



# **Monthly Information Security Tips NEWSLETTER**

**February 2009**

Volume 4, Issue 2

## **Internet Security Trends for 2009**

**From the Desk of Rowland B. Harrison – ODU Information Security Officer**

Our daily lives are becoming increasingly reliant on computers and the Internet. We exchange information, operate businesses and perform financial transactions with little thought of the real risks involved in doing so. Everyday, the volume and complexity of internet threats increases, and the knowledge required to launch a successful attack decreases. Although we develop more robust defenses, internet criminals and hackers devise new ways to attack our computers. These factors create an environment in which education and vigilance are required to help mitigate the risks.

Threats such as identity theft, worms and viruses, loss of sensitive information and other malicious activities are part of an ever-evolving internet security threat landscape. Some of the key challenges we are facing in 2009 focus on application security. Application security is a crucial layer in a multi-tiered information security strategy. Building security in at the beginning of development is an important factor in minimizing potential vulnerabilities.

We've seen the results when vulnerabilities in web applications are exploited, leading to SQL injection attacks, cross-site scripting and other malicious activities. However, a commonly seen scenario includes internet criminals who take advantage of commercial web sites that have poor security. They add code to the web site that silently re-directs the unsuspecting user's web browser to another malicious site designed to infect the user's computer with any number of viruses, trojans and keyloggers.

Another alarming trend continues to be the evolution of internet crime, which has morphed from fairly innocuous web-site hacking and "graffiti" attacks to organized crime syndicates seeking profit. Internet crime is now big business. Attackers want your credit card and other financial information as well as your social security number. According to a recent study by McAfee, the global cost of internet crime due to identity theft and data breaches is an estimated \$1 trillion dollars. Many data thefts are orchestrated by organized crime, both in the U.S. and abroad.

The economic recession is another factor that may impact information security. The risks due to disgruntled insiders are a major concern, and are expected to increase due to the economic downturn and organizational downsizing. Phishing scams and other social engineering attacks will increase, as attackers try to take advantage of bank closings, claims for "easy credit", and employment offers. Phishing attempts are no longer easily detected based on misspelled words in the email, or claims of large sums of money left to you in some foreign location. The phishing scams are becoming more targeted and more "realistic" in appearance.

Email related to holidays and major news events is still a popular vehicle for compromising computers. During February, Valentine's Day email messages were circulated that could infect a user's computer when the attachment was opened or URL was clicked. Once the computer was

infected, the malware would attempt to capture the user's personal information and transmit it to the internet criminals.

### **What can be done to make to protect my computer and my personal information?**

Good security is implemented through a multi-layer approach. Users can minimize risk by following the recommendations below:

- Install and maintain a firewall.
- Use anti-virus and anti-spyware software and set them to auto-update.
- Keep operating system and other software up-to-date by enabling the auto-update feature.
- Be cautious about all communications; think before you click. If an email appears to be a phishing communication, do not respond. Delete it.
- Do not open email or related attachments from untrusted sources.
- If you receive an email appearing to be from a legitimate business, requesting the submission of personal information, it is most likely a scam. Legitimate businesses do not send emails requesting personal information.

**For additional information on protecting yourself from the latest internet threats, please visit:**

Phishing: How to Avoid Getting Hooked! [www.msisac.org/awareness/news/2008-10.cfm](http://www.msisac.org/awareness/news/2008-10.cfm)

Web Browser Attacks [www.msisac.org/awareness/news/2008-10.cfm](http://www.msisac.org/awareness/news/2008-10.cfm)

Online Shopping [www.msisac.org/awareness/news/2007-12.cfm](http://www.msisac.org/awareness/news/2007-12.cfm)

Top Ten Cyber Security Tips [www.msisac.org/awareness/news/2006-10.cfm](http://www.msisac.org/awareness/news/2006-10.cfm)

**For more monthly information security newsletter tips visit:**

<http://www.vita.virginia.gov/communications/publications/InformationSecurityTips>

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

***These tips are brought to you in the Commonwealth of Virginia by the Virginia Information Technologies Agency***

<http://www.vita.virginia.gov/security/>

***in coordination with:***



[www.msisac.org](http://www.msisac.org)