Personal Cyber Security Tips

Scammers, hackers and identity thieves are looking to steal your personal information - and your money. But there are steps you can take to protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have good reason.

Update Your Software. Keep your software – including your operating system, the web browsers you use to connect to the Internet, and your apps – up to date to protect against the latest threats. Most software can update automatically, so make sure to set yours to do so.
Outdated software is easier for criminals to break into. If you think you have a virus or bad software on your computer, check out how to detect and get rid of malware.

Protect Your Personal Information. Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So, every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about why someone needs it and whether you can really trust the request.
In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Protect Your Passwords. Here are a few ideas for creating strong passwords and keeping them safe:

- Use at least 10 characters; 12 is ideal for most home users.
- Try to be unpredictable – don't use names, dates, or common words. Mix numbers, symbols, and capital letters into the middle of your password, not at the beginning or end.
- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies where you do business – thieves can use it to take over all your accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not ask you for your password.
- If you write down a password, keep it locked up, out of plain sight.

Consider Turning On Two-Factor Authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.
Give Personal Information Over Encrypted Websites Only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address. That means the site is secure.
Back Up Your Files. No system is completely secure. Copy your files to an external hard drive or cloud storage. If your computer is attacked by malware, you'll still have access to your files.

*Source: Federal Trade Commission/Consumer Information/Privacy, Identity & Online Secuirty