Metro.net (web)

Resources

- Safety
- Pressroom (web)
- Ask the CEO
- CEO Forum
- Employee Recognition
- Employee Activities
- Metro Projects
- Facts at a Glance (web)
- Archives
- Events Calendar
- Research Center/ Library
- Metro Classifieds
- Bazaar

Metro Info

- 30/10 Initiative
- Policies
- Training
- Help Desk
- Intranet Policy

Need e-Help?

Call the Help Desk at 2-4357

Contact myMetro.net

Take Heed: October is Cyber Security Awareness Month

Identity theft is rampant, says Chief Information Officer Elizabeth Bennett. Drawing on information from the California Office of Information Security, Bennett puts cyber-safety at the office and at home in perspective. Before an e-mail with a virus attached can reach your desktop, ITS has taken an abundance of precautions to protect you and the Metro network from an equal abundance of security risks. The bad news: Identity theft is more likely to happen at home. Read on to find out why cyber security is important and what steps you can take to stay safe.

(Oct. 22, 2009) With reports of cyber crime increasing daily, California Governor Arnold Schwarzenegger has proclaimed October 2009 as Cyber Security Awareness Month.

Days after the Governor's proclamation, two news services ran these headlines:

- Wed, October 07, 2009 — IDG News Service — The head of the U.S. Federal Bureau of Investigation has stopped banking online after nearly falling for a phishing attempt. In June -- the latest month for which figures are available -- the Anti-Phishing Working Group counted nearly 50,000 active phishing Web sites, the second-highest number it has ever recorded.
- Wed, October 07, 2009 — Computerworld — Scammers have grabbed the Hotmail passwords that leaked to the Web and are using them in a plot involving a fake Chinese electronics seller to bilk users out of cash and their credit card information, a security researcher said today. The saga of the compromised accounts started last week, when more than 10,000 Windows Live Hotmail passwords were posted to the Internet. This week, details of another 20,000 Hotmail, Google Gmail and Yahoo Mail accounts went public.

First things first, says the California Office of Information Security. Learn the lingo, recognize the risks and take control of your cyber-responsibility. Here is an easy-to-digest primer followed by the information agency's top ten cyber security tips.

What is Cyber Security?

It seems that everything relies on computers and the Internet now — communication (email, cell phones), entertainment (digital cable, MP3's), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system? Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. Unfortunately, there's no 100% guarantee that

even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

For starters, never even answer an e-mail from a bank or institution wanting to "update" your personal and financial information, such as your social security number, birth date, full name, etc. This is a blatant example of an attempt to steal your identity. Banking and other institutions are required to use the U.S. Post Office to request information like that.

What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them:

- *Hacker, attacker, or intruder* - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious (stealing or altering information).

- *Malicious code* - This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

- *Viruses* - This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

- *Worms* - Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

- *Trojan horses* - A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

top

Top Ten Cyber Security Tips

TOP 10 simple, easy, and basic things that everyone can and should do to protect their computer systems and data from harm by various cyber attacks and other types of security incidents that can cause damage, consume computer resources, or expose confidential information.

Use and regularly update firewalls, anti-virus, and anti-spyware programs.

There are many types of Internet security and safety issues that you should defend against. One of the most effective ways of defending your computer is to use a firewall and up to date

anti-virus and anti-spyware products.

A firewall works by filtering information coming from and going to your network/computer and/or the Internet. It identifies and rejects information that comes from a location or source known to be dangerous or contains information that seems suspicious.

Anti-Virus programs can stop Viruses, worms, and Trojan horses, which are malicious programs that can cause damage to your computer and information on your computer. Those malicious programs can also slow down the Internet access and might even use your computer to spread themselves to your friends, family, or co-workers.

Spyware is a general term used for software that performs certain behaviors such as pop-up advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. An anti-spyware program helps stop such misuse, but they need to be kept up to date in order to detect the newest identified threats as well. Configuring your anti-virus and anti-spyware products to automatically update their identification files on a daily basis is highly recommended.

For more information visit:

> http://www.msisac.org/localgov/info/firewall-guide.pdf
> http://www.msisac.org/awareness/oct05/csab05.pdf
> 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

Properly setup and patch operating systems, browsers, and other software programs.

Whenever security updates or service packs become available for your operating system or programs, it is very important to promptly download them and patch your operating systems and programs. These patches are created to protect systems against potential attacks. Be aware that attacks sometimes occur before updates are released. Make sure you update any software you use for browsing the Internet (Internet Explorer, Firefox, Netscape, etc.) because Internet-based browsing attacks are becoming more common and more dangerous. Other software programs that communicate or interact with the Internet, like e-mail, Web servers, and remote desktop software are especially susceptible to attacks and should be kept current on patches and version levels.

For more information visit:

> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.us-cert.gov/cas/tips/ST05-001.html
> http://www.staysafeonline.com/toolbox/fundamentals/keep_up-to-date.html

Passwords and authentication methods.

Passwords and other authentication methods are ways systems verify that you are who you claim to be. If someone authenticates as you, the system will think it's you. That person can do anything you can do on your computer and the system will log their actions (such as deleting files, sending malicious e-mails, or browsing to inappropriate sites) under your access credentials. 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. Default passwords, names and dictionary words, even in different languages, can be easily guessed or cracked so use complex passwords that are at least eight characters long and 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?" See myMetro.net report 8.25.09: Password protected

For more information visit:

> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.microsoft.com/athome/security/privacy/password.mspx
> http://www.us-cert.gov/cas/tips/ST04-002.html

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 to compromise a system is to simply walk up to an unattended, unlocked workstation or server and access the system so be safe and lock your system when you leave it. It's also 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.

For more information visit:

> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.us-cert.gov/cas/tips/ST04-003.html

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.msisac.org/awareness/oct05/csab05.pdf
> http://www.staysafeonline.com/toolbox/fundamentals/backup_basics.html
> http://www.us-cert.gov/cas/tips/ST04-003.html

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 not the initiator of the transaction. Never share sensitive or confidential information over an unencrypted Internet connection.

For more information on safe browsing tips visit:

> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.us-cert.gov/cas/tips/ST04-013.html
> http://www.us-cert.gov/cas/tips/ST04-012.html

Messaging security – e-mail and instant messaging.

E-mail and instant messaging (IM) are wonderful tools but they can be used or misused in a variety of ways. 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 or an attachment from an unknown sender. If you share personal information with others as a result of answering spam or phishing messages, your identity can also be 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/

Review your computer security.

Evaluate your computer's security periodically and apply appropriate repairs, upgrades, and replacements. If you don't maintain your system's security by keeping it up-to-date, it will eventually be exposed to serious security threats.

For more information visit:

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

Responding to a cyber incident.

Learn how to recognize cyber attacks and know what to do if things go wrong. Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately to the ITS Help Desk, x24357.

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 co-workers, your entire organization's network and data and, ultimately, the citizens who are depending on you.

Material for this article was contributed by the California Office of Information Security.