Internet Safety Basics for First-Timers

Welcome to the Digital World! The internet is an incredible tool for staying connected with family, reading the news, and watching videos. However, it requires a few basic safety habits. Think of these rules like locking your front door or looking both ways before crossing the street.

1. SOCIAL MEDIA: THE "OVERSHARING" TRAP

When you post on platforms like Facebook or X (formerly Twitter), you are not just talking to your friends—you are publishing to the world. Scammers use social media to gather puzzle pieces about your life.

- **Never post your travel plans.** Posting "Wheels up for Hawaii for two weeks!" tells local burglars your house is empty. Wait to post your vacation photos until you are safely back home.
- **Keep family details private.** Scammers use the names of your grandchildren, pets, or high school to guess your passwords or impersonate loved ones in emergency scams (e.g., "Grandma, I'm in jail, please send bail money").
- **Do not take online quizzes.** Those fun Facebook quizzes asking for your "first car," "mother's maiden name," or "street you grew up on" are actually harvesting answers to common bank security questions.

2. MOBILE PHONE SAFETY

Your smartphone is a tiny, powerful computer in your pocket. It faces the exact same risks as a desktop computer.

- **Use a PIN or screen lock.** If you drop your phone at the grocery store, a simple PIN code prevents a stranger from opening your email or banking apps.

- **Ignore unknown text messages (Smishing).** If you receive a text saying "Your USPS package is delayed, click here" or "Your Netflix account is locked," do not click the link. These are traps designed to steal your passwords. Delete the text.
- **Keep your phone updated.** When your phone asks to install a software update, say yes. These updates contain critical security patches to protect you from hackers.

3. PASSWORDS AND LOGIN SECURITY

The locks on your digital doors need to be strong to keep intruders out.

- **Never reuse passwords.** If you use the same password for Pinterest and your bank, a breach at Pinterest gives hackers the key to your money.
- **Write them down safely.** It is perfectly fine to write your passwords in a physical notebook, as long as you keep that notebook hidden securely in your desk drawer at home.
- **Never share login codes.** If a website texts you a 6-digit login code, never read it to anyone over the phone. Scammers will pretend to be bank security and ask for that code to bypass your account security.

> ***The Golden Rule:*** *If an email, text, or phone call creates a sudden sense of urgency or fear (e.g., "Your account will be deleted in 24 hours!" or "You owe the IRS money immediately!"), it is almost certainly a scam. Slow down, hang up, and ask a trusted family member for advice.*