TECH SAFETY

Being smart about technology isn't just about keeping up with the latest devices; it's about protecting your privacy, finances, and personal safety. By learning to recognize common scams — like fake bank calls, emergency money requests, phishing emails, social media and online dating fraud — you can stay confident, connected, and secure in the digital age.

SCAM CALLERS / TEXTS

Scammers can have a caller ID that says they are your bank, debt collectors, or even a government agency. They may say that they have flagged a purchase, need confirmation of your card number, pin number or account information. Scammers may often use threats stating that you are facing legal charges, or even that you missed jury duty.

Never share personal info over the phone. Hang up immediately and call the number on your card, credit reporting agency or your financial branch. Government agencies do not call you directly, if concerned, can call them directly.

IMPOSTOR CALLS / TEXTS

Scammers may use personal details about your loved ones to impersonate them and steal your information. A common tactic involves claiming to be a family member—or saying that your relative is in trouble and urgently needs money. Some scammers even use technology to mimic your loved one's voice, relying on emotional manipulation to gain your trust and access your personal information.

Never share personal information over the phone. Hang up immediately and contact your loved one directly. If they don't answer, leave a message and wait for them to confirm. If the caller claims to be from a hospital or police department, look up the official number on their website and call directly to verify.

ROBO CALLERS / TEXTS

Scammers like to call saying you've won the lottery, cash prize, or most commonly - an extended warranty. They may even be from a charity asking for money. Tech support scammers also may call about your Apple or Microsoft device claiming you have a virus and need access to your device.

Never share personal info over the phone. Hang up immediately. If you are interested in helping a charity, look them up online and see if they have secure donation options. Lotteries, car warranties and tech companies don't call.

EMAIL OR TEXT SCAMS

Phishing emails are designed to steal your information by getting you to click on a link or image. Doing so can install viruses or hacking software on your device. These emails may offer free items, fake coupons, or claim your account is at risk of being closed. They might also include fake invoices or pretend to be from companies like FedEx or UPS asking you to confirm a delivery.

Always verify the sender's email address before clicking anything. Scam emails often use random letters, numbers, or a fake display name that hides the real address. Never click on links— instead, go directly to the retailer or shipping company's official website to check your account or order status.

SOCIAL SCAMS

Social scams involve fake online identities used to gain trust and steal money. Scammers often profess love quickly, refuse video chats or only use Google Meet, and avoid meeting in person. Red flags include requests for money/gift cards, vague profiles with professional photos or inconsistent profile photos, and claims of being overseas to excuse their absence.

Never share personal info, send money or send gift cards. Make sure you end contact immediately. Report the scam to the dating platform and agencies such as the Federal Trade Commission (FTC) or U.S. Secret Service.

WHAT TO DO

If something feels off—trust your instincts. Scammers rely on urgency and fear to trick you into acting quickly. Stay calm, stop communication right away, and take time to verify before responding. Protect your personal information, never send money or click suspicious links, and report the scam to the proper authorities or platforms.

HOW DO I PROTECT MYSELF?

Computer Updates - Make sure you update your computer and phone with updates as these contain security software updates against new attacks.

Security Software - Having extra security software or setting on your emails can help spot fraud scams before you even open them. Contact your device provider for security recommendations and assistance to set up.

Back up your data - Utilize a separate drive to upload important documents, photos or other precious items. Only plug into your device when ready to back up. *Make sure you do this monthly.* Cloud storage is easy for back up as well but having a separate external hard drive is best.

Befriend Safely - When connecting through social medias or dating sites, make sure they are a legit person. Research the person before connecting via message, phone, video or in person. Report them to the site as a fake profile and block them immediately if they are not legit.

WHAT IF I FALL FOR A SCAM?

Contact your financial institutions immediately - If you fall for a scam and disclose your account, card or personal information, call your bank immediately and take the steps to protect your accounts. They will walk you through it. They may recommend new bank accounts or order new cards.

Contact your credit bureau - Contact your credit bureau to freeze any future credit pulls and flag your account. This requires multiple authentications if you want future credit lines or financing. They can protect your credit from scammers trying to open credit lines or mortgages in your name.

Run a virus scan - Run a scan of your devices and computers to check for viruses or malware. It may require you to rest your computer.

Change your Passwords - Immediately change the passwords to your banks, email, social medias, etc. Scammers may try to access and charge or pull money from your accounts or use information for financial gain.

Back up your data - After running a virus scan, back up your documents and photos to a separate hard drive or cloud account in case you need to do a hard reset to your computer.

Report It - This is important to protect others and yourself from future attacks. If using social media or dating sites - contact them regarding the scammer. For internet scams, file a complaint with the Internet Crime Complaint center at **https://www.ic3.gov/.** For an email scam, forward the email to **reportphishing@apwg.org** and block the sender from reaching out to you in the future. There is also an option in your email to report it as well.

OTHER HELPFUL RESOURCES

Customer Financial Protection Bureau
https://www.consumerfinance.gov/consumer-tools/fraud/

Federal Deposit Insurance Corporation
https://www.fdic.gov/consumer-resource-center

Federal Bureau of Investigation
https://www.fbi.gov/how-we-can-help-you