

SUN CITY CENTER COMPUTER CLUB
CYBERCRIMINALS ARE OUT TO GET SENIORS
Scam Safety To-Do List – Check It Off – Stay Safer

STOP & VERIFY	
	Slow down when a message, call, or pop-up creates fear or urgency.
	Verify independently using a phone number or website you already know.
	Never trust caller ID, a familiar voice, or an official-looking message by itself. Let the call go to voicemail.
	Set up the Press 1 feature on your phone to help screen calls. Check with your carrier.
	Use a generic voice for your voicemail message. iPhone>Voicemail tab. Android>Settings>Greeting.
PROTECT MY ACCOUNTS	
	Use strong, unique passwords (at least 14 characters) or a passphrase.
	Turn on MFA or use passkeys.
	Keep devices, browsers, and apps updated. Use PatchMyPC for non-Windows apps.
	Review all accounts for unfamiliar activity.
PROTECT MY MONEY & IDENTITY	
	Set up a trusted contact at your bank, stock, retirement, and credit card companies. Contact does not need access to your accounts.
	Set up a credit limit for all accounts. You will be notified of transactions over the amount.
	Freeze your credit at all three credit bureaus.
	Download a copy of your credit reports to check for errors.
	Shred sensitive documents before throwing them away or cover sensitive information with a black ID theft protection roller.
WATCH FOR THESE RED FLAGS	
	Unexpected links, attachments, QR codes, or pop-ups.
	Requests for gift cards, cryptocurrency, wire transfers, cash, or gold.
	Unexpected requests for passwords, account numbers, Social Security, or Medicare information.
	Anyone asking you to keep a financial emergency secret.
	Money isn't safe at your bank / never send money to "protect" it.

COMPLETE THESE IMPORTANT TO-DOS	
	Create an IRS account/wallet (ID.me) to access tax records.
	Create a my Social Security account.
	Create a Property Fraud alert account with the County Land Records office.
	Create a USPS Informed Delivery account. You receive an email with screenshots of the mail you will receive the next day.
	Create a family emergency code word.
IF I THINK I'VE BEEN SCAMMED	
	Stop communicating with the scammer.
	Close the website: Click on X in the upper right corner- Press Alt+F4- Turn off your computer- Pull the plug. Turn your computer on; DO NOT restore the web page, or the scam will reappear.
	Contact your bank and credit card companies immediately if money is involved.
	Change passwords that may have been exposed. Use Bitwarden for a password manager.
	Tell someone you trust and report the scam.

RESOURCES

- For fraud assistance, call the National Elder Fraud Hotline - 833-372-8311
[National Elder Fraud Hotline | Office for Victims of Crime](#)
- For ID Theft assistance: Identity Theft Resource Center [Identity Theft Resource Center | ITRC](#)
- Better Business Bureau Scam Recovery Toolkit: [Home | BBB Scam Recovery Toolkit](#)
- FBI / IC3: [ic3.gov](#)
- FTC fraud reporting: [ReportFraud.ftc.gov](#)
- IRS Individual Online Account: [Your account | Internal Revenue Service](#)
- my Social Security: [my Social Security | SSA](#)
- Sign up for e-Notification at LA County Tax Collector (title deed fraud): [Assessor - e-Notification](#)
- USPS Informed Delivery: [Informed Delivery - Mail & Package Notifications | USPS](#)
- California DROP (Delete Request and Opt-out Platform): Removes you from 600+ data brokers registered in California [Assessor - e-Notification](#)
- Better Business Bureau: [Find and Report a Scam | Better Business Bureau](#)
- AARP Fraud Watch Network: [Scams & Fraud: Alerts, Prevention Tips & Help | AARP](#)
- Hillsborough County Title Deed Fraud: <https://www.propertyfraudalert.com/select>