The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 18, July 2014

Keeping Kids Safe on the Internet

The Internet provides all of us, including our children, with many benefits such as immediate access to entertainment, educational tools, banking, shopping, and social networking activities. But these benefits come at a price in the form of cybersecurity threats that can be damaging to our personal and professional lives. Many of these threats are unique to kids and must be taken seriously. It is a well know fact that kids are getting online at earlier ages, and spending more time on the Internet. According to the *National Cyber Security Alliance*, kids aged 8-18 spend about 7.5 hours on the Internet each day. With so much time spent online, kids face many cyber threats, including ***cyber predators*** and ***cyber bullying***.

Cyber predators are people who search online for other people and children in order to use, control, or harm them in some way. Children are unfortunately easy targets due to their desire to appear as an adult or to gain attention.

Cyber bullying is the electronic posting of mean-spirited messages about a person, often anonymously. According to a study by the *National Crime Prevention Council*, approximately 40 percent of teens have been victims of cyber bullying.

To help protect your children from these threats, *NetSmartz*, a division of the *National Center for Missing & Exploited Children*, recommends the following security tips and actions:

- Your child should NEVER meet face-to-face with anyone they first meet online without your permission and/or attendance.
- Take an interest in your child's online activities and monitor their communications.
- Teach your child to refrain from talking about sex with anyone they meet online.
- Ask questions immediately, especially if your child is acting suspiciously.
- Teach your child not to reveal personal information.
- Approve all photos and videos ***before*** your child posts them online. Make sure they do not reveal identifying information and are not provocative or inappropriate.

Privacy and Reputation Management

Privacy and reputation management is more of a significant issue for teenagers with over 96 percent participating in social media networks and sharing significant amounts of personal information. According to a *Pew Research Internet Project* 2013 study, 91 percent of teens share photos of themselves, 82 percent share their birth date, 71 percent share their school name, 53 percent share their email address, and 20 percent share their cell phone number. Sharing this information may make teens more at risk for identity theft, cyber predators, and cyber bullying. Parents and trusted adults should educate their teens about responsible online behavior, starting with these tips from *Stop.Think.Connect*.

- Keep your personal information private, including your family members, your school, your telephone number, and your address.
- Think twice before you post or say anything online. Once it is in cyberspace, it is out there forever.
- Only do and say things online that you would do or say in public.
- Use strong passwords with eight characters or more and a combination of numbers, letters, and symbols.
- Don't share your passwords with anyone.
- Think before you click–don't open emails from strangers and don't click on links for unfamiliar sites.
- Use privacy settings on social networking websites such as Facebook.

Cybersecurity is everyone's responsibility - raising responsible online citizens from a young age is a critical step in securing cyberspace for future generations.

Contributing source to this article: U.S. Department of Homeland Security, Stop.Think.Connect. April 2014 update. For more information visit http://www.dhs.gov/stopthinkconnect .

You are a Target for Cyber Crime

Many users have the misconception that they are not a cyber crime target, because unfortunately they believe that their information has no real value. This is a dangerous fallacy on the part of general users. If you have an Internet-connected computer, a smart phone, email accounts, online bank accounts, credit cards, or engage in any type of online activity – you are worth money to cyber criminals.

Why You Are Targeted?

Crimes such as fraud, identity theft and extortion have been favored among thieves for as long as there have been civilizations. The criminal's goal is to make as much money as possible with little risk. Traditionally, this was difficult because criminals had to come in physical contact with their victims. However, this is no longer the case as criminals can easily target any user in the world at little or no cost due to the expansion of global online technology. Almost every aspect of one's life can be accessed via the Internet – banking, savings, and retirements accounts; employment information; driving records; property values; previous and current addresses; personal photos; birth records; credit card numbers; social activity – the list goes on and on. All of this information can be used by criminals to steal your identity, money, or worse – threaten your well-being or the safety of your family.

Today's cyber criminals have become very efficient at stealing incredible amounts of personal financial information through very common social engineering attacks such as phishing. Ultimately, these criminals know that the more credit card numbers that they steal, the more bank accounts that they successfully hack, or the more passwords they compromise, the more money they make. Everyone is a target - you are not being singled out because you are special. Rather, these criminals are targeting everyone connected to the Internet, including you.

According to the SANS Institute, hacking millions of people around the world is not so difficult given the variety of automated tools that are easily accessible via the Internet. For example, criminals can build a database of millions of email addresses and use an automated tool to send phishing messages to each account. This activity costs nothing, and the criminal can use other hacked computers to do the dirty work. The criminal simply sits back and waits for unsuspecting users to fall victim to the attack.

How to Protect Yourself

Fortunately, there are simple steps you can take to help protect yourself from cyber crime.

- **Common Sense**. Common sense is your best defense. If something seems odd, suspicious or too good to be true, it is most likely an attack. ***Never*** click on links in unsolicited emails.
- **Update, Update, Update**. Make sure that any computer or mobile device you use has been fully updated with the latest patches. This is not only important for your operating system, but for any applications you are using.
- **Strong Passwords**. Use a strong, unique password for each of your accounts. This will protect when a website you use is hacked and all the site's passwords are compromised (including yours), your other accounts are safe.
- **Credit Cards and Bank Accounts**. Check your financial statements often, at least weekly (monthly is not enough). As soon as you see any unauthorized activity, report it immediately to your financial institution or card issuer. Utilize automated messages or alerts for unusually large or odd transactions if available.
- **Home Network**. Secure your home network Wi-Fi access point with a strong administrator password and configure the Wi-Fi network to require a password for anyone to join it.
- **Social Media**. Beware of personal information that you post online. The more information you post the more likely you put yourself at risk. Not only can cyber criminals use this information to target you, but information you post may actually identify you or your family as a more valuable target.

Contributing source to this article: SANS Securing the Human Ouch! Security Newsletter. For more information visit http://www.securingthehuman.org .

DOE Cyber Awareness

The DOE OCIO has a robust Cybersecurity Awareness and Training Program that focuses on enhancing the general cyber awareness and knowledge of all DOE employees with the ultimate goal of cultivating a computing environment where cybersecurity behaviors and responses are automatic and consistent. To achieve this goal, the OCIO offers a variety of resources and awareness events throughout the year. The OCIO has recently renovated the Cybersecurity Awareness & Training (CSAT) Warehouse which serves as a central repository of awareness and training resources and materials. This information can be used by any DOE organization to supplement current training and awareness initiatives.
Visit http://energy.gov/cio/training/cybersecurity-awareness-training-warehouse.

*For questions regarding these articles or other cyber topics/issues, please send an email to cybsectrn@hq.doe.gov. For general information on cybersecurity, search **Cybersecurity** on Powerpedia.*