protect your family and loved ones; beware of malicious software

Do you know what software may be installed on your computer? Malicious software can put your personal information and security at risk.

Malicious software can contain security vulnerabilities, infected code, or other harmful elements that can damage your computer and steal your personal information.

What can you do to avoid malicious software:

- Only download software from trusted sources (ex. Google Play or Apple App store; avoid downloading 'free' versions of anything from the internet)
- Keep your software and operating system up to date
- Be wary of emails and links from unknown sources
- Enable firewall protection
- Educate yourself about phishing scams

Allstate cybersafety

Allstate®

protect your family and loved ones
beware of malicious software

Want to go a step further? Work with your family and friends to make sure they do the following before downloading anything from the internet:

- **Be wary of 'free' offerings or things that seem too good to be true** - hackers capitalize on the fact that people want things immediately and for free. Be wary of any site that offers downloads of free movies or anything else that shouldn't be available to consumers for a few months or without a fee.
- **To verify if a site is reputable**, check the website's "About" or "Contact Us" page. Look for phone numbers, a physical addresses, news coverage, or other signs that this is a trustworthy website.
- **Install anti-virus software and scan files** before downloading. The majority of anti-virus software lets you scan files for malicious intent if you right-click on the file you're trying to download. Others will prompt you to open your software first, before it scans the file you just downloaded.
- **Pay attention to file extensions** - look at the letters that come after the file name. Executable files such as .exe or .scr are often considered dangerous and should be avoided. If you downloaded a file with one of the above extensions from a website you trust or a known email, just be sure to scan the file first to ensure it doesn't pose a threat.
- **Back up your device to another (or multiple) locations.** If you do fall prey to a virus, it is recommended that you reset your device and restore your backup to prevent hackers from stealing your data or locking you out of it. In this case, it is helpful to have a back-up with your files, photos, and data so you don't lose anything that is important to you.

Don't take the risk! Protect your computer and data by avoiding malicious software.

Allstate cybersafety

Allstate®