CTS Security Operations Center

Monthly Security Tips NEWSLETTER

December 2012

Cyber Crime and How it Affects You

What is Cyber Crime?
Cyber crime is a term that covers a broad scope of criminal activity using a computer. Some common examples of cyber crime include identity theft, financial fraud, web site defacements and cyber bullying. At an organizational level, cyber crime may involve the hacking of customer databases and theft of intellectual property. Many users think they can protect themselves, their accounts, and their PCs with just anti-spyware and anti-virus software. Cyber criminals are becoming more sophisticated and they are targeting consumers as well as public and private organizations. Therefore, addiitonal layers of defense are needed.

An Example of Cyber Crime
An example of one type of cyber crime is an "account takeover." This happens when cyber criminals compromise your computer and install malicious software, such as "keyloggers" which record the key strokes, passwords, and other private information. This in turn allows them access to programs using your log-in credentials. Once these criminals steal your password, they may be able to breach your online bank account. These criminals can be anywhere in the world and may be able to transfer your money almost immediately.

What are the Effects of Cyber Crime?
The effects of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year.

What Should We Do?
Training and awareness are important first steps in mitigating these attacks. All citizens, consumers, and employees should be aware of cyber threats and the actions they can take to protect their own information, as well as the information within their organization.

So… What can you do to minimize the risk of becoming a cyber crime victim?

1. **Use strong passwords**
   Use separate ID/password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters, and by changing them on a regular basis.

2. **Secure your computer**
   - **Enable your firewall**
     Firewalls are the first line of cyber defense; they block connections from suspicious traffic and will keep out some types of viruses and hackers.
   - **Use anti-virus/malware software**
     Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
   - **Block spyware attacks**
     Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3. **Secure your mobile devices**
   Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources. Do not store unnecessary or sensitive information on your mobile device. It is also important to keep the device physically secure; millions of mobile devices are lost each year. If you do lose your device, it should immediately be reported to your carrier and/or organization. There are some devices that allow remote erasing of data. Be sure to keep your mobile device password protected.

4. **Install the latest operating system updates**
   Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

5. **Protect your data**
   Use encryption for your most sensitive files such as health records, tax returns and financial records. Make regular back-ups of all your important data.

6. **Secure your wireless network**
   Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings (information on doing so can be found in our August of 2012 newsletter.) Public Wi-Fi, a.k.a. "Hot Spots," may also be vulnerable. Avoid conducting sensitive transactions on these networks.

7. **Protect your e-identity**
   Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure especially when making online purchases, or that you've enabled privacy settings (e.g. when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc.). Once something is posted on the Internet, it may be there forever.

8. **Avoid being scammed**
   Never reply to emails that ask you to verify your information or confirm your user ID or password. Don't click on a link or file of unknown origin. Check the source of the message; when in doubt, verify the source.

For More Information:

For additional information about cyber crime, please utilize the following resources:

- **Internet Crime Complaint Center: http://www.ic3.gov/preventiontips.aspx**
- **Norton Cyber Crime Prevention Tips: http://us.norton.com/prevention-tips/article**
- **National White Collar Crime Center: http://www.nw3c.org/services/ic3/complaints**

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™ A DIVISION OF CENTER FOR INTERNET SECURITY

Consolidated Technology Services
Security Operations Center

The mission of the CTS Security Operations Center is to provide centralized information sharing, monitoring, and analysis of Washington State security posture. Contact us at: soc@cts.wa.gov

For more newsletters and tips, visit our SharePoint site at: http://sharepoint.dis.wa.gov/soc/default.aspx