	3	2

88	email	Cont rol- Popu p	7	6	5	7	6	5	45.3	6	6	7	7	5	7	45.0 23	7	4	6	6	5	6	42. 46	5	4	4	5	6	1	1	1	2	1	2	2	2	2	1	1	
89	email	Cont rol- Popu p	7	7	7	4	4	4	65.1 4	6	6	2	4	3	3	20.2 37	6	6	6	6	6	6	14. 89	4	6	5	6	5	2	1	1	1	1	1	2	3	4	1	1	
90	email	Cont rol- Popu p	7	6	7	7	7	7	68.6 48	7	7	1	7	6	2	15.5 6	7	6	7	7	5	3	9.7	7	7	7	7	7	1	1	1	1	1	1	1	1	1	1	1	3
91	email	Cont rol- Popu p	4	4	4	4	3	3	94.5 05	6	7	7	6	6	7	41.1 22	4	4	4	4	4	4	26. 31	3	7	4	5	7	2	2	2	1	2	3	3	3	3	3	3	
92	email	Cont rol- Popu p	7	7	7	2	1	1	105. 596	7	7	7	3	2	1	43.0 99	6	7	6	4	4	5	34. 84	6	7	6	6	7	2	1	1	2	2	2	2	2	2	2	2	1
93	email	Cont rol- Popu p	7	6	7	1	1	1	31.0 83	7	6	6	3	1	4	15.9 09	5	5	6	5	6	5	21. 35	5	7	7	7	6	1	2	2	2	2	2	3	3	3	2	3	
94	email	Cont rol- Popu p	5	6	6	3	3	3	36.0 85	6	7	7	3	2	5	18.3 04	6	6	5	6	6	6	13. 14	5	5	3	2	4	2	2	1	1	2	3	3	2	2	2	2	
95	email	Cont rol- Popu p	6	6	6	2	2	2	8.38 6	6	6	6	5	5	5	20.9 62	6	6	6	6	6	6	15. 52	6	5	5	5	6	2	1	1	1	1	1	3	1	3	1	3	
96	email	Cont rol- Popu p	5	5	5	6	6	6	57.9 68	7	7	4	6	5	2	16.9 34	5	5	5	6	6	6	18. 48	4	6	5	6	6	2	2	2	1	2	3	3	3	2	2		
97	email	Cont rol- Popu p	5	4	6	4	5	6	4.98 6	4	5	2	5	4	5	4.20 5	4	5	6	5	4	3	4.5 7	6	5	4	6	5	1	2	1	1	1	1	2	3	3	2	3	
98	email	Cont rol- Popu p	6	5	6	4	3	3	606. 845	5	4	5	4	4	3	36.3 75	5	6	5	3	2	4	26	4	6	5	6	7	1	1	1	1	1	1	3	2	2	1	1	
99	email	Cont rol- Popu p	6	7	6	4	4	4	69.4 02	7	7	6	4	3	3	18.9 51	6	6	6	4	3	2	27. 26	5	7	7	7	7	2	1	1	1	2	3	3	1	3	3	3	
100	email	Cont rol- Popu p	6	6	6	6	4	4	47.2 03	7	7	6	6	4	4	21.7 35	5	5	5	7	7	7	22. 85	5	6	5	6	6	2	1	1	1	2	3	2	3	1	3		
101	email	Cont rol- Popu p	6	6	6	5	5	4	81.0 01	6	7	3	5	3	2	30.0 63	6	6	5	6	6	6	31. 28	4	5	4	5	5	2	2	2	1	2	3	3	1	2	3		
102	email	Cont rol- Popu p	7	7	6	7	7	7	58.9 62	7	7	7	6	5	3	21.7 54	5	5	6	7	7	7	17. 07	5	6	6	6	7	2	2	1	1	2	3	3	3	2	2		

103	email	Cont rol- Popu p	7	7	7	2	2	2	26.0 64	7	7	7	2	2	6	24.6 08	5	5	5	7	7	7	15. 43	7	7	7	7	7	1	1	2	1	1	3	2	1	3	4
104	email	Cont rol- Popu p	7	6	6	4	3	3	50.8 56	7	7	7	3	3	4	26.3 73	4	4	4	5	5	6	25. 02	5	5	4	5	4	2	2	2	1	2	3	3	1	3	2
105	email	Cont rol- Popu p	6	6	6	6	5	4	41.0 08	7	7	7	6	5	7	18.6 65	7	7	7	7	7	7	10. 18	5	6	5	6	7	1	2	2	1	2	3	3	1	1	3
106	email	Cont rol- Popu p	6	6	6	3	3	3	64.9 5	6	6	6	4	3	3	33.4 76	5	5	6	6	6	7	26. 92	4	6	5	5	4	1	2	2	1	2	3	3	3	1	3
107	email	Cont rol- Popu p	3	3	2	5	5	5	42.5 84	7	7	7	6	6	6	16.3 48	2	3	2	5	5	5	15. 12	7	1	3	3	4	2	2	1	1	2	3	3	4	3	3
108	email	Cont rol- Popu p	5	5	5	6	4	5	71.6 76	6	6	6	6	4	6	29.8 71	5	5	5	6	6	6	31. 38	4	5	5	5	5	1	2	1	1	2	3	2	3	3	3
109	email	Cont rol- Popu p	3	3	4	7	7	7	29.3 66	5	5	6	5	4	7	19.8 94	3	3	3	6	6	6	15. 52	5	6	4	4	7	2	1	1	1	2	3	2	1	3	1
110	email	Cont rol- Popu p	4	3	4	7	7	7	26.6 14	6	6	7	6	6	7	16.3 43	2	2	2	6	6	6	17. 82	5	4	3	4	6	1	1	1	1	2	3	2	1	3	1
111	email	Cont rol- Popu p	5	6	6	7	7	7	111. 67	7	6	4	6	7	4	25.3 62	5	5	6	6	7	7	40. 15	7	6	5	5	4	2	1	1	2	1	2	2	1	3	1
112	email	Cont rol- Popu p	7	6	6	5	4	5	70.1 09	7	6	3	6	6	3	8.06 9	7	6	7	6	4	5	36. 7	6	7	6	5	6	1	2	2	1	1	2	2	1	3	1
113	email	Cont rol- Popu p	7	7	7	7	7	5	138. 455	7	7	7	7	3	6	21.0 12	7	7	7	7	7	7	20. 81	2	6	6	6	7	2	2	2	1	2	3	3	3	2	3

## Raw Data of Experiment 1-2(A)

No	ID	condition	easy	convenient	complex®	secure	safe	protected	choice
1	R_8Gj2zKx6ciqmwol	Single	6	6	6	2	2	4	1
2	R_4SB8TjsQ9PMSeI5	Single	6	6	5	6	6	6	1
3	R_ewU1uzZFSfrwuEND	Single	7	6	7	6	5	6	1
4	R_emPsPNtrnYuv2Pb	Single	7	6	6	5	4	3	1
5	R_eXIBSNAtJyNxO7j	Single	6	6	5	4	4	4	1
6	R_aY1xa38oWKWzUkl	Single	6	6	7	5	5	5	1
7	R_3UyHLBBBBpmO4vj	Single	6	6	5	4	2	6	1
8	R_1XFqLhBj8wwQx2R	Single	6	6	3	5	6	5	1
9	R_eJuF2NdJSQGbloF	Single	7	7	5	5	3	4	1
10	R_9yT1AcB2VviCaUd	Single	7	6	7	6	7	6	1
11	R_7NXrscQTzA6w6xv	Single	7	7	7	6	6	6	1
12	R_85GID35UiiIUPid	Single	5	6	4	3	4	5	1
13	R_9o74G3jeM15kIEB	Single	7	7	6	4	4	5	1
14	R_cSKQQ40lprkHeR	Single	7	6	5	5	4	5	2
15	R_abgPESgcTtFle3r	Single	7	7	6	6	6	6	1
16	R_doJQ0GmGRURICzr	Single	7	6	6	6	7	6	1
17	R_3F4iyTynh0MTCHb	Single	5	5	4	4	4	4	1
18	R_6Y8zicgPVy9hyoR	Single	7	6	7	6	7	6	1
19	R_4ZKIR6mNvPUeP9H	Single	6	7	1	6	6	7	1
20	R_0rBSq5ZF2tbDiVD	Single	7	6	7	7	5	7	1
21	R_0jsNQaNHsvfgElf	Single	6	7	6	5	4	5	2
22	R_3mHI7I7jJK3vVLn	Single	5	4	3	5	4	5	1
23	R_9EwswY9ry9dk9oh	Single	7	7	6	6	6	6	1
24	R_3eBP91UX8zm4Mgl	Single	7	7	4	6	6	6	1
25	R_8BaNGFX6yS48STH	Single	7	7	7	6	6	6	1
26	R_3KL9FUYc7m3Nau1	Single	5	5	6	5	5	5	1
27	R_bkFk0ypNoH6Kj2Z	Single	7	7	7	5	4	4	1
28	R_0GOe7fJgC5kFect	Single	6	7	4	6	6	7	1
29	R_ba8dBS3071OW949	Single	6	6	3	6	5	6	1
30	R_4ZOv0G6ZVYK2d7v	Single	7	5	6	3	4	3	2
31	R_3yjI58NUPCHeuq1	Single	7	6	7	6	5	5	1
32	R_0dHCLpdbDZ3aBsV	Single	7	7	7	6	6	6	1
33	R_3LlJ8J7fadaq9A9	Single	5	3	4	5	6	5	2
34	R_3kP5T83k52Xv8Gh	Single	7	7	7	6	6	6	1
35	R_eXxj20UF2chRgsB	Single	6	6	7	4	4	4	2
36	R_ea0MX5TTr82zztX	Single	7	7	7	6	6	6	1

37	R_9p3TDQQVA5q4bTT	Single	6	5	4	5	4	4	2
38	R_eM57ghTCRLJe7lz	Single	6	6	6	5	5	5	1
39	R_2hmaGKLfipSD4gt	Single	6	5	5	5	4	5	1
40	R_9QSIKEYzcYJ6J7f	Single	6	6	6	6	6	6	1
41	R_3ITFcKMxx20BkH3	Single	6	6	4	5	6	2	1
42	R_d1liCiKYRawE7pH	Single	7	7	7	4	6	7	1
43	R_78I8fq2T8qYWjj	Single	7	7	7	6	6	6	1
44	R_8qVNk6HpRy5BJlh	Single	6	5	2	6	5	6	2
45	R_dnHZG07uWQQvbM1	Single	7	6	6	7	7	6	1
46	R_3ed49IQxP9NUax	Single	6	5	4	4	4	5	1
47	R_9v6pVPanbYKP0oZ	Single	5	5	4	5	5	5	2
48	R_b108q0IWlrF99Z3	Single	6	6	6	5	6	6	1
49	R_diFptq4M9GqON5b	Single	6	3	3	2	6	4	2
50	R_b2vmTnbADqQRRWt	Single	7	7	7	4	4	4	1
51	R_1FhVXUb51aNPdsx	Single	7	7	7	6	6	6	1
52	R_0DuV977CBRvuoNT	Single	5	6	5	5	6	7	1
53	R_06Y7obNp8fclEnH	Single	6	7	2	7	6	7	1
54	R_0eVJTz44osGpAhf	Single	7	6	7	6	6	7	1
55	R_5olXmHKBQ3OSLQN	Single	6	5	2	5	6	5	1
56	R_8Bxdd3xDD6PYHzv	Single	7	6	4	6	6	6	1
57	R_efA2FLhkqchH4k5	Single	6	6	2	6	5	6	1
58	R_73YdvCdffKujJ1r	Single	6	7	2	6	6	7	1
59	R_3C7xeV4agWJx8CV	Single	7	7	7	6	6	6	1
60	R_9M51pVSwZSJgxnL	Single	6	6	1	5	5	6	1
61	R_0Uqx27RRmRn2CrP	Single	7	4	3	5	4	6	1
62	R_2bhwEDUH5J7oFf	Single	7	7	7	4	4	4	1
63	R_dgpqYqDmMZvDM57	Single	7	7	7	5	5	4	2
64	R_b8gqiiuwnYZzyU5	Single	7	6	5	4	4	4	2
65	R_2ct0FSz5P1FKSh	Single	7	6	7	4	4	4	1
66	R_86w9xoyja9jTXfL	Single	5	5	6	3	3	3	2
67	R_5tO1WkIBUKX4xcp	Single	7	7	7	4	4	3	1
68	R_eEyiYrquRhAs1vf	Single	7	7	7	5	4	6	2
69	R_0NS3w2ZVJu4ZQEZ	Single	7	7	7	6	6	6	1
70	R_8qUD3R0TZh04mA5	Single	7	7	7	5	5	5	1
71	R_bvYhklpufxlpkaN	Single	3	4	3	5	4	5	2
72	R_1FH5HmlppeN91u5	Single	6	6	4	5	5	5	1
73	R_a3Nb5vPq2FfrY1	Single	7	7	7	4	4	4	2
74	R_eg72DuFHCngggB	Single	5	5	5	4	4	4	2
75	R_bvbQOYI8HMRuoU5	Single	5	6	2	5	6	5	2

76	R_bkJhHrP42XXN37f	Single	6	7	5	6	7	7	1
77	R_9QscMEbz3GPH1C5	Single	7	7	6	7	6	6	1
78	R_6MrSD3ImxD33RQN	Single	7	7	7	6	5	5	1
79	R_79RIFIRLryAsiyN	Single	5	5	2	5	6	6	1
80	R_39KuhOR5roVW2gJ	Single	6	6	6	5	5	5	1
81	R_3EsxTD39D0D2g4Z	Single	7	7	7	3	2	3	1
82	R_8hTgFHTMRgXPWV7	Single	5	6	6	5	7	6	1
83	R_eJzQz9g8DnrUW1v	Single	6	6	6	4	4	4	1
84	R_d08mdzcVxpFSNZb	Single	6	6	4	6	5	6	1
85	R_6D7hiAFSLZ511Ff	Single	6	6	6	4	4	4	1
86	R_5yZYY8uCnY4A52B	Single	6	6	6	5	5	5	1
87	R_d7gRFqmSTofzcSV	Single	4	3	6	2	3	5	2
88	R_23M54NiPBIZxF6l	Single	6	7	7	6	7	6	1
89	R_d4lwXONQqXxWiW1	Single	7	7	7	4	4	4	1
90	R_6tHnkoENcsGSFL	Single	6	7	6	7	6	6	1
91	R_e9E1h7z75W95OGV	Single	7	6	6	4	4	5	1
92	R_0N7npHGUlrfS41n	Single	7	7	5	7	6	7	1
93	R_1OduuK8elrLBHrT	Single	6	6	6	6	6	7	1
94	R_7PvTX9hFIKavCbH	Single	4	5	5	1	1	1	2
95	R_1S12zZ2F0k4NIQl	Single	6	6	6	4	4	1	2
96	R_agS0FSIDxmFjVWJ	Single	6	7	6	6	7	6	1
97	R_4IqnlIxluHUZIH	Single	5	4	3	1	1	1	2
98	R_6XuTIU193F8Yfxr	Single	6	7	2	6	7	6	1
99	R_cuOddndb8Tpwpet	Single	7	7	7	6	6	6	1
100	R_cBHv4BpfoWU6zsN	Single	6	6	7	6	6	6	1
101	R_5tcVnN462IZ29BX	Single	6	7	6	6	7	6	1
102	R_86rbeAd8BOTkVmd	Single	6	6	6	4	4	4	1
103	R_3wu8Hq0hu2Q0lbn	Single	7	6	5	7	7	6	1
104	R_87HeF8wCyUEYV4p	Single	7	7	7	6	4	7	1
105	R_2nSau57kTbDtGmN	Single	7	7	5	6	6	5	1
106	R_3WNWXgCVNIEqvaZ	Single	6	5	5	6	6	7	1
107	R_26osFfa8uQJcHJP	Single	7	6	2	7	5	6	1
108	R_0MIKwGJQDYMPkxv	Single	7	7	7	4	4	4	2
109	R_24sliN4KfBs6ay1	Single	7	7	7	4	4	2	2
110	R_blad7DnMH3ZswlL	Single	6	6	4	6	6	6	1
111	R_1NR94NeJbBed845	Single	5	5	4	5	6	5	2
112	R_d5SiZSgzdglyvzv	Single	6	5	2	5	5	5	2
113	R_3UyrFSS4YmLnKJ	Single	6	6	5	5	4	5	1
114	R_41N2ignD1UqzSsJ	Single	7	6	5	5	6	5	1

115	R_2aYBgKY866AwVG5	Single	7	7	7	4	3	4	2
116	R_6QcGGeiH4jbNQ8d	Single	6	6	6	5	5	5	1
117	R_7VXtmU4bDL1E8ft	Single	6	6	3	5	6	5	1
118	R_8HQ2xMwNh09TWU5	Single	7	7	7	6	6	7	1
119	R_6F1YNDXXpaVj52d	Single	6	7	6	6	6	7	1
120	R_51My9pAuOGgasrH	Single	7	6	7	6	4	4	1
121	R_ey6SBm2xQLvcr1X	Single	6	6	6	4	4	3	1
122	R_eeXxC1Bw6jwdqAZ	Single	7	6	5	1	1	6	1
123	R_0cc6GrJ0ZwKy341	Single	4	4	5	4	3	4	2
124	R_39NkMjliYKXSS8d	Single	6	7	6	7	6	7	1
125	R_a8yYOvZfBZYG221	Single	4	5	4	5	4	3	2
126	R_2o7sJMYuY9kNRYx	Single	7	6	7	5	6	5	2
127	R_6VxbSYkvdNYW7CR	Single	7	7	7	7	4	7	1
128	R_6KV46GwIMCkykX	Single	5	5	4	5	4	4	2
129	R_5jboeZvY41oQkgB	Single	6	6	6	4	5	5	1
130	R_886ezPsSMHRxkR7	Single	5	5	4	6	6	5	1
131	R_bkjiuwxWgD38Jud	Single	7	7	7	7	4	7	1
132	R_56CvLR6flSg3SOV	Single	7	7	7	6	6	6	1
133	R_9F8pHorCoQECWGN	Single	5	5	2	5	5	5	1
134	R_5bEIZzgekzsBu9T	Single	6	6	5	4	4	4	1
135	R_6iiYiri0iD9S8yV	Single	5	4	5	4	3	4	2
136	R_24dTVhDALma4v8F	Single	3	4	4	3	3	3	2
137	R_0Gr0GN7hacpXtXv	Single	6	6	2	6	7	7	1
138	R_cOx3aNNM87P7svb	Single	5	5	3	4	4	4	2
139	R_54F14K3Gnj46CFv	Single	6	6	5	5	4	4	1
140	R_8Im8YJVXwZVSSeR	Single	7	6	4	7	5	3	1
141	R_eyUhK3XAmOxASoZ	Single	7	7	2	6	4	6	1
142	R_57JxytXq1zZx8X3	Single	4	4	5	4	4	4	2
143	R_3VtrzLLNj11QipL	Single	6	6	6	4	4	4	2
144	R_cAdQLluzk47qJfv	Single	4	2	3	4	4	4	2
145	R_3PBcYU741sAWYJf	Single	7	7	6	6	6	6	1
146	R_43crjGdKKgZAJpz	Single	6	6	6	5	5	5	1
147	R_3kHH0WxTTNnSGHz	Single	6	5	6	2	3	2	1
148	R_7W2aevHPKZQ5duB	Single	4	5	5	3	2	2	2
149	R_9Lwj0VRN5IfddxX	Single	7	6	7	6	5	3	1
150	R_9sHN4ZZn6eyJnw1	Single	7	6	7	4	2	3	1
151	R_2aRd3Nao0jFkx49	Single	6	6	2	6	7	5	1
152	R_b1k9RXIVfocfQQB	Single	7	7	7	5	5	5	1
153	R_eQ0mXh0rtG2cSB7	Single	7	7	6	4	4	4	1

154	R_6PhSqVWKVHfcZ6Z	Single	4	5	4	5	4	4	1
155	R_0MoKB9fwaCUv0Et	Single	5	5	4	4	4	4	1
156	R_8ANyhPEiYqIpVH	Single	7	7	7	6	5	5	1
157	R_5bWQ7ekhKLdSqe9	Single	5	6	7	3	3	3	2
158	R_eRKvFBFhC1UK7Jz	Single	6	6	6	5	5	5	1
159	R_0vqvoIMWu14R2p7	Twice	5	5	4	5	5	5	2
160	R_9AF8Mr8jKePeYO9	Twice	6	5	6	3	4	4	2
161	R_e55AysENGF2Vlat	Twice	6	6	6	5	5	6	1
162	R_b9PevMBZqjJCYRf	Twice	6	5	4	5	4	3	2
163	R_bPd88GoH0KHT2dL	Twice	7	7	7	5	5	5	1
164	R_cusAWmQrPu6LUwd	Twice	4	4	4	4	4	4	2
165	R_bE16XfsdxvX2hn	Twice	7	7	1	7	7	6	1
166	R_0VwoTxZUN2kUjX	Twice	7	7	7	7	7	7	1
167	R_cB0jNj6OIDGy913	Twice	3	3	3	4	5	4	2
168	R_0Bt1qBPXIL971R3	Twice	7	7	7	7	7	7	1
169	R_6nxOGzIGYWPwrvT	Twice	7	7	7	7	6	6	1
170	R_eUThtYLG0ooHYZT	Twice	7	7	1	7	7	7	1
171	R_d4opU2NKtNgnDW5	Twice	7	7	7	6	4	5	2
172	R_9TQAORKe8FhIVf	Twice	5	6	5	5	6	5	1
173	R_78wDOWKOrjmJSRf	Twice	4	5	4	3	5	5	2
174	R_3ejTmGgeeUzSrb	Twice	5	6	2	4	7	6	1
175	R_5A8kg7QBukIBwqN	Twice	6	6	5	6	5	6	1
176	R_0P7mMUXmO0TQMRL	Twice	7	7	1	7	7	7	1
177	R_en8BJZulSRz5a29	Twice	6	6	4	6	5	5	1
178	R_8k7219lobtWzgG1	Twice	6	6	6	7	6	6	1
179	R_2ISsTzCYdQ3qnrF	Twice	5	7	2	4	5	5	2
180	R_0llj4jd1mdnKodL	Twice	7	7	7	7	7	7	2
181	R_7288A7OZKkOdp1X	Twice	7	7	4	5	5	5	1
182	R_1YM6m5m8tP0Y8AZ	Twice	6	6	6	5	5	5	1
183	R_d0fGjXXFp6wf0vb	Twice	7	7	7	6	6	7	1
184	R_8hTol67MjVLpz	Twice	6	5	2	5	6	5	1
185	R_3yiKOAza6van2mN	Twice	5	5	3	5	4	5	2
186	R_6S5FFkPUAJmgdDL	Twice	7	7	7	5	5	5	1
187	R_82ss35nLTJ1dpPf	Twice	6	5	2	7	6	5	1
188	R_bpGEwRToDSgHAsl	Twice	7	7	4	6	7	6	1
189	R_5Bj9s5RXg4o6711	Twice	7	7	1	7	7	7	1
190	R_d3Zax8D3HqwfGp	Twice	7	7	7	6	6	6	1
191	R_elhH5ef75mWwiV	Twice	7	7	7	4	4	4	1
192	R_bKpTtrN7rZiwmZT	Twice	6	6	6	5	4	4	1

193	R_4JdGSeB2D2sSoh7	Twice	7	6	3	7	6	5	1
194	R_cAe2ecmcJH6S0TP	Twice	7	6	6	7	6	7	1
195	R_dgtZbYGDpgxsPXf	Twice	6	5	2	5	5	5	1
196	R_007ldEdw1BLBNkh	Twice	6	6	6	4	4	4	2
197	R_1L0tMztNDksYk8R	Twice	4	3	3	6	5	4	1
198	R_1A2dsmF7wXmoCYR	Twice	6	6	6	7	7	7	1
199	R_3aDRaX7vV5O3YNv	Twice	5	6	2	6	6	6	2
200	R_exHSAFM8d74jDmt	Twice	6	6	6	7	6	6	1
201	R_022I7CxpilJ3EEJ	Twice	6	5	4	5	5	6	1
202	R_3C2Lz3QZcDIURUh	Twice	7	7	6	6	6	5	1
203	R_6WGX4TLF7WzzWl	Twice	7	7	2	6	7	6	1
204	R_eDLl4j6zw7AHOUR	Twice	7	7	7	6	6	6	1
205	R_2ITQZvXruEJb7	Twice	6	5	2	6	6	6	2
206	R_0U5alm8hVZiqEJv	Twice	7	6	3	4	4	4	2
207	R_5v7yq3Udv0yR4Cp	Twice	6	6	6	4	4	4	1
208	R_cA6vIwMRCD1C1p3	Twice	4	3	3	3	3	6	1
209	R_4GFXM6eWQVsXq7P	Twice	7	6	3	5	4	5	1
210	R_a4s7uMBA16Gljud	Twice	6	5	6	4	5	4	1
211	R_bl0Vg3ENNFPJEFv	Twice	6	7	2	6	7	7	1
212	R_6nzIIUzbBbPbnmJ	Twice	4	4	5	5	5	5	1
213	R_cMhPkU3Isuf0m4I	Twice	7	4	4	7	7	7	1
214	R_4ZA0IMOfBMheYIt	Twice	6	4	6	4	4	4	1
215	R_ba9TTR6YXTyoTsN	Twice	6	7	2	7	6	6	1
216	R_0V9Z0ICWy1YJM2x	Twice	5	6	5	5	5	5	1
217	R_aXYezIzvCP3Pjn	Twice	7	7	7	6	6	6	1
218	R_6Psf0LeVbBdlOPH	Twice	7	7	6	7	6	6	1
219	R_51mltOA68odRYRD	Twice	7	6	1	7	6	7	1
220	R_0Gj0RYZzEmAq87j	Twice	7	7	7	4	4	3	1
221	R_1G2XdMpV7vaLSrH	Twice	6	7	3	6	7	6	1
222	R_0H7mDulEYgzU1aR	Twice	6	5	6	5	6	5	1
223	R_d5SxAcnmj71DGDSB	Twice	6	7	4	7	7	6	1
224	R_0vygHshBeDesbEV	Twice	7	7	6	7	7	7	1
225	R_9nleiTEJKSZtkDH	Twice	6	6	3	4	4	4	2
226	R_4T8NV3OcK5ieJ3n	Twice	6	6	5	7	7	6	1
227	R_514Nja2y0p1DUDb	Twice	4	3	6	5	4	4	2
228	R_6Rs43TYsg41oYOV	Twice	6	6	6	6	7	6	1
229	R_cI38kx5ELXocyRT	Twice	7	7	7	7	1	6	1
230	R_blRumTSh5TYWL2d	Twice	6	7	4	4	3	3	2
231	R_2gZDBawxoeXk5G5	Twice	7	7	6	6	7	6	2

232	R_cYffuU043ruOL2J	Twice	4	5	3	5	5	5	2
233	R_5cZmwWynVGqlq7X	Twice	6	5	6	3	3	3	2
234	R_3t7vrEDdEFplrmd	Twice	7	7	6	6	7	7	1
235	R_0cjbq8NKFyy5Nul	Twice	6	5	3	7	7	6	2
236	R_6FgMeBucc4pfln	Twice	4	4	3	3	5	5	2
237	R_esyNnmCau7tl41	Twice	6	6	2	6	6	6	2
238	R_88hOvgn1LcZG0J	Twice	7	7	3	6	4	7	2
239	R_39tPg3kQDasHEDr	Twice	6	6	5	6	7	6	1
240	R_6uqFBGj1vcoMIHX	Twice	7	6	2	3	3	3	1
241	R_4OX9dCpVg2gmd9z	Twice	7	7	7	6	6	6	1
242	R_6WpDbhfQL3LlvaZ	Twice	7	6	1	7	6	5	1
243	R_bsin2Qt9FpivRLn	Twice	6	6	7	5	4	5	1
244	R_ekOBm6llupLWrQh	Twice	7	7	6	6	6	6	1
245	R_3qMR33Zyv9PsZBX	Twice	7	7	1	7	7	7	1
246	R_eOLUn79JiY73Dvv	Twice	6	6	6	4	5	5	1
247	R_bBZS3kfxhW6D6GF	Twice	6	7	6	7	7	7	1
248	R_9U27MOWPPhwhMvX	Twice	6	7	6	6	6	6	1
249	R_bfthgMA33mA1LzD	Twice	6	7	4	7	7	6	1
250	R_1BsSe5tK7RT4Y2V	Twice	6	6	6	4	4	4	1
251	R_a9UufjkqzQLXb6t	Twice	5	5	3	5	5	5	2
252	R_8jNJYLjzxHldwMZ	Twice	6	6	6	5	5	5	1
253	R_3lzoOBORo0PZxjL	Twice	7	7	7	5	5	5	1
254	R_cU2KWmonY77nINL	Twice	5	5	7	5	7	5	1
255	R_3gALVBxHK59PkuF	Twice	4	4	3	5	5	7	2
256	R_7X046mZ4twJA3cN	Twice	4	6	4	3	3	4	2
257	R_bl2knrVe8SAb1sx	Twice	6	6	4	6	6	7	1
258	R_9N9rBq2pdhs4tP7	Twice	7	7	6	7	7	7	1
259	R_3UcVMhnFQu7tyCh	Twice	7	7	4	7	6	6	1
260	R_2IUaQ59HUGHWP4N	Twice	5	5	3	3	5	3	2
261	R_6sdhJ3phdddBpop	Twice	5	6	6	5	6	6	1
262	R_3DeAkEwkrFtYHbL	Twice	7	7	2	6	6	7	1
263	R_3gvSRLaarANDrxj	Twice	7	7	6	7	5	4	1
264	R_3RjMfBiF9yg8oD3	Twice	6	6	4	5	5	4	1
265	R_aXK2uUekz7cwSnb	Twice	7	7	7	7	7	7	1
266	R_3ZWO0UjQsZjycZ	Twice	7	6	6	4	4	3	1
267	R_57v0mZswvFSRP3T	Twice	6	7	6	7	7	7	1
268	R_3rDwmgEMsnt2F2l	Twice	6	6	6	4	3	4	2
269	R_039krKPkLz7AcOp	Twice	7	6	6	5	5	6	1
270	R_4Ue2JXHhMOenkYR	Twice	7	6	6	4	4	4	2

271	R_cXWXuzAILdgKCGx	Twice	4	4	3	5	4	4	1
272	R_5jSuncWmopYd2IJ	Twice	4	4	4	4	4	4	1
273	R_6VBr2P8Z2Mwm2h	Twice	6	5	3	3	3	3	1
274	R_7PTLQ6QMLPH2I5L	Twice	7	6	4	6	7	6	1
275	R_5pzCpoPSekfvLRb	Twice	6	7	7	4	2	4	2
276	R_5tqsqDyTWI4isPr	Twice	6	5	2	5	6	6	2
277	R_02QomeUajBhzdAh	Twice	6	6	5	5	5	5	1
278	R_3L5nLmxtKmVReMt	Twice	6	6	7	4	4	4	1
279	R_aboeIuic0UG80zX	Twice	6	6	6	5	5	5	1
280	R_6x9LbVsy0iiE4CN	Twice	6	6	3	6	5	5	2
281	R_bfnOa2RuB8RNGGV	Twice	5	5	2	7	7	7	1
282	R_3PHDKdAydQPG2c5	Twice	6	7	7	6	6	7	1
283	R_dd2oBatmHxkeF49	Twice	5	5	6	4	4	5	1
284	R_1T9EFjpv6ZRYKHz	Twice	6	6	6	7	6	6	1
285	R_db90ZisXKetkHkx	Twice	6	7	4	6	4	3	1
286	R_bm89tP4eOE0Ss3r	Twice	6	7	7	5	6	6	1
287	R_3qFDXvXTNOguAoB	Twice	6	5	4	5	6	5	1
288	R_0MxCldxXlzTnWT3	Twice	6	7	2	7	6	6	1
289	R_cNnXkFqe4e2wnul	Twice	6	7	2	7	6	6	2
290	R_5BxxR4aOJMpTabH	Twice	3	4	3	4	3	3	2
291	R_cBHzBQNwsoUVjFz	Twice	6	6	6	7	5	5	1
292	R_6xwXFMcOt8P6Elv	Twice	7	6	6	5	5	4	1
293	R_bmwVKV2dzs0AxsF	Twice	7	6	5	7	7	6	1
294	R_a5ByB6UpDifObHv	Twice	5	4	3	5	6	4	2
295	R_bPAqBxS6rt4Bivj	Twice	6	6	4	6	6	6	1
296	R_0wAeLzfxnZx1BmB	Twice	6	5	6	5	4	5	1
297	R_1ZCwL6TsgzmWsB	Twice	7	7	7	7	7	7	1
298	R_5hglzwyziJ7pPiB	Twice	6	6	3	6	6	6	2
299	R_8qOsz7w9Y4btwAl	Twice	6	7	2	2	6	5	1
300	R_2aVKvDxDm78Fikt	Twice	6	6	6	4	4	4	1
301	R_3l9ulaOlwC1Wnfn	Twice	7	7	3	7	7	7	2
302	R_bkGOILye5y5qiq1	Twice	2	2	5	3	6	5	1
303	R_1AEdPceiuF8Cwx	Twice	6	4	6	6	6	6	2
304	R_0TifggCkpsKNwix	Twice	7	7	7	4	4	4	1
305	R_0jOL1OVnm6MS0Hr	Twice	6	6	6	5	6	6	1
306	R_3xQiOmybcDaiscd	Twice	7	5	5	4	4	4	2
307	R_ble7DrdY4ejvMUd	Twice	6	5	6	6	5	6	1
308	R_3UDbfjVlJ2Lk60J	Twice	6	5	4	5	5	5	1
309	R_0xHfl8uax7HKCEJ	Twice	2	5	1	5	3	6	2

310	R_aWZ25VJxO6IurQ1	Twice	2	3	6	3	4	4	2
311	R_72IxJel5LYpg84J	Twice	5	3	4	4	4	4	2
312	R_d7i2pgZpDP5bQqx	Twice	5	4	3	4	3	5	1
313	R_9AyRvV9PkJ8t3vf	Twice	5	5	2	4	4	4	2
314	R_55YN4GAquWXnk2h	Twice	7	6	6	6	6	6	1
315	R_02JNVUPVoCYqlxj	Twice	6	6	4	5	5	6	1
316	R_5aKu667hsQ1d7SZ	Twice	6	6	7	6	6	6	1
317	R_5ASymfdZamdGrkh	Twice	7	7	7	6	7	6	1
318	R_9u8v6ouM8XAsBal	Twice	6	6	6	5	5	6	1
319	R_0AocydVJV5mJWR	Twice	5	5	7	3	3	3	2
320	R_eaLCcsA1gZQRpOt	Twice	4	4	4	4	4	4	2
321	R_5z34hOpb01eEZSd	Twice	6	6	7	7	6	6	1
322	R_6SBylsxT3vScNZH	Twice	7	6	7	6	6	6	1
323	R_7QwV6mpMCC25i4t	Twice	5	4	5	5	6	5	2

## Raw Data of Experiment 1-2(B)

No	ID	easy1	convenient1	complex1®	easy2	convenient2	complex2®	secure1	safe1	protected1	secure2	safe2	protected2	choice
1	R_eezIVeD6rkomhnL	6	6	6	4	4	2	3	4	3	5	6	5	2
2	R_881cCIwRHDlusyV	7	7	7	7	6	7	5	5	5	6	6	6	2
3	R_eR918WsskcuJu2F	7	7	7	6	5	6	6	6	6	7	7	7	1
4	R_740IndsJDf3qJM1	7	7	7	5	2	3	5	5	6	7	7	7	1
5	R_1B1wH2rMAAnYPpP	7	7	7	4	4	7	4	4	4	4	4	4	1
6	R_0qrMDEt0vfdVZU9	7	7	6	4	3	3	5	5	5	6	6	6	1
7	R_2fuFjMIUyxOus9	5	4	3	6	5	4	4	5	5	4	5	6	1
8	R_4V0gzAOkj8pV5ad	7	7	7	7	7	7	6	6	5	7	6	6	1
9	R_6gmJnUJJnrHouV	7	7	1	3	3	5	7	7	7	4	4	4	1
10	R_eVZ51uCQIGwQLYN	7	7	7	7	6	1	6	6	6	7	7	7	2
11	R_0weLmWc4CuQsfv	2	4	3	4	5	3	4	4	4	4	4	5	1
12	R_57v2x070jjlaHX	6	7	6	4	3	4	4	4	4	6	6	5	2
13	R_aXyfnk00TXm47P	5	5	4	3	4	4	3	4	3	3	4	4	2
14	R_065Fhl20USCz7CZ	6	6	5	5	5	4	6	5	5	6	4	4	1
15	R_eeY82QWdOhnOH11	5	4	2	5	7	2	5	7	3	5	4	6	1
16	R_0MJGEB1hWwAr1b	7	7	7	5	2	1	4	3	3	7	7	7	2
17	R_2gfWZIkBWcpkXlh	7	7	7	5	5	5	4	4	4	6	6	6	2
18	R_7UqxNYeiLhOBMvX	5	6	3	4	5	2	4	6	4	5	4	6	1
19	R_2fMVPjFGUVzCjB	5	4	4	4	3	3	5	5	3	6	6	6	1
20	R_cO3nsCL6FQP949L	7	7	7	4	4	3	5	2	5	7	7	6	1
21	R_bsgJ5szC1KC3oot	6	6	2	7	6	6	5	5	5	7	7	7	2
22	R_eo1uegC0Viu3mAZ	7	7	6	5	1	2	6	6	6	7	7	7	1
23	R_cGZjebEP1sTTNOZ	6	6	6	4	4	3	6	6	6	6	6	6	1
24	R_cuT96PGKPrGbleB	7	7	6	6	3	2	3	3	4	5	5	6	2
25	R_2geFqVuZikF1g0d	6	6	6	6	5	3	6	6	6	6	6	6	1
26	R_dppmk364Ug8F8fr	7	7	1	7	7	1	7	7	7	7	7	7	1
27	R_4VeADeraviqAlux	7	6	6	4	4	5	5	5	4	4	5	6	1
28	R_bKoSovUMzoMQ2Rn	6	4	6	3	2	5	4	6	3	5	3	6	1
29	R_eA8LduTlxvJeztP	7	7	7	5	4	5	6	6	6	7	7	7	2
30	R_0ezclpGfobJF9u5	5	5	4	5	6	3	4	5	4	5	6	4	1
31	R_9GBx0lfxmQSGAct	7	7	7	7	7	7	7	7	7	7	7	7	2
32	R_25AqbKy8nREjhlL	7	6	5	3	4	5	4	4	4	5	4	5	1
33	R_ezFMf0pslG6Rs9	6	5	2	5	6	4	6	4	3	5	4	3	1
34	R_6AaKT9jLDdSBc3j	6	6	1	6	6	1	6	6	6	7	6	6	1
35	R_0cuOwb21ldHTM1	7	6	2	6	6	2	5	6	6	5	5	5	1
36	R_e9yB8iXl33cCl9z	7	4	7	5	7	6	3	2	4	6	5	5	2

37	R_9ohZxcdXgWoBZPL	6	6	7	5	5	5	3	3	3	6	6	7	2
38	R_8HtLuPo5pSgKYHH	6	7	7	5	5	5	4	4	4	6	6	6	2
39	R_57ld1DqRErRhTyl	5	6	2	3	3	5	4	4	4	5	5	5	1
40	R_72pbzQtH1jlc7Qh	6	6	5	5	3	5	5	6	5	6	6	6	1
41	R_e40Dy8r2bSgCvZ3	7	7	5	5	5	3	4	4	4	6	4	5	2
42	R_5u0X9dIB4nkHNEp	5	5	5	5	5	5	4	5	5	6	6	5	2
43	R_5oM1XdkL4ZVntAN	7	7	1	1	1	1	4	4	4	6	6	6	1
44	R_0036lzBvII1d7dH	7	6	5	5	4	4	3	3	4	7	6	5	2
45	R_1U37USUchV6qLb	7	7	6	5	5	4	5	4	4	5	4	4	1
46	R_8vKfAlt2gJnrO5v	1	1	7	2	2	6	1	1	1	2	2	2	2
47	R_0VyYm6ecfcpmLsN	7	7	4	4	4	2	6	6	6	7	7	6	1
48	R_4VhqTqzeeGjO0xT	6	6	6	5	5	5	5	5	5	6	6	6	1
49	R_0q7blUy15p3RGhD	1	2	5	1	2	6	1	1	1	1	1	1	2
50	R_01HRvZDH9RxlBb	7	7	7	1	1	1	1	1	3	7	7	7	2
51	R_aWgdBENjCU7q4yF	7	7	7	4	4	4	7	5	5	7	7	7	1
52	R_9nvezZDceQasFjn	6	6	3	4	3	4	6	4	5	4	3	4	1
53	R_dmLr1356Yw9yLVb	7	7	7	6	5	3	5	4	5	7	6	6	2
54	R_78ae8PRtR64MjzD	7	7	7	1	1	1	5	5	5	7	7	7	1
55	R_3HPS5JRvPsuZdSl	5	4	5	4	3	5	4	2	3	3	3	5	1
56	R_0TKIKVqNdYxNvwh	7	6	6	4	4	3	3	3	4	6	6	6	2
57	R_dcHCLHvTBwuUjNb	6	6	7	5	3	6	6	6	6	6	6	6	1
58	R_9XGgYKdJleWAwJL	7	7	2	6	7	2	7	7	6	7	6	6	1
59	R_eg4GWms6la4YwqF	7	7	7	6	4	3	5	4	4	6	5	5	1
60	R_5pe1cZzmGwttnO5	7	6	7	4	3	2	5	4	5	7	7	7	2
61	R_7X1xBKNqERx7KcZ	1	3	6	6	3	6	5	4	2	6	4	3	1
62	R_4JfSdf3bcEuGYJL	6	6	7	5	5	6	5	5	4	4	5	4	1
63	R_cuVM5euLzbGVIt3	7	7	7	5	5	4	6	5	5	5	5	5	1
64	R_3WXOwva7BvZX9gV	7	7	6	5	5	2	4	4	4	6	6	6	2
65	R_3PvJzdcJkxSnrf	7	6	7	2	2	2	6	6	6	7	7	7	1
66	R_eIDM7jdEleOhXFz	7	7	7	5	3	3	3	3	3	6	5	5	1
67	R_bQRtOTVple5LITX	7	5	6	5	4	3	5	4	5	6	6	6	2
68	R_ex1kY5LZ6p4zTlr	7	3	7	3	1	2	5	5	5	7	7	7	1
69	R_7X1hNBGX5SI5Z2	7	7	7	7	7	7	5	5	5	7	7	7	2
70	R_578xiPlgRjYoEYd	7	7	6	2	2	1	4	6	6	7	7	7	1
71	R_3W1OeqvnmW2NISR	7	7	7	5	6	6	6	4	5	7	7	7	2
72	R_eJNUsa3dr7LRNb	7	7	7	5	5	4	4	5	5	6	6	6	1
73	R_8uWliDgDbox8YJL	6	6	5	6	7	1	6	6	5	6	7	6	2
74	R_3UUobJTUQx4Woi9	6	7	2	5	5	3	5	5	5	7	7	7	2
75	R_8xi6MCKkpbRyYbz	6	6	3	2	2	5	5	4	5	3	6	5	1

76	R_8DiSaM8x4w8CGLX	7	7	7	3	3	5	4	4	4	6	6	6	1
77	R_2iBtzXoCgrvm2iD	5	5	5	5	7	7	7	7	5	6	6	5	2
78	R_3R8EPLqWJOigwsJ	6	6	6	4	4	2	5	5	5	6	6	6	1
79	R_cAMLESX4awYIFY9	5	6	4	5	6	4	3	6	5	4	5	5	2
80	R_dnZAh2Pe1yNCSCF	7	7	7	3	3	1	7	7	7	7	7	7	1
81	R_9XYzDxiOva1BO7P	7	7	7	5	4	4	5	4	4	6	6	5	1
82	R_bJ90HbxLFizORHD	7	7	7	6	5	3	5	5	5	7	7	7	2
83	R_eCCeGhsbEnG2pz7	7	7	7	2	2	2	6	7	7	3	4	4	1
84	R_6SBMVrWTzSzMzP	7	7	5	3	3	2	6	6	6	4	4	3	1
85	R_57iB8oKRJyTY2Ff	7	6	7	7	7	6	6	6	6	7	7	6	2
86	R_aXGKY3DoZnTuhZH	7	7	1	1	1	2	5	5	5	6	6	6	1
87	R_aSiZTF4dM4epcV	7	7	2	4	6	3	5	7	6	4	7	6	1
88	R_0SWfFvpj7MlytMh	2	2	6	3	1	5	4	4	5	5	5	5	2
89	R_6KHiuQCK4G1sNL	3	2	6	2	2	5	2	2	2	2	3	2	2
90	R_ehd78HJsv16pyGF	6	5	6	6	6	3	6	5	4	5	4	5	1
91	R_cAsFhYeKFXsvCV7	6	6	6	5	5	3	5	6	5	3	3	3	1
92	R_7QYzu0nPHtq6y33	7	7	7	5	5	3	5	5	5	6	6	6	2
93	R_0j6s7uJyUx9U8Z	7	2	7	2	2	2	4	4	5	7	7	6	1
94	R_dmqrRovTldHhVWt	6	6	4	5	5	4	4	5	5	6	6	5	2
95	R_1RhG68Tydp401YF	7	7	7	1	1	2	7	7	7	7	7	7	1
96	R_8dJEzmFuN4xu29	7	7	7	7	5	7	4	4	4	4	4	4	1
97	R_a3GGdJUvGRxJzNz	4	5	4	5	5	3	5	5	5	5	7	7	2
98	R_9LHVeLBXG3teHT7	6	4	2	5	4	3	6	7	7	7	7	7	1
99	R_eDHks1JyqHMUzH	7	7	5	7	6	5	5	6	6	6	6	6	2
100	R_37pAsTt12J1P8h	7	7	1	1	1	7	7	7	7	7	7	7	1
101	R_4IUxfAhhXJAdGNn	6	5	2	6	5	2	6	5	6	6	7	7	2
102	R_cuvn9OG0k4b3nYp	7	7	7	6	6	2	6	6	6	7	7	7	2
103	R_42EJwShDq599Mrz	6	7	5	6	6	6	6	6	7	6	6	7	1
104	R_00SOB2GGWREcNcT	7	7	7	3	3	5	7	7	7	7	7	7	1
105	R_9TguaeXxYlvMuX3	7	7	7	1	1	1	4	4	5	7	7	7	2
106	R_6tCctVUMLC2Nnh3	7	7	5	6	6	3	6	7	6	7	6	7	2
107	R_ex8cnsy4CGvCho1	5	5	5	6	3	5	4	4	4	4	4	4	1
108	R_6YeMwxKs3XkWXCB	7	7	7	5	4	4	5	4	4	6	6	6	2
109	R_bHHKc1C7EdzIS6N	7	7	7	3	1	2	5	5	5	6	6	6	1
110	R_9vqQ7xMmtaAKKbj	4	5	3	6	6	2	5	4	6	6	7	7	2
111	R_7UMcBYmPjqPvhvn	6	6	3	6	6	3	6	6	6	5	6	6	2
112	R_dmAQNrIhNujrJdJ	6	6	3	6	5	2	5	6	5	6	5	6	2
113	R_07C8Y04WMxuLeU5	7	7	6	1	4	1	6	6	7	7	7	7	1
114	R_6PUKx2xO9AMBjnt	6	7	6	6	7	3	6	6	4	6	6	3	1

115	R_41uPBgYNlrZbOuN	7	7	7	6	3	3	7	6	6	7	7	6	1
116	R_2oErHYoZi8IXUcl	7	7	7	1	1	1	7	7	7	1	1	1	1
117	R_4Sjj3jDDdTGyHMF	6	6	6	6	7	3	7	6	6	6	7	6	2
118	R_5Ab94kAWdHXMUO9	7	7	6	7	6	3	6	7	7	6	6	6	2
119	R_9Y7UsDEtuxpaRf	7	7	7	2	1	2	6	6	6	7	7	7	1
120	R_bx9Ob8xmP3wgHY1	7	7	7	7	1	5	2	3	6	5	4	5	1
121	R_eFxb5VQdOJ78GN	6	4	2	7	7	7	1	1	1	6	6	6	2
122	R_cimlIzmiLC2wjb	6	5	6	4	3	3	4	2	2	5	6	5	1
123	R_3UC6CC84jO8Vzlj	7	7	7	2	2	1	3	2	4	6	6	6	1
124	R_9BjSqJoisX6x6fv	5	6	4	3	4	4	6	2	2	6	6	6	2
125	R_5iDY7m5hY2Xyrs1	7	7	6	5	4	3	4	4	4	5	5	5	2
126	R_39M2ju7nad19WoR	1	1	7	1	1	7	1	1	1	1	1	1	2
127	R_7Puly6SZTpeteQJ	6	6	6	6	2	6	3	3	3	4	4	3	1
128	R_0NukKVlPtYceDlj	7	6	5	5	5	4	7	6	4	5	6	4	1
129	R_abHegtYFKjN7LN3	7	5	2	6	6	5	4	1	5	7	7	6	2
130	R_8B8Fx9SmyaZYF3	4	4	4	4	4	4	4	4	4	4	4	4	1
131	R_3zcvSA5W3nAaX1r	7	7	3	5	6	2	5	5	6	7	6	7	1
132	R_3eJkb0WJphhEshn	7	6	4	6	6	3	7	6	6	5	6	7	1
133	R_9Qy9WpfdVopgmDX	4	4	4	2	7	1	7	7	3	7	6	7	2
134	R_5mBh0BQJ4o7CUip	6	7	6	6	7	2	7	6	6	7	7	6	2
135	R_3E14RbPSfoY8KJT	5	5	3	5	5	4	4	4	4	4	4	4	1
136	R_db68OFYhdxuld09	7	7	1	5	5	2	6	6	6	1	1	7	2
137	R_dm4aBvg0hwqZPIX	7	7	1	6	7	1	7	7	7	7	7	7	1
138	R_bsDFJ0qPcMjyG7r	6	6	5	5	5	4	5	5	5	7	7	7	2
139	R_ag608nX6qRhwGep	5	6	6	2	2	3	3	3	5	3	3	3	1
140	R_cvkje7pc1TykRP7	7	7	7	2	2	2	2	2	5	5	5	5	1
141	R_9mCeZCOMzbAKcMl	6	5	5	2	3	2	3	2	4	6	5	5	2
142	R_eo33RLK3d44WOvr	7	7	7	4	1	1	1	1	1	7	7	7	2
143	R_5ogVfovVBrdhR2t	6	6	6	6	6	5	5	4	5	6	6	6	2
144	R_9ET2HgbYXqx33eJ	7	7	7	1	1	1	7	7	7	7	7	7	1
145	R_8wW1pKcHo8p2fHT	7	7	7	6	2	5	6	6	6	7	7	7	1
146	R_9BJLnmW4CW1W8D3	7	7	7	7	5	7	5	5	6	6	6	6	1
147	R_4NQWo4JshWfHAZD	5	5	4	4	3	4	4	4	3	5	5	4	1
148	R_0on1sOTvvp9972l	4	4	4	4	4	4	4	4	4	4	4	4	2
149	R_29pPRc6eFU88BoN	7	7	7	6	6	7	5	5	5	5	5	5	1
150	R_etluw8zfNMKAXI1	7	7	7	3	2	5	2	2	3	6	6	6	2
151	R_9ST8nHHaSaHxSxz	7	7	7	5	5	2	5	4	5	7	7	6	1
152	R_egps1BI4LT0WWxv	5	5	5	2	1	1	4	4	4	6	6	6	1
153	R_070Jw8zpyUBAXkx	7	7	3	5	6	3	5	4	4	7	7	7	1

154	R_bHFgomNtjgYpzGB	6	7	6	2	3	4	3	3	4	6	6	7	2
155	R_57RXjDP7yUczSn3	6	6	2	3	3	5	6	6	6	3	4	4	1
156	R_9oDyclLLPaq4TDhj	7	5	7	5	3	4	1	1	1	1	7	7	2
157	R_2IEzmeIA2wsZgXP	6	6	6	3	3	2	5	2	3	6	3	5	1
158	R_er0i9OuzgXvoE4J	7	7	1	7	4	3	6	6	6	7	7	7	2
159	R_exHP2UcQc0sYiAR	7	7	7	6	4	6	6	5	3	6	5	3	1
160	R_2t3Ei4u8HfkEU1n	7	7	7	5	5	3	4	4	4	7	5	5	2
161	R_2lu73mOLJypdRaj	7	7	7	5	4	5	4	4	4	6	5	5	1
162	R_6S8kziVqEwwdPwl	7	7	7	6	6	7	4	4	4	6	6	6	2
163	R_bBkh8ggbU9ISOIR	6	6	6	3	2	4	5	4	5	5	4	5	1
164	R_1G66YC6dfYOegCx	7	7	5	2	3	2	5	3	2	5	5	5	1
165	R_4ShliLOSr8M0Y5L	6	6	6	5	5	5	2	2	2	6	6	6	2
166	R_a2XZAyhjBKsuoj	7	7	7	7	5	7	6	4	5	7	7	7	2
167	R_3cXAQGanwukj9f	7	7	7	1	1	1	4	4	7	7	7	7	1
168	R_1ENbmXCFfZxg98N	6	5	4	4	5	2	7	6	6	7	7	7	1
169	R_bcDNmGtSxb1g925	7	7	7	5	5	3	4	4	4	6	6	6	2
170	R_6r41FwUruT3hj	7	7	7	6	6	6	4	4	4	7	7	7	2
171	R_8u27w9uHetFHPnv	6	5	6	5	5	3	6	4	5	6	4	5	2
172	R_bDGEbWwEePdx1Qh	6	6	5	5	2	5	4	5	6	7	6	7	2
173	R_6EHJTPj7j7TEHIN	6	5	3	4	3	2	5	4	4	5	4	4	1

## Raw Data of Experiment 1-3

No	ID	priming	login	Time	easy	convenient	complex	secure	safe	protected	good	favor	like	important	sensitive	concerned
1	R_4PmkZz2uclr75xb	security	single password	95.442	6	5	3	5	5	4	5	5	6	6	4	5
2	R_8jhcAhBKOjKsa7r	security	single password	149.782	7	7	1	5	4	3	5	5	5	7	6	6
3	R_9QBYm1ngPe8kb3	security	single password	163.09	6	6	2	4	4	4	5	5	5	6	3	3
4	R_9mooGM3kcrFujat	security	single password	91.865	7	7	1	3	3	3	4	3	4	7	7	7
5	R_dj6nlxqA43Deux	security	single password	91.779	6	5	5	4	3	4	4	3	3	6	6	6
6	R_4JcjMdsP4g72kmh	security	single password	91.813	5	3	1	3	4	5	4	5	4	5	3	5
7	R_agBO3KZynUV2DGd	security	single password	301.853	7	7	1	4	3	3	4	3	4	7	6	6
8	R_9ttNjjOSMjsFsmV	security	single password	76.825	5	4	5	4	5	5	4	5	6	4	3	5
9	R_2aUmYdYH5nmNFYN	security	single password	63.791	5	4	5	3	4	5	4	4	3	4	5	4
10	R_5coZZRfBfY5BxH	security	single password	83.467	6	6	2	3	3	6	7	6	5	4	6	6
11	R_3PgQTGCO2Rj1rv	security	single password	76.768	7	7	1	7	7	7	7	7	7	7	7	7
12	R_9EO0McYDjmeB5X	security	single password	298.338	7	6	1	7	6	6	6	5	5	7	6	5
13	R_6JUTBF14MweX3sV	security	single password	69.409	6	6	2	5	2	6	5	5	6	7	7	7
14	R_bEhXkPoAKbcmZnj	security	single password	251.079	7	7	1	6	5	5	5	5	5	7	7	7
15	R_85JQoYjjEmV3kY5	security	single password	69.707	6	6	3	6	5	6	6	5	5	7	7	7
16	R_3q4Eek4Psv8jvxj	security	single password		7	7	1	7	7	7	7	7	7	7	7	7
17	R_czQ8qnXRFWSmvid	security	single password	214.646	7	6	2	4	4	4	5	5	5	6	4	4
18	R_5BVtNnikXFG8berH	security	single password	247.605	5	4	5	5	4	4	4	4	4	7	6	6
19	R_0GMAK14M31ztrEh	security	single password	67.51	6	6	3	5	5	4	5	5	4	7	5	5
20	R_8uAMPgAYC5nLOTz	security	single password	128.659	4	4	4	4	4	4	4	4	4	7	6	6
21	R_4GAZJxse3ziqdtH	security	single password	190.831	7	7	1	3	3	3	4	3	3	7	7	7
22	R_bmv2RfghmUudEx	security	single password	155.568	7	7	1	5	5	5	5	5	5	7	6	6
23	R_3l0qRqIEMcPrid	security	single password	220.985	6	6	3	6	6	6	6	6	6	7	7	7
24	R_2culTZvf6Cc1USF	security	single password	67.971	7	7	1	5	5	5	5	5	4	7	7	7
25	R_4PyqubTPU1Rw9SJ	security	single password	185.292	7	6	3	4	4	4	5	5	4	7	5	4
26	R_d561WClc14EeugJ	security	single password	66.224	6	6	3	3	3	3	3	4	4	7	7	7
27	R_0MWSkNSyaOfcNI V	security	single password	63.073	6	7	6	6	6	6	7	6	7	6	7	6
28	R_dmVozCGvpGrbOeh	security	single password	70.804	7	7	7	7	7	7	7	7	7	7	7	7
29	R_86vZRYDZtzPhUWx	security	single password	500.865	7	7	1	4	4	4	5	5	5	6	6	6
30	R_6nUFxxSh7HKzJJP	security	single password	64.562	7	5	4	4	5	5	7	5	5	5	5	6
31	R_0Aljq8ZlIFQw6CF	security	single password	496.461	7	5	2	4	4	4	3	3	3	7	6	6
32	R_2ikx19w9YOhw1S1	security	single password	62.368	6	5	6	5	5	6	6	7	5	7	6	6
33	R_5A4KjUhYncZPZnn	security	single password	151.111	6	6	1	6	5	6	7	7	7	7	7	7
34	R_1Ybr3Btgefth4qh	security	single password	188.359	5	5	2	5	5	5	5	6	6	7	7	6
35	R_82ZzFzkHwEg4EcJ	security	single password	72.99	6	6	4	7	6	6	7	6	6	6	6	7
36	R_eyUYU4i0BXnja0R	security	single password	67.766	7	7	1	6	5	5	6	6	6	7	6	6

37	R_29ONjx4O2mtzstD	security	single password	493.094	6	4	6	5	6	5	6	5	5	6	5
38	R_cOb0aCcGnpiQmR	security	single password	147.544	6	6	6	6	5	5	5	6	6	5	5
39	R_bapRskz3rfneHRP	security	single password	218.169	6	6	3	6	6	6	6	7	6	6	2
40	R_73DhW21ypw5bCWV	security	single password	169.914	7	7	1	5	5	5	6	6	6	7	6
41	R_eLJ5pEB0q23f2W9	security	single password	293.15	7	7	7	7	7	7	7	7	7	6	5
42	R_envXazjd3EqUoU5	security	single password	84.543	6	5	6	6	6	5	6	5	6	6	4
43	R_b4orx1cNp3hqwZ	security	single password	196.359	7	7	1	7	7	7	7	7	7	6	7
44	R_eVvBLAkD03b1Ta5	security	single password	81.073	6	6	2	5	5	6	6	4	6	6	5
45	R_8qvlRTtyyGAm69	security	single password	62.35	2	5	1	3	2	3	4	3	2	5	6
46	R_3wJrxwkzDg1DVpb	security	single password	393.753	7	6	5	7	4	6	7	4	6	7	6
47	R_5aQBMEJ0k6S81jn	security	single password	248.551	5	6	3	6	6	6	6	6	6	7	6
48	R_0vTIH3x5ijBtR53	security	single password	99.44	7	7	7	7	7	7	7	7	7	7	7
49	R_aUXFGWBxmgOcp7	security	single password	184.108	6	6	1	5	4	5	5	5	5	7	7
50	R_881qUK09bpXaMbH	security	single password	262.754	6	5	2	4	4	3	5	4	5	7	6
51	R_78Mu6Q8JY119YCp	security	single password	243.723	5	6	2	4	4	5	5	5	5	7	7
52	R_bCw9TaoXKxtE1HT	security	single password	265.377	7	7	1	6	7	7	7	7	7	7	7
53	R_0fDerDnVL7dCwrb	security	single password	93.752	7	7	1	6	6	6	7	7	7	7	7
54	R_eVYZcfJ5lkvkaTb	security	single password	63.174	2	6	4	4	2	4	3	4	5	5	5
55	R_9N3v2hDQ6e6JJaZ	security	single password	191.119	7	6	2	4	4	4	5	5	6	7	4
56	R_eMDG2S29UqmTgV	security	single password	105.739	5	6	5	7	6	6	7	7	7	6	6
57	R_07b1wixpoenVWZ	security	single password	441.315	4	4	4	4	4	4	4	4	4	5	5
58	R_4Szz2QOe0QNMI	security	single password	126.765	6	6	5	5	5	5	6	6	6	7	6
59	R_6umjbpVwbJzU5D	security	single password	87.861	7	7	1	7	7	7	7	6	7	7	5
60	R_6Jz6XhWyQfHhY9	security	twice passwords	92.422	6	6	2	6	5	5	6	5	5	7	6
61	R_1ERAPUkQkmvffxz	security	twice passwords	71.608	5	5	3	5	5	5	5	5	5	7	5
62	R_6tagNQcnJLTMBE1	security	twice passwords	125.208	7	7	1	6	6	6	6	6	6	7	7
63	R_6SSNsus9pvn31R3	security	twice passwords	107.511	6	6	5	7	6	6	6	6	6	7	7
64	R_86x7UOaDSZUa9dX	security	twice passwords	62.708	6	6	6	5	6	5	5	6	6	6	5
65	R_eM5nAFpFwsbvTv	security	twice passwords	200.165	7	7	1	4	5	5	5	5	5	7	6
66	R_8jGhedWJNiLL7f	security	twice passwords	172.087	5	6	4	5	6	5	5	5	5	6	5
67	R_czLAsrl0gStjYp	security	twice passwords	81.878	4	7	6	5	6	5	6	5	6	5	7
68	R_8dAAMXl92xF3GI	security	twice passwords	163.265	7	6	2	4	4	4	5	4	5	7	7
69	R_821o8eICBtYpT6J	security	twice passwords	107.733	7	7	1	5	4	4	5	5	5	7	6
70	R_81CxmE9xCiPVQh	security	twice passwords	102.493	6	6	2	4	4	5	6	6	6	6	5
71	R_9XBOlebpPOAzeZ	security	twice passwords	74.41	6	7	1	6	7	7	6	7	7	7	6
72	R_eriVuRxxc0IIP7	security	twice passwords	259.19	6	5	2	6	6	4	5	5	5	7	6
73	R_9nprmd8MSRbmmOx	security	twice passwords	443.613	7	7	1	7	7	7	7	7	7	7	7
74	R_2bkybgeHb3aL0cB	security	twice passwords	98.127	7	7	6	5	5	6	7	7	6	7	6
75	R_dhAIHiG90iHbr8x	security	twice passwords	421.142	6	5	3	5	6	5	6	6	6	7	5

76	R_eVgTAqzQ2qk7AKp	security	twice passwords	543.784	7	7	1	6	6	6	6	6	6	7	6	7
77	R_3aWNbdv7bRIQhW5	security	twice passwords	262.702	7	6	2	4	4	4	6	6	6	7	7	7
78	R_6uuk9p2O0kv7W85	security	twice passwords	163.509	7	7	7	7	7	7	7	7	7	7	7	7
79	R_a4d10zdbkqoF3	security	twice passwords	64.309	6	6	2	4	4	4	6	6	6	6	4	4
80	R_9NRifKlxajZiKx	security	twice passwords	231.046	6	6	2	5	5	5	6	6	6	6	5	5
81	R_9FXUSGBQC3xNlI3	security	twice passwords	83.486	4	4	4	4	5	4	4	4	4	6	6	5
82	R_doMYhiGpdmQJqIJ	security	twice passwords	82.048	7	7	1	6	6	6	7	7	7	7	6	5
83	R_3CluRsj7YgYcCnb	security	twice passwords	125.113	7	7	2	6	7	7	7	7	7	7	5	4
84	R_enRbk7jv8LCto5D	security	twice passwords	64.632	5	5	4	5	6	5	5	5	5	7	6	6
85	R_b935Y3eNkVOhlnT	security	twice passwords	78.577	7	6	1	7	7	7	7	7	7	7	7	7
86	R_8vamus9j08cEZpj	security	twice passwords	122.591	6	6	6	6	6	6	6	6	6	7	7	7
87	R_8HPIZzKjKsP07X	security	twice passwords	78.406	5	6	4	6	4	6	7	2	2	6	7	7
88	R_cGWDqz2ttyAZDm	security	twice passwords		6	4	7	5	6	4	7	6	5	6	4	7
89	R_8q3Fsy6TL1HwunX	security	twice passwords	188.41	6	7	1	6	7	6	7	5	7	7	6	7
90	R_d50g0R0DShy4lk9	security	twice passwords	409.027	6	5	5	7	7	7	7	7	7	7	7	7
91	R_dmslmRoCX21yCsR	security	twice passwords	82.285	6	6	2	4	4	4	5	5	5	7	5	5
92	R_d6YcFe901xFZYGN	security	twice passwords	473.484	7	7	1	5	4	5	6	5	5	5	5	5
93	R_1Xs3i84Fic47Vnb	security	twice passwords	90.512	6	6	4	5	5	4	6	6	6	7	7	7
94	R_ekvWy5zeG3UJ8YR	security	twice passwords	101.373	6	6	6	7	6	7	6	7	6	6	6	7
95	R_4Z2gYoSploBBgF	security	twice passwords	441.806	5	4	6	5	6	5	4	5	5	5	6	5
96	R_06qltRy7hMvA3z	security	twice passwords	62.504	6	5	4	5	4	4	5	6	5	5	6	4
97	R_cJerYi5FDAePQx	security	twice passwords	74.889	6	5	3	5	6	5	6	5	3	5	3	5
98	R_8qfOY9WzRd0qqqh	security	twice passwords	90.439	6	6	2	5	4	5	6	6	6	6	6	6
99	R_6RVtkmOATzo9WLP	security	twice passwords	711.973	5	5	2	4	4	5	4	4	5	7	6	6
100	R_eLnPc4jWaUKQM2p	security	twice passwords	94.977	7	6	6	5	5	5	4	4	4	7	6	6
101	R_6u6EvMEYwJzUfLD	security	twice passwords	216.635	6	6	4	5	5	5	4	4	4	7	7	7
102	R_1Rgv6Ev0ezu6fT	security	twice passwords	273.95	6	6	3	5	4	4	5	5	5	7	6	6
103	R_cXWZ6Kp0I5x2DJP	security	twice passwords	90.62	6	5	6	6	7	7	7	6	6	6	6	7
104	R_0MrBulwzni7FFBH	security	twice passwords	179.778	6	6	1	7	7	7	7	7	7	7	7	7
105	R_cZ6kx8eYzW2Hf6t	security	twice passwords	228.16	7	7	1	6	6	6	7	7	7	7	7	7
106	R_1HYNzeVqKITQF7f	security	twice passwords	159.938	4	5	5	5	5	6	5	5	5	5	4	4
107	R_8zRnEiL69zJXgoJ	security	twice passwords	265.493	4	3	2	5	4	4	3	3	3	7	5	5
108	R_00SyCzdRIMK0mCF	security	twice passwords	63.302	7	6	2	6	6	7	6	6	6	7	7	7
109	R_3yjHUUqoiqM175X	security	twice passwords		7	6	2	6	5	6	4	6	5	7	7	6
110	R_0lzeyuw4Vl5hORf	security	twice passwords	61.808	7	6	3	5	5	7	7	6	7	7	6	7
111	R_eze23W7UU7nr75b	security	twice passwords	121.23	7	7	2	7	6	6	6	7	7	7	7	7
112	R_9oVoFPU2ccKPX5H	security	twice passwords	62.057	6	5	3	2	3	3	5	3	3	6	4	4
113	R_428TEzAVES5Niat	security	twice passwords	71.775	7	7	1	5	6	6	7	7	7	7	5	5
114	R_e4EkJUgVkBXVuQZ	security	twice passwords	122.193	7	7	2	6	5	6	6	6	6	6	6	7

115	R_a9L4Md8pIBGQX5j	security	twice passwords	221.642	6	6	5	4	5	5	5	6	6	7	7	7
116	R_9YcpCmNNtMmLff	no priming	single password	110.647	7	7	2	5	5	5	6	6	6	7	6	7
117	R_9GngFBBravWrOd	no priming	single password	68.417	6	6	4	6	6	6	5	5	5	7	5	5
118	R_9GfoAQBJTEI2Bn	no priming	single password	87.508	7	7	3	5	4	5	5	5	5	7	5	5
119	R_6P7D9b5V5ko3Xv	no priming	single password	186.734	7	7	1	6	6	6	7	7	7	7	7	7
120	R_3r7jLGBELx2CpWl	no priming	single password	171.445	7	4	1	4	4	3	6	4	4	7	7	7
121	R_81cCWFGJT6XGBf	no priming	single password	162.441	7	7	2	6	6	5	7	6	6	5	5	4
122	R_41v6BhOUfCGT4h	no priming	single password	143.476	7	7	1	4	4	3	4	4	5	6	4	5
123	R_5omVWesny4uQ90N	no priming	single password	107.108	4	5	5	4	5	4	5	4	2	5	4	5
124	R_73QsFFyUa5VrL	no priming	single password	64.198	6	5	4	3	4	3	4	4	3	7	5	5
125	R_7TFk2QHAC2y1y97	no priming	single password	66.449	7	7	2	5	5	5	6	6	6	6	5	5
126	R_9oEQHadRdijl5Fb	no priming	single password	70.287	7	7	6	6	6	5	7	7	7	7	7	7
127	R_eIOembH4kn4Ex1P	no priming	single password	118.902	6	6	3	5	4	5	6	6	6	6	7	7
128	R_eCFz64REx87DFNr	no priming	single password	167.073	6	6	2	7	6	5	6	7	6	7	7	6
129	R_1H6CZqdgEMETqIZ	no priming	single password	75.065	7	6	6	6	6	6	7	7	7	7	6	6
130	R_9AAjyGauZ4cRjX	no priming	single password	65.914	5	4	6	5	6	5	6	7	5	4	7	5
131	R_b6ZlodW8mDFQPQx	no priming	single password	62.945	6	6	6	6	6	6	6	6	6	5	5	5
132	R_3IRoVGCZRxsCih	no priming	single password	86.087	5	4	5	4	5	5	4	5	5	7	6	7
133	R_5dtmZcHQ5zpWzxx	no priming	single password	144.766	6	6	2	4	4	4	4	4	5	7	6	6
134	R_8iBFn6UbN9hw2V	no priming	single password	103.544	2	3	4	5	6	7	6	5	4	2	3	4
135	R_dh5QMfkwRCku39b	no priming	single password	184.225	5	6	5	6	6	6	6	5	6	7	5	5
136	R_6kU5KuaufyH0RDet	no priming	single password		6	6	7	6	7	6	6	6	7	7	7	6
137	R_cPgcYOJ6PuCEcMB	no priming	single password	414.767	6	6	2	6	2	3	5	5	5	7	6	6
138	R_a9kxlRa6LaEIEh	no priming	single password	132.509	7	7	3	5	5	5	7	7	7	6	6	7
139	R_d41YSKTrrqXDYI5	no priming	single password	78.103	7	7	1	6	6	5	6	7	6	6	7	6
140	R_dbzCYZrZCSrBtEJ	no priming	single password	201.326	4	3	1	1	1	1	4	4	4	7	7	7
141	R_0e0u9xaqU1WjJc9	no priming	single password	119.952	5	4	3	5	6	6	7	6	5	7	6	5
142	R_brLOV8iauBlviiV	no priming	single password	400.348	7	5	2	5	5	5	7	6	5	7	6	5
143	R_eghiXFuJuzmphiZ	no priming	single password	66.661	6	6	2	5	4	4	5	4	4	7	7	7
144	R_2t2sed47xykN5w9	no priming	single password	75.759	3	3	5	3	1	2	2	2	4	7	6	6
145	R_dmPhD7PCmmetiFD	no priming	single password	484.5	6	6	1	5	5	5	5	5	5	7	7	7
146	R_ePVGIVOV70R2Z6J	no priming	single password	168.411	6	7	5	6	5	5	6	5	4	7	6	7
147	R_8H6UAaJeRX7Hio5	no priming	single password	100.511	7	6	7	6	6	7	6	7	6	6	7	6
148	R_6QlhoDMb2h5q8LP	no priming	single password	119.826	6	6	5	6	6	6	6	6	6	5	5	5
149	R_6sPm61kDv1WEQrX	no priming	single password	145.064	7	7	1	5	5	5	6	6	6	7	6	6
150	R_7PUogh7bqunUj	no priming	single password	98.599	5	6	3	4	4	4	4	4	5	7	7	7
151	R_6x9toZqCh1GxN3	no priming	single password	73.773	6	6	4	5	4	4	5	4	5	6	5	5
152	R_6oigGJSdRHe0Vox	no priming	single password	159.884	5	4	3	3	3	2	3	2	3	6	5	4
153	R_2gd6JxdDFzQrWyF	no priming	single password	69.867	7	7	1	6	6	6	7	7	7	7	6	6

154	R_dnd3tfrV0wrn3n	no priming	single password	81.726	6	7	6	5	6	7	6	5	6	5	7	6
155	R_5zPvevkXkFECO6F	no priming	single password	75.31	6	5	2	5	5	5	5	3	3	7	7	7
156	R_9WS4aVKKnJ5la8R	no priming	single password	266.762	7	7	1	5	5	5	5	2	2	7	7	7
157	R_1ze7coGt5K6yXo9	no priming	single password	137.88	6	6	4	6	6	6	5	6	5	6	6	6
158	R_8Jwj0dVoTpU9CB	no priming	single password	88.576	7	7	1	5	4	5	6	6	6	7	6	6
159	R_9HRcqJ9Bhh0ZeVn	no priming	single password	63.891	6	6	6	6	6	7	5	6	6	7	6	6
160	R_2fTeWhTuIgLE7Bj	no priming	single password		6	6	6	7	6	6	6	6	6	7	7	7
161	R_5haH75LlKy5cdYF	no priming	single password	394.601	6	7	6	7	6	6	6	5	6	6	7	7
162	R_6PaEJ54X18sAmCF	no priming	single password	73.394	7	7	1	5	5	5	6	7	7	7	7	7
163	R_9Nz56ZZgDkkErIH	no priming	single password	300.497	7	7	1	4	4	3	6	6	6	7	7	7
164	R_4J9nxiKgTJkSt3T	no priming	single password	70.152	7	7	1	5	3	3	6	1	1	7	6	6
165	R_eEcpZJxvBLIuH3	no priming	single password	176.795	7	7	1	4	3	2	5	4	3	7	7	6
166	R_9SwPk91VvM6Ppjf	no priming	single password	66.101	6	6	4	5	6	5	6	6	6	7	7	7
167	R_bj7JU5x8gRC3xAN	no priming	single password	70.022	4	5	2	6	4	4	6	3	5	5	3	6
168	R_1KXQ64KiyYXnJqt	no priming	single password	63.842	7	6	6	7	6	6	7	6	6	7	6	6
169	R_eXsQwgKsTRIUuDb	no priming	single password	318.714	6	5	4	5	5	4	5	5	5	7	5	5
170	R_0dfxbZRrbl.7Snj	no priming	single password	69.678	4	4	4	4	4	4	4	4	4	4	4	4
171	R_eVysgEnaOg6F85D	no priming	twice passwords	63.74	4	3	5	5	6	6	5	6	6	4	4	5
172	R_eRm9vP7scvCsHZZ	no priming	twice passwords	81.393	6	5	4	3	3	3	4	4	4	7	6	6
173	R_0oim5zVtDSv4j3	no priming	twice passwords	146.597	7	7	2	7	6	6	7	7	6	7	6	6
174	R_8hNvNIF2fH94OqN	no priming	twice passwords	152.306	6	6	2	4	4	4	5	5	5	7	7	7
175	R_6tx2l7WYdufYh13	no priming	twice passwords	133.373	6	5	4	4	4	3	3	3	3	7	6	6
176	R_086xneM205u3WgB	no priming	twice passwords		6	7	2	6	6	7	7	7	7	7	7	6
177	R_29QGRO7jfvh292l	no priming	twice passwords		7	6	1	5	5	5	5	5	6	7	7	7
178	R_20jl8GTk8kR0Lat	no priming	twice passwords	89.488	7	7	6	7	7	7	7	7	7	7	7	6
179	R_cSIRL8yKy9PWqwd	no priming	twice passwords	116.982	7	7	2	5	5	5	6	6	6	7	5	6
180	R_blor8ZJUFKlHrL	no priming	twice passwords	115.772	5	5	5	5	5	5	5	5	5	6	6	6
181	R_1R3tUcuqe3qHazb	no priming	twice passwords	127.629	6	6	2	5	5	4	4	4	4	6	5	5
182	R_3jACrwBbfqq4opD	no priming	twice passwords	69.226	5	7	5	6	5	4	7	5	6	5	7	6
183	R_24WgbBRgcaqejlL	no priming	twice passwords	68.347	7	6	2	4	4	4	5	5	5	6	4	4
184	R_5UQWcEPMrQj5pH	no priming	twice passwords	86.857	7	7	1	7	7	7	7	7	7	7	7	7
185	R_bl3r6XVYVsoI5X7	no priming	twice passwords	121.102	7	6	1	5	5	6	6	5	7	7	6	7
186	R_ahjtGiviM2SwzXv	no priming	twice passwords	179.5	7	7	7	7	7	7	7	7	7	7	7	7
187	R_ekAeBnS1158JkkR	no priming	twice passwords	166.382	6	6	3	5	5	5	6	4	4	6	4	4
188	R_80SiiUvZlKX6utn	no priming	twice passwords	116.921	5	4	3	5	4	4	3	4	3	6	4	5
189	R_cHHLaGtgnOwTigB	no priming	twice passwords	172.822	6	7	3	6	5	6	6	2	2	6	5	3
190	R_2o7vd8b6EUHe3w9	no priming	twice passwords		7	7	1	7	7	7	7	7	7	7	7	7
191	R_1lhJHSGalqcEFWB	no priming	twice passwords	616.556	7	7	1	6	6	6	5	6	6	7	6	6
192	R_aVrBxDN0ka9Iagt	no priming	twice passwords	111.225	6	5	5	6	3	4	5	4	5	5	4	5

193	R_b30PXZ8Ve1IW9Sd	no priming	twice passwords	138.759	7	7	1	7	6	6	7	7	7	7	7	7
194	R_8AoH0Em3FR0LLYF	no priming	twice passwords	69.847	6	6	2	7	7	7	7	7	7	6	5	6
195	R_0chg1fGQ4qzyQyF	no priming	twice passwords	518.407	7	7	1	6	6	7	7	7	7	7	7	7
196	R_3PpHgKhN35YMyrz	no priming	twice passwords	61.238	7	6	1	7	7	7	7	7	7	7	7	7
197	R_ch3Ac5XPZARH0bP	no priming	twice passwords	330.658	7	7	7	7	7	7	7	7	7	7	7	7
198	R_d4Hq77nvwCdJ17T	no priming	twice passwords	90.973	6	5	6	4	6	5	6	5	6	6	5	6
199	R_0AMObBaSosW6a45	no priming	twice passwords	175.169	7	7	1	4	4	4	4	6	6	7	7	7
200	R_8HJM2g2bytNYqh	no priming	twice passwords	131.484	7	6	6	6	6	6	6	6	6	6	7	6
201	R_8dYAyKgK9AcOrbf	no priming	twice passwords	78.848	7	7	1	7	7	7	7	7	7	7	7	7
202	R_9z2OQd3EH6lmdKt	no priming	twice passwords	196.957	7	6	4	5	5	5	6	6	6	7	6	6
203	R_cl6gyvKsxusBIYx	no priming	twice passwords	121.555	7	7	2	6	6	7	7	7	7	7	4	7
204	R_2c5H7hx4qf4gXAh	no priming	twice passwords	173	6	5	2	5	4	4	5	6	6	6	5	6
205	R_2gY0WznmkCCbI8J	no priming	twice passwords	164.085	6	6	5	6	3	4	6	6	6	6	6	6
206	R_08nODMW15X55xVX	no priming	twice passwords	201.356	6	5	2	4	4	5	5	4	5	5	5	5
207	R_1QXDPKwn2PCFYAt	no priming	twice passwords	72.391	6	6	4	4	4	4	5	5	5	7	5	6
208	R_3n0J8Gqpxds0BQ9	no priming	twice passwords	67.015	7	7	1	7	7	7	7	7	7	7	7	7
209	R_eUKzyS1bOjlgidT	no priming	twice passwords	1597.44	7	7	6	5	5	5	6	6	7	7	7	6
210	R_9Y65MhZC86kuvJz	no priming	twice passwords		6	7	5	6	6	5	6	6	4	7	5	6
211	R_2n48725hIZ8UVmZ	no priming	twice passwords	115.485	2	2	3	3	6	3	4	4	3	7	6	6
212	R_3qmA7iFPwDw4cd	no priming	twice passwords	76.115	7	7	1	5	5	4	6	6	6	7	7	7
213	R_d4LfxugOC01mDj	no priming	twice passwords	1245.623	7	7	1	5	5	5	6	6	6	6	7	7
214	R_6fbhxa7dPkQYfrL	no priming	twice passwords	86.996	7	7	1	7	7	7	7	7	7	7	3	2
215	R_5oQp1tSqHd49hUF	no priming	twice passwords	738.727	6	7	6	6	7	6	6	7	6	6	7	6
216	R_9i03LhntdF7MTaZ	no priming	twice passwords	64.313	7	6	2	5	5	5	5	2	1	6	5	5
217	R_6kS8RCxSvE181o1	no priming	twice passwords	89.295	7	7	7	7	7	5	7	7	7	7	7	7
218	R_eyN3U2f3F2qaNH	no priming	twice passwords	83.523	6	6	5	7	6	6	6	7	7	7	7	7
219	R_9X3VeJMqYmKqEp	no priming	twice passwords	126.402	7	7	1	7	7	6	7	6	7	7	5	6
220	R_6WMTpYnAnGxB5eR	no priming	twice passwords	74.972	5	5	3	5	5	5	5	5	5	7	7	7

## Raw Data of Experiment 1-4

No	ID	condition	easy	convenient	complex	secure	safe	protected	techadvan	good	favor	like
1	R_3I9aPwijCHQwHeB	1	7	7	2	6	6	6	5	6	6	6
2	R_1EKm4ojKwC6swjX	1	2	3	5	3	4	4	3	4	3	3
3	R_88Ruf9knLnDX0h	1	6	5	6	4	6	6	5	6	5	6
4	R_3Cs3dwnWtebmjJP	1	5	5	5	5	5	6	5	5	5	5
5	R_4Z8vYhW18Ec2uH3	1	4	6	4	5	5	5	5	5	5	5
6	R_8G34m7Zf7MbkPch	1	6	6	2	6	6	6	7	7	6	7
7	R_0eqChnK0TuFrKQd	1	3	5	4	3	4	5	4	3	4	3
8	R_2fSKJbMyZx4mg8R	1	4	5	3	4	4	5	4	4	4	4
9	R_ctG8QQfocVfPZ3L	1	6	6	4	5	4	5	5	6	6	6
10	R_8uDIDHT66vGs4J	1	5	6	4	5	5	5	5	6	6	6
11	R_7U7kiCw0vwYsIK9	1	5	6	4	5	5	5	6	5	4	5
12	R_9WtlEnZUHCB10Et	1	7	6	3	6	7	7	6	7	7	6
13	R_eEULn6bmGfkidVv	1	7	7	4	4	4	4	4	4	5	5
14	R_eSevijSDthUkFgh	1	4	6	5	6	5	5	4	4	4	4
15	R_eqSSmgP64kPurbf	1	5	5	6	5	6	5	6	5	6	5
16	R_eRM91oW1sR1FEMJ	1	7	7	6	7	5	6	4	7	7	7
17	R_4GHeKZH4P5UhhSZ	1	5	4	4	5	5	4	4	5	5	5
18	R_9yGcCD6MDi5Edq5	1	5	5	5	5	5	5	5	5	5	5
19	R_2awkZRR7KaUxuGV	1	6	6	2	6	7	6	6	7	7	5
20	R_eOJIUhWOY2Xa97v	1	5	5	7	5	5	5	6	6	6	6
21	R_bHs4zrYBdwL0j7D	1	6	6	3	6	6	6	6	6	6	6
22	R_0kw5pyLlpeGABJr	1	5	4	5	4	5	4	5	4	5	6
23	R_5AcTg8bTyv3zSRL	1	4	5	4	5	5	5	5	4	4	4
24	R_8ocgyTVgvJg5CiF	1	5	6	4	6	6	6	7	6	6	6
25	R_6IHCG0MjKuDIEO9	1	4	4	5	6	6	6	4	7	6	7
26	R_8JkBTp5AjDmrHNz	1	4	4	4	4	4	4	5	7	7	7
27	R_3JJ9lmoX94mWU1D	1	4	4	4	4	4	4	4	4	4	4
28	R_8040V2YJV6U2iTb	1	5	6	6	5	3	5	6	5	6	6
29	R_9pPjT9Vdgebs3yZ	1	4	3	5	4	5	4	4	3	4	4
30	R_85NwVHGQejkiDWt	1	5	5	3	5	5	5	4	5	5	4
31	R_eWC6ZpD15Qu9Pa5	1	5	4	4	6	6	6	7	5	5	5
32	R_dbQPGvO1bP2jstT	1	7	6	1	2	1	1	1	1	1	1
33	R_9ZXSsm8CKyaqdVlh	1	5	6	5	5	5	5	4	5	5	5
34	R_cZnYd7vdUZB1uuN	2	3	7	6	6	6	6	6	5	6	6
35	R_eh2Ffd7XYSM0j3f	2	6	6	4	5	5	5	6	6	6	6
36	R_00808Qp7zknCYSh	2	5	5	2	5	5	5	5	5	5	4

37	R_3yqNZ711QXQm4jX	2	5	6	5	6	5	5	6	6	6	6
38	R_4VqS0th8pflkbCR	2	6	6	2	6	6	6	6	6	6	6
39	R_0PWdVIEA3ji7C1	2	6	5	6	5	6	5	4	6	5	6
40	R_8cRq5LYBOulx8cl	2	6	5	4	5	6	5	4	5	6	5
41	R_2atoQlbnVnZnRjL	2	7	7	1	7	7	7	7	7	7	7
42	R_5pXjbIURIT9OSi1	2	2	3	4	4	5	5	4	3	3	3
43	R_0GTUQTxKrpIyhmJ	2	5	7	3	3	5	5	4	3	6	6
44	R_0PtogE25B1YV8Xj	2	6	6	7	6	6	7	6	6	6	7
45	R_4ZulCjUHnQ6U9j	2	5	5	6	6	6	6	6	6	6	6
46	R_0oAubF85QGvzfUN	2	5	4	3	4	4	4	5	5	5	6
47	R_06w0qNw3iKS1LQF	2	4	4	4	4	5	5	6	4	4	4
48	R_1LJTTsMix9SD1MF	2	6	6	2	6	2	5	7	6	6	7
49	R_1ZmBnTqG5NXaA05	2	5	4	5	6	4	5	4	4	5	5
50	R_8Hb34E1YwakSTJ3	2	5	5	4	5	5	5	5	5	5	5
51	R_1GIQSBttH8xB1c1	2	5	5	2	6	6	6	6	1	1	1
52	R_eRlpZTwmw7m52zX	2	6	7	1	6	7	6	6	7	7	7
53	R_1YyR4JhnDqnDDal	2	6	7	1	6	6	6	6	7	6	6
54	R_8xqloo2BzJZ1m1n	2	6	7	7	6	6	5	6	6	5	6
55	R_6Gdl41nYctt0iUd	2	4	3	4	5	6	6	5	5	6	5
56	R_6r2g8cmcDsOihFj	2	5	4	3	5	5	4	5	5	4	4
57	R_7Wnrzt4J0QIRtlb	2	5	6	4	6	7	5	5	3	6	5
58	R_0TaM876SnX8G9i5	2	6	6	1	6	6	6	5	6	5	6
59	R_bCwgDPjYd6ztV9X	2	6	6	3	5	5	5	6	6	6	6
60	R_0Hxr5ZXO05mHpfD	2	6	5	3	5	4	5	6	4	5	7
61	R_cMf3cU24SOepTgx	2	5	5	3	5	5	5	6	5	5	3
62	R_d57M1ynZroK1Wtf	2	5	4	5	6	6	5	6	6	5	7
63	R_e9VJMRjQ3k3KFa5	2	4	4	4	4	4	4	5	4	4	4
64	R_blWb9e7yw4s1hYh	2	5	6	4	6	6	6	6	5	6	6

## Raw Data of Experiment 2-1

No	ID	Description	Fluency	easy	convenient	complex®	secure	safe	protected	techadvance	good	favor	like
1	R_b3qBpZLnK43zDsp	security-oriented	easy	6	6	3	6	4	7	5	6	4	4
2	R_73O5JIAMA4WVzWB	security-oriented	easy	5	5	5	5	5	5	5	6	5	6
3	R_en78Vsxz7YC7hZz	security-oriented	easy	6	5	5	5	6	6	7	6	5	6
4	R_9mCZ4B7xrBezvoI	security-oriented	easy	6	5	2	5	6	6	5	6	6	5
5	R_42d3kD5AmqVDHjT	security-oriented	easy	5	6	4	5	6	7	6	6	6	6
6	R_4Pjhb6upTrE7haZ	security-oriented	easy	6	6	5	6	6	6	7	6	6	6
7	R_7WMZVNi2qlbLh6B	security-oriented	easy	6	6	6	6	6	6	6	6	6	6
8	R_a8DcwsZUssnmZ	security-oriented	easy	6	6	6	6	6	7	6	6	6	6
9	R_3K6KKoEzk2v6PX	security-oriented	easy	7	6	5	5	6	7	6	7	7	7
10	R_3ga6MKIGitQiNf	security-oriented	easy	5	5	5	4	5	5	5	6	6	7
11	R_4Twl1j4kT6Jv1pH	security-oriented	easy	7	7	7	7	6	7	6	7	7	7
12	R_eP8zWb38YeFrhAx	security-oriented	easy	6	5	3	6	7	4	7	7	5	4
13	R_6Fimw43fiz2XTyl	security-oriented	easy	5	5	5	6	6	6	6	5	4	5
14	R_d0YqAvEZIKfUUYB	security-oriented	easy	7	7	7	6	6	5	6	6	5	6
15	R_9zSEcWpSoq8sOEZ	security-oriented	easy	5	6	3	6	5	5	4	5	4	6
16	R_51M5xQZ8cjriud	security-oriented	easy	6	5	2	6	6	6	6	6	7	7
17	R_8vTDOXyj2nu26cB	security-oriented	easy	6	6	1	6	6	6	6	6	5	6
18	R_dng5Jle7B0s5	security-oriented	easy	6	6	7	6	6	6	6	6	6	6
19	R_d7hR6LzHidfUR7	security-oriented	easy	7	7	1	7	7	7	7	7	1	1
20	R_2abbKm7UYbMsf4x	security-oriented	easy	4	6	3	6	5	6	5	5	6	5
21	R_6RnL78jDtfAg2Pj	security-oriented	easy	5	5	6	6	4	6	7	6	6	6
22	R_2gcct5ealzX1f5r	security-oriented	easy	6	6	3	6	4	6	7	6	7	7
23	R_6rIE2gQ0iB5m7z	security-oriented	easy	5	6	5	6	6	6	5	6	6	6
24	R_73AmMZnoGgHI21	security-oriented	easy	7	6	6	7	6	6	7	6	7	7
25	R_8GHX9qmu2f5UgzH	security-oriented	easy	5	4	3	4	4	5	4	5	5	4
26	R_3pWfgmHtarWBdAh	security-oriented	easy	5	5	2	7	7	7	6	7	7	7
27	R_0wiBSzUpziBSg97	security-oriented	easy	5	3	4	4	5	5	5	4	5	6
28	R_3sEokE5EvDM7CZf	security-oriented	easy	5	6	6	5	5	6	6	6	6	6
29	R_e38lrAddTf9DjRX	security-oriented	easy	6	6	1	7	6	6	7	6	7	7
30	R_1Y6tRGjiG4uRH0N	security-oriented	easy	5	6	5	5	6	6	5	6	5	5
31	R_6FfwRqHd9skgrvD	security-oriented	easy	5	4	2	7	7	7	7	6	6	6
32	R_2hrQ13RIDKKJMzn	security-oriented	easy	6	6	3	6	6	6	6	7	7	7
33	R_abDa5ocQcVcjStL	security-oriented	easy	6	6	6	6	6	6	7	7	7	7
34	R_6W23p9oKvZaTDil	security-oriented	font	5	5	6	6	6	6	6	6	6	6
35	R_b1Le31QCK22zRmB	security-oriented	font	3	3	2	6	6	6	7	6	7	7
36	R_2s1hYLcMy3tXzyR	security-oriented	font	5	5	5	4	4	4	7	6	6	6

37	R_8e6IADDG4mrSl6d	security-oriented	font	6	6	5	6	6	6	6	7	6	6
38	R_412QuLTpB4spjHD	security-oriented	font	4	6	5	6	6	6	6	5	5	6
39	R_bC6AhaRF91FDXpz	security-oriented	font	7	7	7	7	7	7	7	7	7	7
40	R_0cfMvddvohEavxb	security-oriented	font	7	7	7	7	7	7	7	7	7	7
41	R_1AASGo31UNLybnn	security-oriented	font	5	5	2	7	3	6	6	4	6	5
42	R_aW3VkfEhpmEtCd	security-oriented	font	5	7	1	7	7	7	7	7	7	7
43	R_0wwi96VH6E6x2zX	security-oriented	font	5	5	5	5	5	5	6	6	6	6
44	R_6PxZJmkqdsxGCB7	security-oriented	font	6	7	4	6	6	6	7	7	6	7
45	R_b0ZYxoRdIAHg1Zr	security-oriented	font	2	2	2	6	6	6	5	3	2	1
46	R_1TYK3P0FTDBmMXb	security-oriented	font	5	5	4	5	5	6	6	5	5	5
47	R_5bWcWgqZv5yGQsd	security-oriented	font	6	7	2	6	6	6	5	5	6	7
48	R_9LVbhS66PFCrbIp	security-oriented	font	4	4	4	4	4	4	4	4	4	4
49	R_5urJGbCkGjXV6df	security-oriented	font	5	5	2	4	6	5	5	6	7	6
50	R_3vKMw8lr2WZl285	security-oriented	font	4	4	3	4	5	4	4	3	4	4
51	R_en5py4YAwC3uNbd	security-oriented	font	3	3	5	4	5	5	5	4	3	3
52	R_9mhoBMXFzQbXaq9	security-oriented	font	6	6	3	5	5	6	6	6	5	6
53	R_9vPUhblqJBS4i3P	security-oriented	font	7	7	1	6	6	5	6	6	6	7
54	R_3abMDW3M5bdZe8B	security-oriented	font	5	5	4	6	5	6	6	6	6	6
55	R_7aoz76gxx2K2Sot	security-oriented	font	4	6	5	5	5	5	5	6	6	6
56	R_abBO4a6ahkiks5L	security-oriented	font	6	3	4	6	5	6	6	6	6	6
57	R_d1mtSKx9VB05rSt	security-oriented	font	6	6	2	7	6	6	7	6	6	7
58	R_da4H07heASHmq1L	security-oriented	font	3	4	4	5	4	4	5	5	5	5
59	R_5C5zsf5S8b4KiCF	security-oriented	font	2	3	6	3	3	2	4	2	3	4
60	R_5hWOlmcR1vCUIkt	security-oriented	font	4	5	3	6	6	2	6	5	6	7
61	R_5iKFIH2M9Ks4Wp	security-oriented	font	4	4	3	6	6	5	6	5	5	5
62	R_8uDAOW6LUxvr3Dv	security-oriented	font	7	7	5	5	5	5	7	7	7	7
63	R_a4zwArIjy7AHFid	convenience-oriented	easy	3	2	6	2	3	4	2	7	2	7
64	R_6K9Oe17FdWpgMit	convenience-oriented	easy	3	2	5	5	4	3	5	3	2	2
65	R_5vuN2sZenzVZzuZ	convenience-oriented	easy	7	7	4	7	7	7	4	7	7	7
66	R_7QmW6l0bDkwNsCV	convenience-oriented	easy	6	6	2	6	7	6	6	6	6	6
67	R_dcfOD4RQmBoVihn	convenience-oriented	easy	3	4	4	2	3	3	2	3	2	3
68	R_8Dixh4eNGVz0QKh	convenience-oriented	easy	4	4	4	6	5	5	6	5	5	5
69	R_baoYZsIpINdAF5H	convenience-oriented	easy	5	4	5	5	6	2	5	4	2	2
70	R_cRWF0EqUl6AXhVr	convenience-oriented	easy	5	6	5	6	6	5	6	6	5	6
71	R_0IBhOSuW0T3fkot	convenience-oriented	easy	7	6	2	6	5	5	6	6	6	6
72	R_3C7JW9QviwBd6cJ	convenience-oriented	easy	5	5	6	4	4	4	4	4	5	5
73	R_3U8Cb48rEVlbaIn	convenience-oriented	easy	6	7	3	4	4	4	7	7	7	7
74	R_dbYa8YDRkMWOt8x	convenience-oriented	easy	4	3	6	2	1	5	5	5	7	6
75	R_agADSeX0gpokh4p	convenience-oriented	easy	6	6	3	6	5	5	6	7	6	6

76	R_a9tLKNHaCghalFT	convenience-oriented	easy	6	5	6	5	5	6	7	7	6	6
77	R_6A6pcFuIDkPvhEF	convenience-oriented	easy	4	6	3	4	5	6	5	5	6	6
78	R_6P8s7RC5QDYMNmt	convenience-oriented	easy	6	5	2	5	6	6	5	6	6	6
79	R_byluDevWOXZIVvv	convenience-oriented	easy	6	7	2	6	6	6	7	6	6	7
80	R_b8T6sO0elTwZzRX	convenience-oriented	easy	6	6	6	6	6	6	6	7	7	7
81	R_5yFqaYscsQLHO4Z	convenience-oriented	easy	6	7	2	7	6	6	6	5	6	7
82	R_bd4ofzAdnAFSSRL	convenience-oriented	easy	6	5	5	5	5	6	6	6	4	4
83	R_0od3RlmsSWwx9UF	convenience-oriented	easy	5	6	4	6	5	6	5	6	6	6
84	R_1Xfl3JkDkHPxgmV	convenience-oriented	easy	3	4	3	6	5	5	4	5	4	4
85	R_bDExbuIMP9vSgJf	convenience-oriented	easy	5	5	3	5	5	5	5	5	5	5
86	R_5z2TDQTKKPPiWPj	convenience-oriented	easy	6	6	5	5	5	5	5	6	2	4
87	R_6L2wD9gfDGPZV3	convenience-oriented	easy	6	6	3	6	6	6	5	3	4	3
88	R_aV77vFaZz4PEAQZ	convenience-oriented	easy	6	5	5	4	4	5	4	5	5	5
89	R_aaAG1JiGFBtyyd7	convenience-oriented	easy	6	5	4	5	6	5	5	6	6	6
90	R_7anT5OIBPZeh2Zv	convenience-oriented	easy	6	5	4	6	4	6	7	7	6	7
91	R_0OmxH1cinmQ4JWR	convenience-oriented	easy	4	5	4	5	4	5	5	5	5	5
92	R_8fb391TGdShJg6V	convenience-oriented	easy	6	6	5	5	3	4	5	6	6	6
93	R_4SpHUql8WTBZilt	convenience-oriented	easy	6	6	4	6	6	6	6	6	6	6
94	R_4UuoEtiJ0aWgoCx	convenience-oriented	easy	7	7	6	6	6	7	6	6	7	7
95	R_doi1RwVgOJRooq0Z	convenience-oriented	easy	5	5	6	5	5	4	5	5	5	6
96	R_1Od5kqZSwoBB1Zz	convenience-oriented	easy	6	6	3	5	6	6	5	5	5	5
97	R_6A1FWWhbedj6vvT	convenience-oriented	font	6	5	6	6	6	6	6	6	6	6
98	R_29V6iyf8SRoCJ4V	convenience-oriented	font	5	6	6	4	4	4	5	4	4	4
99	R_bOTYUNB6ncm8mCF	convenience-oriented	font	3	3	3	4	4	5	4	4	3	4
100	R_4OAB2NiBsNWJrOh	convenience-oriented	font	6	7	2	7	6	7	6	6	7	7
101	R_07cEXcShQIPq49	convenience-oriented	font	6	6	2	5	4	5	5	6	6	6
102	R_3RcLmNq4xIC6Z0N	convenience-oriented	font	3	4	2	6	5	5	6	6	5	6
103	R_aaS48ToqGSQsy9	convenience-oriented	font	5	5	3	5	5	4	5	5	5	5
104	R_cUWs93eVLQmMUd	convenience-oriented	font	6	6	4	6	6	6	5	6	6	6
105	R_bxSP2t0eXiy7a29	convenience-oriented	font	3	7	1	6	7	6	7	7	7	6
106	R_51gi3OBVwjwsg6x	convenience-oriented	font	6	5	5	4	4	5	5	6	5	5
107	R_6RI0qqLH9Gnyzb	convenience-oriented	font	7	7	1	7	7	7	7	7	7	7
108	R_00MZ10XxCooVfxz	convenience-oriented	font	6	6	4	6	6	6	6	6	6	6
109	R_3972ORk238k788Z	convenience-oriented	font	5	5	7	5	5	5	5	6	6	6
110	R_agA4J9k6GzP008d	convenience-oriented	font	6	5	2	7	6	5	6	5	6	5
111	R_0Cx77aQdaDEjWxD	convenience-oriented	font	6	5	6	5	3	5	6	5	6	5
112	R_9AzhjmC3qXYxYZ7	convenience-oriented	font	6	6	6	6	7	6	6	7	6	6
113	R_brT6FnMSTUkdscB	convenience-oriented	font	6	6	5	6	6	6	6	6	6	6
114	R_d6Elzo8Ck8a8xOl	convenience-oriented	font	6	6	3	5	6	5	6	6	5	6

115	R_6scsDvnKvoV6kjb	convenience-oriented	font	7	6	6	6	7	6	6	6	7	6
116	R_ekW5pXITMoVVv9z	convenience-oriented	font	5	4	3	4	5	6	5	4	5	4
117	R_1C82zz9EiTPXSiF	convenience-oriented	font	7	7	7	7	7	7	6	7	7	7
118	R_dp4qcFXOdywablz	convenience-oriented	font	3	4	4	3	4	3	3	3	4	3
119	R_0U7DKzTZKITyWHR	convenience-oriented	font	6	5	6	5	4	5	6	5	6	5
120	R_3qp9MndTyi6rdeR	convenience-oriented	font	4	7	1	7	7	7	7	7	7	7
121	R_cJeqU4irqYF5aoR	convenience-oriented	font	5	6	5	6	5	6	4	5	6	6
122	R_3xXVH44MfiBfE0t	convenience-oriented	font	5	6	2	6	5	6	6	5	6	6
123	R_d0amSY1a9GfYkzX	convenience-oriented	font	4	4	4	3	4	3	3	4	4	4
124	R_6AqLzDogfiPxSDz	convenience-oriented	font	7	7	7	7	1	7	7	7	7	7
125	R_ac94Ts8VUJ89paJ	convenience-oriented	font	6	5	5	6	6	6	7	7	7	7
126	R_6yAWxqWQ3ZhDr6Z	convenience-oriented	font	6	7	2	7	6	7	6	6	7	6
127	R_3fbdVRGdkWQxi9D	convenience-oriented	font	5	6	4	5	6	7	4	5	6	4
128	R_8eadAteZszxwfl1	convenience-oriented	font	7	6	3	5	6	5	4	6	6	5
129	R_5o0SnlvcLBGbsU5	convenience-oriented	font	6	6	6	5	3	3	6	6	5	5
130	R_1EWe2dKnSZfL5X	convenience-oriented	font	3	3	2	6	6	6	7	6	5	5
131	R_0BbnwNvOO6hzO6x	convenience-oriented	font	5	5	3	4	5	5	5	6	5	6
132	R_9T4HhR8983p6DB3	convenience-oriented	font	5	6	6	7	7	7	7	7	7	7

## Raw Data of Experiment 2-2

No	ID	condition	easy	convenient	complex®	secure	safe	protected	techadvance	good	favor	like
1	R_aY8KAyd0MhrBkup	Easy	7	7	7	7	7	7	7	7	7	7
2	R_00I1bKiReE6GuiN	Easy	5	4	3	6	5	4	6	6	5	6
3	R_4T3WhODLbwdrXT	Easy	6	6	3	5	5	5	7	6	1	1
4	R_3fqwOstqqVJprhz	Easy	7	7	6	6	6	6	6	6	6	6
5	R_80KwCIAWLMXJNhH	Easy	4	5	4	4	5	4	3	5	4	5
6	R_3kspXHD9s60lrp3	Easy	6	7	7	7	6	6	7	6	7	7
7	R_9F8In5j77fudYu9	Easy	5	5	3	5	5	6	5	5	5	4
8	R_0wCbhdqZVAofarr	Easy	5	4	4	4	5	4	4	4	4	4
9	R_1EWui8849s6lzBr	Easy	6	5	4	5	4	5	4	4	6	4
10	R_73weu6bIRLg69y5	Easy	4	6	4	4	3	2	5	4	3	6
11	R_b7xujn3nCKiiorr	Easy	5	4	3	4	3	4	5	4	3	4
12	R_bxVA4vEBrcGZVnD	Easy	6	6	5	6	6	6	6	6	2	2
13	R_9zyhileIHb39brn	Easy	6	5	6	4	4	4	5	7	6	7
14	R_cwMYxpPXtuvQ9eZ	Easy	6	7	6	6	6	6	7	7	6	7
15	R_0vm3b9lt7d2pJuB	Easy	6	6	4	5	4	4	6	6	6	6
16	R_08mDrbq3MyCAZHT	Easy	7	6	6	6	6	6	6	7	7	6
17	R_4SdHuYEukyQL99X	Easy	6	6	5	5	6	5	5	6	3	3
18	R_2ahNRUK6FBHrIx	Easy	4	4	4	4	4	3	3	4	4	3
19	R_e8Np8RSlyDgXerb	Easy	7	7	7	7	7	7	7	7	7	7
20	R_6JSnXA4kT0Fw7M9	Easy	6	6	2	7	6	7	7	7	6	7
21	R_0BWHelSO2jXF9Pf	Easy	6	7	3	6	6	6	7	7	6	6
22	R_ab2AiBBVJm4b2O9	Easy	6	5	4	3	3	3	6	5	5	5
23	R_0UoVIXQuzaPJNjz	Easy	4	5	4	3	4	4	3	4	3	4
24	R_dimlg1WkbQDN1kh	Easy	5	5	4	5	5	6	5	6	4	6
25	R_0p4tRYMALOj1r49	Easy	4	6	1	4	6	3	2	4	6	5
26	R_eflcKdYV1SZ5W6h	Easy	6	6	2	5	6	6	7	7	5	4
27	R_5u75UfBZNRlshOB	Easy	5	5	5	6	6	6	6	6	6	6
28	R_b3qY52WUkd1IsN	Easy	6	5	5	6	6	6	7	6	6	5
29	R_6mQWridtORkMB	Easy	4	3	7	6	7	4	3	6	5	2
30	R_8BzW0lz5nyvInK5	Easy	3	3	4	3	4	4	3	4	4	4
31	R_cN5FIWvGg64pJM9	Easy	7	6	6	6	5	6	7	6	6	6
32	R_egSsGTMOV99imzz	Easy	5	4	3	4	4	5	3	5	5	4
33	R_738tfTDAjgl79nn	TechTerm	7	7	7	7	7	7	7	7	7	7
34	R_3KLHIVeFDsSBIEEN	TechTerm	5	6	4	5	4	4	6	5	5	5
35	R_1Gju9EXAYkLkhol	TechTerm	7	7	7	7	4	7	7	7	7	7
36	R_0DtuyYsu2ERMDpr	TechTerm	7	7	7	6	7	6	6	7	7	7

37	R_9zwlqj4ynFQbEgd	TechTerm	6	6	2	6	6	6	6	6	6	6
38	R_899DEVDXgapCGs5	TechTerm	6	6	5	5	6	6	6	6	6	6
39	R_9GmzCzrrzZDUyOZ	TechTerm	5	5	4	6	5	5	6	4	3	3
40	R_6GqlduezsogrQLX	TechTerm	3	4	5	5	5	3	3	5	4	3
41	R_9oeWiv87K1iom69	TechTerm	5	5	3	6	6	6	6	5	3	3
42	R_080TwMOLs9fHHHD	TechTerm	7	7	3	5	5	5	6	6	6	6
43	R_cOsikASLJobumfT	TechTerm	5	4	3	4	5	4	5	5	4	5
44	R_4N765JGq7BzCOOJ	TechTerm	5	6	2	5	6	6	6	5	2	2
45	R_8epRHjyWJ6xxcCF	TechTerm	5	4	3	5	5	4	5	5	4	4
46	R_2hFWWfw40sqeNaR	TechTerm	6	5	5	6	5	5	6	6	5	6
47	R_3lnA7KuprbfFPYV	TechTerm	6	6	6	5	5	5	6	6	6	6
48	R_a3RMkaTWDsgUGwJ	TechTerm	7	6	3	5	6	5	6	5	6	6
49	R_5e2U62o5z4f6QAd	TechTerm	7	7	1	7	5	7	7	6	7	7
50	R_80mUeU9ieswne8B	TechTerm	4	4	4	6	6	6	7	6	7	7
51	R_5tAD12HN2Zm5ut	TechTerm	7	7	4	6	6	6	7	7	7	6
52	R_3F4kNspXaRrcCs5	TechTerm	6	6	6	5	5	5	6	6	6	6
53	R_9Lk5IKwDklhBeFD	TechTerm	7	7	7	5	5	5	5	5	5	5
54	R_d5agmFGK5ZhUPXf	TechTerm	6	5	3	6	6	5	5	6	6	7
55	R_5nI8pth6MgJPbzT	TechTerm	6	6	5	5	5	5	6	6	7	6
56	R_bpZKG73IIfvI6kR	TechTerm	5	6	4	5	5	4	6	5	6	6
57	R_etW8tSQenesikU5	TechTerm	5	6	5	6	6	6	5	5	6	5
58	R_bsmjQE5hD70TFUV	TechTerm	6	6	4	6	6	5	6	5	6	6
59	R_bqtp1mBM8Q9zhIN	TechTerm	7	6	1	6	7	6	7	6	7	7
60	R_3ZTQlj3z1MauHFb	TechTerm	5	5	6	5	5	5	5	5	2	2
61	R_8eTbyLu0qHvtjzD	TechTerm	6	6	3	6	7	6	6	7	6	6
62	R_eal2ene4OzVInCR	TechTerm	6	6	7	5	5	6	7	6	6	6
63	R_23uXe3sxjl3hiXX	TechTerm	6	6	6	5	5	6	7	6	6	6
64	R_b1pgkUWpBNzPYWJ	TechTerm	7	7	5	6	7	7	6	6	6	5
65	R_8CShG2uX2QlvKIF	TechTerm	7	7	1	7	7	7	7	7	7	7
66	R_9AEYSeIDDvwOCMd	TechTerm	7	7	2	7	5	6	4	5	7	4
67	R_2hjRZ8mTNXqYmUd	TechTerm	5	5	3	5	6	5	5	6	6	7

## Raw Data of Experiment 2-3

No	ID	condition	Easy	Convenient	Complex	Secure	Safe	Protected	Tech Advanced	Good	Favor	Like
1	R_0lBqnkaeeZU04iV	No Question	6	5	2	4	4	5	4	5	4	4
2	R_6zgZp60F8UZTs9	No Question	5	5	3	3	2	3	2	5	3	4
3	R_3yfyHkEVJ6V27j	No Question	5	6	3	6	5	6	6	6	5	6
4	R_3JGplHf7JYc42FL	No Question	6	5	3	5	4	4	4	5	5	6
5	R_0w75kof1PTICPMp	No Question	7	6	2	3	3	3	4	5	5	5
6	R_b8xebkRix2wUrXf	No Question	5	5	5	6	4	4	5	5	5	4
7	R_4UfEZP2xV0zWSGh	No Question	5	4	5	4	5	5	5	7	6	7
8	R_eKzno56mb35Najr	No Question	6	6	2	2	2	2	3	4	4	4
9	R_bpSwSzStL4Fazb	No Question	4	5	2	5	5	4	5	6	4	4
10	R_0GMzdqLac95oghT	No Question	4	4	5	3	3	2	3	6	4	3
11	R_7R4zYvaxHULe5lr	No Question	6	5	6	5	6	5	6	5	4	5
12	R_cYorvqmeqja7elL	No Question	7	6	3	3	4	4	5	6	6	7
13	R_3QzrUKtGtrM86h	No Question	2	2	4	5	4	3	5	2	3	4
14	R_74cXKO6cO9scwM5	No Question	6	7	6	4	4	4	4	7	6	6
15	R_bOvhlPJDQjKYFCd	No Question	6	5	6	6	3	5	6	6	5	6
16	R_baq8YnKCdhspJGd	No Question	6	6	3	6	6	7	6	7	6	7
17	R_23NKdeAODUF8zqt	No Question	5	5	3	6	5	6	5	6	5	6
18	R_067GIQa6A6Ffj	No Question	6	5	6	4	6	7	7	5	3	7
19	R_72MKvWI09P3aNHn	No Question	7	7	1	4	4	4	3	5	5	5
20	R_0vo7Q7M5xo4oZfL	No Question	5	6	6	4	5	6	5	6	6	6
21	R_9FVgnFJ9fKGJmrv	No Question	5	5	5	6	5	5	5	6	6	6
22	R_2aFAnkXo7g5dahn	No Question	5	5	4	5	6	5	6	5	6	5
23	R_1HUECwqbqHFetIF	No Question	7	7	1	1	5	7	7	7	7	7
24	R_dfZZOPAzaTBkD5z	No Question	6	7	1	7	7	7	7	7	1	7
25	R_00EaVUx1BtdqOst	No Question	6	5	3	2	2	2	2	3	3	3
26	R_2hiHF6taDgUraa9	No Question	5	5	2	4	3	3	3	5	6	5
27	R_6rQkoZeNrD04wpT	No Question	6	5	2	2	2	2	2	4	4	4
28	R_3JmY4PKyunaUptr	No Question	6	6	7	6	6	5	6	5	6	6
29	R_01ZIGsCRJCx52gR	No Question	5	6	5	5	5	6	7	6	6	6
30	R_81cSAo2o1HOHDfv	No Question	7	5	2	4	4	5	6	6	6	5
31	R_eKYAGzY74Q1el73	No Question	2	3	2	3	2	2	3	2	2	3
32	R_78PuNRla8aUglNj	No Question	4	3	6	4	2	5	6	3	4	5
33	R_3KoV5qJKAzAXqrb	No Question	6	6	2	6	6	6	5	5	6	2
34	R_77MLZRjzaki9peB	No Question	7	7	1	1	1	1	4	6	7	6
35	R_etuYI5MVvO7W3yt	No Question	5	4	5	6	5	4	5	4	5	6
36	R_0CWaBYRuavQiguN	No Question	5	5	5	6	6	6	6	3	4	4

37	R_eUILLUDJbAKh06S9	No Question	6	6	2	6	1	2	2	5	6	3
38	R_bc3DOUL9jVXsGLb	No Question	5	7	6	4	3	4	6	6	5	6
39	R_7V8xvKjCNli3j0h	No Question	3	4	4	2	4	2	3	4	4	3
40	R_0J5JLKqDduNp2J	No Question	5	6	2	5	5	5	6	5	6	6
41	R_6ycRpI0ywemKsTj	No Question	4	4	5	5	6	5	5	5	6	5
42	R_dcnhLeXML0RW473	Two Questions	3	3	5	6	5	5	4	7	7	7
43	R_3vNaGHtuY3IWCwt	Two Questions	4	3	6	1	5	7	5	5	6	5
44	R_6gHjPld7jKmbOJ	Two Questions	7	7	5	6	6	5	5	7	7	7
45	R_6EwuTXHrs4N1EKV	Two Questions	6	6	2	5	5	6	6	6	6	6
46	R_2i3wBKThLhzxORv	Two Questions	6	7	1	7	7	7	7	7	7	7
47	R_1Y2nuoEfm4WQQMI	Two Questions	6	5	3	5	7	6	5	7	6	6
48	R_29Wcli2KtlBKpWl	Two Questions	5	6	4	5	5	6	5	6	6	5
49	R_8lgwQ72M7eetAix	Two Questions	4	5	4	4	3	5	4	5	4	5
50	R_9nVnGej2NPZASaN	Two Questions	5	5	2	5	4	5	6	6	6	6
51	R_6YexW19G60pUjL7	Two Questions	5	6	5	4	5	4	5	4	5	4
52	R_3ZTjiAolakUaSqN	Two Questions	6	6	5	7	5	5	5	6	6	6
53	R_d0fWybm5CZBB5Tn	Two Questions	6	6	2	6	7	6	5	7	7	7
54	R_3HPpjOprRqVnF	Two Questions	4	5	2	7	6	6	6	6	6	5
55	R_bgvmT2bhuyZWVql	Two Questions	5	5	4	5	4	5	3	4	4	5
56	R_805Q0I4GMntsnLT	Two Questions	5	4	2	6	6	6	5	6	6	6
57	R_799JjGheKHlUoxD	Two Questions	5	5	3	4	4	4	4	4	5	4
58	R_4lQgtVInONQIMbb	Two Questions	6	7	1	6	6	6	6	7	6	4
59	R_ex1lhzDYSziEG5D	Two Questions	7	7	1	7	7	7	7	7	7	7
60	R_5pdxkTBEA19ZBJ3	Two Questions	4	4	5	5	6	4	4	4	4	7
61	R_3PFUWlh0Bj8Hr	Two Questions	7	7	1	7	7	7	7	7	7	7
62	R_5cFv29UBD69pOd	Two Questions	5	5	5	5	5	5	5	6	5	4
63	R_9sEiaWuuqn3KhcJ	Two Questions	5	5	4	4	5	5	4	6	5	5
64	R_bwIPfayKULbCWPz	Two Questions	6	5	2	6	5	7	6	6	6	7
65	R_eb8AtwNA1165y8R	Two Questions	6	6	5	7	5	6	5	6	6	7
66	R_2ug4EZH2zWosavX	Two Questions	5	6	5	4	4	5	5	5	5	4
67	R_9SjxW6UP0RlXAtn	Two Questions	6	6	1	6	5	7	6	7	6	6
68	R_3vXqZ2Pk9hemnel	Two Questions	6	5	5	6	6	4	5	5	6	6
69	R_0rfxKN9XZUHyQV7	Two Questions	7	7	7	7	7	7	7	7	7	7
70	R_0iGjAvslrXkRTUx	Two Questions	4	4	2	4	4	4	5	5	5	4
71	R_1FCHRMG0bykFL49	Two Questions	5	5	2	5	5	5	6	5	5	2
72	R_1M7ExG3hNCZEIMB	Two Questions	7	7	2	4	2	6	6	7	7	4
73	R_38UHSUj05i86dbT	Two Questions	5	4	3	5	6	5	3	6	5	4
74	R_3ObLS0vW8fH5UPz	Two Questions	5	5	5	4	4	5	4	4	4	4
75	R_87YGmbaYJGyR8h	Two Questions	5	5	2	6	5	6	5	5	5	6

76	R_8k5BA52hSpCx8zP	Two Questions	5	6	5	5	4	5	6	6	5	5
77	R_bl7o91JDoVCz3ud	Two Questions	3	4	2	4	5	4	5	4	5	5
78	R_9SQdK8jKvu23WcJ	Seven Questions	5	5	4	5	4	6	6	5	5	4
79	R_8iigU287gOXYAL3	Seven Questions	6	6	2	5	5	5	5	7	7	7
80	R_9MOxdW7FvnJQ0Lj	Seven Questions	1	2	6	7	7	4	4	5	3	3
81	R_9F9VguJgfBWuLD7	Seven Questions	5	5	4	6	6	6	6	6	6	6
82	R_6sdDOWeDQh5XqB	Seven Questions	5	4	5	6	6	6	6	6	6	6
83	R_5BTzcZ01BrTaykB	Seven Questions	7	7	2	5	5	5	6	5	6	6
84	R_0wElfKObB72Xzv	Seven Questions	5	6	5	6	5	7	6	5	6	4
85	R_bvWwtHbGCTQ5CQt	Seven Questions	5	5	3	4	4	5	5	5	5	5
86	R_6J8Eso4xuwTGSf	Seven Questions	4	3	6	5	2	3	5	5	4	5
87	R_d4QdKc6RxGyquMt	Seven Questions	7	6	7	7	6	7	6	7	7	6
88	R_9TBI4yPLKSnkUFD	Seven Questions	5	6	1	5	6	5	5	5	6	5
89	R_bmhRi74aaAToxIF	Seven Questions	7	5	6	4	7	5	6	4	6	5
90	R_1GmeJSxYN20VFOd	Seven Questions	7	7	3	6	5	5	6	5	6	7
91	R_exjhJz7no0TUXRj	Seven Questions	6	6	5	5	6	5	6	2	3	2
92	R_bKKVQegoRg9nK4Z	Seven Questions	3	4	4	6	6	5	4	5	4	5
93	R_5yDtgpuQPuYT2Nn	Seven Questions	4	5	5	4	4	4	4	5	4	4
94	R_6FD8X9W6Nuf4FW5	Seven Questions	4	4	5	7	7	7	5	7	6	6
95	R_cLPsVRhe0j9pdyJ	Seven Questions	6	7	5	4	7	6	5	5	7	4
96	R_ODGJYJvECruTfHn	Seven Questions	5	4	3	6	5	4	4	4	4	6
97	R_b8H2trWrXt25L	Seven Questions	5	6	5	5	5	6	6	6	5	5
98	R_3x7e14VW36ljdj	Seven Questions	6	6	6	6	5	6	6	7	6	7
99	R_2gkp0TW7VEVy5rD	Seven Questions	3	1	6	5	5	4	3	6	5	5
100	R_0NvKWjogZDxjqlt	Seven Questions	6	6	5	5	6	7	6	6	5	5
101	R_b7WKThO1kxWo1bn	Seven Questions	6	5	6	5	6	5	6	6	6	5
102	R_3t1BFPcJTdkB0Vf	Seven Questions	4	3	3	4	3	4	5	4	4	5
103	R_1yTLy4ueWZKAglf	Seven Questions	5	3	5	4	4	4	4	5	4	2
104	R_20j5edAlnOUbhaJ	Seven Questions	5	4	4	3	6	5	4	5	4	3
105	R_aXX0JydSFLN6NVP	Seven Questions	6	6	6	6	5	5	6	6	7	7
106	R_5A1buMcDuefePqJ	Seven Questions	4	4	4	4	4	4	4	4	4	4
107	R_6kVfKJltypRzhUp	Seven Questions	5	4	5	4	5	4	5	5	5	6
108	R_4HkB3ObBboq5ioR	Seven Questions	3	4	4	3	4	4	4	5	3	4
109	R_dcoRj6al0TkjGbX	Seven Questions	6	6	2	5	4	4	5	5	6	6
110	R_8wgH3mhHlx3UQe1	Seven Questions	7	7	7	7	6	6	6	6	6	7
111	R_erkMjWdOsX5MP3f	Seven Questions	6	6	3	4	4	5	4	5	6	5
112	R_esabRYTRia1BNLT	Seven Questions	5	6	2	5	5	5	5	6	2	2
113	R_7VyYN7252BOUK85	Seven Questions	4	4	4	5	5	5	4	5	5	5
114	R_6Wmh2JKEqLFKEjb	Seven Questions	4	4	4	2	2	2	5	2	2	2

115	R_8jNPgLRCaPvwuTH	Seven Questions	6	6	2	6	5	5	6	6	6	6
-----	-------------------	-----------------	---	---	---	---	---	---	---	---	---	---

## Raw Data of Experiment 2-4

No	ID	condition	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Easy	Convenient	Complex	Secure	Safe	Protected	Tech Advanced	Good	Favor	Like
1	R_40Vx l7z2lD RM3QN	Two Questions	First pets name	First school attended						4	4	4	5	4	5	4	7	7	7
2	R_1lX efaNWa 30a4xD	Two Questions	What is the model of your first car?	Who is your favorite teacher?						4	4	3	5	5	3	3	4	4	4
3	R_9HO DyNuF owxk6e l	Two Questions	what is your pet name.	what is the name of your first love.						5	5	4	5	4	4	5	6	6	5
4	R_9yvv 3KiMh S1mQX b	Two Questions	what's your best friend's last name?	what's your uncle's first name?						6	5	2	4	4	4	4	5	5	5
5	R_8CF P4GdV vh7OK X3	Two Questions	my lover name?	my wife's pet name?						5	4	5	4	5	5	4	6	5	6
6	R_bsge MjXntX YfVXL	Two Questions	what is ur pet name	what is your favorite teacher name						7	7	5	6	6	6	6	7	7	7
7	R_8FV 3PP7Zn qFVEYl	Two Questions	What street did I grow up on?	Where did I graduate high school?						3	3	5	5	6	5	6	4	5	5
8	R_3dVz 0Z9nCz TrQFf	Two Questions	What is my mother first name?	what is my father first name?						4	7	4	6	5	6	4	6	4	5

9	R_7agJ WlryaK dphkx	Two Questions	What is your favorite color	What is your father's middle name							4	6	6	5	4	4	4	5	6	5
10	R_9Tu KEClm eYueGg d	Two Questions	Your first pet name?	Your favourite hollywo ord actor?							5	6	6	5	6	5	5	6	5	6
11	R_9shm kIDkdj XyxNz	Two Questions	what is your childhood name	what is your favourite fruit							6	6	2	6	6	6	6	7	6	7
12	R_bNN xyoJva QTaGF	Two Questions	what is your favorite game	what is your nickname							6	6	1	6	6	6	6	6	6	6
13	R_8lR Rd7S1l vDkJO5	Two Questions	What was your best friend's name as a child?	What's the name of your favorite actor?							5	4	3	2	2	2	3	5	5	4
14	R_8A4n rELnY2 iCdzD	Two Questions	my father birth place	mother birth place							7	6	4	5	4	4	5	7	4	6
15	R_dm1 dlsWhP viaEoR	Two Questions	Name of my first girlfriend	My dream job							6	6	2	5	4	5	6	5	7	6
16	R_0B9 XbHeen tCv4mp	Two Questions	What is favorite icecream flavor?	What is the name of my grandm other?							7	6	1	6	6	6	7	7	6	7
17	R_eDQ 59LiK8 AWNJ Qx	Two Questions	My Birth Place.	My Date of Birth							6	5	2	5	4	4	4	5	5	5
18	R_cYIV ZDnQl zr8emF	Two Questions	Favourite sports player	Name of first school							4	5	2	3	3	4	3	5	6	4

19	R_79Bu Z8sWC CtqFUH	Two Questions	My Favourite Food?	My Best Friend Name?							7	6	2	5	2	6	5	7	6	5
20	R_9Ahl 0ZaMA id1FEF	Two Questions	what is your favorite color	what is the name of your best friend							2	3	2	3	6	5	7	6	3	3
21	R_dmah 1NzgAp w3yFj	Two Questions	what is my pet's name	what is my younger brother's middle name?							6	6	2	5	5	4	3	5	5	5
22	R_bIag uBKgD Selqux	Two Questions	favorite book	favorite teacher							4	4	4	5	5	5	5	4	4	4
23	R_3Ua1 zSa6At MLRC1	Two Questions	Place of birth. ?	Who is your 1st teacher ?							6	5	1	6	6	6	7	7	6	7
24	R_6x3O jDj4Iz sBcp	Two Questions	Marca laptop	marca telefon							6	6	4	5	4	5	5	6	6	6
25	R_6Gc3 eyvaIM NV7j7	Two Questions	Who was your favorite musician?	What was your favorite song?							5	5	5	5	5	5	5	5	5	5
26	R_0vR3 ZITrwq fnVUp	Two Questions	what is your first baby name?	what is your mom in law name?							7	5	6	6	6	5	6	6	6	6
27	R_b9IZ Occ7edl Xfet	Two Questions	When was my first date?	What is my favorite colour?							6	6	3	4	4	5	5	5	5	5
28	R_daPP cE9ALf 92gCN	Two Questions	my name	my place							4	3	5	5	4	5	6	5	6	5
29	R_1YTs v0Nv0 YY0u3j	Two Questions	who was your childhood hero?	what is your pet name?							6	5	2	6	6	5	6	6	6	5

30	R_8pM xeuZyB S9rgDr	Two Questions	What is your favourite Book ?	Where do you live ?							5	6	6	6	2	6	4	5	2	2
31	R_8FYa EX1pBi yguvV	Two Questions	gopal	pushpa							6	4	3	5	5	4	6	5	4	6
32	R_3mJx Sp9Qq RuJxIj	Two Questions	What's my mother's maiden name?	What's my uncle's name?							7	7	4	6	4	4	4	7	7	7
33	R_bIKF Yp33oZ vyMex	Two Questions	What is your mother's grandson name?	What is your father's grandson name?							5	5	5	5	5	5	5	5	5	5
34	R_0Cxc 2KJj7k3 4ekB	Two Questions	what is your pets name?	what is your best friend's name?							4	4	4	4	4	5	4	5	4	5
35	R_3JEE 4eZfhq Av9I3	Two Questions	MOM'S NAME	FAVORITE SPOT							6	5	5	6	5	5	6	5	5	5
36	R_bsm1 Vai00ps A7L7	Seven Questions	What is the name of the high school you graduated from?	What is the name of your first pet?	Who is your favorite sports team?	Where is the first place you worked?	What is your favorite food?	What is your brand of your current car?	What is your favorite movie?		5	5	4	6	5	5	5	6	5	5
37	R_cYn3 Y7wK mmZcT kx	Seven Questions	what is your favourite food in childhood?	what is your favorite games during school days?	what is your nick name in your school?	what is your best friend's name?	which is your hometown?	How did you go to school?	who is elder brother?		6	6	6	6	6	5	6	6	5	6

38	R_0ILT BjkRYll dzYF	Seven Questions	What is your car/bike NO. ?	Who is your favourite actor ?	What is your pat name ?	What is your first teach er's name ?	What is your first school name ?	Who is your favourite international hero ?	Who is your favourite cricket er ?	6	7	1	4	3	2	2	5	5	3
39	R_4Zx DLpHl 5FLHy B	Seven Questions	what is your best teacher name ?	what is your pet name ?	what is your favourite movie name?	Who is your best hero ?	what is your best colour ?	What is the best tourist place you like ?	what is your weight ?	5	5	3	6	6	5	5	6	6	6
40	R_2e0l hlqESC ufacd	Seven Questions	A3HBQMBW 7XGZUM	MALE	PASS WORD	E - MAIL	DATE OF BIRTH	AGE	WORK ER	6	7	6	5	6	6	6	6	7	6
41	R_6XM lIk6fF mMFL	Seven Questions	First pet name	First school attende d	Place of honey moon	Colle ge attende d	First bestfri ends name	favorit e city	favorit e color	6	6	2	5	5	5	5	5	5	5
42	R_393q RcgbS msJQV	Seven Questions	what is your name?	what is your father name?	what is your mother name?	are you marri ed?	whats your father ?	whats your mother ?	Do you have bother s or sisters ?	7	7	1	7	7	7	7	7	7	7
43	R_aVG CvLoLr eCGw3 X	Seven Questions	What is your mother name?	What is your pet animal?	What is your first school?	What is your first child name ?	First teache r name ?	What is your pet name?	What is your first phone numb ers?	7	7	7	7	7	7	7	7	7	7
44	R_43pw nvxpH UhxVb L	Seven Questions	what is your mother name	what is your mobile no	what is your nickna me	who is your favourite anim al	who is your favourite teache r	which actor is your most favourite	what you like the most	6	6	2	5	5	6	6	5	5	6
45	R_315u 7iVAux dfjep	Seven Questions	childhood friend name	mother middle name	favorite color	Neph ew name	last 4 digit mobil e numbe r	highest qualifi cation	favorit e game	7	7	5	6	4	6	5	7	7	7
46	R_9ozE lBRlkj DQ8Z	Seven Questions	first school	first car	first job	child hood addre ss	nieces birthd ay	place i hate	favorit e color	5	4	5	6	4	3	3	4	4	4
47	R_bdxy R97cID w2xlr	Seven Questions	my pet name	my mother name	my father name	my sister name	my best friend	my girl friend	my schoo l name	5	4	5	4	4	5	4	6	5	4

48	R_dcA1 eFICw1 ykBbb	Seven Questions	mother name	father name	brother name	zip code	old password	mobile number	company	6	6	6	5	6	5	6	5	4	5
49	R_38IE U7Q8X U1o6W x	Seven Questions	my mother	my father	my friend	my sister	my brother	my son	my daughter	6	5	4	5	5	6	7	6	5	6
50	R_6hyjl QSluhY zW2p	Seven Questions	what is your favorite color	what you like most	which is your best place	who is your role model	best food	favorite actor	favorite movie	6	6	6	6	6	6	6	6	6	6
51	R_7X8 SaodFrt cucqp	Seven Questions	what is your name	what is your dog name	what is your lover name	what is your dad name	what is your mother name	what is your brother name	what is your sister name	5	6	3	6	5	4	6	5	5	4
52	R_dnhD Xkemvs 1Yz4h	Seven Questions	What is your fathers middle name?	Name of middle school?	What was your first pet's name?	Where were you born?	What is your mother's maiden name?	High school mascot?	College mascot?	6	7	3	6	6	6	6	6	6	6
53	R_8dBb V9xYb O9CoB	Seven Questions	What is your first school name?	What is name of your best friend?	What is your date of birth?	What is your pet's name?	What is your mom's maiden name?	What is your father's maiden name?	What is your village name?	6	6	6	6	5	6	6	6	5	6
54	R_d6hL chQmv 6U3JVr	Seven Questions	what is your mother name	what is your father name	what is your brother name	what is your sister name	what is your pet name	what is your diary name	what is your friend name	5	4	3	4	4	4	4	5	4	5
55	R_9sG8 SmlWx wGwJ3	Seven Questions	your pet's name?	your birth place?	your nick name?	your first car's name?	name of your first love?	first name of your dad?	your first school?	6	5	6	7	5	6	6	6	7	6
56	R_3V3s Sx87kl OiME5	Seven Questions	gender	color	school	mother	maiden	father	wwe	3	5	1	6	2	4	5	5	4	6
57	R_4U13 Ehkmm 54fG73	Seven Questions	what is your pet name?	what's colour you need?	what is your date of birth?	who is your best friend?	when is your child birthday?	what is your mother tongue?	what's color your favorite?	5	6	5	6	5	5	6	3	4	3
58	R_72M GFxnh R1gGM B	Seven Questions	What was your first pet name?	What was the name of your first school?	What is your favorite game?	What is your favorite tv show?	What is your favorite country?	Who is your favorite artist?	What is your favorite celebrity?	5	5	5	6	6	6	5	6	6	6

59	R_eeBZ sVuRD q2FNL7	Seven Questions	what is your favourite drink?	what is your pet's name?	where do you want to spend a week vacation?	what is your native language?	who is your favourite cricket player?	what is your best friend's name?	who is your first lover?	3	4	4	5	5	5	4	4	4	3
60	R_bygH slkj8ah VKrX	Seven Questions	name of pet	name of school	name of the city you stay in	mothers maiden name	what is the day of your birth	year you were born	place where you were born	5	5	5	5	4	4	5	5	4	5
61	R_5zM o6ByUt 3KT3e9	Seven Questions	your pet's name	your favourite colour	best movies	best friend	best place	favourite drink	favourite food	6	6	4	6	6	6	7	7	6	6
62	R_8uj8 8OfEw Wv8C9	Seven Questions	mother name	date of birth	bike registration number	lover name	blood group	college name	home town	6	7	7	6	5	6	7	2	3	1
63	R_bNH T0kbR9 NQnq B	Seven Questions	what is your first girlfriends name?	who is your favorite cousin?	what is your first mobile number?	what is your favorite past time?	what is your pets name?	which is your favorite dish?	what is your friends name who works at post office?	4	4	2	6	4	4	4	3	3	4
64	R_bvYr J3mJ8z MyRT	Seven Questions	what is your height	what is your complexion	what is your first language	where do you live	what do you like in food	what is your education status	what is your marital status	7	5	4	6	6	5	5	4	3	3
65	R_6Eao y5wWy ER86K V	Seven Questions	What is your first phone number?	What is your mother's maiden name?	What is your favorite pet?	What is your spouse's name?	What is the number of your library card?	What is your father's maiden name?	What is your car number?	5	5	5	5	5	5	6	5	5	4

## Raw Data of Experiment 3-1

No	ID	condition	easy	convenient	complex	secure	safe	protected	good	favor	like	authentic1	authentic2	authentic3	authentic4	integrity1	integrity2	integrity3
1	R_3mJsGLCFiBwmoOR	single	7	7	1	3	2	2	4	4	4							
2	R_5ikiilvb3bj3ql	single	5	6	3	4	4	5	5	6	2							
3	R_1ZignN8wBLPUk85	single	6	7	3	5	5	5	6	6	6							
4	R_cAZFof6ehAyGXeR	single	7	7	1	7	7	7	7	7	7							
5	R_8cBugNfcjRTcsip	single	7	6	1	4	4	4	5	4	4							
6	R_0ksaXzKbvCQFOMR	single	7	7	1	7	6	6	7	7	7							
7	R_9B6nR0myk2wbXlp	single	7	7	7	7	4	4	5	5	6							
8	R_6uG9Cisg1a3aHr	single	7	6	1	2	2	7	5	5	4							
9	R_9FTgFZfv6wmSMvz	single	6	6	6	7	6	6	6	5	5							
10	R_74KquM6HOSRwbKR	single	7	6	1	5	6	6	7	6	6							
11	R_agjMu1QvNPxapp3	single	7	7	1	5	5	4	5	6	5							
12	R_1LnCNzT2dlqNZyd	single	7	7	7	7	7	7	7	1	1							
13	R_9WVlarEzjG73YV	single	7	6	6	7	7	6	7	7	7							
14	R_cd7WXBH6TBWUrb	single	7	6	2	6	5	4	6	2	2							
15	R_acad8hQaEvCXZit	single	4	5	6	5	6	5	6	6	6							
16	R_57m4lq6wzqlTKB	single	7	7	1	4	4	4	5	7	7							
17	R_0qSbZj6zi8m2Xo9	single	6	6	5	6	4	5	4	5	5							
18	R_2hox75zldPLkS0d	single	6	6	6	7	7	7	7	6	6							
19	R_8nWfY2RrcKck77	single	7	6	1	4	2	2	3	2	2							
20	R_cZ6pPaQ7NxTD7O5	single	6	6	2	4	4	4	5	5	5							
21	R_2leSEiZarSli mFf	single	7	7	1	4	4	4	5	5	5							
22	R_0IABFeF13dAeMXr	single	7	7	7	6	7	7	7	6	6							
23	R_9vHM5O7R2Qgfnff	single	5	5	5	5	5	5	5	6	6							
24	R_0vVnkgCuWm70nPL	single	4	5	4	5	6	5	5	5	7							
25	R_3WvZXKnaVEiI3BH	single	7	5	6	5	7	5	7	5	5							
26	R_6kU3U7DglnbAfk	single	6	6	6	6	6	6	6	6	6							
27	R_bp1dmUNRUzHRqqV	single	7	6	6	7	5	5	6	7	6							
28	R_ahkUjxqoHaKUTiZ	single	7	7	2	7	6	7	7	7	7							
29	R_783hl7URvvhKyeV	single	6	6	2	5	5	5	6	6	6							
30	R_5alVyTmaHfl5DuJ	single	6	5	4	3	2	4	6	5	4							
31	R_788ECKwe8aJVk8d	single	7	7	7	2	1	3	6	7	7							
32	R_elmmihw1zptL9fT	single	6	5	3	6	5	6	6	5	6							
33	R_8wvAA4I22RXFAID	single	7	7	2	6	5	4	6	6	6							
34	R_b8TosyJmEeoboyh	single	7	7	1	7	6	6	7	6	7							
35	R_bxe1t2RefRbf3vL	single	5	5	5	5	3	4	5	5	5							
36	R_6yfZYyEsUMQ9cAR	single	7	7	1	6	5	6	7	7	7							

37	R_bDRgzq8oo0f7wAB	single	7	6	2	5	4	4	6	6	6							
38	R_aVm3tSIF8o87ngh	Twice with debiasing	5	5	3	5	5	5	5	5	5	5	5	5	5	5	5	5
39	R_4S76d0Xa6jgUSN	Twice with debiasing	7	7	1	6	6	6	7	7	6	6	6	7	6	6	5	6
40	R_781Y0kDfgU1wCJ7	Twice with debiasing	4	6	5	4	5	4	6	5	4	5	4	5	6	5	4	4
41	R_6zpTrtyAtiAgbd3	Twice with debiasing	4	5	3	5	5	5	5	6	6	5	6	5	5	5	4	4
42	R_eKyfQ7aPd3VwMPb	Twice with debiasing	6	5	2	5	5	5	6	6	6	5	6	5	4	5	5	5
43	R_7PsMpVYdPH14nAN	Twice with debiasing	4	7	4	7	4	7	6	5	4	5	4	6	3	2	7	7
44	R_cTjYOB5qut4ZQ4l	Twice with debiasing	7	7	1	4	4	4	5	5	4	4	4	3	7	5	6	5
45	R_7QglnW9ahJSyVv	Twice with debiasing	5	6	3	5	6	5	6	6	5	6	4	5	6	6	4	6
46	R_bjglm3A2RV PnD3D	Twice with debiasing	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
47	R_2mDKcL2XI OvNST3	Twice with debiasing	7	7	1	7	7	7	7	7	7	7	7	7	6	7	7	6
48	R_1TVTeIbY1N4ZDZX	Twice with debiasing	5	6	2	6	6	6	6	6	7	6	6	6	2	6	6	6
49	R_3KqGf9iyaXw8GY5	Twice with debiasing	6	6	5	6	6	6	7	7	7	6	6	6	2	6	6	6
50	R_8l0rqUe5hYpbePb	Twice with debiasing	7	7	1	6	6	6	7	7	7	6	6	6	2	6	6	6
51	R_deHmWBeSr7DhRmB	Twice with debiasing	4	5	6	7	6	6	7	7	6	4	5	5	6	5	5	6
52	R_6KUUNDQ6HzdLK2F	Twice with debiasing	5	4	4	5	4	5	5	4	5	4	5	4	5	3	5	3
53	R_7TIq8zF81qEkgf	Twice with debiasing	6	6	2	6	6	6	6	6	6	6	6	6	2	6	6	6
54	R_3dhrtYTVuX6FZH	Twice with debiasing	6	6	1	6	6	6	7	6	6	5	5	6	1	6	6	6
55	R_1WYRRQ4h73clbwn	Twice with debiasing	6	5	7	5	6	7	7	4	5	5	6	5	4	5	4	7
56	R_e58RIFumg5buZsV	Twice with debiasing	6	6	1	6	6	6	6	6	6	6	6	6	1	6	6	6
57	R_cTuqsj9awQZNFQh	Twice with debiasing	7	6	1	6	6	6	6	7	6	6	6	6	1	6	7	6
58	R_8np3IPHSCAaRSSN	Twice with debiasing	5	4	5	3	5	5	4	5	4	5	4	5	3	5	3	5
59	R_41NSrYWwuZ4YnxX	Twice with debiasing	7	7	6	6	7	7	7	5	5	7	6	6	2	7	6	6
60	R_eFH17BfEk8ReyQl	Twice with debiasing	5	5	2	6	6	6	6	6	6	5	5	5	5	5	5	5
61	R_eYf8VBmAtqE2gXr	Twice with debiasing	3	3	5	4	4	4	4	4	4	4	4	4	4	4	4	4
62	R_9B7WnjlbKUjlsN	Twice with debiasing	6	6	6	7	6	6	7	5	6	5	6	5	6	6	7	6
63	R_7WHd9pFnrBHkyZn	Twice with debiasing	7	5	1	5	3	5	6	6	7	3	4	5	4	3	4	4
64	R_0MnvZp1XS83Z53	Twice with debiasing	6	6	1	6	5	6	6	6	5	5	6	6	1	6	6	6
65	R_8bM6DKigsOhXH1P	Twice with debiasing	3	5	4	5	3	4	5	5	3	4	3	5	4	5	4	3
66	R_bxUOLVqQxAyaRvL	Twice with debiasing	5	6	6	5	5	5	6	6	5	5	4	5	6	5	5	4
67	R_0uCWWeZsucdW7oF	Twice with debiasing	4	3	6	4	3	5	3	4	5	4	2	4	3	3	3	5
68	R_8qugy5ik3dqkNKd	Twice with debiasing	6	7	6	6	7	6	7	6	7	6	5	6	6	5	6	6
69	R_3myPdMnLe9PUgVT	Twice with debiasing	6	5	2	6	3	5	6	6	6	6	5	5	5	6	5	6
70	R_1XiQkMpNq1bMHf	Twice with debiasing	6	5	6	6	5	6	6	6	6	5	6	4	6	5	4	6
71	R_8HsuB5BAgRHK5i5	Twice with debiasing	5	5	3	4	5	4	4	4	4	4	4	4	2	4	4	4
72	R_37Rno1aX2EbZnNj	Twice with debiasing	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5
73	R_ez0jCWtrFd0XgDr	Twice with debiasing	7	7	1	6	5	6	7	7	7	6	6	6	2	6	6	6

## Raw Data of Experiment 3-2

No	ID	Fluency	Description	easy	convenient	complex®	secure	safe	protected	techadvance	good	favor	like
1	R_b3FHj18XjX0n2ER	easy	security-oriented	6	6	3	5	6	6	6	7	6	6
2	R_0eJns1zrUVE1et	easy	security-oriented	6	7	2	5	6	7	6	5	5	6
3	R_czKAZ4EeDxtTzj	easy	security-oriented	5	3	3	4	4	5	5	5	4	5
4	R_bdSXpzhPBd8Opf	easy	security-oriented	6	6	3	7	5	6	7	6	5	6
5	R_cwpKAGqTgzE9HBr	easy	security-oriented	6	5	6	6	5	5	6	6	6	6
6	R_3KKYYbHgFMjmvb	easy	security-oriented	2	3	6	2	5	4	6	5	5	3
7	R_8GlXbGN1w0sexYV	easy	security-oriented	7	7	7	7	7	7	7	7	7	7
8	R_8ellMTyOIOoZbn	easy	security-oriented	7	6	7	7	7	7	7	7	7	6
9	R_02muk8ZR38gpWUB	easy	security-oriented	5	5	4	4	1	2	6	7	7	7
10	R_1XMuh4jCNmHoEt	easy	security-oriented	5	6	4	5	6	5	6	5	6	6
11	R_dilTJDebTbjYrP	easy	security-oriented	5	6	2	5	5	6	6	6	5	6
12	R_0J4zpWrxDKED8Md	easy	security-oriented	6	7	5	6	7	6	6	6	6	6
13	R_b9KUmWIPgG44G8t	easy	security-oriented	6	5	4	5	6	6	6	5	5	6
14	R_3eeHY6hS0C5ylhz	easy	security-oriented	5	5	3	6	4	6	4	5	5	6
15	R_dg031wic22jpkpf	easy	security-oriented	6	6	1	6	5	6	7	6	7	7
16	R_8qWbnjBv2zKXVr	easy	security-oriented	5	3	4	4	5	4	4	4	3	5
17	R_9nxdRLSUAUVsJnv	easy	security-oriented	5	5	3	5	5	5	5	5	5	5
18	R_6ywCXuQ1oXsrECV	easy	security-oriented	7	7	7	7	7	7	7	7	7	7
19	R_b03AcE4EdH6toV	easy	security-oriented	6	6	7	6	5	6	7	7	7	7
20	R_8enylaSD1E9SroV	easy	security-oriented	6	5	5	6	5	7	5	6	5	6
21	R_2sEuyRiHogq0Phb	easy	security-oriented	5	6	5	5	6	4	6	4	6	6
22	R_20ki3hGdFxpJl8Z	easy	security-oriented	4	5	5	6	6	5	5	7	6	6
23	R_4JfpFvjeAdZmCx	easy	security-oriented	6	5	4	5	5	6	5	4	5	6
24	R_9Lj1lh8YL4bWWp	easy	security-oriented	7	7	7	4	4	4	6	7	7	7
25	R_9Nptl8WzuevURwh	easy	security-oriented	4	3	5	6	5	4	4	5	6	6
26	R_5avy95h0wA8Cgct	easy	security-oriented	3	3	3	5	3	5	5	4	5	4
27	R_dal3oLr8hkFhyjH	easy	security-oriented	5	5	4	5	4	5	5	4	4	4
28	R_6Pg1v1VrDXglhzv	easy	security-oriented	7	6	2	7	7	7	7	7	7	7
29	R_9zU8vd0U3Ib4mc5	easy	security-oriented	5	5	5	5	5	5	5	5	6	6
30	R_3wRztv3lFigwOtd	easy	security-oriented	5	5	5	4	5	4	3	5	5	5
31	R_er0swlSBwtR5q2F	easy	security-oriented	6	6	4	6	6	6	6	6	6	6
32	R_6LMCFoBQHhHemEJ	easy	security-oriented	4	5	6	5	3	6	4	4	5	4
33	R_6h5QzEYMB8NS8uh	easy	security-oriented	6	6	3	6	5	6	6	5	6	5
34	R_8i7DEIZwcl2HTn	font with debiasing	security-oriented	6	7	4	7	7	6	6	7	7	7
35	R_0VS2ZfyNqaDKg8B	font with debiasing	security-oriented	7	7	1	7	7	7	7	7	7	7
36	R_86Tsgvk9nhP5jf	font with debiasing	security-oriented	7	6	5	6	6	5	5	5	6	6

37	R_9AmR9NMbMzDzNwp	font with debiasing	security-oriented	6	6	6	6	6	6	6	6	2	2
38	R_9tYa9leCB006FIX	font with debiasing	security-oriented	5	6	5	6	5	5	6	5	6	5
39	R_aaY65pGaak70TAh	font with debiasing	security-oriented	5	5	6	4	3	5	5	4	3	3
40	R_d1qdSyovNwev0yN	font with debiasing	security-oriented	7	7	3	7	6	6	5	6	6	7
41	R_6Ycrhixv0TieuON	font with debiasing	security-oriented	5	6	5	4	4	5	5	5	6	5
42	R_cTMHrvqRjmPcQsJ	font with debiasing	security-oriented	5	5	4	3	4	4	5	6	7	6
43	R_eY9fMx42FAP8uVv	font with debiasing	security-oriented	5	6	3	4	5	6	5	6	5	5
44	R_8qOyZmg1HJ8Xyu1	font with debiasing	security-oriented	3	2	7	3	3	4	3	3	4	5
45	R_eyYDTuw7VxWVbD	font with debiasing	security-oriented	4	4	4	5	6	6	7	7	7	7
46	R_eOKriFi1HmdTwoJ	font with debiasing	security-oriented	6	6	6	6	6	6	5	6	6	6
47	R_8359WjVPI1ZFBXf	font with debiasing	security-oriented	6	4	6	4	4	5	5	5	6	4
48	R_e5uKmjxywwdiAIL	font with debiasing	security-oriented	5	6	5	4	4	5	5	6	5	5
49	R_dp91GqTKwS1EbAx	font with debiasing	security-oriented	5	3	3	7	5	5	3	5	6	7
50	R_3BEDaRBiULpjU4B	font with debiasing	security-oriented	6	6	7	6	7	6	7	7	7	7
51	R_9Aakz4ZZuDnolkp	font with debiasing	security-oriented	6	7	6	7	7	6	6	7	6	6
52	R_0enRSrqPcEsD2oR	font with debiasing	security-oriented	5	5	4	5	5	5	5	5	5	5
53	R_6o4iEHwN1pJX9P	font with debiasing	security-oriented	5	5	5	2	2	2	6	3	2	2
54	R_cD7g8sUpY2OuxL	font with debiasing	security-oriented	4	4	4	4	4	4	4	4	4	4
55	R_2hGAVswmSN35j5H	font with debiasing	security-oriented	6	6	4	5	5	6	6	6	6	7
56	R_eveYOxVUnB0PlP	font with debiasing	security-oriented	4	5	4	6	5	6	5	5	5	5
57	R_9MIUGOz7HnvbN1r	font with debiasing	security-oriented	4	6	1	7	7	4	5	7	6	7
58	R_0oHnJU3vxmXz7yB	font with debiasing	security-oriented	2	1	2	3	2	2	1	2	1	1
59	R_06xvcJsmV8sJc1f	font with debiasing	security-oriented	6	5	6	4	4	5	5	5	3	3
60	R_4lw7wZ9A2TBdwoZ	font with debiasing	security-oriented	5	7	4	6	5	6	6	6	2	6
61	R_2huWhiteOp1tv4p	font with debiasing	security-oriented	4	4	3	3	5	3	3	4	3	3
62	R_0HxEMeHvKwGauCp	font with debiasing	security-oriented	7	7	6	6	6	6	7	6	7	7
63	R_6XulQzqejByTaqp	font with debiasing	security-oriented	4	3	3	4	3	5	4	5	3	5
64	R_9nUu0nRacjANrKJ	font with debiasing	security-oriented	4	5	3	4	3	4	5	4	4	4
65	R_6ureCLnA5cGMPml	font with debiasing	security-oriented	4	4	2	5	5	5	6	4	4	4
66	R_3K3m6VR7Wia7ISF	font with debiasing	security-oriented	5	5	5	4	4	4	3	4	3	3
67	R_3HNbOUZ3s0zpDjB	font with debiasing	security-oriented	6	6	6	6	7	6	7	6	7	7
68	R_bpXhQk5L1RLAef	easy	convenience-oriented	6	6	6	6	6	6	6	7	7	7
69	R_1YtgXrHmUj6ymjP	easy	convenience-oriented	5	6	3	5	6	5	5	4	4	4
70	R_e8TXtVC9BlobD0N	easy	convenience-oriented	4	5	3	3	3	4	5	4	5	4
71	R_cCvCQRXLKz6Qr5j	easy	convenience-oriented	6	6	6	6	6	6	6	7	7	7
72	R_81RBCp1QsYuV9KR	easy	convenience-oriented	6	6	4	4	5	6	6	5	6	6
73	R_0SWyxSxZiCiRsqx	easy	convenience-oriented	7	6	3	6	5	6	7	6	7	6
74	R_6YeJzWGRHzgDCjX	easy	convenience-oriented	6	6	6	5	5	5	6	7	6	6
75	R_4YPihdBvm8irVkh	easy	convenience-oriented	5	6	6	5	3	2	2	2	2	3

76	R_aXliBkm7eUx88Sh	easy	convenience-oriented	6	6	6	5	5	5	6	6	6	6
77	R_d4E7eBF4m1RZMV	easy	convenience-oriented	4	4	4	4	4	4	3	4	4	4
78	R_bIKQAswMnt4wKfF	easy	convenience-oriented	3	5	5	3	4	5	5	4	3	4
79	R_dm0qDrVS7FJcyix	easy	convenience-oriented	4	5	4	3	4	5	6	5	4	3
80	R_bgfFPBEgSyt9pJ3	easy	convenience-oriented	7	6	7	5	6	7	6	5	6	7
81	R_808AWm2ly9qb4N	easy	convenience-oriented	6	6	3	5	5	5	6	5	5	6
82	R_9RIRJzBIVfDdF2d	easy	convenience-oriented	6	5	2	5	4	5	5	4	5	5
83	R_bpBkYrGajjt1mNT	easy	convenience-oriented	2	2	5	3	3	3	3	3	1	2
84	R_eDKIKtEtUJLwix	easy	convenience-oriented	5	6	3	4	6	5	5	6	5	5
85	R_3vBK2h6OvQpzKDP	easy	convenience-oriented	7	6	7	7	7	6	6	7	7	7
86	R_dm08yQIYQaUqRfL	easy	convenience-oriented	7	5	5	6	3	4	4	5	2	4
87	R_d11hbF6k8cR9Sbb	easy	convenience-oriented	4	3	3	3	4	4	3	5	3	5
88	R_3CYHd3HHiwmlVP	easy	convenience-oriented	5	4	3	4	6	4	4	5	6	5
89	R_0q5TFXkwXqZfT9P	easy	convenience-oriented	6	5	7	5	6	6	7	5	7	5
90	R_6Apd8QgsNkMmJT	easy	convenience-oriented	6	7	1	7	6	6	7	7	7	7
91	R_byDQ8XUHKjBBqkd	easy	convenience-oriented	6	5	6	5	5	4	4	5	5	6
92	R_3VriOAhWabDG1IF	easy	convenience-oriented	7	7	1	7	7	7	6	7	7	7
93	R_8B6V1V9jb9plMGx	easy	convenience-oriented	6	6	6	6	6	6	7	7	7	7
94	R_ahs3xrMDEUAkcAd	easy	convenience-oriented	6	6	6	4	3	3	6	5	2	1
95	R_bHFfBFJDAZx29T	easy	convenience-oriented	4	5	5	5	6	6	5	6	7	2
96	R_4HK0w3p4UgbVSCx	easy	convenience-oriented	6	5	3	6	5	5	6	6	6	5
97	R_3ruXKaXgEJ71UuF	easy	convenience-oriented	4	6	2	7	6	5	5	7	6	5
98	R_9KuzZVigOSp22Vw1	easy	convenience-oriented	5	4	3	4	4	4	4	5	4	5
99	R_0VXXbHSDS6aJGB	easy	convenience-oriented	5	5	5	4	4	4	5	5	4	5
100	R_aaVfeUYu719lkSF	easy	convenience-oriented	4	5	4	5	4	6	5	5	5	6
101	R_9uJmTuPKuTLx5ad	easy	convenience-oriented	4	5	4	4	3	3	5	6	5	7
102	R_ebsZIRq5stP0Qtf	easy	convenience-oriented	6	6	5	5	5	5	6	6	6	6
103	R_782bqnalImGcvEF	font with debiasing	convenience-oriented	6	6	2	6	6	6	6	6	2	2
104	R_eKvHRyyP3M5GbQh	font with debiasing	convenience-oriented	5	5	4	4	4	4	7	5	5	5
105	R_9BI3bDchjblxkY1	font with debiasing	convenience-oriented	7	7	6	7	7	7	7	7	7	7
106	R_eQjL1TFEV9mPkAB	font with debiasing	convenience-oriented	6	6	5	6	6	6	6	6	3	6
107	R_9nIXebsgxUEI8n3	font with debiasing	convenience-oriented	5	3	6	5	4	6	4	5	4	6
108	R_42fR6RvcVDMVsr	font with debiasing	convenience-oriented	3	4	4	4	3	5	6	5	6	6
109	R_0f95tj3IRfqrNvD	font with debiasing	convenience-oriented	3	2	3	4	5	4	4	3	2	2
110	R_broESYpeFjBHg8d	font with debiasing	convenience-oriented	5	6	3	5	6	6	6	5	6	6
111	R_eRRqll5qbadXR3f	font with debiasing	convenience-oriented	5	4	3	4	4	4	4	3	4	5
112	R_82f7VxnpwHelFL	font with debiasing	convenience-oriented	5	4	3	4	5	5	3	3	4	5
113	R_6fGtVQCZp5fFqJ	font with debiasing	convenience-oriented	6	5	2	6	4	5	4	4	5	6
114	R_bwRBISxPglmj8Kp	font with debiasing	convenience-oriented	6	5	4	6	5	4	3	6	5	3

115	R_b3ZxXV6KaVeU3r	font with debiasing	convenience-oriented	6	6	5	5	5	6	6	6	6	6
116	R_2rCjCVBRsiqBTet	font with debiasing	convenience-oriented	4	4	3	5	5	4	5	6	5	5
117	R_8CY0dy5FhiEhHRr	font with debiasing	convenience-oriented	2	4	4	6	5	7	1	2	1	7
118	R_74flK3eK3JwHqd	font with debiasing	convenience-oriented	7	7	6	7	6	7	6	7	6	7
119	R_ePdBAAKUmGmHBKl	font with debiasing	convenience-oriented	6	6	5	6	6	6	6	6	2	2
120	R_9XFzGyTbKDIqdZb	font with debiasing	convenience-oriented	3	5	6	3	6	6	5	5	3	6
121	R_2uaMaWyAbL4hud	font with debiasing	convenience-oriented	6	6	6	5	5	5	5	6	5	6
122	R_4GgHhjJNKKFXDxz	font with debiasing	convenience-oriented	5	5	4	5	6	5	5	5	5	6
123	R_6FjCpEHCODmWCs5	font with debiasing	convenience-oriented	5	5	4	3	4	5	4	5	5	4
124	R_8JIWv3CQ6gR13IH	font with debiasing	convenience-oriented	4	4	4	5	3	4	5	5	3	3
125	R_5grf9FqInkiVwHj	font with debiasing	convenience-oriented	7	6	6	5	7	5	5	5	3	5
126	R_9AWgaN9834lxbql	font with debiasing	convenience-oriented	6	5	2	6	7	6	7	7	7	7
127	R_2m09X2mwtNMJTtB	font with debiasing	convenience-oriented	6	7	6	4	4	4	7	6	6	6
128	R_8qNv5RBxGEs9U33	font with debiasing	convenience-oriented	6	6	3	6	5	6	5	6	5	6
129	R_0MPCm9EYeHQI2cZ	font with debiasing	convenience-oriented	5	6	5	6	5	5	5	5	6	6
130	R_e8xgnsxY8zzLxSB	font with debiasing	convenience-oriented	6	5	2	4	5	6	4	5	6	5
131	R_3sZsIOO6yE3EObP	font with debiasing	convenience-oriented	7	7	7	7	7	7	7	7	7	7
132	R_beLpwql66dCmb1r	font with debiasing	convenience-oriented	6	6	2	6	6	6	6	7	7	7
133	R_9Llbz0ECnHXPduB	font with debiasing	convenience-oriented	4	3	3	3	5	3	4	3	5	3
134	R_390yveSSUU1AEBf	font with debiasing	convenience-oriented	2	2	3	5	3	5	5	5	4	5
135	R_8Gqdu4WQ00OyrU9	font with debiasing	convenience-oriented	7	6	1	7	6	6	7	6	7	7

## Raw Data of Experiment 3-3

No	ID	Question	Naive Theory	Easy	Convenient	Complex	Secure	Safe	Protected	Tech Advanced	Generation	Good	Favor	Like
1	R_1HUUZUCoaQU00nH	Two Questions	Easy Naive	6	6	4	7	6	6	6	1	7	6	7
2	R_esXwgg1A34rQIH	Two Questions	Easy Naive	7	7	7	7	7	7	7	1	7	4	5
3	R_8951IzAeb0npY6V	Two Questions	Easy Naive	6	5	6	6	5	6	5	1	4	4	6
4	R_eqSHjXP1RMvX50p	Two Questions	Easy Naive	3	3	5	6	5	6	6	1	5	5	4
5	R_cOrZcDGzr4s0W5	Two Questions	Easy Naive	5	5	2	4	6	3	2	1	6	6	5
6	R_cIJXmet8ocEoWEJ	Two Questions	Easy Naive	7	7	2	7	7	7	7	1	7	7	7
7	R_7JTJTj2z68oGYER	Two Questions	Easy Naive	6	6	2	6	4	6	5	1	7	7	7
8	R_a9PmyXKtTSC67A1	Two Questions	Easy Naive	6	6	6	6	5	6	6	1	6	6	7
9	R_cSmTJWoiKx1Wcd	Two Questions	Easy Naive	6	6	5	6	5	6	6	1	6	5	5
10	R_73Sm0npVMRkKdv	Two Questions	Easy Naive	5	5	5	5	5	4	5	1	7	5	1
11	R_6ySF8UN5SEUthsN	Two Questions	Easy Naive	6	6	2	6	6	6	6	1	6	6	6
12	R_ac02uuJwrqkdUs5	Two Questions	Easy Naive	7	7	7	7	7	7	7	1	7	7	7
13	R_2bovUyOulzncjIx	Two Questions	Easy Naive	5	5	5	4	5	5	4	2	4	5	4
14	R_cvkjXfH4WBwxFeB	Two Questions	Easy Naive	5	6	2	5	6	6	5	1	5	5	5
15	R_9yKAcj3EIoCBcrj	Two Questions	Easy Naive	6	5	2	5	5	4	5	2	5	5	6
16	R_5tYiYkGsdw0kOY1	Two Questions	Easy Naive	6	6	2	5	5	5	6	2	6	6	6
17	R_5cDR8dYoi21q4F7	Two Questions	Easy Naive	6	6	4	5	5	5	6	2	5	5	5
18	R_TTCkdwv4UYcKjVr	Two Questions	Easy Naive	6	6	6	6	6	6	6	1	6	6	6
19	R_5pgFfbnR4JXMMML	Two Questions	Easy Naive	5	5	2	6	6	6	6	1	6	6	6
20	R_06QWbhTJEDqcYpD	Two Questions	Easy Naive	7	7	2	6	6	6	6	1	7	6	7
21	R_bdXcPyOhr2S83fT	Two Questions	Easy Naive	6	7	2	7	7	7	6	1	7	7	7
22	R_cVwBEeLZ4BFYkpn	Two Questions	Easy Naive	4	4	5	5	4	4	4	2	4	4	4
23	R_3Ffe4n3gE29youx	Two Questions	Easy Naive	5	5	4	4	6	6	6	1	6	6	6
24	R_7ZJKPNLDoC4tr6d	Two Questions	Easy Naive	5	5	5	6	5	5	6	1	6	6	6
25	R_dhQsA3u6M2brbIH	Two Questions	Easy Naive	4	4	4	4	4	4	4	2	4	4	4
26	R_3QhZGr9bTqkeXz	Two Questions	Easy Naive	6	6	2	6	6	5	5	1	7	7	6
27	R_6mo5ZkRVY0mAQyV	Two Questions	Easy Naive	7	4	6	3	2	4	4	2	5	6	4
28	R_e3TmQUmHzrAPIad	Two Questions	Easy Naive	5	2	2	6	6	5	6	1	6	4	5
29	R_1Ybr3rz0F1tCpN3	Two Questions	Easy Naive	5	4	4	6	6	6	5	1	6	5	5
30	R_5B11tSWgelcoCH3	Two Questions	Easy Naive	5	3	4	3	4	5	4	2	4	3	4
31	R_bCQe0Ug46IOsC8Z	Two Questions	Easy Naive	5	6	3	5	5	4	5	1	7	6	5
32	R_6nEN9H3zYn2j4A1	Two Questions	Easy Naive	5	5	4	6	6	6	6	1	6	6	6
33	R_2smrlqvwlfhjl	Two Questions	Easy Naive	7	7	7	7	7	7	7	1	7	7	7
34	R_a2HoGXAUTcwr5P	Two Questions	Easy Naive	6	6	5	7	3	4	2	1	6	2	2
35	R_5AXplG6mhVZNXnv	Two Questions	Easy Naive	4	5	5	7	4	7	7	1	5	6	4
36	R_byzK23ldURKQR4p	Two Questions	Easy Naive	5	4	4	3	5	4	5	1	5	4	6

37	R_7WjUPDG2cqTKBYF	Two Questions	Easy Naive	4	5	5	7	7	7	7	1	5	6	6
38	R_4ZTsb7sVsEXXF	Two Questions	Easy Naive	6	6	7	5	6	6	5	2	6	6	7
39	R_dpbn0LzsPuEIZH	Two Questions	Easy Naive	6	5	6	5	6	5	5	1	6	5	6
40	R_6KEBvQFTlydranj	Two Questions	Easy Naive	7	7	1	7	4	4	7	2	7	7	7
41	R_6PZAAFoIaChK58x	Two Questions	Difficult Naive	6	5	2	6	5	6	5	1	5	4	5
42	R_77Kq0Jo5BupDx8V	Two Questions	Difficult Naive	7	7	7	7	7	7	7	1	7	1	7
43	R_cnKyojZthX0rahT	Two Questions	Difficult Naive	1	2	6	6	6	7	6	1	3	2	2
44	R_sakeyA96ZsEj6lL	Two Questions	Difficult Naive	7	7	1	6	2	7	7	1	7	7	7
45	R_ctG7k2H2UcCNZE9	Two Questions	Difficult Naive	6	6	2	6	6	6	6	1	6	6	6
46	R_ePc89RRsG6ihvhj	Two Questions	Difficult Naive	7	7	7	7	4	4	7	1	7	7	7
47	R_d0c0L4zZTAMsWSF	Two Questions	Difficult Naive	7	7	2	7	7	7	7	1	7	6	7
48	R_cw2jsZQ73K0Jzut	Two Questions	Difficult Naive	5	5	2	6	6	6	6	1	6	6	6
49	R_5i4tstOd2XrFiMI	Two Questions	Difficult Naive	5	5	6	6	5	7	6	1	6	6	7
50	R_3lwBPmnEiqsteUB	Two Questions	Difficult Naive	5	5	3	2	2	3	2	1	5	5	5
51	R_bC1szFu4hG713r7	Two Questions	Difficult Naive	6	6	7	7	5	6	6	1	6	6	6
52	R_2oBysDCeLZkHRpr	Two Questions	Difficult Naive	7	7	2	7	7	6	6	1	7	6	7
53	R_6hWU00zkS0K1VMF	Two Questions	Difficult Naive	7	7	2	6	6	7	7	1	5	6	6
54	R_bpA3NqxM389vvlr	Two Questions	Difficult Naive	6	6	3	5	5	5	5	1	5	5	5
55	R_9RdVqFta2Yoa6fr	Two Questions	Difficult Naive	6	5	2	5	4	5	5	1	5	4	4
56	R_7R7mlhXYOgvesHH	Two Questions	Difficult Naive	4	5	2	5	2	4	4	1	6	5	5
57	R_78RbSOA1QMgHqXH	Two Questions	Difficult Naive	5	5	4	5	5	5	5	1	5	5	5
58	R_9M4KJovTKigLcLj	Two Questions	Difficult Naive	7	7	6	6	6	6	6	1	7	7	7
59	R_8vKdCQuskmEaHg9	Two Questions	Difficult Naive	6	6	5	6	6	7	7	1	6	5	6
60	R_d4jZXwGO23rLJ89	Two Questions	Difficult Naive	6	6	2	7	7	7	6	1	7	7	7
61	R_eUHLALs11eRIYh	Two Questions	Difficult Naive	4	4	5	4	5	4	5	1	5	5	5
62	R_9HUufnxQp2FwrFr	Two Questions	Difficult Naive	6	5	3	6	5	6	5	1	5	5	6
63	R_e9HsCzJ1Q1Cr88d	Two Questions	Difficult Naive	5	5	5	4	4	5	5	1	6	3	3
64	R_9tpFRdSFAHiJz7	Two Questions	Difficult Naive	6	6	2	5	4	4	2	1	5	5	5
65	R_5j13xfsr8L5lh65	Two Questions	Difficult Naive	3	4	5	4	4	3	4	2	5	5	4
66	R_0kQawn04Q3tdsY5	Two Questions	Difficult Naive	5	6	2	7	7	6	5	1	6	6	6
67	R_4YqMRbB1oDs8Cyh	Two Questions	Difficult Naive	5	5	6	6	6	5	5	1	6	6	6
68	R_868si0LqNtAm1bD	Two Questions	Difficult Naive	7	6	1	4	4	4	5	1	6	6	6
69	R_8CSOkk1JHqmNnV3	Two Questions	Difficult Naive	6	5	2	6	4	6	6	1	6	2	2
70	R_cv10itGH9sB9Wt	Two Questions	Difficult Naive	6	7	2	7	5	6	6	2	6	6	6
71	R_819LmgSgc10q4Zv	Two Questions	Difficult Naive	6	5	4	5	6	6	4	1	6	5	5
72	R_eXvstYamBr5MjNH	Two Questions	Difficult Naive	5	6	2	6	5	5	5	1	6	5	6
73	R_eqvtMyxn0hWNfKJ	Two Questions	Difficult Naive	5	5	4	4	4	3	4	1	7	6	6
74	R_6f2RlhOMk91R3	Two Questions	Difficult Naive	4	5	6	4	3	4	5	1	5	4	3
75	R_8D5BH5VUx0c61H7	Two Questions	Difficult Naive	4	3	5	7	7	7	6	1	6	7	6

76	R_38IZ4C1h4gYnKYZ	Two Questions	Difficult Naive	6	6	3	6	6	6	6	1	6	6	6
77	R_3yr6GLAAmkC0B0h	Two Questions	Difficult Naive	5	5	5	6	6	5	5	1	5	4	5
78	R_3JArPbcaMTSK949	Two Questions	Difficult Naive	5	5	2	5	6	6	6	1	6	6	6
79	R_6Ll66Qpp8IRALX	Two Questions	Difficult Naive	5	5	4	5	5	4	4	1	5	6	6
80	R_b8vMEBoA709mv9	Two Questions	Difficult Naive	4	5	4	4	5	5	5	2	6	5	2
81	R_6Ls6eA949796Jvf	Seven Questions	Easy Naive	5	5	4	5	4	4	4	2	4	4	4
82	R_25ZRvZqz7TEC4Kx	Seven Questions	Easy Naive	4	4	3	4	1	1	3	2	1	1	1
83	R_dhiRWe68xMWPzKd	Seven Questions	Easy Naive	4	4	4	7	7	7	7	2	6	6	7
84	R_bvCe5DLXr4up4pf	Seven Questions	Easy Naive	4	4	5	6	6	6	6	1	5	5	5
85	R_cSiI7E4mE1KHuh7	Seven Questions	Easy Naive	4	3	5	3	3	7	6	1	6	4	2
86	R_a9piL.GakYigyV5X	Seven Questions	Easy Naive	5	6	2	7	5	6	6	1	7	6	7
87	R_6JR6DKwKcbmZz5H	Seven Questions	Easy Naive	7	7	1	7	7	7	7	1	7	7	7
88	R_5dRCGjo5AZu0posB	Seven Questions	Easy Naive	5	5	5	5	5	5	5	1	5	5	5
89	R_aeI0uhWum0xFFFH	Seven Questions	Easy Naive	6	6	3	7	6	5	6	1	6	5	6
90	R_bsl4Hk4pAmcP605	Seven Questions	Easy Naive	4	3	5	3	3	2	3	1	2	3	3
91	R_cYISi3icsTO44sd	Seven Questions	Easy Naive	6	3	7	4	6	4	6	2	2	4	3
92	R_aVPM48szlKR4pf	Seven Questions	Easy Naive	7	6	7	6	7	6	7	1	7	6	6
93	R_6IEchUpmshgYFql	Seven Questions	Easy Naive	5	5	2	6	5	6	5	1	5	5	5
94	R_3VmEwCfzknNsR9P	Seven Questions	Easy Naive	6	6	4	5	6	5	4	1	7	7	6
95	R_2tRX6XT1NYN60ER	Seven Questions	Easy Naive	6	6	3	6	6	6	5	1	6	6	7
96	R_2i6yxjxyDCVHURn	Seven Questions	Easy Naive	7	7	1	7	7	7	7	1	7	7	7
97	R_7Px64z8W1WxOPE9	Seven Questions	Easy Naive	7	7	1	6	5	7	7	1	7	7	7
98	R_4UXwpdPKpIVHo6V	Seven Questions	Easy Naive	6	6	5	6	7	7	6	1	7	6	6
99	R_cwxSAr1dlbnbbaR	Seven Questions	Easy Naive	4	6	3	2	1	5	5	1	4	4	1
100	R_0kv16IJXtq2qIPH	Seven Questions	Easy Naive	4	5	5	4	5	4	5	1	5	4	5
101	R_2sD27nxPjv1h0zz	Seven Questions	Easy Naive	6	5	2	6	6	5	6	1	7	7	5
102	R_cZlq6BKsisovaCx	Seven Questions	Easy Naive	7	5	2	4	5	5	6	1	6	3	6
103	R_5cJx4Plm3zkyYPH	Seven Questions	Easy Naive	6	6	4	6	5	6	5	2	6	5	5
104	R_9HtCmftH9vGLix	Seven Questions	Easy Naive	1	1	7	5	6	7	4	1	3	2	2
105	R_4YgaYPGZBKSFpX	Seven Questions	Easy Naive	6	5	3	2	2	2	3	1	4	4	2
106	R_005UdDAzruFpt1b	Seven Questions	Easy Naive	5	5	3	5	5	4	4	1	4	6	5
107	R_9NNO62OsvMRmUQJ	Seven Questions	Easy Naive	5	5	3	4	5	4	3	1	4	4	3
108	R_eqFYizRFGJOPTH7	Seven Questions	Easy Naive	7	6	5	6	6	5	6	1	6	5	6
109	R_bkH8yM8bsr2esjH	Seven Questions	Easy Naive	7	6	5	4	5	3	5	2	5	4	6
110	R_el2bl35SVcn7HP7	Seven Questions	Easy Naive	5	5	5	5	5	6	5	1	7	7	7
111	R_6Sh3OM5YxdZAVQV	Seven Questions	Easy Naive	6	4	5	6	5	6	4	1	6	5	5
112	R_0oiRiTpmGcFtGQt	Seven Questions	Easy Naive	6	6	2	5	6	7	6	1	7	7	7
113	R_88S1Lids286zPyR	Seven Questions	Easy Naive	7	7	7	7	7	7	7	1	7	7	7
114	R_b10koRskQnPs7uR	Seven Questions	Easy Naive	6	6	5	6	5	6	4	1	6	6	6

115	R_9MjC8hQ1GPtrCsd	Seven Questions	Easy Naive	5	4	5	5	4	4	5	1	5	4	6
116	R_eVTQG5ZqkRFDleh	Seven Questions	Easy Naive	2	1	2	4	4	3	1	1	4	2	3
117	R_6Vkda2nkyI0ZpUp	Seven Questions	Easy Naive	4	3	3	4	3	4	5	1	4	3	3
118	R_beKdCJkKiAPkiOh	Seven Questions	Easy Naive											
119	R_5nhBxWcy4IufyvP	Seven Questions	Difficult Naive											
120	R_8oYdo9rUboLo3xb	Seven Questions	Difficult Naive	7	6	3	7	6	7	6	1	7	7	7
121	R_50jWV0wP8JY4Box	Seven Questions	Difficult Naive	1	1	1	1	1	1	6	2	1	1	1
122	R_0BXWTHKdjTOJHP	Seven Questions	Difficult Naive	3	3	5	3	3	4	3	2	2	3	4
123	R_9AoFuPATiAFvWND	Seven Questions	Difficult Naive	4	4	5	4	5	4	4	1	3	4	5
124	R_77IBrd7GFqbXc9	Seven Questions	Difficult Naive	2	3	6	5	4	6	3	2	5	6	6
125	R_bDvcfgWUD8vHDP3	Seven Questions	Difficult Naive	7	7	6	7	7	6	7	1	6	6	7
126	R_5tFngEvxBgAQV	Seven Questions	Difficult Naive	6	6	4	7	6	5	6	2	7	7	6
127	R_bmAa60fwXFeuoZ	Seven Questions	Difficult Naive	6	6	4	7	6	6	5	1	7	6	6
128	R_eg0mAi0wiU68RY9	Seven Questions	Difficult Naive	6	5	6	6	7	7	6	1	7	6	5
129	R_8d22PEBCVZVwlv	Seven Questions	Difficult Naive	3	5	4	6	6	6	6	1	5	4	5
130	R_1G2GGY2mYnRz72l	Seven Questions	Difficult Naive	1	1	3	7	7	7	7	2	2	1	1
131	R_6ipL5iNBuq2wfAN	Seven Questions	Difficult Naive	4	4	5	4	5	5	5	1	4	4	4
132	R_9mmKhXtut4cAA4t	Seven Questions	Difficult Naive	6	4	5	6	4	6	6	1	6	5	6
133	R_8CY0lmbVG7quKAJ	Seven Questions	Difficult Naive	5	5	4	6	5	6	5	2	5	2	3
134	R_dhT70yznCC6xUzj	Seven Questions	Difficult Naive	5	5	6	5	4	5	6	1	5	6	6
135	R_eEwZ3U0GANUeOGx	Seven Questions	Difficult Naive	4	6	4	6	5	7	5	1	6	5	7
136	R_6PzvA3z2ecncE1n	Seven Questions	Difficult Naive	1	1	7	7	7	7	7	1	4	4	4
137	R_0SxtHkh2R0Phho9	Seven Questions	Difficult Naive	4	3	6	6	6	6	4	1	6	5	6
138	R_6JTRrr0xFFEglxj	Seven Questions	Difficult Naive	6	5	2	4	5	5	6	2	6	5	5
139	R_9oz5Y0cNH12YabP	Seven Questions	Difficult Naive	6	6	2	4	4	3	3	1	4	4	5
140	R_bQw0qZowUo1tM8J	Seven Questions	Difficult Naive	7	7	1	6	4	6	4	1	7	7	7
141	R_6M5lyk0Tk5rNFOZ	Seven Questions	Difficult Naive	6	6	2	6	6	6	5	1	7	6	5
142	R_0k7yTk4HnXPRX2R	Seven Questions	Difficult Naive	5	5	3	5	5	5	4	1	6	5	5
143	R_9ZhoFe7YskzplLz	Seven Questions	Difficult Naive	1	1	6	6	5	1	2	1	3	2	2
144	R_cLLxmM2033Nk5O5	Seven Questions	Difficult Naive	6	5	5	6	6	6	4	1	3	3	4
145	R_3JCNBfwXZ4ZLD3n	Seven Questions	Difficult Naive	4	5	5	5	6	6	6	1	5	5	4
146	R_dbdj1xXCvidboMd	Seven Questions	Difficult Naive	5	6	6	5	6	6	6	2	5	5	6
147	R_7W29N8A35RyPxsh	Seven Questions	Difficult Naive	5	5	6	6	6	5	5	2	6	6	6
148	R_5ASvDjZ7LlHEcKB	Seven Questions	Difficult Naive	4	5	7	5	4	3	4	1	5	4	3
149	R_8983MXd05IIsd9z	Seven Questions	Difficult Naive	5	5	2	5	5	6	6	1	5	5	5
150	R_baAqXdyw2tAION	Seven Questions	Difficult Naive	7	7	5	6	7	7	6	1	7	6	6
151	R_0pSs9759SHoGwfj	Seven Questions	Difficult Naive	5	5	2	4	5	4	5	2	5	5	2
152	R_3m9WRZ43dCWS8VD	Seven Questions	Difficult Naive	6	7	1	7	7	7	7	1	7	7	7
153	R_cT0FIKKEgt8tVP	Seven Questions	Difficult Naive	6	6	5	2	6	7	5	1	6	5	6

154	R_egNugceHOkNsynX	Seven Qeustions	Difficult Naive	7	7	1	7	7	7	7	1	7	7	7
-----	-------------------	-----------------	-----------------	---	---	---	---	---	---	---	---	---	---	---