Everything you need to protect the people you love from fraud

zapscam.com

TABLE OF CONTENTS

This kit is provided free by zapscam.com. Share it with anyone who needs it.

THE TOP 15 SCAMS TARGETING YOUR FAMILY

Each entry below explains how the scam works, the biggest red flag to watch for, and what you should do if you encounter it.

■ AI Voice Cloning Scams

How it works: Scammers gather audio samples from publicly available sources such as YouTube videos or social media. They use AI software to analyze and replicate the voice of a targeted individual, creating convincing fake messages. The scammer contacts the victim using a spoofed phone number or via email, playing the cloned message.

The #1 red flag: The caller is requesting immediate action without giving time for verification.

What to do:

• Verify the identity of the caller using an alternate means of communication, such as calling back a known number.

• Discuss potential scams with family members and establish a code word or phrase to confirm authenticity in calls.

■ Charity Scams

How it works: The scammer identifies a charitable cause that resonates with potential donors, such as disaster relief efforts or support for underprivileged children. They contact the victim through phone calls, emails, text messages, or social media posing as a representative from a well-known charity. Using emotional appeals and urgent requests, they convince the victim to donate immediately by providing credit card information or sending money via wire transfer services like Western Union.

The #1 red flag: Requests for immediate payment or donations without providing detailed information about how the funds will be used.

What to do:

• Verify the legitimacy of any charity by checking its registration status with your state's attorney general's office or using websites like Charity Navigator.

• Do not give out personal information over the phone, especially financial details.

Gift Card Scams

How it works: The scammer contacts the victim through a phone call, text message, email, or social media platform, claiming to be from an official entity such as the IRS, FBI, or a power company. The scammer creates a sense of urgency by threatening arrest, utility disconnection, or other dire consequences unless immediate action is taken. They instruct the victim to purchase specific gift cards (like Walmart, Target, or iTunes) and provide the card numbers over the phone.

The #1 red flag: A caller requests immediate payment using a gift card or demands you purchase specific types of gift cards.

What to do:

• Hang up immediately if someone demands a gift card payment and report the incident to the FTC at IdentityTheft.gov/report-identity-theft.

• Do not engage with texts, calls, or emails that threaten legal action unless you can independently verify their legitimacy through official channels.

Government Grant Scams

How it works: Scammers contact the victim by phone or email, claiming to represent a government agency offering grants. They create urgency by saying that funds are limited and will run out quickly unless immediate action is taken. The scammer asks for personal information such as Social Security numbers or banking details under the guise of processing the grant.

The #1 red flag: Requests for money upfront to process a grant

What to do:

• Contact the local office of the government agency mentioned to verify the claim

• Report any suspicious activity to the FTC at IdentityTheft.gov

---

Grandparent Scams

How it works: Scammers call the grandparent using a spoofed phone number to appear as if it's coming from their grandchild's location or device. The scammer claims they are in distress and need immediate funds for an urgent situation, such as paying bail or medical bills. They urge the grandparent not to inform anyone else about the emergency to avoid embarrassment or further complications.

The #1 red flag: The caller is asking for immediate financial help without providing specific details or proof.

What to do:

• Verify the identity of the caller by asking specific questions that only your grandchild would know.

• Hang up and contact the alleged 'grandchild' or their parents directly through known phone numbers or social media to confirm the situation.

■ Investment & Crypto Scams

How it works: Scammers identify potential targets through social media or cold calls, often posing as legitimate investment advisors or representatives from reputable firms. They offer attractive investment opportunities with guaranteed high returns to lure the victim into making a deposit. Once funds are transferred, scammers may request additional investments or simply disappear without providing any returns or access to the initial investment.

The #1 red flag: Unsolicited offers promising high returns

What to do:

• Educate yourself and your loved ones about common scam tactics
• Always verify the legitimacy of any investment offer by contacting a trusted financial advisor or checking with official organizations like the SEC or FINRA

■ IRS & SSA Impersonation

How it works: The scammer contacts the victim through phone calls, emails, or even in-person visits. The caller claims to be from the IRS or SSA and states that there is a problem with the recipient's account or tax return. Scammers may threaten legal action or arrest if the individual does not comply with their demands immediately.

The #1 red flag: Unsolicited contact demanding immediate payment of taxes or fees.

What to do:

• Hang up and do not provide any personal information.
• Call back using the official number from the IRS (1-800-829-1040) or SSA (1-800-772-1213) to verify if there is a real issue.

■ Medicare Scams

How it works: The scammer contacts the victim via phone call or email pretending to be a Medicare representative. They offer free health services or medical equipment under false pretenses, requiring personal information such as Social Security numbers. Victims provide their details, believing they are securing important benefits.

The #1 red flag: Unsolicited calls or emails from individuals claiming to be Medicare officials

What to do:

• Verify any claims by calling your local Medicare office directly using a known, official number
• Never provide personal or financial information over the phone unless you initiated the call to an official entity

---

■ Phishing & Smishing

How it works: Scammers send an email or text message appearing to be from a legitimate source. The message contains urgent language, threatening consequences if the recipient doesn't act immediately. A link is provided that leads to a fake website designed to capture personal information.

The #1 red flag: Urgent or threatening language in messages

What to do:

• Never click on links from unknown senders.
• Contact the supposed sender directly using a known phone number or website, not one provided in the message.

Prize & Lottery Scams

How it works: Scammers contact victims through phone calls or emails claiming they've won a lottery or prize draw. The scammers request personal information such as social security numbers, bank account details, or identification documents to verify the winner's identity. They demand an upfront fee for taxes, processing charges, shipping costs, or insurance on the winnings before releasing the prize or money.

The #1 red flag: Unsolicited contact claiming you've won something.

What to do:

- Contact a local consumer protection agency if you suspect a scam.
- Notify your financial institution to monitor for any fraudulent activity on accounts.

QR Code Scams

How it works: Scammers create a QR code linked to a fraudulent website. They distribute this QR code through emails, social media posts, flyers, or even physical signs placed strategically. The unsuspecting victim scans the QR code with their smartphone.

The #1 red flag: The email or message looks suspiciously urgent and demands immediate action.

What to do:

- Verify the source of any QR code before scanning it by checking with known contacts or organizations.
- Use a reliable QR code scanner app that warns about potential scams.

Romance Scams

How it works: The scammer creates a fake online profile using stolen or fabricated personal information. They engage in long-term communication to build trust and establish an emotional connection with the victim. Once trust is established, the scammer begins making excuses for why they need money, often citing emergencies or urgent travel needs.

The #1 red flag: The person avoids video calls or face-to-face meetings.

What to do:

- Discuss online safety with aging parents and educate them on common scam tactics.
- Encourage reporting any suspicious activities or attempts at fraud to the FTC, FBI IC3, or BBB.

SIM Swapping

How it works: Scammers gather personal information about their target through various means like social media or data breaches. They contact the victim's mobile carrier and pose as the legitimate account holder to request a SIM card replacement. Once the scammers have control of the new SIM, they receive all calls, texts, and two-factor authentication codes meant for the original owner.

The #1 red flag: Unexpected notifications about a password reset or other security changes in your accounts.

What to do:

- Contact your mobile carrier immediately if you suspect SIM swapping and request to lock your account.
- Enable two-factor authentication (2FA) on all accounts but use an authenticator app instead of text-based 2FA whenever possible.

Tech Support Scams

How it works: Scammers contact the victim through a pop-up ad or unsolicited phone call, claiming there's an urgent problem with their computer. They ask for remote access to the victim's device and may install software that allows them full control over the system. The scammer then identifies non-existent problems, such as malware or system errors, which need immediate repair.

The #1 red flag: Unexpected contact from tech support via phone or pop-up ads

What to do:

- Hang up and independently verify the company's contact information if contacted by phone.
- Never grant remote access to your device from unknown sources.

Virtual Kidnapping

How it works: Scammers contact the victim using a spoofed phone number or social media account pretending to be their loved one. The scammer claims they have been kidnapped and need money for ransom, threatening violence if demands are not met. The victim is instructed to keep the situation secret from authorities and loved ones, often speaking in code over phone calls or text messages.

The #1 red flag: Contact from a loved one through uncharacteristic methods or sudden urgency.

What to do:

- Contact local police and inform them of potential virtual kidnapping attempts immediately.
- Verify the safety and whereabouts of loved ones through direct communication methods if possible.

THE FAMILY CODE WORD SYSTEM

What it is

A secret word or phrase your family agrees on ahead of time to verify identity during phone calls. If someone calls claiming to be a family member and asks for money or personal information, you ask for the code word before doing anything.

Why it works

Modern scammers can fake voices with AI, spoof caller ID, and even create deepfake video. But they cannot know a word your family chose in private. A code word is the simplest, most reliable defense against impersonation scams.

How to set it up

1. Pick a word that is easy to remember but impossible for an outsider to guess. Do NOT use a pet's name, birthday, anniversary, or anything on social media.
2. Share the code word ONLY in person — never over text, email, or phone.
3. Establish the rule: if someone calls claiming to be family and asks for money or urgent help, you ask for the code word before doing anything.
4. If the caller doesn't know the word or makes excuses, hang up immediately and call the real family member directly on a number you already have.

Our family code word: _____

Date set: _____

Family members who know it: _____

PHONE & EMAIL SAFETY CHECKLIST

Print this page and put it on the refrigerator. Review it with your family.

- ☐ I verify unexpected calls by hanging up and calling back on a known number.
- ☐ I never give out personal information to incoming callers.
- ☐ I don't click links in text messages from unknown numbers.
- ☐ I have a family code word set up.
- ☐ I check my bank and credit card statements monthly for unauthorized charges.
- ☐ I use different passwords for different accounts.
- ☐ I have two-factor authentication enabled on my email.
- ☐ I know that no government agency will ever ask for gift card payment.
- ☐ I know to call 1-800-829-1040 to verify any IRS communication.
- ☐ I shred documents with personal information before discarding them.
- ☐ I do not share verification codes sent to my phone with anyone.
- ☐ I verify charity requests at give.org before donating.
- ☐ I never allow remote access to my computer from an unsolicited caller.
- ☐ I keep my phone's operating system and apps updated.
- ☐ I review my credit report at least once a year at annualcreditreport.com.

WHAT TO DO IF YOU'VE BEEN SCAMMED

If you or someone you love has fallen victim to a scam, follow these steps as quickly as possible. Speed matters — the sooner you act, the better your chances of limiting the damage.

First 24 Hours

- Call your bank or credit card company immediately. Tell them you were the victim of fraud and ask them to freeze your accounts and reverse any pending transactions.
- Change your email password first — email is the master key to all your other accounts. Then change passwords on banking, social media, and other important accounts.
- If you paid with gift cards, contact the gift card company immediately with your receipt. Some funds may still be recoverable.

File Reports

- Federal Trade Commission (FTC): ReportFraud.ftc.gov
- FBI Internet Crime Complaint Center: ic3.gov
- Your local police department — get a report number for your records

Freeze Your Credit

Contact all three credit bureaus and place a credit freeze. This is free and prevents anyone from opening new accounts in your name.

- Equifax: 1-800-685-1111 | equifax.com/personal/credit-report-services
- Experian: 1-888-397-3742 | experian.com/freeze
- TransUnion: 1-888-909-8872 | transunion.com/credit-freeze

Monitor Your Accounts

- Check bank and credit card statements weekly for the next three months.
- Review your credit reports at annualcreditreport.com.
- Set up fraud alerts with the three credit bureaus.

It's not your fault.

Scammers are professionals. They study human psychology and run these schemes full-time against thousands of people. Being scammed does not mean you are careless or foolish — it means someone with training and experience targeted you. What matters now is taking action,

protecting yourself going forward, and knowing that you are not alone. If you need to talk to someone, the AARP Fraud Watch helpline is available at 877-908-3360.

HOW TO TALK TO YOUR PARENTS ABOUT SCAMS

Talking to your parents about scams can feel uncomfortable. Nobody wants to sound like they're lecturing a parent. Here's how to start the conversation without making anyone defensive.

✖ The Wrong Way

> "Mom, you need to be more careful online. You're going to get scammed."
> "Dad, please stop clicking on things. You don't know what you're doing."

This approach sounds condescending, even if you don't mean it that way. It puts them on the defensive and makes them less likely to come to you when something suspicious happens.

✔ The Right Way

Frame it as asking for their help, sharing something interesting, or admitting your own vulnerability. Try one of these:

> "Hey Mom, I was reading about this new scam that's targeting people in our area. Can I tell you about it?"
>
> "Dad, I almost fell for this scam email the other day. Want me to show you what it looked like?"
>
> "I've been reading about phone scams — can we set up a code word so we always know it's really us calling?"
>
> "I saw on the news that scammers are using AI to clone voices now. It's wild. Have you heard about that?"

Tips for the conversation

- Make it about protecting the whole family, not about them being vulnerable. "We should all be doing this" is better than "You need to do this."
- Share your own close calls. Everyone has almost clicked a bad link or answered a suspicious call. Admitting that makes it a conversation between equals.
- Ask questions instead of lecturing. "Have you ever gotten a weird call like that?" opens a dialogue. "You should never answer unknown numbers" shuts it down.
- Bring it up naturally. A news story, a scam text you received, or this kit are all good conversation starters.
- Make it easy to ask for help. The goal is for them to call you when something feels off — not to handle everything alone.

zapscam.com

Free forever. One email per week.
Join families across the country who are fighting back against fraud.