Top Cybersecurity Tips

Think before you click.
Cyber-criminals often use current news, sensational topics, and promises of shocking photos and video to get you to click on malicious links. Don't fall for it! Stop and think before you click.

Get anti-virus protection and keep it updated.
Anti-virus (AV) software scans files for certain patterns or signatures of known viruses. Virus authors continually release new and updated viruses, which is why it is important to always have the latest AV version installed on your computer.

Keep your computer software and device apps updated.
Don't leave your computer vulnerable. Keep your systems patched and up-to-date with the latest security patches from vendors. Doing so will help prevent malware infections and keep your systems protected.

Back-up your pictures and documents.
Information can easily be lost or compromised due to an equipment malfunction, an error, or a virus. Schedule automatic backups of your information on a regular basis and take advantage of cloud services.

Create strong, unique passwords for every site.
Passwords are a major defense against hackers, and developing good password practices will help keep your sensitive personal information and identity more secure.

- Passwords should have at least 10 characters, include uppercase and lowercase letters, numbers, and symbols.
- Avoid common words; some hackers use programs that try every word in the dictionary.
- Never use personal information (your name, children's names, dates of birth, etc.) that someone might already know or easily obtain.
- If you believe your system has been compromised, change your passwords immediately.
- Use different passwords (or at least a variety of passwords) for each online account you access.
- If you must write down your passwords, keep them in a secure location away from your computer. Under no circumstances should you store them in a document on your computer!

Be careful on public Wi-Fi connections.
Using a public Wi-Fi network not only puts your personal devices at risk, but also exposes your traffic to everyone else using the same network. Cyber-criminals can potentially access any information you provide, such as credit card numbers, confidential information, or passwords.

Be mindful of e-mail and phone call fraud attempts.
You may receive an email posing as a bank, lawyer, widow, or ill person asks you to help them with money, inheritance, validating your password or lottery winnings… this is called "Phishing".

- Never follow links or instructions from unknown or untrusted sources
- Never send sensitive information through e-mail
- Log out when you are finished

Question what you see in e-mails and pop-ups.
Sometimes in surfing the web, the bad guys will use pop-ups or malicious advertisements to make you believe your computer has become infected. Use your real anti-virus to run a scan of your computer.

Download and stream from proper sites only.
Look for the lock and "s" in the URL

Don't search the internet for movies, music, apps, etc. then just download what you find in the search results. This is extremely dangerous and will open your computer to malware - not to mention that it could be illegal due to copyrighting and other intellectual property rights' laws.

Do not post sensitive information on social media sites.

- What goes on the internet, stays on the internet
- Get permission before posting pictures of others
- Do not put sensitive information on social media
- Do not post that you are going out of town