Online Safety & Security

"The Internet is a superhighway of information and the police don't patrol it. You have to patrol it yourself." - Bill Gates (Microsoft co-founder)

Misinformation/Disinformation
Anyone can make a website

Threats: Scams, Social Engineering, Phishing
What To Watch For:

- Most websites are designed for some sort of personal gain
- Never trust a website from a non-reputable source
- Don't always trust the first few search results
- Only visit websites you know
- Avoid clicking on a website's ad banners
- Watch out for sites with names similar to brands you know
- Watch out for email "from companies you know"
- Beware of information that sounds "too good to be true"
- Always check sources!

Personal Information
Who are you giving your information to?

Threats: Identity Theft, Cyberstalking, Hacked Web Accounts
Information at risk: Name/Address, Phone Number, Email Address, Credit Card/Bank Info, Favorite Color/Pet/etc.
What To Watch For:

- Check the URL of the site you are on before filling out forms
- Check for signs - like a web address with https:// and a closed padlock next to the URL address
- Don't trust emails saying you need to "validate your account info", even if they are using the company logo
- Don't respond to pleas for money from "family members," people who claim to be attracted to you but need money, deals that sound too good to be true, lotteries you didn't enter, or other fraud scams

Only put information on the internet that you would want **EVERYONE** to know!

Social Networks

<u>Anybody can make a Facebook page, with whatever name they want…</u>

- Don't just trust that somebody is what their name says
- Never give out personal info unless you know the person in real life, and you're sure it's them!
- Always put as little personal info on your Facebook page as possible…
- Facebook Games are not always run on their website

Check your Privacy Settings!!!

- Control how people can search for you and make comments
- Manage who can see your profile or photos tagged with your name

Do not post anything you wouldn't want seen on a billboard!
Do not post anything you wouldn't say to your grandmother!

Geolocation

Most smartphones have GPS technology allowing a user's precise location to be shared by apps and on websites. Social networking sites such as Facebook use this and encourage their users to "check-in" or share their locations.

Children also may share their locations unintentionally through pictures taken with their smartphones; these photos often have geolocation data embedded in them. Consider disabling the location services (GPS) on smartphones before allowing children to post photos online.

Protecting Children Online

Kids spend a lot of time using:

- E-mail
- Blogging
- Online Games
- Instant Messaging /Chat
- Social Networking
- Web browsing in general

Do you know what websites your child likes to visit?
Do you know how mch time your child spends on each?

Kids have much of the same concerns adults do, but also:

- Revealing TMI
- Identity Theft
- Inappropriate material
- Cyberbullying
- Online predators
- Webcams

Do you know if your child has encountered any of this during their time spent online?

Cyberbullying & Online Harassment

- The internet can be thought of as an anonymous "location"
- **Trolls:** Some people just like to agitate others
- **Flame War:** When people misunderstand something you typed, and begin a heated counter-argument
- Fake rumors are quite common online
- Cruel photoshopping of pictures is also a semi-regular thing
- Don't take anything that is said online seriously (sticks & stones)
- **If someone threatens you or your loved ones with physical harm, contact the police <u>IMMEDIATELY!</u>**

How To Protect Kids Online

Make any report of abuse to <u>www.cybertipline.com</u> or **1-800-THE-LOST**

- **Social Networks:**
  Omit any identifying information from all online posts: full names, ages, locations, phone numbers, and school names.

- **Free Online Games:**
  - Talk to your kids about cyberbullies, who may harass gamers.
  - Online scam artists may promise virtual goods in an effort to get credit card information.
  - Predators may send inappropriate content or use a game's communication functions to arrange in-person meetings. Remind them that people they don't know OFFLINE are considered strangers!
  - Even game consoles allow for Internet Gaming now.
  - Know what games your child is playing and walk into the room while they are playing to watch them occasionally.
  - Keep the computer or game console centrally located, in an area where people traffic frequently.

Protect Your Computer!
Think of how little you can do without it!

- Keep all software (including your web browser) updated: Windows Update
- Download software updates from the manufacturer's website: Adobe Flash Player & Java
- Install legitimate antivirus and antispyware software, and know what their logo looks like
- Be sure your AntiVirus is UP TO DATE!
- Check that you are using a firewall
- Protect your wireless router with a password
- Before you open an attachment or click a link in an email message, check with the actual person that it is real
- Don't trust "Security Warnings" or scans that start while you are searching the internet
- **Clear your cookies:** wikihow.com/Clear-Your-Browser's-Cookies

Malware
malicious software or programs designed to do bad things on your PC

virus: computer program that attaches itself to other files/programs, and cause some sort of harmful activity
worm: a self-replicating virus that does not need to attach itself to other files
trojan: a type of software that tricks you into running it, allowing worse malware access to your computer
backdoor: a "secret way" into your computer, caused by a virus or trojan
rootkit: malicious software that hides outside of the normal view of the system and requires special software to remove
keylogger: a software which captures keystrokes, mouse clicks and screenshots, and emails them to an individual
dialer: an older malware which made your dialup modem dial certain 900 phone numbers, charging you for the call
ransomware: software which "holds your computer ransom", requiring you to send money to an unknown individual
spyware: software which tracks where you go and what you type on the internet, and sends the info to a third-party
adware: software which loads additional ads (or replacement ads) while you browse the internet
malicious BHOs: add-ins for your web browser which may redirect your browsing or pop up ads
rogue security software: software posing as legitimate antivirus software, claiming you are infected when you aren't
zombie: an infected computer that has been compromised by a hacker, computer virus or trojan, so that the hacker can use the computer for misdeeds
botnet: a bunch of compromised computers (zombies), used to commit mass misdeeds

Malicious Files

You never know what you're getting when you download a file

- Pay attention when installing a new program
- Be sure you know what it is you just agreed to
- When you download something, note the file name
- The file name can be anything the site's owner wants
- Only download files from reputable websites
- Most coupon websites use the Coupons.com plugin
- Watch out for sites that say you need an "upgrade"
- **Watch out for the word "Free"!**
- Beware of "game downloaders" or "installers"

PASSWORDS

- Create strong passwords and keep them secret
- Computer login passwords should be easy to remember, but impossible to guess
- Create passwords made up of long phrases or sentences that mix capital and lowercase letters, numbers, and symbols.
- Almost any password longer than 20 characters is unbreakable
- Use different passwords for different sites, especially those that keep financial information
- Use a password checker to learn how strong your passwords are:

http://www.passwordmeter.com
https://howsecureismypassword.net

Making Stronger Passwords

- How to make an equally strong and easy to remember password:
- Pick a phrase you can remember with a number in it, like "A bird in the hand is worth two in the bush."
- Change that number (in this case, "two") to its numerical equivalent: A bird in the hand is worth 2 in the bush
- Condense the phrase by only using the first letter of each word: Abithiw2itb
- Add some special characters you can remember: #Abithiw2itb!

Be sure your family and friends know as much as you do about online safety!
You are only as secure as the people you connect with!
Be safe and happy internetting!