ONLINE SAFETY TIPS FOR SENIORS

Being online lets you stay abreast of current events, connect with friends and family, shop, manage your finances, play games, and anything else you can think of. Just as you fasten your seat belt before driving, take precautions before using the Internet to be sure you are safe and secure.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

KNOW THE RED FLAGS
To begin with, if anyone contacts you and insists on payment by a wire transfer or gift card, it's a scam. End the conversation immediately.

VERIFY TO CLARIFY
Be suspicious of emails, text messages, or phone calls that create a sense of urgency and require you to respond to a crisis or give sensitive information, such as your credit card number or bank account information. Don't respond immediately. Hang up or walk away from the computer and contact a trusted source to verify the legitimacy of the request.

WHEN IN DOUBT, THROW IT OUT
Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting.

PASS IT ON

The FTC has found that older adults are more likely than younger consumers to report losing money on tech support scams, prize, sweepstakes & lottery scams, and family & friend impersonation. To learn more about these scams so you can educate yourself and those you love, visit: **www.ftc.gov/passiton**

KEEP A CLEAN MACHINE
Keep all software on all internet connected devices current. These updates not only improve the security of your device, but also improve its functionality. Stop clicking postpone on that update.
Pro Tip: Configure your devices to automatically update or to notify you when an update is available.

ONLINE SAFETY TIPS FOR SENIORS

LOCK YOUR DEVICES
You lock the front door to your house, and you should do the same with your devices. Require a passcode to unlock your phone or tablet. Securing your devices keeps prying eyes out and can help protect your information in case your devices are lost or stolen.

MAKE A LONG, UNIQUE PASSPHRASE
Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember. (for example, "IL0veCountryMusic!."). Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.

OWN YOUR ONLINE PRESENCE
Every time you sign up for a new account, download a new app, or get a new device, ***immediately configure the privacy and security settings*** to your comfort level for information sharing. Regularly check these settings (at least once a year) to make sure they are still configured to your comfort.

SHARE WITH CARE
Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes such as stalking. Just because a website asks you for your address, photo, or mother's maiden name, doesn't mean you actually have to answer honestly.

PEOPLE AREN'T ALWAYS WHO THEY SAY THEY ARE ONLINE
Adults of all ages need to be wary of strangers and those appearing to be your friends or loved ones online. It is too easy for criminals to hide their true identity and appear trustworthy. If someone asks to be your friend on a social media platform, only accept their request if you know them. If someone online asks you for money or sensitive information, pick up the phone and call a trusted number. Dating online? Don't send money or sensitive financial or personal information to anyone you have never met.

ADDITIONAL RESOURCES

FTC: Pass It On for Seniors
www.ftc.gov/passiton

NCSA: Own Your Role in Cybersecurity: Start With the Basics
https://staysafeonline.org/resource/own-your-role-in-cybersecurity/