Cyber Safety

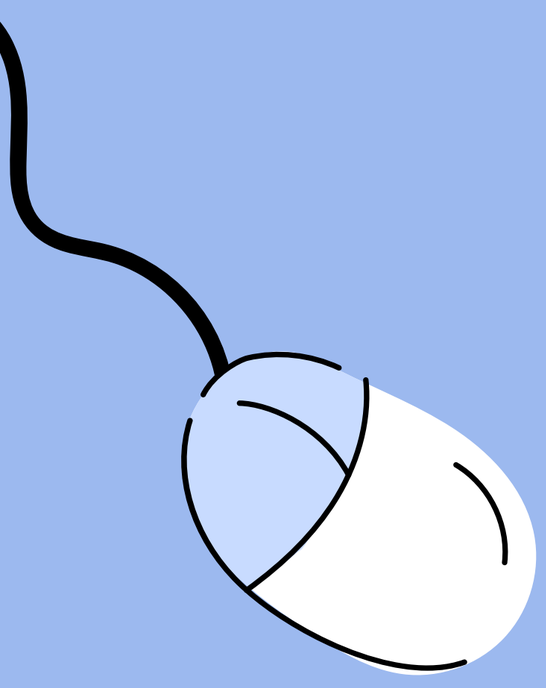
Password Tips

Never Share Your Password

Keep your passwords safe. Use a secure and reliable password manager.

Do Not Make Passwords Easy to Guess

- **Do not inlcude personal information like your name, family names, or pet names which can easily be found on social media**
- **Avoid using common words. Substitute letters for numbers. punctuation marks or symbols.**
  - **Ex: @ can replace an "a" and an ! can replace an "I"**



Get Creative

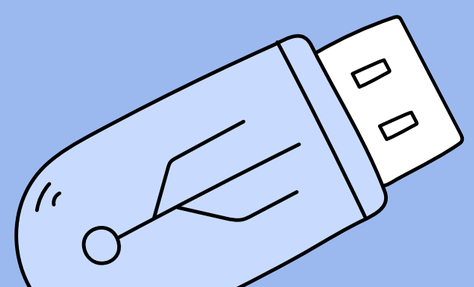
- **Use phonetic replacements like "PH" instead of "F." Or make deliberate misspellings, like "enjin" instead of "engine."**
- **Use a long password. Make it a sentence of at least 12 characters. Focus on special phrases you will remember.**
  - **Ex: I love Country music.**

Unique Account, Unique Password

Having different passwords for various accounts helps prevent cyber criminals from gaining access to all accounts and personal info.

Double Protection

Double your login protection. Enable multi-factor authentication (MFA) to Ensure that the only person who has access to your accounts is you.



Cyber Safety

Clean Machine Tips

Keep Security Software Current

Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

Protect ALL Devices

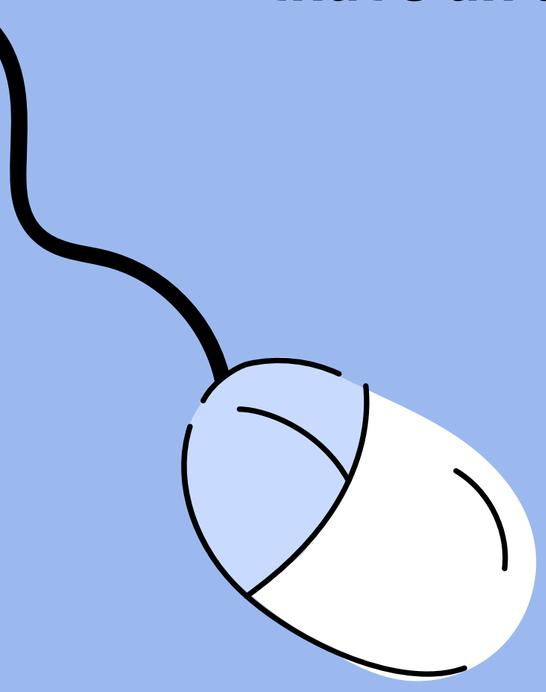
Protect all devices that connect to the internet. Along with computers, smartphones, gaming systems and other web-enabled devices need protection from viruses and malware.

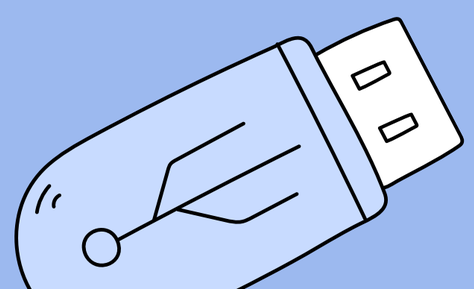
Automate Software Updates

Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

Plug & Scan

USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.





Cyber Safety

Connect With Care

When in Doubt Throw It Out

Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Get Savvy about Wi-Fi Spots

Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine. Do not connect to open Wi-fi hot-spots if the source is not secure.

Practice Safe Browsing.

A single careless click can expose your sensitive information. Think before you click!

Protect Your $$$

When banking and shopping, check to be sure the site is security enabled. Look for web addresses with “https://” or “shttp://,” which means the site takes extra measures to help secure your information. “Http://” is not secure.

Stay safe online!