Cyber Safety Tips

Cyber Safety 101

Keep a Clean Machine.

- Keep software current.
- Automate software updates.
- Protect all devices that connect to the Internet.
- Scan all external mass storage devices and your machine for viruses and malware regularly.

Protect your personal information.

- Secure your accounts and take advantage of additional ways to verify your identity before you conduct business online.
- Make passwords complex. Combine capital and lowercase letters with numbers and symbols.
- Separate passwords for every account.
- Write it down and keep it safe.
- Own your online presence. Set privacy and security settings on websites to your comfort level.

Connect with care.

- When in doubt, throw it out. Links in e-mail, tweets, posts and online advertising are often the way cybercriminals compromise your computer.
- Get savvy about Wi-Fi hotspots. Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- Protect your money when banking and shopping. Take extra measures to help secure your information by looking for web addresses with “https://” or “shttp://”.

Be web wise.

- Stay current. Keep pace with new ways to stay safe online.

- Think before you act and be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- Back it up. Protect your valuable digital information by making an electronic copy.

Be a good online citizen.

- Safer for me more secure for all. What you do online has the potential to affect everyone. Practicing good online habits benefits the global digital community.
- Help the authorities fight cybercrime. Report stolen finances or identities and other cybercrime to the Internet Crime Complainant Center at http://www.ic3.gov and the Federal Trade Commission at http://www.onguardonline.gov/file-complaint .[1]

Cyber Security for Electronic Devices

Any piece of electronic equipment that utilizes a computerized component is vulnerable to software imperfections and vulnerabilities. This may include items such as cell phones, tablets, video games, car navigation systems etc. The risks increase if the device is connected to the internet or a network that may be accessible by a hacker. Security tips related to how to protect electronic devices can be found at http://www.us-cert.gov/ncas/tips/ST05-017 .[2]

Internet Crime Schemes & Prevention Tips

Stay current with ongoing Internet trends and schemes identified by the Internet Crime Complainant Center at http://www.ic3.gov/crimeschemes.aspx .Review preventative measures to stay informed prior to making online transactions at http://www.ic3.gov/preventiontips.aspx#item-1 .

Who to Contact if You Become a Victim of Cybercrime

Local law enforcement - Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency (either police department or sheriff's office) has an obligation to assist you, take a formal report, and make referrals to other agencies, when appropriate. Report your situation as soon as

[1] DHS, Stop.Think.Connect Tip Sheet, http://stopthinkconnect.org/tips-and-advice/
[2] US-CERT, Cyber Security for Electronic Devices, http://www.us-cert.gov/ncas/tips/ST05-017

you find out about it. Some local agencies have detectives or departments that focus specifically on cybercrime.

IC3 - The Internet Crime Complaint Center (IC3) will thoroughly review and evaluate your complaint and refer it to the appropriate federal, state, local, or international law enforcement or regulatory agency that has jurisdiction over the matter. IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance). Complaints may be filed online at http://www.ic3.gov/default.aspx.

Federal Trade Commission - The FTC does not resolve individual consumer complaints, but does operate the Consumer Sentinel, a secure online database that is used by civil and criminal law enforcement authorities worldwide to detect patterns of wrong-doing, leading to investigations and prosecutions. File your complaint at https://www.ftccomplaintassistant.gov/FTC_Wizard.aspx?Lang=en. Victims of identity crime may receive additional help through the FTC hotline at 1-877-IDTHEFT (1-877-438-4388); the FTC website at www.ftc.gov/IDTheft provides resources for victims, businesses, and law enforcement.[3]

Additional information on what to do if you become a victim can be found at http://staysafeonline.org/ncsam/resources/victims-of-cybercrime-tip-sheet .

Social Networking Safety

While the popularity of social networking sites continue to increase, so do associated security risks. Although the majority of users do not pose a threat, malicious individuals may be drawn to such sites due to accessibility and the amount of personal information made available. Security tips on how to stay safe on social networking sites can be found at http://www.us-cert.gov/ncas/tips/ST06-003 .[4]

Resources for Keeping Kids Safe Online

http://kids.getnetwise.org/
http://www.netsmartz.org/Parents
http://www.microsoft.com/security/family-safety/childsafety-steps.aspx

[3] National Cyber Security Alliance, StaySafeOnline, http://staysafeonline.org/ncsam/resources/victims-of-cybercrime-tip-sheet
[4] US-CERT, Staying Safe on Social Network Sites, http://www.us-cert.gov/ncas/tips/ST06-003

Additional Resources

- Download tip sheets, posters, and other materials made available through the U.S. Department of Homeland Security STOP|THINK|CONNECT campaign at http://www.dhs.gov/national-cyber-security-awareness-month.

- Sign up for security alerts, tips, and other updates by subscribing to mailing lists and feeds on the US Computer Emergency Readiness Team website at http://www.us-cert.gov/mailing-lists-and-feeds .

- Educate yourself through the Multi-State Information Sharing & Analysis Center National Webcast Initiative (MS-ISAC). The National Webcast Initiative is a collaborative effort between the U.S. Department of Homeland Security's National Cyber Security Division and Multi-State Information Sharing & Analysis Center as a means to provide timely and relevant cyber security education and information to a broad audience. Webcasts are available to the public free of charge. Upcoming webcasts can be found at http://msisac.cisecurity.org/webcast/ .