Staying Safe

On the Internet

Be Very Careful

When you are
on the Internet

Beware!

- Think before quickly posting on the Internet.
- In emails, postings, or anything online, realize it can become public and can't be undone.
- Siri and Alexa listen all the time.
- "Everyone knows Sarah" from her posts.

- https://www.youtube.com/watch?v=ThxmgXMBpoM

Personal Information

- Think before you post anything online or share information in emails. What you post online, can be seen by anyone. Sharing personal information with others you do not know personally is one of your biggest risks online.
- Sharing sensitive information such as your address, phone number, family members' names, car information, passwords, work history, credit status, social security numbers, birth date, school names, passport information, driver's license numbers, insurance policy numbers, loan numbers, credit/ debit

Photographs

- Photos taken from smartphones embed the GPS Coordinates in the photo, which will allow others to know the location of where the picture was taken and may be used to find you.
- Beware of this when posting photos to online social media sites. Remember that pictures posted online may be copied, altered, and shared with many people without your knowledge or consent, unless you use privacy settings to limit who has access to the pictures.

Emails, Phishing, and Malware

- Beware opening emails from unknown people or sources. Clicking on links or downloading attachments may infect your computer.
- Some viruses harm your computer, while others have the ability to steal your personal information.
- Be skeptical when receiving emails that look as if they came from your bank or other financial institution asking you to verify or enter personal or financial information.
- In general, beware of email scams and websites that try to trick you into sharing your personal information

Emails, Phishing, and Malware cont.

- Beware of scams using links directing you to a website or providing you with a phone number to call.
- Remember legitimate customer service representatives never ask for personal information or passwords.
- Don’t respond to unsolicited emails, never click on links in these emails, and be cautious if you are asked to respond quickly.
- Purchase or download a good antivirus suite with spyware protection.

More about phishing...

- How to Stay Safe Online and Prevent Phishing Attacks: https://www.youtube.com/watch?v=xyE43Gz4AW8

- Phishing comes in Many Forms: https://www.youtube.com/watch?v=Tgpa4RdKJbU

Updates

- Keep your computer’s operating system, browsers, antivirus, and other software up-to-date with the latest or daily security patches.

Cyber info...

- For an amazing amount of additional information visit https://www.us-cert.gov/ncas/tips
- Former NSA Hacker Reveals 5 Ways To Protect Yourself Online: https://www.youtube.com/watch?v=-ni_PWxrsNo
- Online security basics: Essential steps to stay safe online: https://www.youtube.com/watch?v=2La1rexLj-A

Strong Passwords

- Use 10 characters and combinations of upper and lower case letters, as well as symbols, and numbers. The Tech Talk page on the WWC website has information on easy to remember strong passwords.
- Do not include personal information.
- Consider changing your password at least every 90 days when information is sensitive. Never leave passwords near your computer or in plain sight.
- Use different passwords for various online activities because if one password is compromised, all will be compromised. Never share your password.

Social

- Beware of meeting people in-person whom you meet on the internet or through emails. Not everyone is honest with their identity, age, gender, and intentions. If necessary, do your research using public records and consider seeking reputable references.
- If you decide to meet someone, never go alone, let others know where you are going, meet in a very public place, and have your cell phone readily available.

Parental (and Grand-parental) Controls

- Parents (and grandparents) should consider applying parental controls by their internet service provider and/or blocking software on family computers and smartphones to limit the internet to safe websites.
- Contact your internet provider if you have questions. Be sure to research your options regarding parental controls on products.
- "I'm 10": https://www.youtube.com/watch?v=xZHq4CQekTY

Webcams

- Be careful when using webcams. They can be high-jacked and turned on remotely. This allows others to illegally view and listen to individuals without their knowledge. Consider turning them off or disconnecting them when not in use.
- Limit or do not allow your children or grandchildren to use webcams and talk to them about the risks.

Wireless

- Beware when connecting your laptop or mobile device to unsecured networks. Computer hackers on the same network can intercept your internet use and in some cases access files on your computer.
- Consider password protecting your home wireless network and using a personal firewall program for additional protection.

Shopping

- Avoid purchasing goods and services from websites that do not have secure check-out using “HTTPS.”
- Pay attention to the address line on the checkout page which asks you to enter your credit card information. If the page does not have an “S” following “HTTP” in the address line, consider shopping somewhere else. Also look for the little lock.
- Be aware that some information transmitted on HTTP pages is done so using plain text which can be intercepted by computer hackers.

Selling

- Be cautious when selling and listing items in local ads or elsewhere online.
- Never meet a buyer alone. If necessary, consider meeting in a public place, like inside a post office, courthouse, or bank rather than a parking lot.
- Beware of posting photos taken from smartphones for online ads. You could be sharing your home address with a criminal.

Public Computers

- Avoid typing sensitive information on public computers, such as those in a public library or an internet café. Spyware may be installed on these computers that record your every keystroke. Also, you never know who may be watching your activity.
- Never select the feature that automatically signs you on to email or check any box to “Remember my Password” on websites.

Norton Lifelock

How to keep your personal information safe on social media

- Treat the “about me” fields as optional.
- Become a master of privacy settings.
- Know the people you friend.
- Create and use an “off-limits” list.
- Always log out when you're done.
- Create strong, private passwords.

Places to find info on Internet Security

- parental control: http://www.projectsafechildhood.gov
- wireless: https://www.us-cert.gov/ncas/tips
- https://www.justice.gov/usao-ndga/protecting-yourself-while-using-internet

Some simple hints

- Slow down when looking for and at things on the Internet.
- There’s no need to hurry. Hurrying makes you do stupid things.

Just Be Smart Online

- Be aware of your surroundings.
- Don’t believe everything you see or read online.
- Trust but verify.
- Always look to make sure the site is secure before buying anything.
- Think!