

DIGITAL & ONLINE SAFETY CHECKLIST



Be Skeptical

If something seems strange, stop what you're doing and think through the situation. Never give out passwords or let someone into your electronic device if you can't verify their identity.

Stay Up-to-Date



Don't ignore updates for your computer (or any device). Be sure to perform system and security updates as soon as possible. Devices without the latest updates are the easiest for malicious people or software to attack.



Change Passwords

Common passwords like birthday or kids' names can be found in public records and thus easier to hack. Older passwords may have been compromised via internet leaks. Set a calendar reminder to change your passwords every 45-60 days.

Skip The Quiz



Social media quizzes can be fun, but may be a front to capture personal information. Answers like pet names, high school info, and favorite movies are often used for password verification; sharing such details puts your accounts at risk.



Trust but Verify

Think twice before giving out any info over the phone. It's a common scam to impersonate IRS, bank, or company reps you would otherwise trust. When in doubt – hang up and call them directly from a verifiable number on their website.

Back It Up



Some malicious attacks can only be resolved by a full reset of your device. If it comes to that, a recent back up to an external drive or the cloud will be your data's saving grace. So remember to back up all of your devices frequently!

- REMINDER: Your financial institution will never call you to request information received via text (SMS) or pressure you to reset your online banking password