



July 2011

Volume 4, Issue 1

Special Interest Articles:

- Password Change Project.
- Identity Finder is available.
- IT Security Lab takes first place.



IT Security Office • 1300 Torgersen Hall • 540/231-1688 • www.security.vt.edu

Password Change Project

To ensure that strong passwords are being used, Virginia Tech's IT Security Office will be requiring many of your passwords to be changed by July 1, 2011.

What passwords must be changed by July 1, 2011?

- All PID passwords.
- All Hokies passwords for full user accounts and sponsored accounts.
- Central IT Oracle ID passwords for the production databases Banner, Warehouse, VaTech, Foundation, and GIS.

If you do not change your password by

July 1, 2011 then your password will expire. Expired passwords will need to be changed to allow account authentication. Changed passwords will be active for 12 months.

Visit www.vt.edu/password for more information on the Password Change Project and guidance on changing your password.



IDENTITY FINDER: Digital Packrats Beware

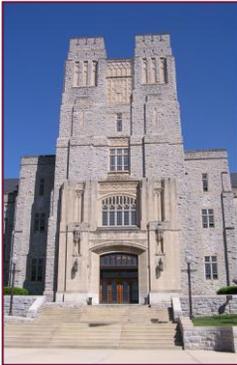
The IT Security Office often encounters users that have data they simply no longer need or are not supposed to have. These "digital packrats" often put the university at risk of data exposure every time a virus or malware compromises a machine. It has been observed that the best way to protect this data is locate it and remove it. Locating this data has proved challenging with freeware tools and has been a perceived barrier to remediation.

Virginia Tech has purchased Identity Finder to help reduce the risk this undiscovered data poses. Identity Finder helps locate SSNs, credit card numbers, and even passwords. It has an easy to use interface that helps users deal with those dreaded "false positives".

Identity Finder is available for Windows and Mac operating systems and can be obtained can be downloaded from Software Distribution's website at <http://network.software.vt.edu>. Information on installation and getting started can be found at www.security.vt.edu/idf.

The Identity Finder Console is also available for use by departments that have system administrators capable of installing and administering the software. For information on the Identity Finder Console contact Nicolas Pachis at npachis@vt.edu.





"Identity Finder helps locate SSNs, credit card numbers, and even passwords."



"Securing the Human" Online Awareness Training

Online cyber awareness training is now being offered to Virginia Tech by the IT Security Office. This training represents an excellent opportunity for departments to ensure their staff is aware of cyber issues.

The training is self-paced and provides progress reporting. If you are interested in this training for your department or yourself, please contact Rich Sparrow at rich.sparrow@vt.edu.



Virginia Tech Hosts Inaugural Cyber Security Summit

Excerpt from the full article located here: <http://www.ece.vt.edu/news/articles/cybersecuritysummit.html>

On Saturday, April 2, 2011, student teams from Virginia Tech, the University of Maryland, Howard University, the US Military Academy at West Point, and the Community College of Baltimore County participated in Virginia Tech's inaugural Cyber Security Summit.

The summit featured a morning of presentations from speakers in the cyber security field, followed by an afternoon competition where teams faced off in efforts to attack and defend computer networks.

With nearly 60 attendees, the event was organized and hosted by Virginia Tech IT security analysts, graduate students from the IT Security Lab, and the Linux and Unix Users Group. ECE students played a critical role: Stephen Groat was in charge of the organizing and Matt Dunlop, Will Urbanski, Andrew Moore, and Phillip Kobezak all provided high levels of support for the capture the flag exercise.

ECE professor [Joseph Tront](#) and ITSO's Randy Marchany acted as consultants to the event, and ECE's Charles Clancy provided Hume Center funding to support participants and speakers.

Graduate Students in Security Lab Take First Place!

Matthew Dunlop, Stephen Groat, and William Urbanski recently won first place poster at the 2011 Graduate Student Assembly Research Symposium. Their research on dynamically obscuring Internet Protocol version 6 (IPv6) hosts is aimed at bringing privacy, anonymity, and security to network users. With the inevitable transition to IPv6 on the horizon, this research is extremely relevant and groundbreaking.

The team also took third place at the 2011 National Security Innovation Competition sponsored by the National Homeland Defense Foundation with their entry of the MT6D, Moving Target IPv6 Defense device.

For more information see the article published on VT News: <http://www.vtnews.vt.edu/articles/2011/05/051111-research-itsecurityproduct.html>

Virginia Tech IT Security Office

1300 Torgersen Hall

Phone:
540/231-1688

E-mail:
itso@vt.edu

Website:
www.security.vt.edu

Fake Antivirus and Friends

Fake Antivirus infections are nothing new to the Virginia Tech campus and they are easy to detect. However, it has been recently observed by the IT Security Office that many of these Fake AV infections are now accompanying other malware. This other malware includes TDSS rootkits and Zeus variants. Machines that are infected with Fake AV should no longer be considered clean by just removing the Fake AV.

Fake AV infections occur predominantly from users clicking on an ominous popup window. If you notice a Fake Antivirus pop-up, don't click anywhere on the pop-up window, it isn't safe. Instead use a keyboard short-cut to kill the window/program.

For example on Windows some applications support **Alt-F4** to close out the application.

The safest method is to force quit the web browser using the **CTRL-ALT-DELETE** command sequence and to end the web browser process.

Finally, let your IT support know immediately if you think you may have been infected.

BE SECURE, BE UNIQUE.

CHANGE YOUR



It's a university requirement to change all PID, Hokies, and Oracle/Banner passwords by July 1, 2011.

 **VirginiaTech**
Invent the Future®