Web Use and Your Safety

Online Identity

Social networking sites are not the only source of your online identity. Many apps and smart devices collect and share your personal information, and contribute to your online identity. These include, but are not limited to:

- Fitness and health trackers
- Professional networking apps
- Dating apps and websites
- Secure chat
- Neighborhood advisory apps
- Audio-enabled personal digital assistants and the smart devices they support, such as phones, TVs, and speakers

Feeding off the data collected by these apps and devices, as well as information available in public records, online data aggregators collect and catalogue information about you. This information can be used to further target you, such as with scams posing as advertisements that are tailored to your preferences. You should opt out of data aggregation and use these apps and devices with caution.

Identity Protection

To protect your identity:

- Ask how information will be used before giving it out
- Pay attention to credit card and bank statements
- Avoid common names/dates for passwords and PINs
- Never share passwords and PINs
- Pick up mail promptly
- Do not leave outgoing postal mail in personal or organizational mailboxes, unless secured with a locking mechanism
- Shred personal documents
- Refrain from carrying SSN card and passport
- Order credit report annually

To respond to identity theft if it occurs:

- Contact credit reporting agencies
- Contact financial institutions to cancel accounts
- Monitor credit card statements for unauthorized purchases
- Report the crime to local law enforcement

Cookies

A cookie is a text file that a web server stores on your hard drive. Cookies may pose a security threat, particularly when they save unencrypted personal information. Cookies also may track your activities on the web.

To prevent cookies from being saved to your hard drive:

- If you have the option, set your browser preferences to prompt you each time a website wants to store a cookie
- Only accept cookies from reputable, trusted websites
- Confirm that the site uses an encrypted link
    - Look for “h-t-t-p-s” in the URL name
    - Look for an icon to indicate the encryption is functioning
- Be especially aware of cookies when visiting e-commerce sites or other sites that may ask for credit card or other personal information

Note: Not all https sites are legitimate and there is still a risk to entering your information online.

Compressed URLs

Exercise caution with compressed URLs, such as TinyURLs (e.g., https://tinyurl.com/2fcbvy):

- Compressed URLs convert a long URL into a short URL for convenience but may be used to mask malicious intent
- Investigate the destination by using the preview feature to see where the link actually leads
    - Use an Internet search engine to find instructions for previewing a specific compressed URL format (e.g., TinyURL, goo.gl)

Internet Hoaxes

Internet hoaxes clog networks, slow down internet and e-mail services, and can be part of a distributed denial of service (DDoS) attack. To protect against internet hoaxes:

- Use online sites to confirm or expose potential hoaxes
- Don’t forward e-mail hoaxes
- Follow your organization’s policies on loading files onto workstations and laptops

Malicious Code

Malicious code can do damage by corrupting files, encrypting or erasing your hard drive, and/or allowing hackers access. Malicious code includes viruses, Trojan horses, worms, macros, and scripts. Malicious code can be spread by e-mail attachments, downloading files, and visiting infected websites.

Protecting Against Malicious Code

To prevent viruses and the download of malicious code:

- Scan all external files before uploading to your computer
    - Follow your anti-virus software’s instructions on how to scan files
- For personally-owned devices, research any application and its vulnerabilities before downloading that “app”

- For Government-owned devices, use approved and authorized applications only

Mobile code can be malicious code. To prevent damage from malicious mobile code:

- Only allow mobile code from your organization or your organization's trusted sites to run
- Contact your security Point of Contact (POC) or help desk for assistance, especially with e-mails that request personal information

To prevent the downloading of viruses and other malicious code when checking your e-mail:

- View e-mail in plain text and don't view e-mail in Preview Pane
- Use caution when opening e-mail: Look for digital signatures if your organization uses them. Digitally signed e-mails are more secure.
- Scan all attachments
- If authenticity cannot be confirmed, delete e-mail from senders you do not know
- Don't e-mail infected files to anyone
- Don't access website links, buttons, and/or graphics in an e-mail or a popup generated by an e-mail message

Incident Indicators

Beware of suspicious behavior that may indicate a cybersecurity incident or malicious code attack:

- Sudden flashing pop-ups that warn that your computer is infected with a virus
- Sudden appearance of new apps or programs
- Strange pop-ups during startup, normal operation, or before shutdown
- The device slows down
- Appearance of new extensions or tabs in the Web browser
- Loss of control of the mouse or keyboard