SHIELD
Information Protection Newsletter
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
your energy partner®
OPPD
Omaha Public Power District

Cyber Crime: You Are the Target

When talking about computer crime, we often hear the observation from computer users that they aren't rich and therefore what they have isn't worth much to a cyber criminal. This just isn't the case. Cyber crime is an enormous problem affecting hundreds of thousands of people a day worldwide.

First criminals can use your personal information to steal your identity, money, and damage your financial reputation. They can also use information you have to attack others. Secondly, there is the matter of scope and ease of access. Rather than physically breaking into thousands of homes and rifling through personal papers, cyber criminals make Internet technologies do their dirty work, often without your knowledge that anything strange is going on.

Throughout history the easiest way to attack a city, a country or an organization has been by targeting people working normal jobs in important places. Employees who are unaware of the cyber threat can be an organization's greatest vulnerability when they click on malicious links in email and web sites or bring infected USB sticks to work from home.

The first step in beating cyber crime is for everyone to realize that regardless of their position in the organization, they are all targets for cyber criminals. If employees think that they have nothing of value, then they may not know how to protect themselves, their families, and our company from attack.

Thanks to the Internet, cyber criminals can and do attack millions of people all day, every day. They literally target everyone in the world who has computer access and they make billions of dollars. Attackers can do this using sophisticated software that fully automates computer hacking. In using these tools, hackers scan the entire Internet looking for software flaws or configuration errors and then automatically exploit those weaknesses. In another very successful approach, cyber criminals use email and specially crafted messages designed to play either to fear or curiosity.

Using databases containing millions of email addresses, cyber criminals count on the law of averages that sooner or later someone will fall for their deceptive messages and click on a link that downloads malicious software to steal information they can turn into cash, such as credit cards or personally identifiable information. With each success, they gain additional information, like email addresses, to expand their attacks.

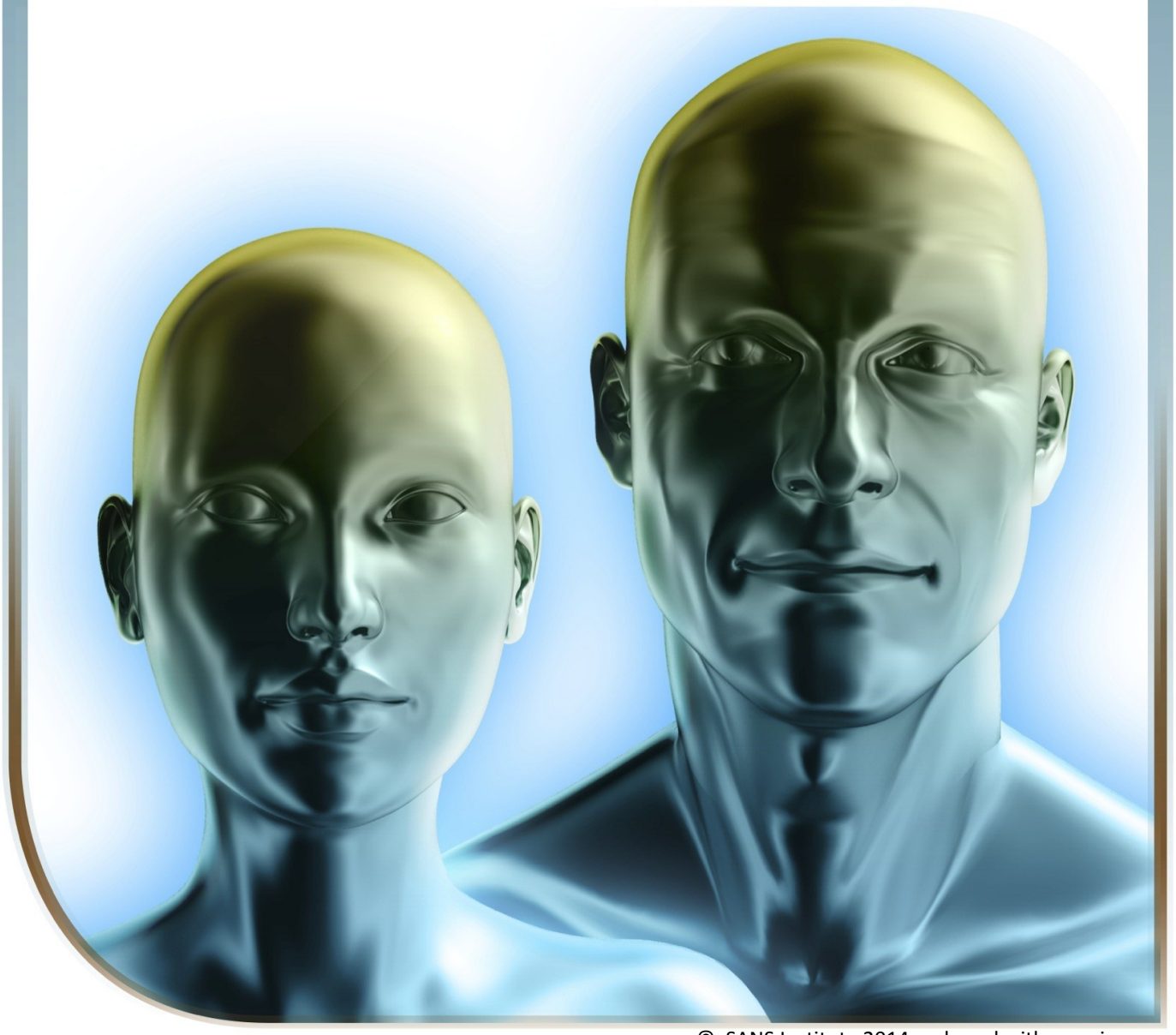
According to the SANS Institute, an organization devoted to security training and awareness, cyber crime has become very sophisticated during the past ten years,. You might hear security experts refer to cyber crime as an ecosystem, and for good reason. In the beginning, cyber criminals were lone wolves. They had to be jacks of all trades. This meant they had to have the skills to program their own hacking software, manually locate and hack into vulnerable systems, steal account information, and transfer or wire stolen money, not to mention sending out spam,.

Today's cyber criminals are now specialists. Each now has his or her own specific field of expertise, allowing them to work together within a highly organized community. For example, one group may be dedicated to developing and supporting sophisticated hacking software, while another group specializes in hacking into other computers or stealing personal information. Still other groups work to sell compromised computers or stolen bank accounts, and an entirely different group transfers and launders stolen money.

The Sans Institute says an entire cyber crime economy has emerged, which is constantly improving its tactics and becoming more effective and efficient in making money every day. These criminals form a highly sophisticated threat, one that will be with us for many years to come.

You Are The Target

Your accounts, computers and devices have tremendous value to cyber criminals. The first step to protecting yourself is understanding that you are under attack.



Don't' believe everything you read:

Use Email safely

Email has become one of the major ways we communicate. For many companies use email to provide information on goods and services, such as shipment confirmations or even online bank statements. Since it has become so widespread, it is not surprising that cyber criminals make email attacks as one of their primary attack methods.

Cyber criminals know it is very easy to counterfeit legitimate-looking email from someone or organizations that you trust. They can use your trust to get you do things you normally wouldn't do like open an unexpected email attachment or click on an unknown web page link.

Attacks of this type are called "phishing" attacks, since the attacker is trying to hook you into believing the "baited" email is legitimate. It was originally coined to describe attecks intended to steal online banking user names and passwords.

Phishing attacks are broadcast in the same way as spam, using compromised machines rented out to the attackers by another group of cyber criminals. They don't really have a specific target in mind, but depend on the sheer number of phishing emails in order to hook their victims.

Most attacks rely on the victim doing something once they open the phishing email . To keep from being a victim, follow these simple steps.

- **Don't trust unexpected email from friends.** Trust your gut. Call your friend or business contact to make sure they sent it.
- **Be suspicious of email directed to "Dear Customer" or some other general greeting**.
- **Be suspicious of messages requiring immediate action or promises threatening consequences.** Fear can trip you up.
- **Be suspicious of messages from organizations that contain spelling or grammatical errors.** Big companies hire writers to ensure they have professional looking communications.
- **Think before you click.** Hover your mouse orver the link and see if the displayed link matches the actural one.
- **Be careful opening attachments.** Open only those you were expecting. Keep in mind that cyber criminals can craft malicious software that you anti-virus may not initially detect.
- **Above all, exercise common sense.** If a message sounds too good to be true, it is likely a phishing attack. Report the message to the IT Service Desk and follow their instructions.

Spear Phishing

Many email attacks are designed to reach as many people as possible to increase the cyber criminal's chances of success. However, they haven't forgotten that there are key people in targeted organizations who have access to very valuable information that they can sell on the cyber criminal underground web sites. Email attacks targeting key people is called spear phishing. This can be highly dangerous to an organization like ours.

Rather than just send out the usual phishing email to thse key people, cyber criminals will analyze the organization then determine who will receive their malicious email. They collect as much information as possible from public sources like search engines and even the targeted company's web sites. They also search social media sites like LinkedIn or Facebook. Once they have learned as much as possible, they create believable, customized phishing email designed to fool the targeted individual into opening an infected attachment or clicking on a malicious web link.

For extra information about Spear Phishing attacks, visit the Anti-Phishing Working Group web sites at **http://www.apwg.org/resources/technical-whitepapers/**,

Use Email Safely

Email is the number one method cyber criminals use to attack their victims. Be suspicious of odd emails or emails that seem too good to be true.

Think before You Click:

Browsing the Internet Safely

Web browsers like Internet Explorer, Firefox, and Chrome are a powerful tools for good or ill. Your web browser great help to helping you be more productive and we depend on it for a number of important applications. Unfortunately the very features that make it helpful to you are also very helpful to cyber criminals.

Cyber criminals have created new attacks to take over your PC through your web browser and built malicious websites that use these attacks to hack your web browser. Once the web browser has been compromised, attackers can easily gain control of your PC often without your knowledge. It's up to you at work and at home to protect your web browser and user it wisely.

Protect your browser, our customers, your fellow employees, and yourself by following these steps.

- **Patch your browser.** Use the latest version of your web browser and keep it patched. Enable automatic updating so you don't have to do it.
- **Avoid plug-ins and Add-ons.** Cyber criminals write attacks for plug-ins lke Adobe Flash, Adobe Reader, and Java and even Apple QuickTime. Very few plug-ins have auto-updating features, so install and manually update those you absolutely need.
- **Scan all downloads.** User your anti-virus to every file you download before you install or open it.
- **Ensure website filtering is enabled.** For instance, Internet Explores uses SmartScreen Filter to help identify malicious web sites.
- **Additional Security Settings.** We have set up additional security for Internet Explorer here at work, but consider raising the security settings on your home PCs and mobile device browser settings.

Avoiding Sketchy Sites

As described in the May newsletter, the internet is like a big city, filled with everything you need. In every city, there includes good neighborhoods and bad neighborhoods. Good neighborhoods are made up of websites that are reputable and trustworthy. Bad neighborhoods are made up of sites that are designed to attack your computer or steal your data. Here are some tips to try and identify whether a site is legitimate:

- **Check the domain.** A misspelled URL or an improper domain structure can send you to a malicious site, posing as a legitimate one. Here's an example of a sneaky domain misspelling. Can you spot it?

  www.quiznos.com vs. **www.guiznos.com**

- **Check the location of where links are actually headed.** Right-click the link and select Properties. From here you can determine the actual URL. Does the URL match what the link claims to take you to?
- **Heed warning signs on the site.** If it asks you for unneeded personal information or attempts to download mystery software to your computer, there is a good chance it is malicious.

The easiest way to avoid these malicious sites is to trust your gut. If the site looks strange or too good to be true, use commons sense and avoid the site.

For more information , check out

"How to Identify and Protect Yourself from an Unsafe Website." *Information Security RSS*. Boston University, n.d. Web. 25 June 2014.

NERC CIP Requirement:

Annual Cyber Security Training Program

The North American Electric Reliability Corporation (NERC) is a non-profit international regulatory authority that has been given the mission to ensure the reliability of bulk electric power in North America. NERC is subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.

NERC develops and enforces a number of regulatory standards. The NERC Critical Infrastructure Protection (CIP) standards require that an annual cyber security training program be established and maintained.

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training pro-gram shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate-ate to personnel roles and responsibilities:

The proper use of Critical Cyber Assets;

Physical and electronic access controls to Critical Cyber Assets;

The proper handling of Critical Cyber Asset information; and,

Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

Beginning on July 1, 2014 OPPD employees and contractors with authorized cyber and/ or authorized unescorted physical access to OPPD Critical Cyber Assets shall be officially notified and required to partake in the annual re-certification of OPPD NERC CIP Security Training.

The annually recertification period begins Tuesday July 1, 2014 and will conclude on Tuesday, September 30th, 2014. OPPD employees who are currently NERC CIP authorized shall receive a notification via email on July 1, 2014. OPPD contractors who are currently NERC CIP authorized are to contact their OPPD sponsor for information pertaining to the re-certification training.

If training is not completed prior to September 30th, 2014 physical access and/ or electronic access to OPPD NERC CIP facilities and associated Cyber Assets will be revoked.

For more information pertaining to OPPD's NERC CIP Training or the Annual re-certification period, please contact , Mike Nickels – (402) 552-5036; manickels@oppd.com or Suzanne Krajicek – (402) 552- 5165;