

GUIDE TO PREVENTING Scams

Tens of thousands of people nationwide are victims of a scam every year—in 2024 alone, scams cost Americans \$47 billion.

As the *New York Times* reported,

“People of all ages and socioeconomic levels are potential targets, but older Americans are particularly vulnerable. They’re more likely to have amassed savings, and they’re perceived to be more isolated or perhaps less computer savvy.

“There are also more entry points for scammers now—in our text messages, social media, dating sites or online groups. That silly personality quiz you just whizzed through on Facebook? It might have been created by fraudsters phishing for personal details...”

If you’ve been scammed...

- Do NOT send more money to “undo” the scam
- Do NOT try to fix it alone—get help!
- Do NOT ignore the incident out of embarrassment
- Do NOT blame yourself

I hope you find this guide a helpful starting point in preventing or dealing with the aftermath of a scam.

Sincerely,



Gale A. Brewer
City Council Member

How scams work.

WHEN scammers contact you—by phone, text, email or even in person—it will likely be unsolicited, urgent (often with a deadline), about a problem or a prize that you’ve “won.” Here are typical categories:

Impersonation. Callers pretending to be your bank, a government agency—the IRS, the Social Security Administration, U.S. Immigration and Customs Enforcement, or your healthcare insurer, including Medicare or Medicaid. A text could even come from EZ Pass, saying you owe money—even if you don’t have a car!

Scammers may describe an overdue bill, an issue with back taxes, or threaten a cut in benefits, and then ask you for personal information such as an account number or social security number. Don’t give them anything!

Another kind of impersonation is using AI to sound like a relative or friend. They urgently ask for money—there’s been an accident, or they’ve been jailed, or a vacation has been ruined. They want payment via gift cards, bank transfers, or your credit card number.

Medical Devices. Automated “Robocalls” which offer free or discounted medical alert devices ask you to “press 1” to receive the device or discount. (These calls sometimes offer the option of “press 2” to opt out of future calls, which then alerts the scammers to a working phone number, to be used for future scam calls!) The caller is then connected to a live operator who uses conversational scare tactics to elicit personal and financial information. There is no free lunch (or device!).

Lottery or Sweepstakes. Calls, texts, or emails about a “prize” that you’ve won, but which require payment of “taxes and processing fees.” The scammers promise that the prize will be delivered soon, but no prize ever comes.

Charity. A fraudster claiming to represent a

nonprofit organization, sports team, or law enforcement charity to solicit donations—often via Paypal, Venmo, or Zelle—and offer to input info on your phone (while quietly sending money to themselves without your consent).

Computer Technical Support. Scammers can pose as tech support professionals from well-known companies like Microsoft or Apple and ask for remote access to your computer. If you give them access, they can then install malware or keystroke capture software on your computer to steal your account and password information.

Investment. A scammer will allege that their “financial service” will offer low risk and great returns. Cryptocurrency is often involved.

Social Media. If you receive an odd Facebook or Instagram message from a friend or relative, they were likely hacked. Don’t click any links sent from odd messages or anyone you suspect of being hacked. Phone your friend to confirm they sent it.

Gift Cards. Scammers pretend to be a government official, a relative in distress or a colleague at work and direct you to buy gift cards and give them the PIN numbers. Government agencies do not call!

Internet/Email Fraud. Unsolicited pop-up windows on your computer claiming to be anti-virus software actually install computer viruses when you click on them.

What to do if you suspect a phone or text scam:

- Do not give out personal or financial information (even if they already have some, often easily found online).
- Hang up on suspicious or unsolicited calls.
- Do not click on links from unknown or suspicious texts or emails.
- Do not pick up the phone from unfamiliar numbers. You can always call back later after listening to their voicemail.
- Do not let others use your phone
- Check in with friends or family members to see what they think.

How to respond if you do talk to scammers:

- “I don’t make financial decisions without consulting someone I trust.”
- “I’ll check with my family and get back to you”
- “I don’t give personal information over the phone. Goodbye.”

Follow the three S’s to prevent being victimized:

SLOW DOWN: Scammers press for immediate action. Instead, pause and think through if what you’re being told is plausible. You can always respond at a later time through official contact channels. Do not hesitate to call someone you trust and ask them what they think.

SUSPECT: Be suspicious of anyone asking for personal information (Social Security number, phone number, date of birth).

SECURE: If applicable, freeze credit card, change passwords, call institution scammer is referring to and warn them of potential account usage by scammer.

Other Prevention Tips:

- Enable two-factor authentication for accounts
- Freeze your credit if concerned
- Use strong, unique passwords
- Change passwords and PINs often
- Monitor bank and credit statements
- Shred all bills, credit card receipts, credit applications, insurance forms, bank statements, expired charge cards, and pre-approved credit offers before throwing them into the garbage (or go paperless if you’re handy with your computer).

Credit freezes and fraud alerts: If you’re a victim...

- Place a free credit freeze and/or a fraud alert on your credit report. The FTC recommends contacting each of the credit bureaus:
 - Equifax (800) 685-1111
 - Experian (888) 397-3742
 - TransUnion (888) 909-8872
- Report to your bank or credit card company and close the compromised account
- File a police report
 - Precinct 20: 212-580-6411
 - Precinct 24: 212-678-1811
- Report the incident to the FTC (877)-382-4357 or identitytheft.gov
- Keep records (and notes) of your calls!

Additional resources:

- To help remove your name from scammers’ call lists, contact the National Do Not Call Registry: donotcall.gov or 1-888-382-1222.
- If you suspect tax-related identity theft, contact the IRS at 1-800-829-1040.
- AARP Fraud Watch Helpline: 877-908-3360.
- Report to the Social Security Administration at oig.ssa.gov/report or call 1-800-269-0271
- For guidance and referrals, visit the US Dept. of Justice Elder Initiatives: www.justice.gov/elderjustice or email elder.justice@usdoj.gov.
- To report fraud against anyone age 60 or older and get next steps from a case manager, contact the National Elder Fraud Hotline at 1-833-372-8311 (10am-6pm Monday-Friday). ovc.ojp.gov/program/elder-fraud-abuse/national-elder-fraud-hotline
- To help report Medicare fraud to the right authorities and get assistance in securing your Medicare account call the Medicare Rights Center at 800-333-4114 or visit www.medicarerights.org
- To report a financial crime and access victim resources, contact Manhattan District Attorney Alvin Bragg’s Office of Financial Crimes Helpline at 212-335-8900; manhattanda.org/victim-resources/financial-crimes
- To report a mortgage relief scam and guidance on next steps, contact the Mortgage Relief Scam (Center for NYC Neighborhoods): 212-639-9675 or visit on.nyc.gov/4kJ9wnO.
- For professional referrals and the latest articles: Weinberg Center for Elder Justice at theweinbergcenter.org/elder-justice
- To report scams and receive guidance and support, contact the NYS Division of Consumer Protection at 1-800-697-1220 or visit dos.ny.gov/consumerprotection
- Consumer Financial Protection Bureau (CFPB): consumerfinance.gov or 1-855-411-2372.



STAY UP TO DATE: **Sign up for my E-News & follow me on social media!**

These print newsletters are only sent twice a year; please join 17,000 New Yorkers in subscribing to my weekly email newsletter! Sign up online at bit.ly/BrewerSubscribe @GaleABrewer

BOOKMARKS *(links are case sensitive!)*

Go Delete Yourself From the Internet. Seriously, Here’s How.

Wall St. Journal gift link: on.wsj.com/45DmXBU

Delete Yourself, Part 2: Your Personal Data on the Dark Web.

Wall St. Journal gift link: on.wsj.com/3T5MQCx

Your iPhone is a target for thieves. Do this to help protect your data.

Washington Post gift link: wapo.st/454OKL6

Google’s free tool to find and remove your personal information.

myactivity.google.com/results-about-you

10 Tips to protect seniors from being scammed.

Hebrew SeniorLife short link: bit.ly/43p8rvQ

The new scams to watch out for.

Consumer Reports short link: bit.ly/CR-NewScams

Share what you know—pass it on to stop scams.

Federal Trade Commission: consumer.ftc.gov/features/pass-it-on

AI voice-cloning scams: a persistent threat with no guardrails.

Axios: axios.com/2025/03/15/ai-voice-cloning-consumer-scams

AI is perfecting scam emails, making phishing hard to catch.

Axios: axios.com/2025/05/27/chatgpt-phishing-emails-scam-fraud

How to Avoid Online Scams and What to Do if You Become a Victim.

New York Times: www.nytimes.com/2024/08/10/business/online-scams-advice.html