



Cyber Security Awareness

October is National Cyber Security Awareness Month which is an annual campaign to raise awareness about cybersecurity. We live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. This is the perfect time of year for individuals, businesses, and other organizations to reflect on the universe of cyber threats and to do their part to protect their networks, their devices, and their data from those threats.



Why it's Important

- Within the past year, personally identifiable information has been stolen in a number of significant cyber data breaches, impacting industries like health care, government, finance, corporate, and retail.
- The use of malware by online criminals continues, and of the available intrusion devices, the "bot" is particularly pervasive, allowing attackers to take control remotely of compromised computers. Once in place, these "botnets" can be used in distributed denial-of-service attacks, proxy and spam services, additional malware distribution, and other organized criminal activity.
- Cyber criminals perpetrate a wide variety of crimes online, including theft of intellectual property, internet fraud, identity fraud, and any number of financial fraud schemes.
- Sexual predators use the internet and social media to target the youngest and most vulnerable victims.
- And many criminals use the so-called "dark web" or "dark market" websites that offer a range of illegal goods and services for sale on a network designed to conceal the true IP addresses of the computers on it.

Computer Tips

- Use a firewall as well as cyber security software, such as antivirus and antispyware, that will scan for computer security threats and uninstall them. Ensure all of your protection measures, as well as your operating system and software, are up to date. Also, change your passwords every 90 days for better information security.
- Before submitting credit card information online, look at the URL to ensure you're on a HTTPS (Hypertext Transfer Protocol Secure) site. Be wary if a site requires information that isn't necessary for a transaction. Information security is more important than anything you could buy.
- With the proper software installed, stolen laptops can be tracked to a physical location if they are connected to the Internet. Other software gives you remote access for computer security with the ability to erase your files or send them to a secure data center for recovery via the Web.



Email and Social Networking Tips

- Always question the legitimacy of emails and social networking messages that ask for money or personal information. Spear phishing attacks mimic communications from a business to persuade you to divulge personal information. Legitimate business won't contact you to verify your account.
- Public profiles on social networking sites put you at risk by exposing information, such as your full birth date, hometown, employment history, etc., that a criminal could use to pose as you. Use privacy settings to ensure your personal information isn't public knowledge.
- Don't open unknown attachments, don't click on unknown links, and don't share too much information online. That's a lot for don'ts but when your identity and computer could be at risk, it's better to play safe. The rewards aren't always worth the risks.



Mobile Phone Tips

- Mobile phones can do more and be more personalized than ever before. Just be wary that you might pay the price when you download or purchase applications or ringtones. Some may come with a virus attached that steals your personal information.
- Your mobile phone likely offers multiple layers of protection. At a minimum, activate PIN access to your phone. Also consider password protecting your email as well as any applications, such as banking or social networking, that provide access to sensitive information.
- You may receive a counterfeit text message that appears to be from a legitimate bank or credit card company asking you verify your account information. Once you supply your information via phone or web, it will be in the hands of criminals. Be aware of information security by knowing when to ignore a text message.



Protect Your Children

- Talk to your kids about sexual predators and explain about potential online dangers. Explain about the “[grooming process](#)” and warn them about some of the tactics an online predator may use.
- Install parental control software. Don’t forget to inform your children that you have done this. Explain to them that that you are not spying on them - you are keeping them safe!!
- Place the computer in a family room or somewhere visible (not in your child’s bedroom). But remember that your children have other means of accessing the internet and communicating with potential predators. Pay attention to other computer and internet-enabled mobile devices.
- Most social networking sites require that users be age 13 and over. Make sure your kids follow these age restrictions.
- Limit and monitor the amount of time your children spend on the internet, and at what times of day. Too much time online, especially at night, may be a sign of a problem.
- Discuss [cyberbullying](#) with your children and recognize the signs that your child may be a victim.



Where to Report Cybercrimes

- **Local law enforcement** - Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency has an obligation to assist you, take a formal report, and make referrals to other agencies.
- **IC3** - The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complaints may be filed online at www.ic3.gov
- **Federal Trade Commission** - The FTC does not resolve individual consumer complaints, but does operate the Consumer Sentinel, a database that is used by civil and criminal law enforcement authorities worldwide. File your complaint at <https://www.ftccomplaintassistant.gov>
- **Your Local Victim Service Provider** - Most communities in the United States have victim advocates ready to help following a crime. Find local victims service providers here <http://ovc.ncjrs.gov/findvictimservices/search.asp>

Additional Resources

Pennsylvania Emergency Management Agency: <http://www.pema.pa.gov>

ReadyPA: www.readypa.org

Federal Emergency Management Agency: www.ready.gov

Department of Homeland Security: www.dhs.gov

Federal Bureau of Investigation: www.fbi.com

Federal Trade Commission: www.ftc.gov

