R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Identity Theft Protection and Cyber Safety Resources

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Welcome and thank you for attending the R.O.S.E. Fraud Awareness & Protection Program! We trust you will find this information useful and will incorporate some or all into your daily life.

We have compiled this information from reliable sources. Always make sure you are on the verified website/calling verified phone numbers as these could be updated.

Please contact us with comments, questions, etc.

Office phone: (602) 445-7673

Website: www.roseadvocacy.org

Email: info@roseadvocacy.org

Mailing address: PO Box 50280, Phoenix, AZ 85076

Scan QR code or email us with a testimonial and sign up for our newsletter.

Donation

ROSE
SCAN ME

Newsletter Sign Up

ROSE
SCAN ME

R.O.S.E.
Resources/Outreach to Safeguard the Elderly

SECTION 1: YOUR CREDIT

Check Your Credit

- annualcreditreport.com

Credit Monitoring and Alerts

Credit monitoring and alerts will give you an alert about any activity involving your credit. While this can quickly bring a potential problem to your attention; you will not know if someone has used your identity until after it happens. An added benefit is to find a credit monitoring service that includes dark web scanning and social security number tracking.

Here a few of the many companies with credit monitoring services.

- CreditWise® from Capital One
- American Express® MyCredit Guide
- Chase Credit Journey
- Experian Dark Web Scan + Credit Monitoring

For more information on credit monitoring and alert services, read this article *"These services provide you with free credit monitoring alerts so you can spot fraud early"* by Alexandria White Updated October 1, 2024.

It is best to read information about different credit monitoring and alert services, both free and paid subscriptions, to determine which one would work for your needs.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Fraud Alert

- Regular fraud alert – use this when you are concerned about identity theft. It makes it harder for someone to open a new credit account in your name. It is free and lasts one year.
- Extended fraud alert – use this when you have had your identity stolen and completed an FTC (Federal Trade Commission) Identity Theft report at www.IdentityTheft.gov or filed a police report. It makes is harder for someone to open a new credit account in your name and removes you from unsolicited credit and insurance offers for five years. It is free and lasts for seven years.
- Active Duty alert – use this when you are on active military duty. It makes it harder for someone to open a new credit account in your name and removes you from unsolicited credit and insurance offers for two years. It is free and lasts for one year.

Credit Freeze

Anyone can freeze their credit for free, even if your identity has not been stolen. You will need to freeze at all three credit reporting agencies.

- Equifax – www.equifax.com 1-888-378-4329
- TransUnion – www.transunion.com 1-888-909-8872
- Experian – www.experian.com 1-888-397-3742

- Make sure you are on the verified website or calling the verified phone number.

- Be sure to save the passwords when you freeze your credit; you will need these if you decide to thaw your credit freeze.

- Freezing your credit will not guarantee safety, it is a strong defense against identity theft.

Source: Federal Trade Commission

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 2: ONLINE ACCOUNTS

Passwords

People use passwords that are often very easy to crack – and often times reuse passwords and use something that is easy to remember like child's name, birthdate, pet's name, etc. This information is easily accessible by looking at social media. Once the scammer finds one ID and password combination that works, the scammer will try that same combination on other websites - knowing people reuse their passwords. A very common password that is still used is password123, this is giving the scammer the keys to your account.

Password managers or vaults are a great tool to store all your passwords and will help you generate new, random passwords. The PCMag article, *"The Best Password Managers for 2024"* by Kim Key, updated October 4, 2024, has pros/cons of different password managers.

Browser password managers (i.e. Google, Firefox, Chrome, etc.) can be an option. If you are going to use one of these browser password managers, please make sure you know what all they offer and do not offer especially with security features. Passkeys can be an option. It is a passwordless login option which uses your device to login.

With any password option, scammers find ways to access your account logins. Do your research and understand the security features, benefits, etc. before you make a decision on which one to use.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Create a Strong Password

Here is a suggestion on how to create stronger passwords, please do not use this example, create your own strong base password.

Current strategy suggests a minimum of 16 random characters

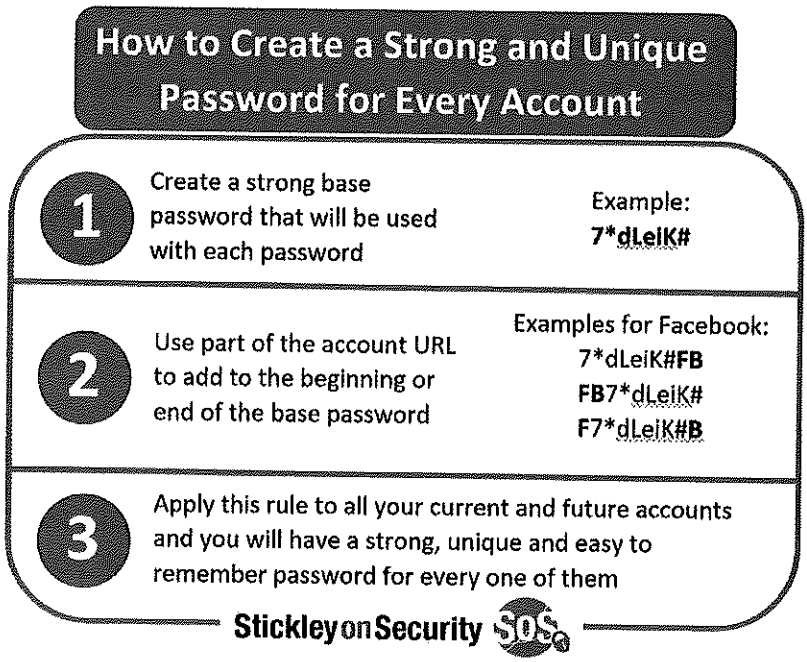


Photo source: SOS Daily News

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Multi Factor (or 2 Factor) Authentication

Passwords are not enough these days to secure your accounts. Multi factor, or 2 factor, authentication (MFA or 2FA) is an extra layer of security for your accounts. One item to look at when choosing one of the multi factor authentication apps is whether the app will back up the account information (encrypted) in case you no longer have the phone where you installed the app. Also, authenticator apps provide more security than getting your authenticator code through a text message.

Google and Microsoft Authenticators are probably the most well-known authentication apps and there are other options. The PCMag article *"The Best Authenticator Apps for 2024"* by Kim Key updated October 21, 2024, has reviewed a handful of authenticator apps. Read the article to learn more about authenticator apps and determine which one is best suited for your needs.

When getting a new mobile phone, make sure all information in your authenticator app transfers to your news phone or you could be locked out of those accounts.

Multi factor or 2 factor authentication is in the account settings. You can turn it on and then provide information on how you would like to receive the codes.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 3: PAYMENTS

Check Washing

Check washing fraud is when someone intercepts your check, uses chemicals to wash away the ink, and rewrites the check to their benefit. Sometimes they will leave your signature intact or they will fraudulently sign the check. Checks can be stolen, or the scammer will print fake copies of a check.

In an article from the United States Postal Inspection Service dated October 13, 2023, https://www.uspis.gov/news/scam-article/check-washing, Postal Inspectors recover more than $1 billion in counterfeit checks and money orders every year.

Helpful Tips:

- Use a gel-ink pen to write your checks. The gel ink does not come off when chemicals are used to wash the check.
- If using the blue collection boxes at the Post Office, deposit you mail before the last collection time of the day and try to avoid using these boxes on holidays and weekends.
- When sending checks or other sensitive personal information, avoid using blue postal collection boxes not located at the Post Office.
- Do not leave mail in your personal mailbox, retrieve your mail daily.
- If you are going on vacation, put a vacation hold on your mail.
- Try to avoid using initials for the Payee. For example, do not write "S.R.P." The criminals can simply add "rice" to the Payee name to make it look like it was made out to "S.R.Price" and deposit it into a fake account.
- Monitor your bank account regularly and balance your checkbook.
- Destroy any old or unused checks. Do not throw them in the garbage.
- For more information, read Frank McKenna's September 11, 2022, article *"Fraud Check Washers Hate This Very Ordinary $2 Pen"*

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Debit vs Credit Card

When making the choice between using a debit card or a credit card, there are a few important safety considerations to consider:

1. Credit cards have a **zero-liability policy** which means you are not responsible for any unauthorized transactions if your card has been stolen or compromised. You will have to report the fraud promptly, but you have more recourse than you would with a debit card.

2. You can also dispute charges for goods or services that were not provided, were damaged, lost, or are incorrect through a **Dispute Resolution Process.** This is not something that is offered by debit cards.

3. Some credit card companies offer additional **warranty and purchase protections** for items that have broken or are defective after the manufacturer's warranty has expired.

Source: Angie Montoya
September 17, 2024

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Swipe vs Tap vs Chip

Tap and chip have been effective but scammers have can also get your card information when using both tap and chip. They are using shimmers to get your chip information and by standing close to you when you tap. The scammers can also install malware in the point-of-sale terminal that will make your chip or tap not work so your only option is to swipe your card. It is easier for the scammer to get your card information from the magnetic swipe on your card as the magnetic swipe is not encrypted.

Unfortunately, it does not take long for a scammer to insert a card skimmer or shimmer into a machine and it is hard to tell the difference.

Please be aware of your surroundings when using your credit or debit card and understand the risks. In addition to swipe, both tap and chip have risks and your card information can be compromised – use credit card for purchases. You have more recourse for fraudulent charges. You debit card can be a gateway into your bank account that is tied to your debit card.

Put alerts on your card(s) so you are notified of every transaction and can mitigate fraudulent charges.

Please watch this video for more information from U.S. Secret Service Asst. Special Agent Charles Leopard. https://youtu.be/xxpJtlEREdA?si=IpIgjnewUw63EpJO

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 4: DEVICE

Antivirus Software

Have a good antivirus software on all of your devices. This will help detect malicious software from infecting your device. Once the antivirus software is installed, make sure that it stays on (scanning your device all the time) and is up to date. The following is taken from the PCMag.com article *"The Best Antivirus Software for 2024"* by Neil J. Rubenking updated September 24, 2024. The article has a lot of information on different antivirus software and compares the pros/cons of different antivirus software solutions.

- Bitdefender
- Webroot
- Norton
- McAfee

And many more listed in this article. There is also live links to their best antivirus software and a comparison of these antivirus software. Some have a free version as well.

Whichever antivirus product you decide to use, make sure it is running all the time on your devices. If the software is not running, it cannot detect malicious sites, viruses, etc.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Silence Unknown Callers

You might be on the Do Not Call Registry but unfortunately scammers ignore the registry. Blocking numbers is a good tool but scammers use many different phone numbers.

- Some of the mobile phone carriers offer apps to block calls and messages.
  - AT&T – ActiveArmor and Call Protect
  - Verizon® – Call Filter
  - T-Mobile – Scam Shield App
  - US Cellular – Call Guardian® App
  - Check with your carrier

- Silence Unknown Callers is available on both Apple and Android phones. This feature automatically silences calls from numbers NOT saved in your contacts. The caller can leave a voicemail, and the call will appear in your recent call list.

  - Apple phones for calls – settings > phone > scroll down to Silence Unknown Callers > turn this on.
  - Apple phones for texts – settings > messages > scroll down to Unknown & Spam, turn on Filter Unknown Senders. This will sort messages from people who are not in your contacts into a separate list.
  - Android phones for calls – phone app and tap the three dots at the top right > settings > blocked numbers > turn on Unknown feature.
  - Android phones for texts – messages app and tap the three dots at the top right > settings > spam protection > turn this on.

As mobile phones are constantly updating their software, these instructions can change.

There are many apps available, some free and some paid subscriptions, to help with spam calls and messages. Make sure you know what the app will and will not do, security features, access to your information, etc. before you make a decision.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Accessibility Options on your Android Phone
Hearing Impaired

Live Caption – caption videos and spoken audio

- ▶ Settings > Accessibility > Live Caption (running Android 10 or later – check the version of your phone by going to Settings > About Phone > Android Version)
- ▶ You can also use Live Caption on Google's Chrome browser. Click on three vertical dots (More) > Settings > Accessibility > toggle on Live Caption

Live Transcriptions – converts speech to text (Android 6.0 and later)

- ▶ Go to Settings > Accessibility > Live Transcribe
- ▶ You can also configure your phone to vibrate when someone says your name or when a conversation resumes after a lull.

Live Transcribe & Notification app – built in on Pixel phones but you need to download and install the app on most other Android devices.

- ▶ Go to Settings > Accessibility > Sound Notifications > tap Open Sound Notifications. Then you can select sounds you want your phone to listen for like, fire/smoke alarms, sirens, pets, doorbells, etc.
- ▶ In addition, you can go to Settings > Notification Preferences > can illuminate your phone's flash to alert you > Custom Sounds where you can add sounds like washing machine beep, so you know when it is done.

Hearing Aids – pair them like any other Bluetooth device.

- ▶ Go to Settings > Connected Devices > Pair New Device
- ▶ You many also have the option to pair through Settings > Accessibility > Hearing Devices > Pair New Device

Real-Time Text

- ▶ Open phone app, tap three vertical dots (Menu) > Settings > Accessibility > turn on RTT or TTY

Settings can change with phone updates.

Read full Wired article (Simon Hill, June 12, 2024).

Source: Wired

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Accessibility Options on your Android Phone
Vision Impaired

Customize your display settings

- Settings > Display > change brightness, colors, and theme.
- Settings > Display > Display Size and Text > choose a font size, icon size, and bold or contrasting text that works for you.

Reading mode

- Removes ads, menus, and other website clutter and get streamlined versions of online articles that only display the important text and images.
- Settings > Accessibility > Reading Mode > Allow to turn it on.
- When you want to use it, simply tap the onscreen accessibility button.

Magnify or Zoom

- Settings > Accessibility > Magnification

Audio Descriptions – describe what is on your device screen and tell you about alerts and notifications

- TalkBack – Accessibility > TalkBack > Use Talkback
- Select-to-Speak – Settings > Accessibility > Select-to-Speak. Once activated you can access it with a two-finger swipe up or three-finger swipe if TalkBack is on.

Voice Commands

- Settings > Accessibility > toggle on Voice Access (if option is not available you will need to download the Voice Access app.
- If full voice control is too much, you could use Google Assistant to open apps, tweak settings, and more.
- You can make changes to Google Assistant by going to Settings > Google > Settings for Google Apps > Search, Assistant and Voice > choose Google Assistant.

Read the full Wired article (Simon Hill June 13, 2024) for more information.

These settings can change with phone updates

Source: Wired

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Accessibility Options on your iPhone

Hearing impaired (in beta testing as of June 12, 2024)

Live-Captioning System

- ▶ Settings > Accessibility > Live Captions > turn on Live Captions (Beta) – requires iPhone 11 and later running iOS16.
- ▶ Closed Captions + SDH (subtitles for deaf or hard of hearing) – Settings > Accessibility > Subtitles & Captioning > turn on Closed Captions + SDH

Sound Recognition

- ▶ Enables your iPhone to listen for various sounds (fire/smoke alarms, pets, doorbells, knocking, crying, glass breaking, and more).
- ▶ Go to Settings > Accessibility > Sound Recognition > turn on > click on Sounds to choose which sounds to recognize.
- ▶ You can also use LED Flash for Alerts – go to Settings > Accessibility > Audio & Visual > LED Flash for Alerts

Apple Made for iPhone (MFi) hearing aid program. You can connect supported hearing aids to an iPhone via Bluetooth.

- ▶ Go to Settings > Accessibility > Hearing Devices > choose your hearing device > Start Live Listen.

Real-Time Text – depends on your region and carrier.

- ▶ Go to Settings > Accessibility > Answer All Calls as RTT/TTY. You can also choose RTT/TTY Call when calling someone.

Read the full Wired article (Simon Hill, June 12, 2024) for more information

These settings can change with phone updates

Source: Wired

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Accessibility Options on your iPhone
Vision Impaired

Customize your display
- ► Settings > Display > tweak things like brightness, colors, and theme
- ► Settings > Display > Display Size and Text > choose font size, icon size and bold or contrasting text

Magnify or Zoom
- ► Settings > Accessibility > Zoom

Audio Descriptions
- ► VoiceOver – Settings > Accessibility > set your preferred speaking rate, select voices for speech, set up braille output, and more.
- ► If VoiceOver is too much – Settings > Accessibility > Spoken Content >
  - ○ Speak Selection to have a Speak button pop up when you select text.
  - ○ Speak Screen to hear the content of the screen when you swipe down from the top with two fingers
  - ○ Typing Feedback to choose to have characters, words, autocorrections, and more spoken aloud as you type.
- ► Audio descriptions of video content – Settings > Accessibility > turn on Audio Descriptions

Voice Commands
- ► Settings > Accessibility > Voice Control > Set Up Voice Control

Read the full Wired article (Simon Hill June 13, 2024) for more information.

These settings can change with phone update

Source: Wired

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 5: OTHER TIPS

Verify a Charity

Periodically we get calls from charities asking for donations. When there is a crisis (i.e. hurricane, flood, tornado, war, etc.), these calls seem to increase. Scammers contact you and create a compelling reason to get you to donate money to help during a time of crisis. Verify charity before deciding to donate.

- IRS – https://www.irs.gov/charities-non-profits/tax-exempt-organization-search Click on the "Tax Exempt Organization Search Tool", then click on "Search for Tax Exempt Organizations" box. You can then input the charity's employer identification number and click search. The results will show you the charity's name and you can click on the charity's name to get more information on their nonprofit status. You can also call 1-877-829-5500.
- Charity Navigator – https://www.charitynavigator.org and type in the charity's employer identification number in the Charity Search section at the top of the page. Information about the charity will be displayed. There will be an alert if the charity is reported/confirmed to engage in misconduct or questionable practices or is a fake charity. You can also call 1-201-818-1288.
- Make sure you are on verified website and calling verified phone number.

It is best to search by employer identification number (EIN) as sometimes the name of the organization is different with the IRS. For example, R.O.S.E. Resources/Outreach to Safeguard the Elderly is listed as Rose Resources Outreach to Safeguard the Elderly.

Keep in mind that it takes the IRS some time to get the charity's information uploaded into their system. Charity Navigator gets their information from the IRS. If you are dealing with a newer charity, ask the charity to see their IRS Tax Determination Letter. In the end, you will need to decide if you want to donate to the charity. Call charity with a verified number or donate on the charity's verified website.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Identity Protection Pin (IP PIN) with IRS

The IP PIN helps the IRS verify your identity when you file a tax return.
Even if you are not required to file a tax return, the IP PIN protects your IRS account. An IP PIN is a six-digit number that is issued to you and a good proactive step to protect you if someone else files a tax return using your information. Only you and the IRS will know your IP Pin.

If you have an online account at IRS.gov you can use this to get your IP PIN. If you do not have an account, you will have to set one up to get verified before you can request the IP PIN online.

Do you prefer not to get the IP PIN online, you can complete an application or request in-person authentication for an IP PIN. (Call IRS 800-908-4490). Make sure you are calling the verified phone number.

- IP PIN is valid for one calendar year
- New IP PIN is generated each year
- IP PIN must be used when filing any federal tax return
- Both spouses can get an IP PIN when filing jointly

Your IP PIN should only be given to your tax professional. The IRS will never call, email, or text asking for your IP PIN. Lost your IP PIN – you can find it by logging into your online IRS account or call the IRS at 1-800-908-4490 for assistance. Make sure you are calling the verified phone number and on the verified website.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Property Deeds

Deed fraud is on the rise in Arizona and across the United States. The Attorney General's office warns Arizonans of a disturbing trend with deed fraud over the last couple of years. It is very easy to transfer the title of your home with a fraudulent signature especially if you own your property free and clear. Scammers have a tendency to look for vacant homes where the owner recently passed away.

You can still be a target, especially if there is no lien (mortgage or otherwise) on your home, if you live in your home. Here is a 2022 video with a criminal investigator at the Attorney General's Office with more information.
https://youtu.be/cqmyE7qDsJo?si=14EYGHSeFFpKXS-5

Helpful Tips:

- ▶ All AZ counties are required to have a deed alert system in place by the beginning of 2025. Check your County Recorder's website or call to sign up for this alert. This alert will notify you when there is a change in your deed, it does not prevent the change from happening. https://recorder.maricopa.gov/
- ▶ Periodically check your deed at your County Recorder's Office. You can search by parcel number.
- ▶ Some credit monitoring companies will also monitor your property deed.
- ▶ Check with your insurance agent regarding your home policy(s) coverage should you need to hire an attorney to recover your property deed.
- ▶ If you use and identity theft protection service, inquire if this service will cover your property deed and any expenses you incur to recover your deed.

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Medicare

Every year Medicare has Medicare Annual Enrollment Period (AEP) when Medicare beneficiaries can review and change their coverage for the following year. The AEP runs from October 15th to December 7th each year. Information for the Medicare plans are available beginning in October of each year.

Medicare agents are not allowed to talk about plan benefits until after October 1st each year.

The Centers for Medicare & Medicaid Services have strict policies regarding these dates.

Should you receive calls about new Medicare plans, updates, etc., always call and talk to your current Medicare agent before making any changes. Your current Medicare agent should have all this information and be able to guide you accordingly.

Protect your Medicare number and Medicare card – this is personal identifiable information.

Review your Medicare statements for charges, dates of service, etc. and report any discrepancies to your provider's office.

Medicare will not call you to sell you anything or visit you at your home.

Medicare card is lost or damaged – Order or print and official copy of your Medicare card on your online account or call 1-800-MEDICARE (1-800-633-4227).

Railroad Retirement Board (RRB) benefits – you can call 1-877-772-5772 to get a replacement card.

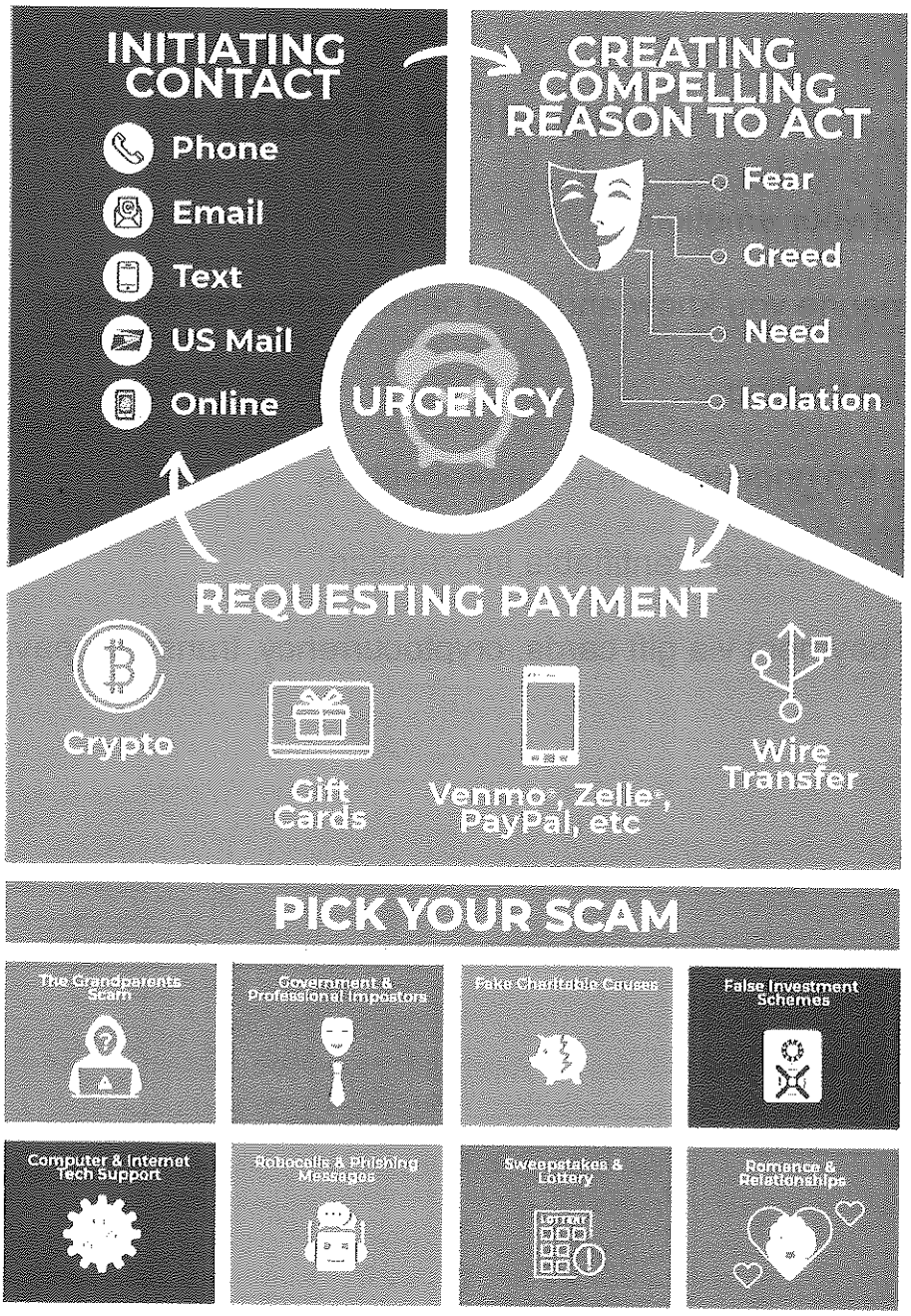
Source: Medicare

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Tips and Tools

- Be aware of your emotions
- Talk to someone you know and trust before acting on anything
- Verify before trusting
- If it sounds too good to be true…it probably is
- Protect your personal identifiable information
- Beware of payment via gift cards, cryptocurrency, transfers, payment apps.

ANATOMY OF A SCAM



A scam is a fraudulent scheme that deceives individuals or organizations to obtain money or sensitive information. Scammers use false promises and misleading tactics, posing as legitimate entities or individuals. They exploit trust and vulnerability through various channels like phone calls, emails, or social media. It's crucial to be vigilant and report any suspicious activity to authorities.

www.roseadvocacy.org

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 6: REPORTING

Reporting a Fraud or Scam

Why should you talk to someone and report a fraud or scam?

- A friend/family member may have experienced the same scam.
- It could help your friend/family member have knowledge about the scam.
- The Federal Trade Commission works to shut down the scammers and file suit.
- Information can help investigators build a case against the scammer.
- Your story makes a difference – all information helps the Federal Trade Commission and investigators know what scammers are doing.

Report identity theft at identitytheft.gov and get a recovery plan or call 1-877-438-4338

- Tell them what happened. They will ask questions about your situation.
- Get a recovery plan based on your situation.
- Put your plan into action. Once an account is created, they will walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

Report Medicare fraud at https://oig.hhs.gov/fraud/report-fraud/ or call 1-800-633-4227.

Report all other fraud and scams to reportfraud.ftc.gov or call 1-877-382-4357

- Report a scam, a company, or an unwanted call.
- Find out what you can do to protect yourself.
- FTC will use and share reports with law enforcement to help with investigations.

You can also report a fraud or scam to your local FBI at 1-800-CALLFBI or your local Attorney General's office (Arizona 1-602-542-4579)

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

SECTION 7: SAFETY CHECKLIST

Credit and Payment

- ☐ Check your credit
- ☐ Freeze your credit or monitor credit reports
- ☐ Enable transaction alerts on credit cards
- ☐ Use credit card (not debit) for purchases
- ☐ Monitor bank accounts and deeds

Devices and Online

- ☐ Anti-virus software running all the time
- ☐ Password manager/strong passwords
- ☐ Use 2-factor/multi factor authentication
- ☐ "Silence Unknown Callers" on cell phone
- ☐ Install software updates
- ☐ Recognize, report, delete junk email & texts

R.O.S.E.®
Resources/Outreach to Safeguard the Elderly

Safety Checklist Continued

- ☐ Backup important documents and files

Other

- ☐ Get an IP PIN with IRS
- ☐ Be aware of your emotions
- ☐ Talk to a trusted person
- ☐ Verify before trusting
- ☐ Use secure Wi-Fi, not public Wi-Fi
- ☐ Consider using VPN (especially if public Wi-Fi is only option)
- ☐ Keep personal information confidential