

## VT IT Security News...

### Departmental Risk Assessments

The IT Security Office is once again providing the resources and tools to help in completing your risk assessment. Please feel free to contact Wayne Donald ([wdonald@vt.edu](mailto:wdonald@vt.edu)) if you would like assistance in understanding the process involved in completing a risk assessment.

Please reference the following site for instructions and the forms associated with completing the risk assessment:

<http://www.security.vt.edu/RiskAssessment/riskassesmentmain.html>

### Departmental Computer Support Symposium

The Departmental Computer Support Symposium--DCSS--is presented each April and October. The symposium allows support personnel from various departments on campus to learn more about information technology trends on campus.

**Date:** April 22<sup>nd</sup>, 8am - Noon

**Location:** Owens Banquet Hall

**Sponsor:** Information Technology

**Contact:** Susan Brooker-Gross

[srb144@vt.edu](mailto:srb144@vt.edu)

540-231-1715

Spring topics to include:

- Kay Heidbreder, University Counsel, on copyright issues
- Anne Moore, Assoc. VP Learning Technologies, on the ResearchChannel consortium
- Updates on: CAS, Shibboleth, and personal digital certificates

Requests for presentations or attendance should be submitted to Susan Brooker-Gross via email.

### Virginia Tech Spring SANS Courses

**Date:** March 3 – 8th, 2008

**Location:** 2150 Torgersen Hall

**Sponsor:** Information Technology

**Contact:** Randy Marchany

[marchany@vt.edu](mailto:marchany@vt.edu)

**Website:** [www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect)

## VA SCAN News...

The Virginia Alliance for Secure Computing and Networking (VA SCAN) exists for the purpose of strengthening information technology security programs within the Commonwealth of Virginia.

<http://www.vascan.org>

### VASCAN Conference at Virginia Tech October 6-7<sup>th</sup>, 2008.

VA SCAN's fifth annual conference will be held on Monday and Tuesday October 6<sup>th</sup> and 7<sup>th</sup> at Virginia Tech Blacksburg, Virginia. Don't miss this opportunity to hear leaders in the IT security field discuss current issues and share ideas on effective IT security practices next year.

## State and National IT Security News...

### Educause Security Conference

**When:** May 4<sup>th</sup> – 6<sup>th</sup>, 2008

**Where:** Arlington, VA

Sponsored by the [EDUCAUSE & Internet2 Computer and Network Security Task Force](#), the 2008 Security Professionals Conference annual meeting brings together information security professionals, IT staff, and others from across the higher education community. The Security 2008 conference will include keynote speakers, pre and postconference seminars, corporate displays, and sessions that address technical solutions, security policies and procedures, and management issues, including security training and awareness. View resources from past conferences at [www.educause.edu/conference/security/](http://www.educause.edu/conference/security/)

# IT Security Tips and Services...

## Security Reviews by the IT Security Office

The IT Security Office will regularly scan for vulnerabilities on Virginia Tech's network to help identify potential problems that could result in data disclosures, illegal use, weak systems that are attractive for attacks, etc.

Security reviews are also conducted on a regular basis for areas that are required by policy (or law) to verify a secure operating environment. For example, requirements from the Payment Card Industry (PCI) for systems that collect credit card data, HIPPA in terms of health related information, and others.

In all of these cases, the IT Security Office will follow-up by contacting and working with areas to eliminate problems that may be discovered.

Areas may request security review be done in a specific area by contact Brad Tilley at [brad.tilley@vt.edu](mailto:brad.tilley@vt.edu).

## Maintaining a Secure Website

The IT Security Office would like to remind everyone to make certain you follow a few guidelines if you would like to use a website that hosts web applications, web services, or may contain confidential data.

Please consider the following when setting up and maintaining a secure website:

- Web service software must be installed and configured in accordance with vendor security recommendations.
- Only those web services or applications specifically needed should be enabled. Web services, applications, and sample content not needed should be disabled.
- Web server software, web applications, additional software modules, and application software should be kept up to date with security advisories and patches must be applied as promptly as possible.
- Web technology solutions developed by vendors or third-party developers unresponsive to patching security vulnerabilities should be replaced with a secure alternative.
- The web server must be configured to adhere to

Virginia Tech IT Policy 7025: Safeguarding Nonpublic Customer Information and Virginia Tech IT Policy 7010: Policy for Securing Technology Resources and Services.

- Web applications that store or transfer sensitive data must use asymmetric encryption to ensure that the data is protected per Virginia Tech IT Policy 7025.
- Content uploaded through web applications should be stored outside of the document root. Uploaded content should be reviewed before it is made public.
- Web servers and web applications must not run with elevated privileges (e.g. "root" or "Administrator") and must remain segmented from the system processes.
- Secure mechanisms must be used to allow developers to install new, or update existing, content.

## SANS Top 10 Cyber Threats, 2008

Twelve cyber security experts identified and ranked the most damaging and likely attacks to be faced in cyberspace in 2008.

1. Attacks That Exploit Browser Vulnerabilities and Trusted Web Sites
2. Attack of the Botnets
3. Cyber Espionage seeking large amounts of data using phishing techniques
4. iPhones and VOIP Beware
5. Insider Attacks
6. Advanced Identity Theft from Persistent Bots
7. Increasingly Malicious Spyware
8. Web Application Security Exploits
9. Increasingly Sophisticated Social Engineering Including Blending Phishing with VOIP and Event Phishing
10. Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.)