VOLUME 2, ISSUE 4

DECEMBER 2009

InsighT to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter

In this Issue:

Top 10 Security Tips 1,2

Automatic Software Updates/Patching 3

Quick Security Highlights 4,5

How do I update Windows applications? 5

The Top 10 Security Tips (from MS-ISAC)

This article provides the TOP 10 Cyber Security Tips that you should use to protect your computer system.

1. Think Before You Click

Always think before you click on links or images in an email, instant message, or on web sites. Be cautious when you receive an attachment from unknown sources. Even if you know and trust the sender of the email, instant message, web site, or a friend's social networking page, it is still prudent to use caution when navigating pages and clicking on links or images.

2. Use Hard to Guess Passwords

Good password practices will help keep your personal information and identity more secure. Passwords should have at least eight characters with uppercase and lowercase letters, numerals and symbols.

3. Avoid Phishing Scams

Phishing is a form of identity theft in which the intent is to steal your personal data, such as credit card numbers, passwords, account data, or other information. Do not reply to emails that ask you to “verify your information” or to “confirm your user-id and password.”

Top 10 Security Tips (from page 1)

4. Shop Safely Online

When shopping online always know with whom you're dealing. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission. Always remember to pay by credit card and keep a paper trail.

5. Protect Your Identity

When visiting web sites, it's important to know what information is being collected, by whom and how it will be used. Web sites track visitors as they navigate through cyberspace, therefore, data may be collected about you as a result of many of your online activities. Please keep in mind most legitimate web sites include a privacy statement. The privacy statement is usually located at the bottom of the home page and details the type of personally identifiable information the site collects about its visitors, how the information is used - including with whom it may be shared - and how users can control the information that is gathered.

6. Dispose of Information Properly

Before discarding your computer or portable storage devices, you need to be sure that the data contained on the device has been erased or "wiped." Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software.

7. Protect Your Children Online

Discuss and set guidelines and rules for computer use with your child. Post these rules by the computer as a reminder. Familiarize yourself with your child's online activities and maintain a dialogue with your child about what applications they are using. Consider using parental control tools that are provided by some Internet Service Providers and available for purchase as separate software packages.

8. Protect Your Portable Devices

It is important to make sure you secure your portable devices to protect both the device and the information contained on the device. Always establish a password on all devices. If your device has Bluetooth functionality and it's not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device. Encrypt data and data transmissions whenever possible.

9. Secure Your Wireless Network

Wireless networks are not as secure as the traditional "wired" networks, but you can minimize the risk on your wireless network by enabling encryption, changing the default password, changing the Service Set Identifier (SSID) name (which is the name of your network) as well as turning off SSID broadcasting and using the MAC filtering feature, which allows you to designate and restrict which computers can connect to your wireless network.

10. Back-Up Important Files

Back-up your important files minimally on a weekly basis. Don't risk losing your important documents, images or files!

Automatic Software Updates and Patching

Security vulnerabilities are flaws in the software that could allow someone to potentially compromise your computer. Vulnerabilities in commonly used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office are prime targets of attacks on computers connected to the Internet.

Recent statistics reported show that 48% of the cyber attacks identified in the second quarter of 2009 were targeted against vulnerabilities in Adobe Acrobat/Adobe Reader[1] and in October 2009 Microsoft released patches for a record number of security holes. No one is immune to vulnerabilities, so we need to understand the risks and take appropriate mitigation measures.

> ***Note*:** *Many organizations have formal processes to patch systems that will automatically update all appropriate software. In these situations, no end user action is required. However, this is always important for home computers.*

Why do I need to update my software?

Software updates fix problems in the software, add functionality, and most importantly, fix vulnerabilities that impact the security of the software and subsequently your computer. These vulnerabilities can lead to your computer—and information that resides on it—being compromised. You can be at risk by opening documents, viewing an email which contains malicious code or visiting a web site hosting malicious content. Seventy percent of the top 100 web sites hosted malicious content or contained a link designed to redirect users to malicious sites.[2]

What is a software patch and when should I install software patches?

A patch is software that is used to correct a problem to an application (software program) or an operating system. Computer companies are continuously addressing security vulnerabilities in computer software which could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the software vendor typically issues a patch to correct the problem. This patch should be applied as soon as possible since the average time for someone to exploit this security hole can be as little as a few minutes. Most major software companies will periodically release patches, usually downloadable from the Internet, that correct very specific problems in their software programs.

My computer has dozens of software programs-- which ones do I need to update and how often?

One of the challenges facing the average computer user is to know which software needs to be updated and how often.

Many software programs include a feature called "auto update." This feature allows the computer to check for updates at periodic intervals. The software will automatically check for updates and save them to your computer.

At a minimum, you should enable the auto update feature on the following products:

- **Anti-virus and Anti-spam signatures**: anti-virus and anti-spam software requires regular updates to virus and spam signatures to remain effective. New viruses and other types of malware appear every day and the anti-virus/anti-spam vendors release new signatures on a daily basis or more often to stay on top of the new threats.
- **Windows Office software:** Word, Excel, Outlook, etc.
- **Internet Browsers:** e.g., Internet Explorer (Microsoft), Firefox (Mozilla), Safari (Apple) and Chrome (Google).
- **Adobe products:** e.g., Adobe Reader, Adobe Acrobat, Flash, Shockwave
- **Media Players:** e.g., Windows Media Player (Microsoft), QuickTime (Apple), Real Player (Real Networks) and Flash Player (Adobe)
- **Java (Sun Microsystems)**: Java is software that is installed on most computers to allow users to play online games, conduct online chats, and view images in 3D, among other functions.

- **Other software programs that communicate or interact with the Internet**, like e-mail, web servers, and remote desktop software which are especially susceptible to attacks and should be kept current on patches and version levels.

Sources: 1) F-Secure; 2) SC Magazine

Office of the CIO, Cyber Security Newsletter

650 W State St
Boise ID 83720

Phone: 208-332-1851
Email: terry.pobst-martin@cio.idaho.gov

CHECK OUT THESE LINKS

Security Websites:

Good websites to surf:

http://www.sans.org/

http://www.cert.org/

http://www.msisac.org/

http://csrc.nist.gov/

http://www.issa.org/

http://www.infragard.net/

http://www.ic3.gov/

http://www.securityfocus.com/

http://www.snopes.com/

http://www.nationalterroralert.com/

If you act defensively on the internet, you'll be safer.

Just like driving defensively, you should browse defensively. Watch out for the bad guys!

Quick Security Highlights

December 22, from *The Register* – IPhone Worms can Create Mobile Botnets. A detailed analysis of one relatively malign worm in a recent spate of iPhone worms indicates that criminals will likely be able to turn IPhones into bots, or zombies, as a part of a mobile botnet. The IKee-B (Duh) iPhone worm, released in late November, exploited default root passwords on jailbroken iPhones to turn the smartphones into botnet clients under the control of a server based in Lithuania. The worm affected iPhone users in The Netherlands, and specifically targeted customers of Dutch online bank ING Direct. Security researchers at SRI International - which has been noted for top notch work in dissecting the Conficker botnet - published an analysis of the iPhone botnet on Monday that warns users of Apple's device and similar smartphones to expect more of the same in future. Warnings about mobile malware have been circulating for years. But it's only since the advent of iPhones and other smartphones, allowing decent internet access with what's essentially a mini-computer, that such risks have become tangible.

December 21, from the *SCMagazine* – Malicious e-Cards and Brittany Murphy "News" flood inboxes. Security researchers are warning that 2 separate threats (the usual holiday malicious e-greeting cards scam and phony news links to Brittany Murphy death related sites) both share a goal to install malware on victims' computers.

1) A virus analyst at Sophos has announced the expected new wave of spam purporting to be Christmas-related electronic greeting cards sent from Hallmark has begun. The phony e-card link doesn't bring happy holiday wishes, but instead installs a trojan known as VBInject. It has become routine that major holidays bring increases in e-card scams. People should avoid clicking on links to e-cards from anonymous or un-recognized senders.

2) Meanwhile, the untimely death of an actress has, as is now the norm, given rise to a number of poisoned search attacks, said McAfee Avert Labs. Searches for news on the death of Brittany Murphy or "famous actress dies" or "famous actress 8 mile" have resulted in a number of false results trying to lure users to websites pushing rogue anti-virus programs or other malware. The ploy is a common one for attackers hoping to cash in on a curious public seeking news on a major media story.

News or Malware?

Quick Security Highlights (continued)

December 21, from *The Register* – Twitter hack linked to Internal Security Breach. For about an hour last Friday, December 18th, visitors to Twitter were redirected to a protest site rather than the Twitter micro-blogging site. The site they were redirected to held a webpage that stated Twitter had been hacked by the "Iranian Cyber Army." In addition to boasting about hacking the social site, the group also protested the US interfering with the recent Iranian elections.

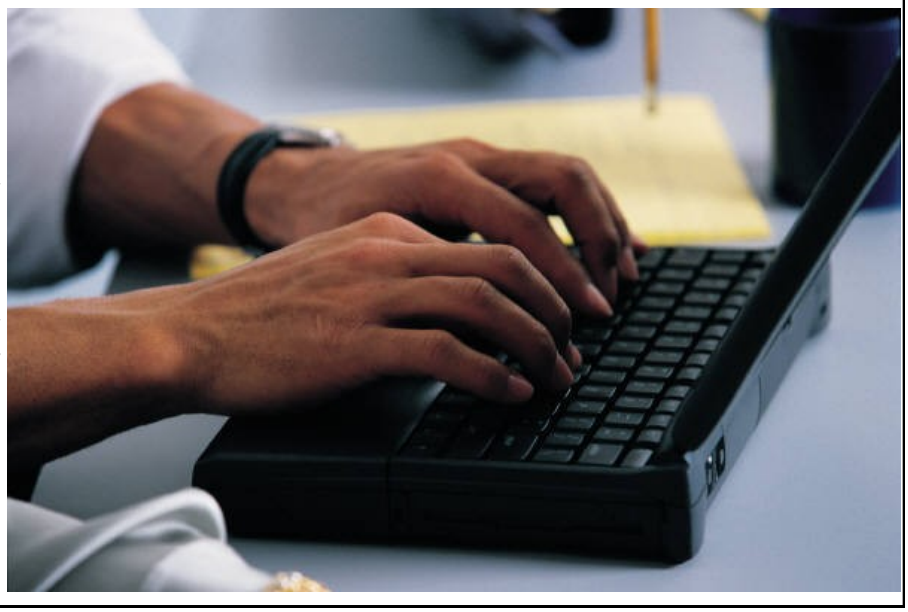
The worrisome part for Twitter was that valid credentials were used to cause the redirection of visitors browsers, meaning the security of the site is again highlighted as a problem.

December 18, from *V3.co.uk* – Botnet gets into "pump-and-dump" scam. A huge Botnet named 'Donbot' has recently been identified as implementing a rash of stock-related spam e-mails that persuade the recipients to invest in a low-priced stock. The increased purchasing raises the price of the stock and the spammer then sells it at a profit. Researchers at MessageLabs stated that, though these scams were common in the past, they have almost disappeared in the last few years. This could be the first sign that, as experts have been predicting, the increasingly competitive market could lead criminals to more of this type of pump-and-dump scam or other creative confidence schemes.

How do I update my Microsoft Windows applications?

Windows Update is a Microsoft service that provides updates for the Windows operating system and other Microsoft software. Installing Windows updates, such as "service packs" and other patches, is necessary to keep your Windows system secure.

To activate Windows Update, go to Settings/Control Panel/Automatic Updates. When you turn on Automatic Updates, Windows routinely checks the Windows Update web site for high-priority updates that can help protect your computer from the latest viruses and other security threats.



These updates can include security updates, critical updates, and "service packs." Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs, or notifies you as these updates become available.

Be sure to set the auto updates to daily, as patches can be released at any time.