

ANTI-VIRUS NOT JUST FOR COMPUTERS



Most people spend more time shopping and surfing the web on cell phones and tablets, watching videos, answering emails, and playing games than on their laptops. So, practicing good cybersecurity when using these devices like you would your computers is essential, including anti-virus software that scans your files and your incoming email for viruses and then deletes anything malicious that it finds. Use these action-item tips to ramp up your online cybersecurity:

- 1. Install a reputable Anti-Virus software:** Ensure that you have a reliable and up-to-date Anti-Virus software installed on your device. Choose well-known brands that offer regular updates and high detection rates.
- 2. Keep your Anti-Virus software up to date:** Regularly update your Anti-Virus software to ensure you have the latest virus definitions and protection against emerging threats.
- 3. Enable automatic scanning and updates:** Enable automatic scanning of your device and automatic updates for your Anti-Virus software. This will ensure that your device is regularly scanned for viruses and malware, and that your software always has the latest protection.
- 4. Be cautious when downloading or opening attachments:** Avoid downloading files or opening email attachments from unknown or untrusted sources. These can often contain viruses or malware that can compromise your device.
- 5. Regularly scan your device:** Run regular full system scans using your Anti-Virus software to check for any potential threats or infections. Set up a schedule for automatic scans to ensure your device is regularly checked.
- 6. Use a firewall:** Enable and configure a firewall on your device. A firewall can help block unauthorized access and protect your device from external threats.
- 7. Keep your operating system and applications updated:** Install updates for your operating system and applications as soon as they become available. These updates often include security patches that can protect your device from known vulnerabilities.
- 8. Exercise caution while browsing:** Be cautious when visiting websites, especially those that are known to distribute malware. Stick to reputable websites, avoid clicking on suspicious links, and be wary of pop-up ads.
- 9. Use strong and unique passwords:** Create strong, unique passwords for your online accounts. This will make it harder for hackers to gain unauthorized access to your accounts and personal information.
- 10. Regularly backup your important data:** Implement a regular backup plan to store copies of your important files and documents. In the event of a virus or malware attack, having backups will ensure that you can recover your data.

REMEMBER, anti-virus software is only one layer of protection you need. Safe browsing habits and updating your devices and software are just as important to ensure the security and privacy of all your internet devices. Are you expecting to receive or give new devices this holiday season? Follow and share these tips so everyone can be #CyberSecure.