



# Enterprise Security Office Monthly Security Tips NEWSLETTER

January 2012

Volume 7, Issue 1

*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 cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

## Cyber Security Emerging Trends and Threats for 2012

During 2011, cyber security incidents included theft of intellectual property and government data, hacktivism, malware targeting mobile devices and a resurgence of the Zeus Trojan, which targets financial information. Protecting against these attacks was a key challenge for organizations of all sizes in both the public and private sectors.

What is in store for 2012? Below is a brief round up of the cyber security threat landscape highlighting some of the challenges we can expect during the next 12 months.

### **Mobile Devices and Apps**

The use of mobile devices will continue to grow in 2012, consequently, so too will the volume of attacks targeted to these devices. Every new smart phone, tablet or other mobile device provides another window for a potential cyber attack. Closely tied to the trend of more smart phones and tablets being deployed in the enterprise will be the influx of new apps for those devices. Location-based mobile apps and games all pose potential threats. The risks include access to information such as physical location or contacts lists, as well as the ability for the apps to download malware, such as keyloggers or programs that eavesdrop on phone calls and text messages. Hackers are quickly learning how to harvest legitimate applications and repackage them with malicious code before selling/offering them on various channels to the unsuspecting user.

### **Hactivism**

Attacks carried out as cyber protests for a politically or socially motivated purpose are expected to increase, especially in light of the activist movements continuing to take place across the country and around the globe. Common strategies used by hactivist groups include denial of service attacks and compromise of user credentials to gain access to data, along with posting of emails, credentials, credit card information and other sensitive exfiltrated information.

### **Search Engine Optimization (SEO) Poisoning**

Cyber criminals will continue to take advantage of the 24-hour news cycle to target visitors searching on the most popular keywords or sites and infect users via sites designed to look like legitimate news services, Twitter feeds, Facebook posts/emails, LinkedIn updates, YouTube video comments, and forum conversations. We expect cyber criminals to take advantages of notable news events such as the London Olympics, U.S. presidential elections, and Mayan calendar predictions.

### **Social Engineering**

Social engineering tactics—including the use of rogue anti-virus to entice users into clicking on malicious links—will continue. Experts also anticipate that in 2012 we will also see a growth in fake registry cleanup, fake speed improvement software, and fake back-up software mimicking popular personal cloud services.

### **Advanced Persistent Threat**

Advanced Persistent Threat (APT) refers to a long-term pattern of targeted hacking attacks using subversive and stealthy means to gain continual, persistent exfiltration of intellectual capital. The entry point for espionage activities is often the unsuspecting end-user or weak perimeter security. APT is likely to remain high in 2012. Whether focused on exploiting vulnerable networks for use as a storage location or relay point, or to gain insider information, cyber espionage will remain a consistent threat to networks.

### **Spear Phishing Attacks**

Spear phishing is a deceptive communication (e-mail, text or tweet) targeting a specific individual, seeking to obtain unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are

more likely to be conducted by perpetrators seeking financial gain, trade secrets or sensitive information. Spear phishing is often the nexus to cyber espionage and will continue to grow.

### What Can You Do?

By using sound cyber security practices, users and organizations can strengthen readiness and response to help defend against the myriad of challenges and mitigate potential impacts of incidents:

- Make sure that you have encryption and password features enabled on your smart phones and other mobile devices.
- Use strong passwords, ones that combine upper and lower case letters, numbers, and special characters, and do not share them with anyone. Use a separate password for every account. In particular, do not use the same password for your work account on any other system.
- Properly configure and patch operating systems, browsers, and other software programs.
- Use and regularly update firewalls, anti-virus, and anti-spyware programs.
- Do not use your work email address as a "User Name" on non-work related sites or systems.
- Be cautious about all communications; think before you click. Use common sense when communicating with users you DO and DO NOT know. Do not open email or related attachments from un-trusted sources.
- Don't reveal too much information about yourself on social media websites. Depending on the information you reveal, you could become the target of identity or property theft.
- Verify Location Services settings on mobile devices.
- Allow access to systems and data only by those who need it and protect those access credentials.
- Follow your organization's cyber security policies and report violations and issues immediately.
- Learn to recognize a phishing website. Visit <https://www.phish-no-phish.com> to learn ways to identify a phished website.

### For More Information:

- Verizon: [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf)
- Symantec: [http://www.symantec.com/content/en/us/enterprise/white\\_papers/b-symc\\_intelligence\\_qtrly\\_jul\\_to\\_sep\\_WP.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_jul_to_sep_WP.en-us.pdf)
- Websense: <http://www.websense.com/assets/reports/2012-Predictions-WS-Security-Labs.pdf?cmpid=pmr11.11.17>
- SANS Institute: Security Predictions 2012 & 2013 -- <http://www.sans.edu/research/security-laboratory/article/security-predict2011>
- Georgia Tech: Emerging Cyber Threats Report -- [http://www.gtisc.gatech.edu/doc/emerging\\_cyber\\_threats\\_report2012.pdf](http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf)
- Imperva: Security Trends 2012: [http://www.imperva.com/docs/HL\\_Security\\_Trends\\_2012.pdf](http://www.imperva.com/docs/HL_Security_Trends_2012.pdf)

For more monthly cyber security newsletter tips, visit: [www.msisac.org/awareness/news/](http://www.msisac.org/awareness/news/)



**The MS-ISAC, a Division of the  
Center for Internet Security**  
[www.msisac.org](http://www.msisac.org)