State of WEST VIRGINIA
Monthly Cyber Security Tips
NEWSLETTER

OCTOBER 2006 Volume 1, Issue 5

October 2006 Cyber Security Tips

From the Desk of the West Virginia Information Security Office – Jim Richards, Director (jimrichards@wvgot.org

October 2006 Cyber Security Tips

1. **Use and Regularly Update Anti-Virus, Firewalls, and Anti-Spyware programs**

There are many types of Internet security and safety issues that you need to defend against. One of the most effective ways of defending your PC is to use a firewall, and up to date anti-virus and anti-spyware products. A firewall works by examining information coming from and going to your network and/or the Internet. It identifies and rejects information that comes from a dangerous location or seems suspicious. If you set up your firewall properly, hackers searching for vulnerable computers usually can't even detect your computer.

Viruses, worms, and trojans horses are malicious programs that can cause damage to your computer and information on your computer. They can also slow down the Internet, and they might even use your computer to spread themselves to your friends, family, co-workers, and the rest of the Web. Good anti-virus products are constantly kept up to date, so maintaining your virus identification is important regardless of which product you choose. These anti-virus programs work by identifying specific behaviors and files and stopping them from accessing your system, causing damage and further propagating themselves.

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. You might have spyware or other unwanted software on your computer if see pop-up advertising even when you are not on the web, your default web page changes without your consent, a new toolbar appears and you can't get rid of it, or your computer slows down dramatically or crashes. Just like good anti-virus products, anti-spyware products need to be kept up to date in order to detect the newest identified threats, so maintaining your subscription is important regardless of which product you choose.

For more information visit:
http://www.staysafeonline.com/toolbox/fundamentals/defend_yourself.html
http://www.us-cert.gov/cas/tips/ST04-005.html
http://www.us-cert.gov/cas/tips/ST04-016.html

2. **Properly setup and patch Operating Systems, Browsers, and other software programs**

Software makers routinely create updates for their products, in some cases to provide feature improvements, but also as the first line of defense in keeping your computer as secure as

possible. Whenever updates become available, it is very important to promptly patch your operating systems and programs. Sometimes these patches are created to protect systems against potential attacks, and sometimes dangerous attacks already exist by the time updates are released. Of special note, you want to make sure you update any software you use for browsing the Internet as well (Internet Explorer, Firefox, Netscape, Opera, Amaya, etc.) because Internet-based browsing attacks are becoming more common and more dangerous. Other software programs that communicate or interact with the Internet, like Email, Web Servers, and Remote Desktop software are especially susceptible to attacks, and should be kept current on patches and version levels, also.

For more information visit:
http://www.staysafeonline.com/toolbox/fundamentals/keep_up-to-date.html
http://www.us-cert.gov/cas/tips/ST05-001.html

3. **Passwords and Authentication methods**

Passwords and other authentication methods like using tokens, keys, or biometrics are ways systems verify that you are who you claim to be. If someone else uses your credentials, the system will think it's you. That person could do anything you could do on your computer, and the system would log their actions (such as deleting files, sending malicious emails, or browsing to inappropriate sites) under your access credentials. It is therefore very important to protect both your access and yourself by using strong passwords or even 2-factor authentication schemes. Furthermore, don't share your passwords and access codes, don't store them in unencrypted files, and don't' write them down unless you then place them in a locked, secured location.

Passwords need to be strong and complex so that they are not easily guessed and they are not quickly cracked. Default passwords, names, and dictionary words, even in different languages, can be easily guessed or cracked, so use complex passwords that have numbers, letters, and special characters in them. Passwords aren't much use if you cannot remember them, so use a pass-phrase instead. The phrase "Would you like 3 scoops of ice cream?" can become the strong password "Wul3$o1c?" which is not easily guessed nor cracked.

For more information visit:
http://www.microsoft.com/athome/security/privacy/password.mspx
http://www.us-cert.gov/cas/tips/ST04-002.html

4. **Lock your workstation/laptop when you leave it, and configure it to automatically lock after a short period of inactivity**

One of the fastest ways of compromising a system is to simply walk up to an unattended, unlocked workstation or server and access the system. No passwords to break, no equipment to set up, no permissions to circumvent, just start typing and clicking and everything's accessible by the attacker. E-mail access, project files, confidential records, and personal files could all be easily compromised. In addition, it could take mere seconds for someone to open an anonymous-access service to your machine, or install a backdoor into the system. The attacker could then rifle through your folders, files, and applications at a later time and at their convenience. If someone does do something malicious via your account, the system will record the event as done by you, not by someone else. Be safe and lock it when you leave it. For Microsoft systems you can lock the system with the <Ctrl><Alt><Del> combination, or <Windows Tab><L> for Windows XP.

In addition, it's very easy to get sidetracked and stay away from your desk longer than you anticipate, so configure your system to automatically lock after a short period of inactivity. It is an easy way to help protect your account and the items you have access to. Lockout after fifteen minutes of inactivity is recommended and shorter periods for critical systems or even laptops when you are traveling.

For more information visit:
http://www.us-cert.gov/cas/tips/ST04-003.html

5. **Backup important files regularly**

There are many ways you can lose information on a computer. A destructive virus, a power surge, lightning, floods, a big magnet, or sometimes equipment just fails. If you regularly make backup copies of your files and keep them in a separate place, you can get some, or even all, of your information back in the event something happens to the originals on your computer.

For more information visit:
http://www.staysafeonline.com/toolbox/fundamentals/backup_basics.html
http://www.us-cert.gov/cas/tips/ST04-003.html

6. Be cautious when using the Internet

Browsing to non-work related sites can increase the risk of becoming infected with spyware, viruses, and other malicious code. Download files and install programs only when you are authorized to do so, and only when there is a real need. Know with whom you are dealing on the Internet – anonymous doesn't necessarily mean safe, and many criminals are very good at impersonating real financial organizations like banks and credit card companies. Never share personal or confidential information if you are uncertain of the recipient's identity or if you are uncertain that they need the information in question. Even when you are certain with whom you are dealing, never share sensitive or confidential information over an unencrypted internet connection.

For more information on safe browsing tips visit:
http://www.us-cert.gov/cas/tips/ST04-013.html
http://www.us-cert.gov/cas/tips/ST04-012.html

7. Messaging Security – Email and Instant Messaging

Email and Instant Messaging (IM) are wonderful tools but they can be used or misused in a variety of ways. As a general rule, do not send confidential or sensitive information, like social security numbers, account numbers, or secret information through unencrypted e-mail or IM. Do not open a message that is of a questionable nature, such as when it has an unusual attachment or it is from an unknown sender. Spammers can try to validate targeted email accounts in order to continue spamming to them, and malicious code is often spread via email or even Instant Messaging attachments. Also remember that email and news are subject to forgery and spoofing, so apply common sense before assuming a message is valid. While hoaxes do not actually infect systems like a virus or a Trojan-Horse program, they are still time consuming and are a drain on departmental resources.

Phishing is a special type of email or IM attack. A phisher sends out a fake notice like 'your credit account has been disabled', a plea for help, or a note about an enticing subject which also contains a link to a malicious website. Your system can get infected with spyware, viruses, or even a Trojan horse sometimes by just clicking on that link and visiting such a site. If you share personal information with others as a result of answering such messages, your identity could even get stolen.

For more information visit:
http://www.microsoft.com/athome/security/email/attachments.mspx
http://onguardonline.gov/phishing.html
http://www.consumer.gov/idtheft/ddd/index.html
http://hoaxbusters.ciac.org/

8. Review Your Computer Security

Evaluate your computer's security periodically, and apply appropriate repairs, upgrades, and replacements. Maintaining your computer is kind of like maintaining your car. You need to check the fluids, the tire pressure, the engine belts and fan, make sure the brakes and accelerator works, make sure the doors close and lock properly, and then fix or replace the items that are broken in order to keep your car in good working order. If you don't maintain your car, even if you are the safest driver in the world, eventually it will break down. Similarly, if you do not review and update your computer's security, it will also break down, allowing bad things to happen to it.

For more information visit:

http://www.staysafeonline.com/toolbox/how_to/index.html

9. Responding to a Cyber Incident

Learn how to recognize cyber attacks, and know what to do if things go wrong. Ask if your agency has a cyber security incident response plan and a cyber security incident response team (CSIRT), and if so use it when appropriate. Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately. If you don't know how to report a cyber incident, ask someone in your IT department or your Help Desk how to do this. Office of Technology Help Desk 1-304-558-1257.

10. Remember that cyber security is everyone's responsibility

Just like one leak can sink a boat, one data leak, one security breach, or one malicious worm can sink an organization. By protecting yourself and the systems entrusted to you, you are protecting your fellow personnel, your entire organization's network and data, and ultimately, the citizens that are depending on you.

For more information on issues specific to our organization, please visit:
(Organization's security homepage) for example, http://www.cscic.state.ny.us/

Brought to you by:	
MS-ISAC http://www.msisac.org	US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM