MID-CONTINENT
PUBLIC LIBRARY

INTERNET SAFETY

Access Technology

INTERNET SAFETY IS IMPORTANT

Internet safety is not just the ability to avoid dangerous websites, scams, or hacking. It's the idea that knowledge of how the internet works is just as important as being aware of your internet safeguards.

We all have a digital identity we need to protect, so when exploring the web or checking email, there are practices that can prevent most of the dangers that can be found online.

Notes

ANTIVIRUS SOFTWARE

The most important step is to make sure that you have some sort of **antivirus software** available to you. Most PCs come with pre-installed firewall software called Windows Defender.

It protects you from **malware** and can perform searches on your computer to scan for viruses. You can also download anti-virus software to protect you against ransomware, spyware, and other harmful software attacks that can introduce **viruses** to your computer.

VOCABULARY

Cookies - Small text files added to your computer by websites when you visit them. These small files track how you navigate each website.

Encryption - The process of encoding a message or information in such a way that only authorized users can access it.

Malware - Malicious software or code (more specifically: Trojans, worms, spyware, adware, etc.) that is designed to damage the computer or collect information.

Phishing - A scam that involves sending a fraudulent email soliciting personal information from an unsuspecting user.

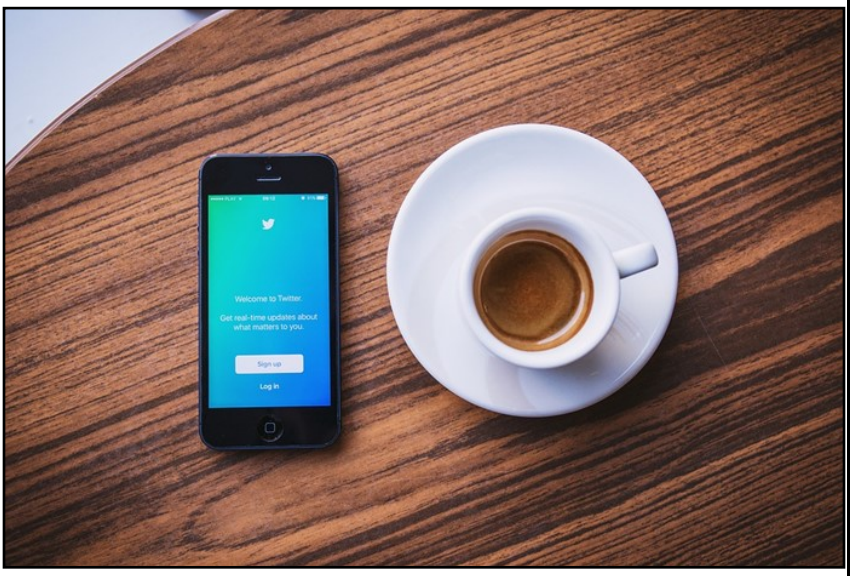
Spam - Any unsolicited email or junk mail.

Spoofing - The forgery of an email sender so that the message appears to have originated from someone or somewhere other than the actual source.

Virus - A self-replicating program that typically arrives through email attachments and multiplies on the hard drive, quickly exhausting the computer's memory.

SOCIAL MEDIA

Protecting yourself on social media is just as important as keeping your browsers and email secure.



- Turn off location services for photos and within apps
- Keep personal info to a minimum
- Log out of accounts when not in use on public or shared devices
- Perform frequent privacy setting assessments and updates.

SOCIAL MEDIA

- Don’t post that you are away from home.
- Don’t tag people in photos without permission.
- Confirm with someone before you give their personal information to someone else.
- Do not friend people that you do not know or trust.
- Discover how to block or unfriend followers on social media.

Notes

PASSWORDS

Passwords are primary way to secure your online accounts. Here are some tips to follow:

- Length of at least 6 characters, more are better
- Mix upper and lower cases with numbers and special characters
- Avoid using “dictionary terms” or one-word passwords
- Do not share your passwords with anyone
- Do not include personal details in passwords
- Follow new password guidelines
- If compromised, change your password immediately

Notes

Tip: Use a sentence, phrase, or line from a song and add some numbers to create great passwords.

PASSWORDS

A password manager can keep track of your passwords and generate passwords for you if you need a stronger one. Some password managers include: Dashlane, Keeper Security, LogMeOnce Password, and Sticky Password.

Most importantly of all, most password managers include a feature called Two-Factor Authentication.

Two-Factor Authentication is an extra layer of security for your accounts that requires not only the password and username credentials, but a supplemental piece of information that fall into at least two of the following categories:

- Knowledge: something you know
- Possession: something you have
- Inherence: something you are (like fingerprint reader, voice recognition, retina scanners)

EMAIL SAFETY

Spam emails are unsolicited, anonymous, wide-spread mass mailings with malicious intent.

They may request sensitive information or financial data from users by advertising contest rewards, health supplements, mysterious package shipment information, unclaimed offshore wealth, and a host of other unrealistic claims.

Approximately 60% of all email is spam. Think of spam like the junk mail you receive everyday in the mail

Notes

EMAIL SAFETY

There's no way to have an email inbox completely free of spam, but there are things you can do to keep your inbox tidy.

- If an unsolicited email sounds too good to be true...it probably is! So read the email subject line carefully before deleting it.
- Do not give out your email too often
- Have more than one email address to separate business and personal accounts
- Search for unsubscribing tools to roll all of those pesky subscriptions into one email so that you can unsubscribe safely:

  - Unroll.Me
  - Unsubscriber
  - Sanebox
  - Unlistr

SURFING SECURELY

In today's digital world, we now have a wide range of access to the internet from a handful of browsers: Internet Explorer, Google Chrome, Mozilla Firefox, and many more. Each browser has its own kind of protections in place to make you feel safer about who and what you may encounter on the internet. As you explore the internet, keep some things in mind:

- Implement features that give you security without compromising your convenience.
- Fit your security to your needs and habits.
- Trust your intuition.

Notes

SURFING SECURELY

Each browser has a combination of these features and settings that you can set to create a **safe**, secure searching environment. But it's important to understand what these features do in order to use them **effectively**.

- **Browsing history**: A log of all of your activity while using a browser
- **Pop-up blockers**: Prevent pop-up windows by closing them immediately
- **Location services**: Allow or deny websites to know where you're located for statistical purposes
- **In-Private Searching**: A mode in a browser that prohibits the collecting of your activity in your browser history, cookies, or site data that you input into forms

Notes

SECURED SITES

When entering personal information on a website, turning on private browsing, or creating strong passwords and usernames, there are a few things that you can do to be a **safe** internet user.

- Make sure a website is **secure** before entering any personal information. Look for the following characteristics:

https://www.website.com

- A secured site uses **encryption** to protect your information from phishing scams and fraudulent activity. To be a secured site, there are two elements that must be present: a URL that begins with **HTTPS** rather than HTTP and a **closed padlock** icon location depending on the browser.

Notes

SECURED SITES

Before entering your information in an unsecure site, ask yourself:

- Is it **sensitive** information?
- What could happen if somebody **intercepted** it?

Notes

PRIVATE BROWSING

Accessing private browsing windows will differ on each browser. They are a great tool if you share devices or use public computers and don't want your personal information saved in the browsing history and cookies. But, remember, they won't hide internet activity from people with administration rights to your computer like your school, employer, or internet service provider.

Notes

PRIVATE BROWSING

Settings and more > New InPrivate window
OR
Keyboard shortcut:
Ctrl + Shift + P

More menu > New Incognito Window
OR
Keyboard shortcut:
Ctrl + Shift+ N

Open Menu > New Private Window
OR
Keyboard shortcut:
Ctrl + Shift + P

Notes

PASSWORD TIPS

- Take time to retire your passwords every two months.
- Avoid using the same password for every account.
- Find out if your accounts have been compromised: *haveibeenpwned.com.*
- Delete old accounts if you're not using them. They can be a liability if someone gains access to your personal information, even if you haven't used them in a while.
- To find out how to delete old accounts, *backgroundchecks.org/justdeleteme* can assist you.

Online Learning opportunities:
mymcpl.org/online-learning

MID-CONTINENT
PUBLIC LIBRARY