When you're ahead of the game, you can't be gamed.

10 Ways to Be Cyber-Secure at Home

Identify your perimeter

Less is more! The fewer connected devices and entry points you have, the safer your network is.

Update software and devices regularly

Regular updates make you less vulnerable to attack. Only download updates from the manufacturer and enable auto-updates when possible.

Secure your Wi-Fi network

Routers often have default credentials that people don't know about. Disable the "remote configuration" option in your router and change both your Wi-Fi password and your router password.

Watch out for insecure websites

Always use HTTPS for sensitive communications. Don't ignore browser warnings and always remember to check the website address carefully for misspellings and oddly-placed letters or numbers. When in doubt, manually enter the URL in your browser.

Back up your files

Backups save your information if your device breaks or is taken over by an attacker. Back up files to a removable device that can be locked away safely, such as a CD or flash drive.

Don't download carelessly

Files can contain malware, and websites aren't always what they appear to be. Always verify sender identity before downloading files and remember: If it comes from an oddly-spelled email or is hosted on a site that makes your browser generate a warning, stay away!

Encrypt devices to deter thieves

Encryption renders files unreadable without the correct key. Some devices offer the option to encrypt individual files or the entire device. Consider which solution suits your needs best.

Practice password safety

Choose long passwords containing uncommon words. Use unique passwords for sensitive accounts and a password manager to help you remember them.

Always use antivirus software

Antivirus needs updates, too! Set it to auto-update.

Keep yourself informed

New cybersecurity bugs and attacks pop up every week. Staying informed about the latest threats will help you be safe!

INFOSEC

Learn more at infosecinstitute.com