

[view in your browser](#)



[Click above to see your card!](#)

In this newsletter

About R.O.S.E.
Peace of Mind
4th Annual Golfers FORE Senior Protection
Tournament
Thank YOU
Mobile Phone or Mobile Computer?
Android Malware Alert
Beware of Online Shopping Scams
Conversation Starters
Data Breach
FBI PSA
Update Your iPhone Now!

Monthly Mailer Newsletter
Connect With Us
Join With Us...

About R.O.S.E.

R.O.S.E., a 501(c)(3) non-profit, is creating change by providing awareness, resources, tips, and tools for financial scams that typically target the older adult population...

Mission

To prevent the financial exploitation and defrauding of the older adults through advocacy and education.

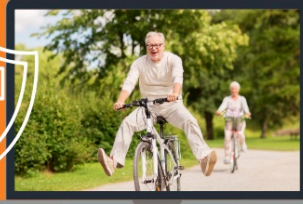
Vision

Retirement should be the best years of your life; it should be protected at all costs.

Goal

To reduce the number of victims and losses of financial frauds.

Peace of Mind



Knowledge That Protects

Peace of mind begins with education – knowing how to spot a scam before it happens. R.O.S.E. is working to reach more communities across Arizona, bringing education and protection from scams to those most at risk.

As the holiday season approaches, scams become a greater threat. Through our support, we're helping older adults recognize the warning signs before it's too late.

And with your help, we can continue sharing trusted information and tools to keep those we love safe and informed through our community talks, resources, newsletters, social media, and weekly radio show.

Help keep seniors in our community empowered and protected.

SUPPORT R.O.S.E. ADVOCACY

4th Annual Golfers FORE Senior Protection Tournament



Thank you to the following sponsors:

[Choice Financial Planning](#)

[Gallop Technology Group](#)

[RJM Consulting](#)

[Tom Plachecki](#)

Our largest fundraiser is coming up - 4th Annual Golfers FORE Senior Protection tournament at AZ Grand Golf Resort on Friday, April 10, 2026, 7:20am shotgun start.

Mark your calendars! You don't want to miss this fun-filled event.

Our goal this year is \$38,000 which helps us expand our program across Arizona.

How you can help -

1. We have many different sponsorship levels available from \$7,000 Champions of Safety Sponsor to \$250 Green or Tee Box

2. Register a foursome for golf and save \$100 using earlybird discount code through December 31, 2025.

3. We have volunteer opportunities available starting now and through the event. [Email](#) Joyce for more information.

4. We are actively working on auction procurement - gift cards, experiences, spa certificates, wine baskets, hotel/airline certificates, and much more.

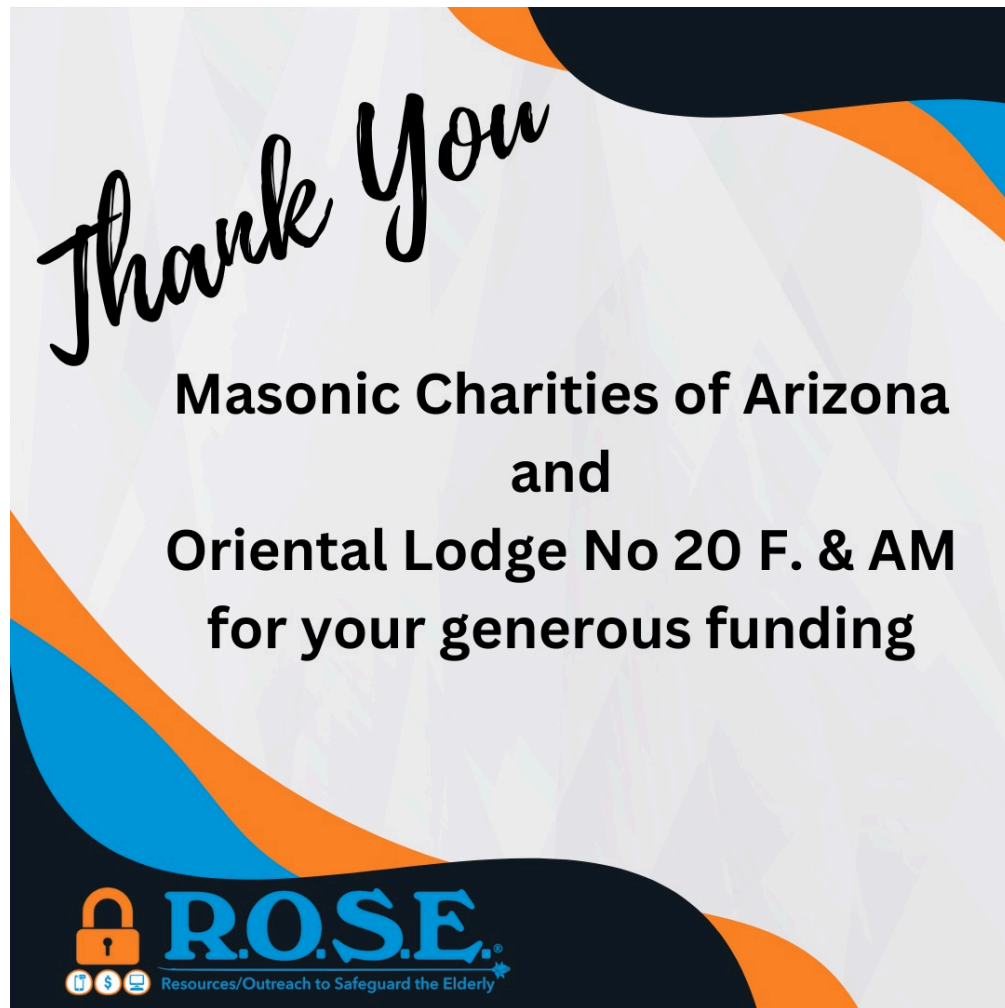
5. Want to save even more on your golf foursome, register for a sponsorship (\$1,600 to \$1,000 levels) and get your golf foursome for \$600.

More information and register, click [here](#).

Mobile Phone or Mobile Computer?



THANK YOU



Android Malware Alert

SCAM ALERT

Android Malware Stealing Card Info for ATM Withdrawals

NGate malware can steal your card details and PIN right from your Android phone and use them to withdraw cash at an ATM. This dangerous malware spreads through fake bank texts, emails, and phone calls urging you to download a “security app” from outside the Google Play Store.



ROSEADVOCACY.ORG

SCAM ALERT: New Android Malware Stealing Card Info for ATM Withdrawals 🚨

Hackers don't need your physical debit card anymore—NGate malware can steal your card details and PIN right from your Android phone and use them to withdraw cash at an ATM. This dangerous malware spreads through fake bank texts, emails, and phone calls urging you to download a “security app” from outside the Google Play Store.

Once installed, attackers capture your NFC activity and drain your account without you ever knowing.

How to protect yourself:

✓ Never download banking apps from links in texts, emails, or social media

✓ Only use official app stores

✓ Don't share financial info with anyone who contacts you unexpectedly

✓ Hang up and call your bank using the number on your card or statement

✓ Use reputable mobile antivirus protection

Stay alert and share this to help others stay safe! 🛡️ 📱 Encourage them to subscribe to our newsletter for up to date scam information.

Beware of Online Shopping Scams



TIP TUESDAY

Holiday Shopping

Fake emails, text messages, and phone calls are increasing, all designed to steal your personal and financial information.



ROSE
Resources/Outreach to Safeguard the Elderly

Stay Safe from Mobile Shopping Scams This Holiday Season! 🌲 📱

Holiday deals can be amazing—but scammers know it too. Fraud is on the rise, with phishing emails, fake text messages, and even scam phone calls trying to steal personal and financial information. Stick to trusted shopping apps, avoid clicking links from unexpected texts or emails, and be cautious with any app asking for unnecessary permissions.

Tips to stay safe:

- Only use verified websites
- Avoid links from emails or ads
- Watch out for fake “too good to be true” offers

- ~~Enable two-factor authentication~~
- **Keep an eye on your bank statements for any unusual activity**
- **Put alerts on your credit cards to mitigate fraudulent charges**

Remember: shopping should be joyful, not risky. Stay alert, shop smart, and protect your information this holiday season! 🌐🌟

Conversation Starters

LIVE on K4HD Radio at 8 AM PT on Tuesdays

LET'S TALK ABOUT SCAMS

A SCAM AWARENESS PODCAST

with
JOYCE PETROWSKI

K4HD

LISTEN LIVE at www.k4hd.com or download the K4HD Radio App.

The banner features a portrait of Joyce Petrowski on the left. The background is blue with white and orange text. A magnifying glass graphic is positioned over the word 'SCAMS'.

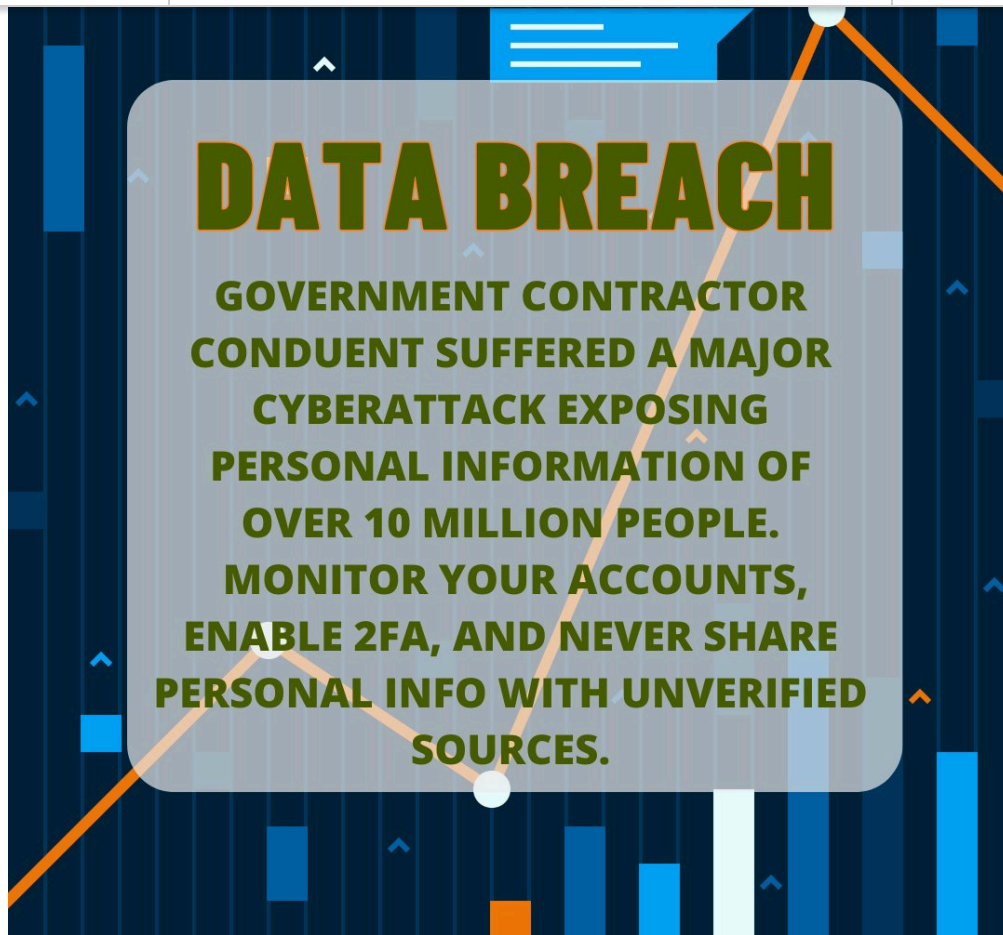
not. For most of us, it takes several reminders to make something a habit.

Scam prevention should be a habit for everyone, no matter your age. Want to help your older loved ones make scam prevention a habit and help them in protecting their legacy?

Subscribe to our YouTube channel by clicking the picture above and click subscribe. Our weekly radio show episodes and shorts are there for you to watch. There are many conversation starters here. Check out the live shows, shorts to get your conversation starter today.

Making scam prevention part of your regular conversation goes a long way in protecting everyone involved especially your older loved ones.

Data Breach



🔴 DATA BREACH ALERT: Conduent Government Services 🔴

R.O.S.E. is sharing this important alert to help protect you and your loved ones.

Conduent — a major government contractor that supports Medicaid, child support, food assistance, tolling systems, and other public programs — has confirmed a large-scale data breach affecting over 10 million people nationwide. Hackers accessed the system from October 2024 to January 2025 and may have stolen personal information, including Social Security numbers, medical records, and insurance details.

Affected states include Texas, Washington, South Carolina, New Hampshire, Maine, Oregon, Massachusetts, and California. Individuals will be notified directly by mail, and Conduent has set up a call center to answer questions.

While there's no evidence yet that the stolen data is being misused, R.O.S.E. encourages everyone — especially seniors and

🔒 How to Protect Yourself:

- **Monitor your bank, credit, and benefit accounts frequently**
- **Enable two-factor authentication wherever possible**
- **Use strong unique passwords or a password manager**
- **Consider using Passkeys instead of Passwords**
- **Install reputable antivirus/malware software**
- **Consider identity-theft protection or data removal services if needed**
- **Never respond to unexpected calls, emails, or texts requesting personal information – always verify through official channels**

Your safety is our priority. Stay informed, stay cautious, and reach out if you need help understanding scams or data breach risks.

FBI PSA



A recently issued PSA from the FBI is warning about bank impersonation and account takeover. This year alone the FBI has received more than 5,100 complaints with losses exceeding \$262 million!

A technique scammers use in this type of fraud is social engineering where the scammers tricks the account owner into giving over their login credentials including MFA codes by

or customer support personnel. Once the scammer has access to the account, they change the password and start draining the account. In some instances the scammer used fear tactics that the account was used to make fraudulent charges.

The scammers are using fake websites to impersonate the financial institution and Search Engine Optimization (SEO) poisoning. This is where the scammer purchases ads that impersonate the financial institution's legitimate ads.

Helpful tips:

1. Use strong antivirus/malware software on all your devices, including your mobile phone as this is a mobile computer.
2. Always verify before trusting the contact and the compelling reason to get you to act.
3. Consider using Passkey vs Password. The Passkey is biometric information.

Read the full [FBI PSA](#)

Update your iPhone Now!



APPLE UPDATE

HEADS UP

Apple has released urgent iPhone updates to fix a serious flaw that lets hackers hijack your device through something as simple as a malicious font hidden in an email, website, or document.

If you haven't updated yet — do it now!

HEADS UP!

Apple has released urgent iPhone updates to fix a serious flaw that lets hackers hijack your device through something as simple as a malicious font hidden in an email, website, or document.

If you haven't updated yet — do it now! 📱

Go to Settings → General → Software Update and install the latest version (iOS 26.0.1 or iOS 18.7.1).

Protect your personal info, banking apps, and privacy — don't let a fake font fool you. 🛡️

More Scam Alerts

SCAM ALERT

Fake Customer Service Numbers on Google

Scammers are posting fake customer service numbers on Google that look real — but lead straight to fraud. Never call the first number you see online or allow remote access to your phone or computer. Always verify contact info directly through your bank or the company's official website.

ROSEADVOCACY.ORG



SCAM ALERT

Veterans Scam Alert: Stay Protected

Scammers are posing as the VA or veteran support services to steal personal and financial information. If someone contacts you claiming to “speed up” or “increase” your benefits, don’t click links or share details – verify directly through VA.gov.

[ROSEADVOCACY.ORG](https://roseadvocacy.org)



Monthly Mailed Newsletter

We provide our monthly newsletters through the mail as well. Know someone who would benefit from this knowledge? Email [Joyce](#) with name and address and they will be added to the distribution list. Scams against seniors have become so prevalent, we all need reminders to be aware of scammers. Our monthly newsletter will not only provide valuable information and tips, it is also a reminder to stay vigilant.

Connect With Us



The spider web effect with sharing information. You share this information with your contacts who then share with their contacts and so on. This valuable information then gets to more and more people exponentially.

We need many different touchpoints for information to be top of mind and a habit. We don't want you to live in fear, we want scam awareness and prevention to be top of mind and a habit for you and your loved ones! Everyone will be contacted by a scammer, probably multiple times.

Here are our touchpoints and remember it only takes a few minutes to follow, like, subscribe, etc.

- 1. Sign up for our monthly email newsletter [here](#)**
- 2. Sign up for our monthly mailed newsletter - email Joyce at joycepetrowski@roseadvocacy.org**
- 3. Follow us on [Facebook](#) and [Instagram](#)**
- 4. Connect with us on [LinkedIn](#)**

6. Visit our [website](#) for resources

7. Watch or listen to our new radio show - Let's Talk About Scams at [K4HD Radio at k4hd.com](#). Missed an episode, all episodes are on our [YouTube Channel](#). Visit our [Let's Talk About Scams website](#).

We want everyone to protect themselves from scams!

Join With Us...



Monthly donation - every monthly donation amount helps! Help support the older adults in your community. Make your monthly recurring donation [here](#).

into your [walmart account](#), go to Account, then go to Giving & Impact, and select ROSE Resources Outreach to Safeguard the Elderly as your charity of choice.

Fry's Food Store - Fry's will donate a percentage of your shopping to your charity of choice. R.O.S.E. Resources/Outreach to Safeguard the Elderly would love to be your charity of choice. Log into your [account](#) and select R.O.S.E. Resources/Outreach to Safeguard the Elderly or MY964 to link your Fry's VIP card with us. Every time you shop, Fry's will make a donation to us and it does not cost you anything extra!

Email or Text scams - we like to use real life examples of scam texts and emails in our presentations and on social media.

Please forward to info@roseadvocacy.org

Volunteer - get involved by giving your time. We have different volunteer positions available including board and advisory committee positions. Contact

Joyce at joycepetrowski@roseadvocacy.org or (602) 445-7675

Regular donation - Your [donation](#) helps us to continue to provide our effective presentations to the older adults at no cost to them.

Sponsor - Do you want to help older adults protect themselves and their hard-earned assets? We have developed a sponsorship program to help deliver our life-changing presentations to the older adult population. [Learn more](#) and become a sponsor!

SUBSCRIBE



- Share this newsletter with your family & friends
- Encourage them to subscribe



Copyright © 2022 R.O.S.E. Resources/Outreach to Safeguard the Elderly, All rights reserved.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).