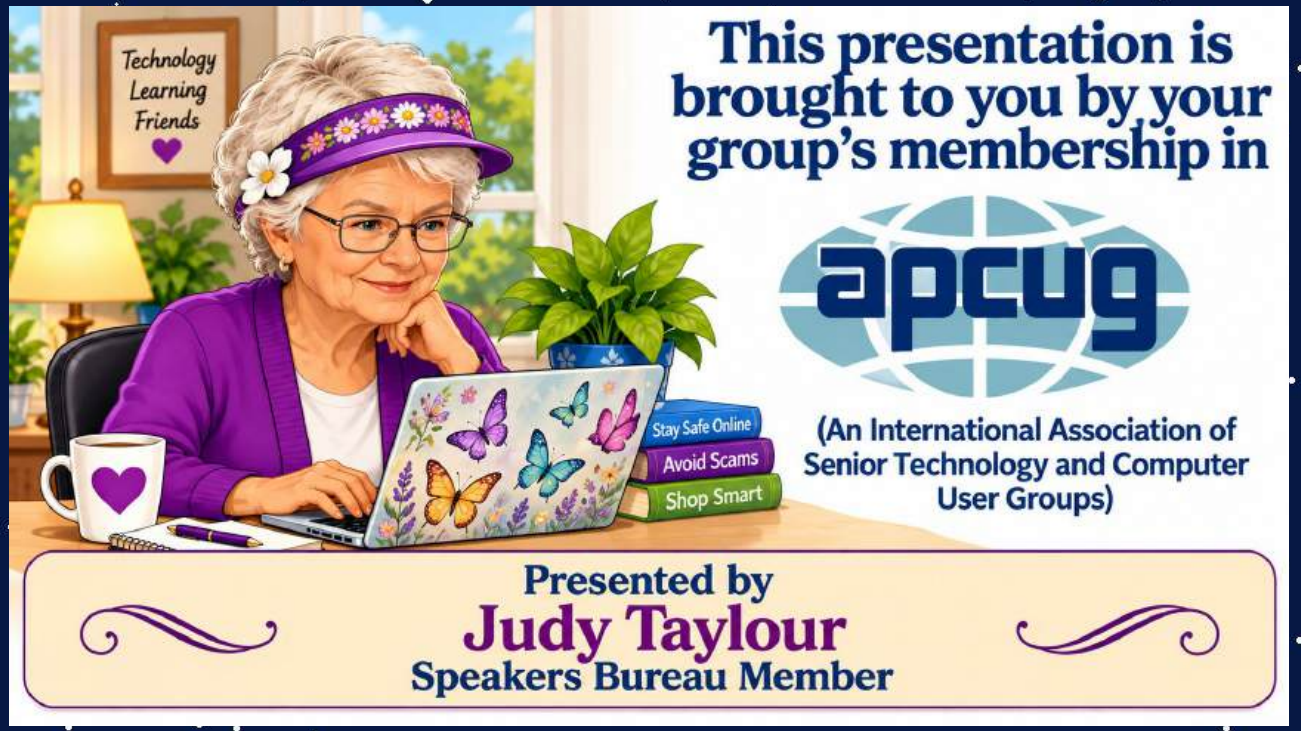


HOLIDAY SCAM SAFETY

Shop, Give, and Celebrate Safely

STOP • VERIFY • THEN ACT

SENCOM
November 2026


Technology
Learning
Friends
Stay Safe Online
Avoid Scams
Shop Smart
This presentation is brought to you by your group's membership in
apcug
(An International Association of Senior Technology and Computer User Groups)
Presented by
Judy Taylour
Speakers Bureau Member

Set up 2FA before Shopping

Choose Your 2FA Method

- Authenticator app (Google Authenticator, Microsoft Authenticator, Authy) — generates time-based codes, works offline, less vulnerable to SIM swap
- Hardware key (YubiKey, RSA SecurID) — highest security, phishing-resistant
- SMS (text) — easiest but less secure; use only if no other option
- Email
- Backup codes — store securely for recovery



Tip: Pick one primary method for all accounts to avoid confusion

Set up 2FA before Shopping

Prioritize Accounts - Enable 2FA in this order

- Email (Gmail, Outlook, iCloud) — critical for password resets.
- Payment services (PayPal, bank apps, credit card portals).
- Shopping platforms (Amazon, eBay, Walmart, etc.).
- Cloud storage (Dropbox, Google Drive).
- Social media

- By setting up 2FA on your email, payment, and shopping accounts before you shop, you add a strong barrier against account takeover and fraud

Set up 2FA before Shopping

Example for Amazon

- Sign in and go to Your Account > Login & Security.
- Select Edit next to Two-Step Verification.
- Choose Get Started and follow the prompts.
- Enter the code from your chosen 2FA method to verify.

Store Recovery Codes

- During setup, each service will give you recovery codes — save them in a secure location (password manager, encrypted file, or safe)

Fake Holiday Websites

- Online shopping scams are the number one scam reported to BBB Scam Tracker.
- Hundreds — Thousands — of fake holiday-themed stores are already “stocked” and live, combining realistic branding with AI-driven design to trick shoppers.
- Treat any unfamiliar “too good to be true” site with caution and verify before you buy.
- FBI advice: Don't click on ads in social media posts. Go directly to the website where you want to shop. Type the address into the URL. "Otherwise, there's a significant possibility that you're going to be scammed."



Black Friday Scams

- Worldwide: AI tools have found more than 10,000 fake shopping websites in a massive Black Friday scam. Evidence suggests that the operation is controlled by a single Chinese-speaking operator
- Scammers often make small changes to legitimate brand names, such as adding letters, inserting hyphens, or using unusual domain extensions, to make fake online stores look authentic.
- Don’t click a link from Google, social media, or an AI assistant; type the brand’s official website address i official app.
- Beware of payment logos; they might take you to a fake location that looks the same as the one you use.



https://tinyurl.com/4jrbyfuv

Empty Gift Cards

- U.S. gift card market is estimated to generate $507.1 billion in revenue in 2026.
- 1 in 5 have reported giving gift cards with no money on them.
- Thieves target gift cards to steal PIN numbers, barcodes, etc.
- Look closely at the PIN number to be sure it is still covered.
- Buy gift cards behind a counter or online.



Gift Card Idea

- Both physical and digital cards can be used for Apple Store purchases, the App Store, iTunes, Apple Music, Apple TV+, Apple Arcade, Apple Books, iCloud storage, and other Apple services.
- Physical: Has a **16-digit code** on the back that the recipient will use to redeem the balance.
- Digital: Apple will email the gift card to the recipient. You can include a personal message. The email contains a Redeem Now link that adds the balance to the recipient's Apple Account.





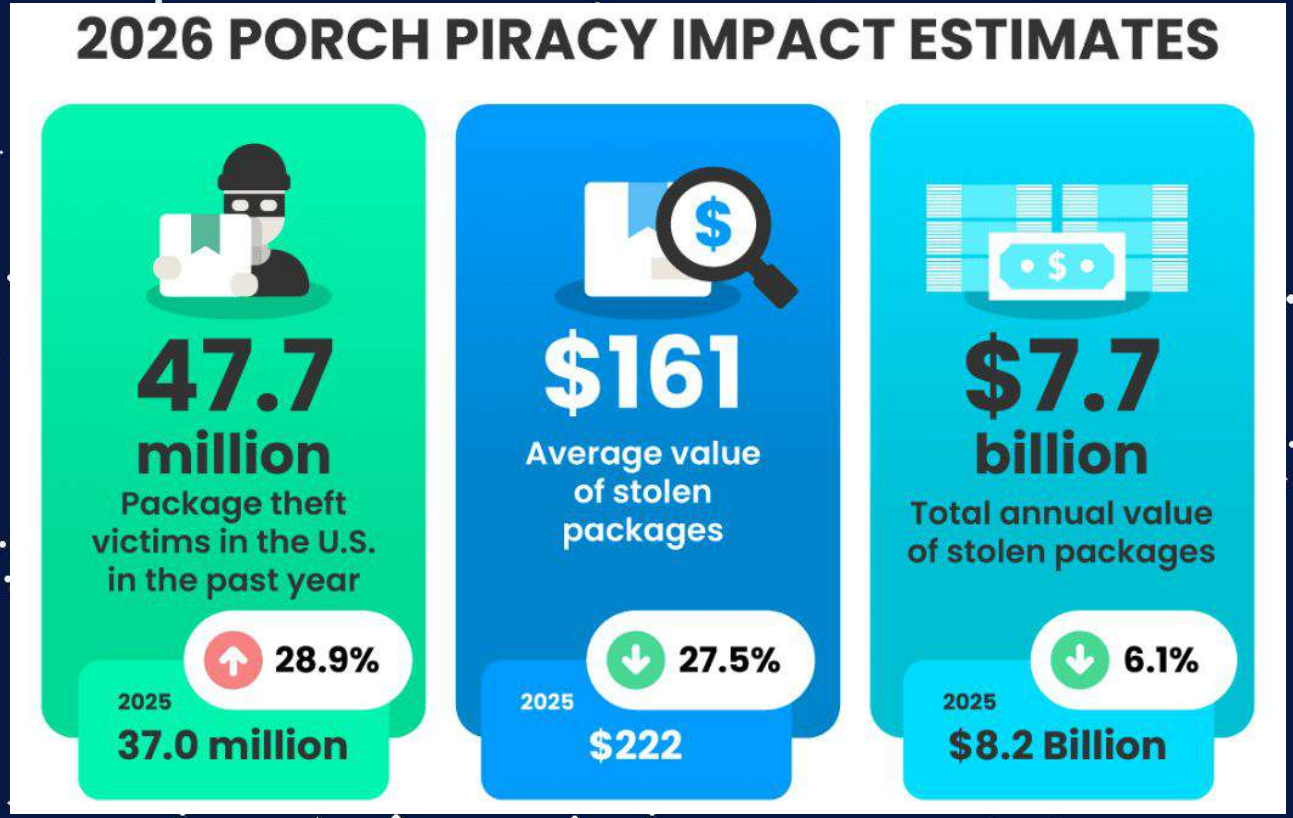


Bogus Charitable Giving

- Important time of year for legitimate charities to solicit funds.
- 2025 - Charity scams cost Americans $7.9 million in 2025.
- Fraud spikes after major disasters, holidays, and other high-empathy events.
- ALWAYS check out a charity at:
- https://www.charitynavigator.org/



Porch Pirates



2026 Package Theft Report: Statistics & Trends | Security.org

How to Stop Porch Pirates

- Have packages delivered to a secure location, such as an Amazon Locker, Whole Foods Amazon Counter, UPS Access Point.-
- Schedule deliveries when someone is home
- Use visible security cameras and motion-activated lighting as deterrents.-
- The best way to stop package theft is to keep packages out of sight and out of reach.



Find a Whole Foods Market Store Near You

Online Coupon Scams

- According to the FTC, consumers in the United States reported losing $12.5 billion to fraud in 2024 — the highest reported losses the FTC has ever recorded.
- Some do not use coupons, and others are extreme couponers.
- The holiday season is bursting with safe and malicious offers
- Scammers create look-alike brand pages and polished graphics, then post an eye-popping “limited-time” discount with a link.
- The hook is simple: they push you to share, comment, or tag friends so the post spreads through real people’s feeds.

Online Coupon Scams

- Test it directly on the brand's official platform and look for key warning signs of scams
- Look for coupons on Groupon
- https://www.groupon.com/



Mystery Shopper Scam

- Mystery shoppers are real, and they get paid for what they buy or the service. But….
- Would you like to make $50 an hour?
  - Become a Mystery Shopper
- Call this number if you are interested
- You call, and they want money for a list of locations
- Might send you a check for buying products, tell you to deposit it, and wire money back for “taxes,” “fees,” or some other reason.
- Classic scammer move. Wiring money is like sending cash.



Vacation Hotel Scam

- You receive an email from the hotel where you are staying while visiting relatives during the holiday season.
- You used their payment app.
- Oops, they have discovered incorrect transaction information on your credit card.
- Please complete the attached refund form to receive your refund.
- Downloading the form adds malware to your device.



Vacation Hotel Scam

- When you arrive, there is no reservation.



Don’t Share Away from Home Information

- You are going on your dream holiday trip and want to share the information with your friends.
- Travel safety experts warn that sharing your location or confirming you’re away from home on social media can make you vulnerable to theft, scams, or unwanted contact.
- Even a humorous cartoon or meme that includes your travel location, time, or personal details can be exploited by criminals.
- This is especially relevant for seniors, who may be more targeted due to perceived vulnerability.



The BEST Gift to Give this Year!

- You see it advertised everywhere – TV, Social Media, X, Instagram, and more.
- This is the gift everyone wants
- Your grandkids are driving you crazy
- Check it out at the manufacturer's website
- Use CamelCamelCamel.com to check price history
  - Tracks over 20 million products across major retailers and provides comparison charts and watchlist alerts
- Ask your favorite chatbot to check/track prices



The Marketplace Buyer Scams

You list something for sale

- Buyer wants to send a code to verify you are real
- DO NOT send verification codes to strangers.

You find an item at a great price

- On marketplace sites, ensure the seller has a history of completed, positive transactions.
- Seller wants payment through Zelle, Venmo, or Cash App before you pick it up or it is shipped.
- Use protected payment methods and meet safely.

The Marketplace Buyer Scams

- LAPD offers “E-Commerce Exchange Zones” in select police station lobbies and some Ralph’s grocery stores for safe in-person online transactions, but there is no official LAPD-run delivery service for goods.



The Fake Invoice

- You receive a bill or invoice for something you never bought or subscribed to.
- Or, the email appears to come from a trusted source.
- Always look closely at the email's address to ensure it matches the contact information you have .
- Your account is going to be suspended.
- You need to pay immediately.
- Security software – Geek Squad – 365 Renewal – iCloud photo storage – Amazon account – PayPal -- email links
- Might have a link to a landing page of an illegitimate URL



Friend Gift Exchange

- Receive a text or email from a scammer pretending to be a friend, asking you to participate in a gift exchange with friends using gift cards
- Where did the scammer get your friend's information?
- Social media
- Sends a list of friends
  - Asks you to choose one and click on a link to buy the gift card that will sent to the friend
- The results?
  - Scammer now has your account information



Holiday Lunch QR Scam

- Your tech club is getting together for a holiday lunch and is going to a new restaurant.
- There is no parking lot; you can only park at a parking meter.
- Hmm, has a scammer attached a fraudulent sticker to the original QR code sticker?
- Scanning it opens a website controlled by the scammer rather than the official parking service.
- The page copies municipal or parking-app branding and asks for a zone, plate number, parking duration, and payment card.

Holiday Lunch QR Scam

- Your Warning signs include:
- A QR sticker placed over another label
- Peeling edges, mismatched colors, or poor alignment
- A payment domain unrelated to the posted operator
- A page asking for excessive personal information
- A small “verification” charge followed by another request
- No confirmation in the official parking app
- A meter that lists a different payment method or zone



The Prize Scam

- Scammers send calls, texts, or emails, claiming you've won something valuable — like a car, cash, or electronics — often using the name of a well-known sweepstakes company to appear legitimate.
- You are busy with the holiday season and don't remember buying a ticket, etc.
- You need to pay fees, "taxes," or "shipping charges" to claim the prize, click on a link, or call a 900 (pay-per-minute) number.
- Search the company's official website and contact them directly
- It's one of the too good to be true scams.



Check Washing or Mail Theft Scam

- Postal Inspectors recover over $1 BILLION in counterfeit checks & money orders each year.
- Deposit your outgoing mail in blue collection boxes before the last pickup or at your local Post Office™
- Criminals remove mail deposited in U.S. Postal Service collection boxes by using keys stolen from mail carriers or by fishing them out with string and something sticky — like rodent glue traps or a glue-covered bottle.

Check Washing or Mail Theft Scam

- Never leave your mail in your mailbox overnight.
- If you're going to be gone during the holidays, have your mail held at the Post Office or have it picked up by a friend or neighbor.
- Use a blue Gel pen when writing your checks.
  - Gel ink soaks into paper and may be more difficult to remove than ballpoint pen ink, according to authorities.



Recovery Scam

- A recovery scam occurs when criminals contact victims of previous scams, claiming they can help recover lost money, prizes, or investments—but only if the victim pays upfront fees or provides personal information.

How does this happen?

- **Sucker lists**: Databases of previous scam victims sold or traded among criminals.
- **Online monitoring**: Forums, social media, and complaint sites where victims discuss scams
- **Search engine and social media ads**: Targeted ads for “money recovery” services.



Protecting Yourself

Avoid using your debit card. Money taken directly from your bank account.

- Avoid using your debit card. Money is taken directly from your account.
- When you use a credit card for online shopping, the charge typically appears as **pending within seconds to a few minutes**, though it takes 1 to 5 business days to fully post and settle on your account.



Use a virtual credit card number

- Most major credit card companies offer single-use numbers. You use these numbers instead of your actual credit card number, but they still appear normally on your statement.

Protecting Yourself

- Be extra vigilant when reviewing and responding to emails.
- Watch out for too-good-to-be-true offers (on social networks).
- Never agree to reveal your information just to participate in a promotion.
- Don’t accept requests on social media from people you don’t know in real life.
- Wait to post pictures and comments about your holiday travel until you have already returned home.



Protecting Yourself

- If you are asked to copy and paste some code into your web browser to get a prize or special offer, do NOT do it.
  - The code is usually a script that will create all kinds of havoc for you.
- Have a current security program that you keep up to date.,
- Run an anti-malware program like Malwarebytes on a regular basis.



Protecting Yourself

- Download program/apps from reputable websites.
  - Apple App Store – Google Play Store – Microsoft Store
- Stop and smell the roses when downloading apps.
  - Uncheck boxes for other ‘apps’ included with the one you want to download.
  - Use Unchecky.com to uncheck the boxes (BobG)
  - Smartphone apps: Does the app really need access to your contact list?



Protecting Yourself

- Examine the permissions requested by the app.
- Safe apps only ask for permissions necessary for their core functionality.
  - A calculator app should not request access to your camera or contacts.
- Check the update history; apps that are regularly updated are more likely to have patched security vulnerabilities



Protecting Yourself

Use a VPN

- Encrypts your internet connection
- Protects your privacy from ISPs and advertisers
- Helps you stay safe on public Wi-Fi
- Reduces tracking by masking your IP address.

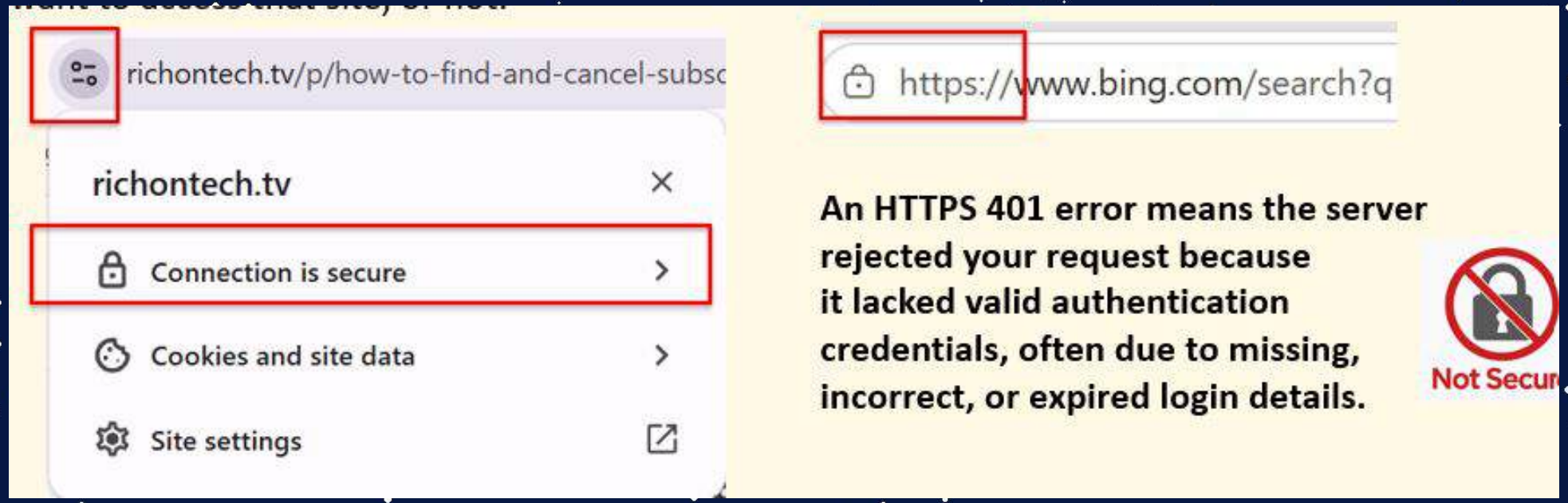


Make Sure the Site is Secure

- Firefox, Safari, and Edge still display a padlock (or similar lock glyph) for secure HTTPS pages.
- Chrome websites: Click on the graphic to the left of the URL (Uniform Resource Locator – website address). See the locked padlock.
- This change was made because nearly all sites now use HTTPS, and the padlock was often mistaken for a trust signal rather than an encryption signal.
- If I go to a website that is not encrypted, I get a pop-up that let's me decide whether I want to access that site, or not.



Make Sure the Site is Secure



SCAMMERS USE



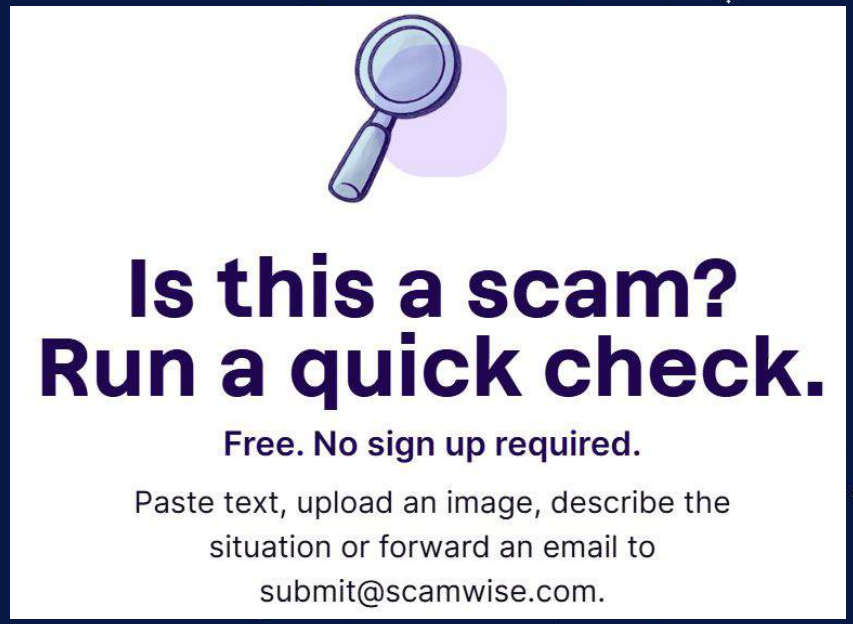
STOP • VERIFY • THEN ACT



Scamwise: A scam verification website

- Check out Rich On Tech's review on LA's Channel 5. Https://www.youtube.com/watch?v=xiqp1oiaPQI&t=75s

- I double-checked and asked my browser: it is a safe, legitimate website.
- The answer was yes: Created by Los Angeles-based cybersecurity firm Savi Security, it is a free, AI-powered tool that analyzes suspicious texts, emails, links, phone numbers, and websites for signs of fraud.



Scamwise: How Does it Work?

- **Free Analysis:** You can paste text, upload screenshots, or forward emails to submit@scamwise.com without creating an account or paying a subscription.
- **AI & Threat Intelligence:** It checks messages against hundreds of scam signals, behavioral patterns, and third-party databases.
- **Clear Guidance:** Instead of just a simple yes-or-no, it provides a verdict, explains why a message looks suspicious, and suggests what steps to take next.

THINGS TO KEEP IN MIND

- **Second Opinion Tool:** While Scamwise is a helpful safety net, no AI tool catches 100% of new or sophisticated scams. Always double-check sensitive transactions through official, independent contact methods.
- **Privacy:** When submitting content, avoid sharing sensitive personal information.

BBB SCAM TRACKER

- **Search and Lookup:** Users can search the database using keywords, phone numbers, email addresses, URLs, or geographic location to see if others have reported similar scams
- **Reporting Scams:** Consumers can submit reports about scams they encounter, whether or not they were victims. Reports are reviewed by BBB staff before being added to the public database, and personal information is never displayed
- **Scam Map:** A live heatmap shows reported scams across the U.S. and Canada, allowing users to see which scams are trending in their area.
- **Tracking Losses:** The platform tracks financial losses associated with scams, helping users understand the scale and impact of different fraud
- **Alerts and Tips:** The tool provides practical advice and warnings to help consumers avoid falling victim to ongoing scams

https://www.bbb.org/scamtracker

BETTER BUSINESS BUREAU