Chevron Retirees Association

Cybersecurity Presentation

August 12th, 2026

Agenda

- Welcome and Introductions
- Scams to recognize
- Accounts and Devices
- Spam and Phishing
- Payments and Money
- Artificial Intelligence
- Social Media
- Additional Resources

What is Elder Fraud?

Fraud targeting an elderly victim, which is defined as adults aged 60 and older.

These financial crimes can be perpetrated by a stranger or someone close to the victim, such as a family member or caregiver.

Elder Fraud Statistics

- More than **201,000 complaints** from people 60 and over.
- Older adults were swindled out of more than **$7 billion in 2025.**
- Older adults targeted by fraudsters suffer an **average loss of $38,500.**

Why Are Older Adults Frequent Targets? – 1 of 2

- Older adults have had more time to build wealth than younger adults. They could have substantial assets such as properties, savings, and retirement accounts.
- Some are more vulnerable because of aging and health issues.
- Some live alone and are more trusting of strangers due to loneliness.

Why Are Older Adults Frequent Targets? – 2 of 2

- Some may not want to report fraud because of embarrassment, or because they fear being considered unable to manage their own finances.
- Some are less familiar with technology and may be unable to spot the scams.

Elder Fraud – Common Scams – 1 of 2

- **Tech support:** A pop-up or caller claims your computer is infected and asks for remote access or payment.
- **Government impersonation:** Threats of arrest, prosecution, tax trouble, or benefit cancellation.
- **Family emergency:** A loved one is supposedly in trouble and needs money immediately.
- **Romance / companionship:** Trust is built over time; then money requests begin.

Elder Fraud – Common Scams – 2 of 2

- **Package / Account Alert:** A fake delivery or account notice pushes a link or attachment.
- **Bank Fraud Alert:** A "bank" instructs you to transfer money, share a code, or install an app.
- **Investment / Crypto:** Promises of guaranteed returns, urgency, secrecy, or moving funds.
- **Prizes / Refunds:** You must pay a fee or provide account info to receive money.

The Rule That Beats Most Scams

STOP

Pause

VERIFY

Use a trusted path

ACT

Only after checking

- **Bank email?** Open the bank app yourself.
- **Family emergency?** Call a known number.
- **Package text?** Go to the retailer or carrier website directly.

Scenario: The Voice Sounds Real

"Grandma, I'm in trouble. Please don't tell anyone. I need money right now."

Do not trust the voice by itself.

Call the person back using a number you already know, or contact another trusted family member.

Create a family "safe word" or verification question before you need it.

Account Security

Best — **Passkey or security key**
Phishing-resistant when properly implemented

Very good — **Authenticator app MFA**
A strong second step

Good — **Text-message code**
Better than password-only; not as strong

Avoid — **Password reused on many sites**
One breach can unlock multiple accounts

Passkeys and MFA

Passkeys

Use your phone, fingerprint, face, or device PIN instead of typing a reusable password.

Use them when offered, especially on major accounts.

Multi-Factor Authentication

A second proof after your password.

Prefer passkey/security key or authenticator app. Text codes are still better than password-only.

Password Managers

Why Use One?

- Creates long, unique passwords
- Fills the right password on the right site
- Reduces reuse and memory burden
- Used across multiple devices

Practical Advice

- 1Password and Bitwarden are both reasonable choices
- Apple/Google/Microsoft built-in managers are also fine
- Protect the master account with MFA/passkey

Sign-In Myths and Tools

Sign in with Google/Apple	Usually reasonable on sites you trust. It avoids creating another password; protect the main account strongly.
Incognito / private mode	Useful on shared devices or for a fresh session. It does not make you anonymous or stop scams.
VPN	Useful in some situations; it does not stop phishing, fake websites, or payment scams.

Question to ask: "What problem is this tool actually solving?"

Spam vs. Phishing – What's the Difference?

Spam E-mails: Unsolicited bulk messages that are typically commercial in nature.

Phishing E-mails: Malicious emails designed to trick people into falling for a scam. Typically, the intent is to get the recipient to reveal financial information, passwords, or other sensitive data.

Red Flags

Red Flags: Warning signs that alert you of potential issues.

Red Flags - Indicators of Email Scams – 1 of 4

- **Suspicious sender address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greeting and signature.** Both a generic greeting such as “Dear Valued Customer” or “Sir/Ma’am” and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

Red Flags - Indicators of Email Scams – 2 of 4

- **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service such as Bit.ly to hide the true destination of the link.

Red Flags - Indicators of Email Scams – 3 of 4

- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable organizations have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting you to download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency to persuade you to download or open an attachment without examining it first.

Red Flags - Indicators of Email Scams – 4 of 4

- **Requests you to take an action or disclose information.** A cybercriminal may add a sense of urgency to the message, prompting you to click a link or open an attachment to take immediate action. They may also ask that you provide sensitive information such as your username and password.

Remember to Stop and Think before acting on e-mails.

Browsers, ad blockers, and antivirus – 1 of 2

- **Safer Browsing:** Keep your browser updated. Consider ad/tracker blocking if you are comfortable managing it.
- **Extensions:** Install fewer extensions. Add only ones you trust and keep using.
- **Antivirus:** On Windows 11, Windows Security includes Microsoft Defender Antivirus.

Browsers, ad blockers, and antivirus – 2 of 2

- **Updates:** Turn on automatic updates for operating system, browser, phone, and apps.
- **Backups:** Use cloud backup or an external drive, especially for photos and documents.
- **Avoid Doubles:** Running multiple security products can create confusion and performance problems.

Protecting Your Money

Credit card = purchase protections

Payment app / wire / crypto / gift card = often like cash

Use payment apps for:

- People you know and trust
- Small personal payments
- After confirming the recipient

Be suspicious when:

- A stranger insists on Zelle/Venmo
- A "bank" tells you to move money
- Someone demands secrecy or urgency

Tap to Pay Vs. Inserting a Card

Tap / Mobile Wallet

Card/device stays in your hand. Wallet payments use tokenization, so the merchant does not receive the actual card number.

What is the real risk?

Being tricked into paying the wrong person, approving a fake invoice, or responding to a fake fraud alert.

Review statements and app alerts.
Report unauthorized charges quickly.

AI: Good Tool and Bad Tool

What AI Gives Scammers

- Polished phishing with no spelling errors
- Personalized messages at scale
- Voice cloning and fake videos
- Fake profiles, fake reviews, fake documents

What AI Gives Defenders

- Faster detection of suspicious patterns
- Better spam and fraud filtering
- Help summarizing and triaging alerts
- Stronger monitoring for organizations

Social Media Safety

- Review privacy settings and friend requests
- Be cautious with travel plans and public photos
- Avoid posting school, routines, birthdays, and personal identifiers
- Be careful with quizzes that collect "security question" answers
- Assume public posts may be copied, scraped, or reused

Before posting: "Would this help someone impersonate me?"

If Something Goes Wrong

1	**Stop communication**	Do not reply, click more links, or let remote access continue.
2	**Protect accounts**	Change passwords from a clean device; enable MFA.
3	**Call money institutions**	Bank, credit card, retirement account, payment app.
4	**Report and preserve**	Save messages/screenshots; report to FTC/FBI/local law enforcement as appropriate.

Additional Resources

- Visit https://MarinCounty.gov/Cyber
- Sign up for **Marin CyberSafe News**, our monthly cybersecurity newsletter,
- **Free Cybersecurity Awareness Training -** https://learnsecurity.amazon.com/

Open Discussion and Q&A

Thank You

August 12th, 2026

Photo Credit: Jeff Wong