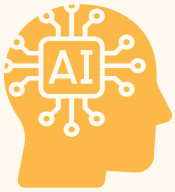
# How scammers are stealing people's money

**To steal people's money, scammers utilize technology that allows them to reach thousands of people easily and cheaply, as well as payment methods and currency that help them access money quickly and leave no trace.**

## SPOTLIGHT ON TECHNOLOGY: ARTIFICIAL INTELLIGENCE




Artificial Intelligence (AI) is a technology that allows machines to mimic certain human-like behavior, such as speech or writing. For example, new chatbots and language processing tools can answer detailed questions, write compelling essays, and develop computer code. While this technology can be used for good, these powerful tools can also be exploited by bad actors to make scams more sophisticated and convincing. This section describes AI technology, how it can be used in fraud and in scams, and what warning signs to look out for.

### How is AI used?

**Chatbots:** A chatbot is a computer program that may use AI to simulate human conversation and could be used maliciously to obtain, store, or manipulate your personal data.

**Voice Cloning Technology:** Voice cloning uses AI to create voice models that sound like the real voice of someone you may know.

**Deepfakes:** A deepfake is an AI-generated video or image that is made to look authentic.

## AI ACCELERATES THE EFFECTIVENESS OF PRE-EXISTING SCAMS

Here are the main AI-based scams to watch out for:

**AI-Powered Phishing Attacks:** Phishing attacks, where fraudsters deceive individuals into revealing sensitive information, have become increasingly sophisticated with the use of AI. Using AI, scammers can quickly personalize phishing emails, imitate sophisticated dialogue, and bypass traditional spam filters, making it harder for individuals to distinguish between genuine and fraudulent communications.

**Family Emergency Scams:** In family emergency scams, scammers convince targets that their family member is in distress to obtain cash or private information. Scammers can utilize voice cloning and deepfakes to impersonate a loved one who claims they are in danger and needs money immediately.

**Romance Scams:** Fraudsters employ AI to create and operate fake profiles on dating websites and social media platforms. AI-powered chatbots then simulate realistic conversation to build trust, with the goal of tricking the target into sending them money.

It may be difficult to know if someone is using AI-technology in a scam. **One thing is certain: AI makes traditional frauds and scams more convincing and easier to deploy on a larger scale.**

### Tips to protect yourself:

Do not share sensitive information via phone, email, text, or social media.

Do not transfer or send money to unknown locations.

Consider designating a “safe word” for your family that is only shared with family members and close contacts.

Do not provide any personal or sensitive information to an online chatbot.

Report potential scams to the authorities and the companies involved.

## SPOTLIGHT ON PAYMENT METHODS: CRYPTOCURRENCY, PEER-TO-PEER (P2P) PAYMENTS & GIFT CARDS

**Cryptocurrency:** Cryptocurrency is a type of digital currency that only exists electronically. Cryptocurrency transactions may not be mediated by a trusted third party, are pseudonymous, and are difficult to track, which can make this payment method a useful mechanism for fraudsters. It is also preferred by scammers because they get the money instantly, and the payments are typically not reversible.

Cryptocurrency payments can be used in a variety of schemes including fake investment scams and false friendship or romance scams. These scams may also be used together: cryptocurrency investment scams can begin with scammers initially hooking victims through a false romance, and then progress to requests for money for an alleged investment.

A common technique scammers use is to build a relationship with their victims over time, earning their trust and then convincing them to invest in a fraudulent scheme, which results in significant financial losses; this is referred to as a "confidence investment scam," which is discussed further in this book. Once the scammer has gained the trust of the victim, scammers pressure victims to "invest" in a specific cryptocurrency platform by promising high returns and using sophisticated tactics to create a

sense of legitimacy. In reality, the platform is fake and controlled by the scammers, who disappear with the "invested" funds once they have accumulated enough money from unsuspecting investors.

The Federal Bureau of Investigation (FBI) found that adults ages 60 and older lost nearly $1.7 billion to scams involving cryptocurrency in 2023, a reported increase of nearly 52 percent from 2022.[8] The FBI also found that the largest losses among older adults involving cryptocurrency were crypto-related investment scams with over $716 million in reported losses.[9]

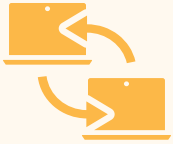
**Tips to protect yourself:**

- Ignore advice and offers to help you invest in cryptocurrency – it is most likely a scam.
- If you meet someone on a dating site or app, and they want you to send them cryptocurrency or show you how to invest in crypto, it is almost certainly a scam.
- Ignore return on investment (ROI) claims that seem too good to be true.
- Do not engage with "investment managers" who reach out to you and make promises on ROI.
- A celebrity will not contact people directly to sell cryptocurrency. Do not respond to any messages purporting to be from a celebrity.
- Do not accept "free" cryptocurrency from strangers.

- If you have been a victim of a cryptocurrency scam, be wary of anyone claiming they can recover your funds, as this could be another scam. Scammers often target the same person more than once because they perceive them as vulnerable, trusting, and potentially less likely to report the fraud or seek legal recourse after the initial victimization.
- **Be aware**: No legitimate business will demand that you pay in cryptocurrency. This is always a scam.

To learn more about cryptocurrency and how to protect yourself from crypto-related scams, the FTC has helpful information at **consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.**

The FBI has also released guidance for cryptocurrency scam victims, which can be found here: **www.ic3.gov/Media/Y2023/PSA230824**.



**Peer-to-Peer (P2P) Payments:** P2P payments are transactions between two parties with separate bank accounts, mediated through a third-party website or mobile app. These platforms can be abused by scammers because, like cryptocurrency, scammers receive the money instantly after a transfer is initiated. While many P2P payment companies employ advanced systems to flag and freeze suspicious transactions, these platforms are often unable to reverse a transaction once money is sent. These apps may also lack the same protections against fraud that traditional banks and credit cards now employ.

In 2023, the FTC received more than 65,300 reports from consumers who sent money to fraudsters via P2P payment apps, like CashApp, Venmo, or Zelle, with reported losses totaling nearly $210 million.[10] These reports represent an increase of 5 percent since the year prior, but reported losses are 28 percent higher than those reported in 2022.[11]

### Tips to protect yourself:

- Never send payments to someone you don't know. Take your time to be sure that you are sending money to the right person.
- Set up fraud alerts in your P2P payment app, or with the bank or credit card account that you linked to the app. Fraud alerts can let you know if personal information is changed or when transactions are made.

- P2P payment apps have social media elements, like lists of friends. Avoid sharing information like your address, phone number, and other personal details. As on social media, ignore friend requests from people you do not know.
- Any business that exclusively takes P2P payment apps or pre-paid debit card payments should be avoided.
- Like any other financial website, protect your account with a strong password. Use two-factor authentication.

**Gift Cards:** Gift cards continue to be primary methods used by scammers to request and steal money from older adults who reported scams to the Committee's Fraud Hotline. When the victim sends the scammer the gift card number, the scammer immediately uses the balance, making it impossible to get the money back.

In 2023, the FTC received more than 41,600 reports of gift card scams, resulting in nearly $217 million in reported losses.[12]

### Tips to protect yourself:

- If you paid a scammer with a gift card, tell the company that issued the card right away.
- If you buy gift cards to give away or donate to family and friends, buy the gift cards from stores you know and trust. Check the protective stickers on the card to ensure that they do not appear to have been tampered with.
- Always keep your receipt and a copy of the gift card. The number on the gift card and the store receipt will help you file a report if you lose the gift card or need to report a scam.
- Beware of the signs of scams, like requests to buy gift cards at several stores or to purchase a specific type of gift card.

- **Be aware**: No business or government agency will ever tell you to buy a gift card to pay them. This is always a scam.

For more information on gift card scams and how to protect yourself, visit the FTC at **consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams**.

# Scams to Watch Out For

In 2023, the Committee's Fraud Hotline received 536 new complaints from individuals across the country. These complaints bring the total number of complaints registered with the Fraud Hotline since 2013 to nearly 12,300.

Many of these frauds are also reported to the FTC. Through report collection, investigations, and other administrative actions, the FTC's Bureau of Consumer Protection stops unfair, deceptive, and fraudulent practices employed by both companies and individual scammers.

Reported frauds account for nearly 2.6 million of the 5.4 million complaints reported to the FTC in 2023.[13] Common fraud categories include imposter scams, online shopping and negative reviews, prizes and lottery scams, and investment-related fraud. Other less common, but still prevalent, scams include debt collection scams, mortgage scams, and home repair scams.[14]

## IMPOSTER SCAMS

Imposter scams are the most pervasive of all scams reported to the FTC, with over 850,000 reports in 2023.[15] These scams can appear in many different forms as scammers find new ways to target victims. The next five sections will discuss some of the most prevalent imposter scams commonly used to target older adults.

SCAM SURVIVOR

### Gary Schildhorn

**Person-in-Need Scam Survivor**

PHILADELPHIA, PENNSYLVANIA

"In February of 2020, I was driving to my office when my phone rang. It was my son, Brett. He was upset and crying. He told me he needed my help. He said [he] was in a car accident, and he was arrested. He said [he] may have a broken nose and his arm was hurt. The car he hit was purportedly driven by a pregnant woman who was injured. He reported that he was assigned a public defender named Barry Goldstein…I told him I would call Goldstein and call him right back. He said, "you can't, they took my phone, get me out, please."

I am a father and a lawyer. My son was hurt, he was in trouble and a pregnant woman was injured. This call instigated and required immediate action by me. I first

attempted to look up Mr. Goldstein. Before the search results came back, my phone rang. It was Mr. Goldstein. He told me he met with my son. He said Brett was hurt but was going to be okay.

He said the Judge had ordered a high bail of $150,000 and that I would need 10 percent of that amount in cash to bail him out... He asked if I was in a position to help my son. I assured him I was. He then… told me to call the court and arrange for bail... I called the number he provided. They answered, "Montgomery County Court House" …[and] confirmed they were holding my son… [They] also reported that…the judge …had lowered bail to $90,000.

[The Montgomery County Court House] then told me that in order to bail [my son] out I would have to use the county bail bondsman, but that there was a problem. The only bondsman available had a family emergency and was not in town…[They] suggested that I call Mr. Goldstein back because he would be able to assist. I placed the call.

Mr. Goldstein agreed to post a bond and informed me I would need to wire him $9,000. He stated he was a member of a credit union, and I would have to go to certain kiosks to wire the money. I later learned that these were bitcoin [a type of cryptocurrency] kiosks. He then told me that he was attending an out-of-town conference and would be leaving for the airport in two hours. I needed to hurry.

This series of calls all occurred within a few minutes. It was not until the calls stopped and I was driving to the bank that I had an opportunity to think. I called my daughter-in-law, Kim, told her what happened and asked her to alert my son's office that he had been in an accident.

A few minutes later, I received a Facetime call. It was Brett. "Dad, Kim called work and they put me on the phone." "You are being scammed; see, I'm fine." Shock, relief, and anger—one emotion followed the other. I said to Brett that there was no doubt in my mind that it was his voice on the phone—it was the exact cadence with which he speaks.… **How did they get my son's voice? The only conclusion I can come up with is that they used artificial intelligence, or AI, to clone his voice.**

*Excerpts taken from Mr. Schildhorn's testimony provided to the Aging Committee in November 2023.*


# Person-In-Need & Grandparent Scams

As Gary testified in November 2023, bad actors may impersonate family members or friends in "person-in-need" or "grandparent" scams. Imposters may pretend to be a grandchild or a law enforcement officer who has detained the target's grandchild. They may also use AI to clone the voice of someone the individual knows to claim they are in trouble and need money to help with an emergency, like getting out of jail, paying a hospital bill, or leaving a foreign country. Scammers play on emotions and trick concerned family members into sending them money. Similar schemes can use the voices of nieces, nephews, children, or others. Between January and September 2023, the FBI's Internet Crime Complaint Center (IC3) received more than 195 reports regarding grandparent scams, resulting in at least $1.9 million in reported losses.[16]

## RED FLAGS

These are common signs that you may be facing these types of scams:

- The person on the line asks you to send money immediately and shares specific details on how to

do so. They may suggest you send the money via gift card, wire transfer, or cryptocurrency.

- The "grandchild" or "law enforcement officer" on the line asks you to keep the incident a secret, despite the supposed urgency of the situation.
- The caller rushes you and asks you to make immediate decisions with little to no information.
- The caller reports to be in a situation or place that does not align with the typical behavior of the person they claim to be.

## STEPS TO PREVENT AND RESPOND

- Hang up and call the number of your family member or a friend that you know to be genuine to ensure they are safe.
- If the person claims to be a law enforcement officer, hang up and call the relevant law enforcement agency to verify the person's identity and any information shared. **Be aware:** law enforcement will never contact a family member to collect bail money on behalf of someone else.
- Verify the story with trusted family and friends, even if you have been told to keep it a secret.
- Check your social media privacy settings and limit what information you share online. Criminals may try to use personal details to better target their scam and make it all the more convincing.

- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.
- **Helpful Tip:** If you sent money to a scammer through a wire transfer, report it to the FBI's IC3 within 72 hours of the transfer at **ic3.gov**. They may be able to help recoup some of your lost funds.

## MORE INFORMATION

- To handle these calls, the FTC has helpful tips at **www.consumer.ftc.gov/articles/0204-family-emergency-scams**.
- The FCC provides more information on how to avoid these scams at **www.fcc.gov/grandparent-scams-get-more-sophisticated**.
- The FBI released a public service announcement about these scams, which can be viewed at **www.ic3.gov/Media/Y2023/PSA231117**.
- To learn more about how AI is used in these types of scams, the FTC has helpful information at **consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes**.

# Financial Services Impersonation & Fraud

Scammers may impersonate financial services firms, such as banks, debt collectors, or mortgage servicers. For instance, scammers may pretend to be debt collectors and attempt to trick their targets into paying debts that do not exist. They may harass or threaten their intended victims with penalties or jail time if they refuse to pay. Mortgage relief scams involve promises related to refinancing and lies about the terms of a loan. According to the FTC, in 2023, there were over 124,400 reported cases of debt collection fraud and nearly 26,200 reported cases of mortgage fraud.[17] In 2022, fake bank fraud warnings were the most reported text message scam,[18] with a median reported loss of $3,000.[19]

### Reports from the Fraud Hotline

A woman from Florida reported that she received a call from a scammer who was impersonating her bank. The scammer had spoofed the victim's Caller ID so it looked as if Bank of America was contacting her. The victim was then instructed by the scammer to send $950 through Zelle and CashApp.

## BEWARE: PHISHING SCAMS

Phishing scams deceive people into giving away sensitive information by pretending to be legitimate organizations or businesses. Scammers use fake emails, text messages, or websites that mimic real ones, urging quick action through links or attachments. The data stolen through phishing is often used for identity theft or financial fraud. To protect yourself, verify the authenticity of unexpected messages, avoid suspicious links, and use strong and unique passwords.

## RED FLAGS

These are common signs that you may be facing these types of scams:

### Bank Impersonation Fraud

- You receive a text message, phone call, or email indicating that your account information has been compromised. They may ask for personal information like usernames, passwords, PINs, and Social Security Numbers to "secure" your account. They may also ask you to transfer funds using a P2P payment app, like Cash App, PayPal, Venmo, or Zelle.
- Banks will never contact you and ask you to share sensitive personal information over the phone, via text message, or email. They will never ask you to transfer money to anyone, including yourself, or ask you to provide personal information to obtain a refund or issue a correction.

### Debt Collection Fraud

- The person calling you says you will go to jail if you don't pay the debt they are describing. It is illegal for debt collectors to threaten to have someone arrested for not paying their debts.
- The person calling will not tell you to whom you owe money. Legitimate debt collectors will always tell you who the creditor is, even if you don't ask them.
- Legitimate debt collectors provide ample time to pay off your debt and will work with you. Scammers will pressure you to pay while they have you on the phone.

### Mortgage Relief Fraud

- The person calling and presenting the opportunity for a mortgage has not been referred to you by trusted friends and family.
- You are pressured into signing documents without the chance to consult an attorney.
- There are blank sections in the documents you are asked to sign. These blank sections can be filled out by the scammer after you've signed.
- You are pressured to pay up front before you get any services.

## STEPS TO PREVENT AND RESPOND

### Bank Impersonation Fraud

- Do not trust Caller ID. Scammers can "spoof" your Caller ID or falsify the information transmitted to your Caller ID so it hides their identity or allows them to impersonate a person or business.
- Do not click on unexpected links or respond to unexpected texts.
- If you receive a suspicious call, text, or email, hang up the call and don't respond to the text message or email. Call your bank or financial institution directly using verified contact information, such as the phone number on the bank's website or on the back of your bank card.

### Debt Fraud

- Ask for a written debt validation letter. Debt collectors are obligated by law to send you detailed information about the debt you owe. Scammers will object to this request.
- Ask the person calling you for the collector's name and the name of the debt collecting agency they work for. If they say they are with law enforcement or an attorney, ask for their badge number, agency, or law firm. Scammers may object to or have trouble responding to these requests.

### Mortgage Fraud

- Before signing any documents, consult with an attorney to be sure it is a legitimate mortgage. If the person attempting to get you to sign aggressively objects to you consulting an attorney, they may be a scammer.
- Be sure to carefully read any documents before signing. If you have questions, ask the person attempting to get you to sign. If they brush aside your concerns, they may be a scammer.

Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

## MORE INFORMATION

- The American Bankers Association has more information about bank impersonation scams at **www.banksneveraskthat.com**.
- The FTC provides more information about loans and debt-related scams at **consumer.ftc.gov/credit-loans-debt**.
- The Office of the Comptroller of the Currency (OCC) has more information about scams at **www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html**.

# Tech Support & Computer Scams

Computer-based scams involve con artists pretending to be associated with a well-known technology company, such as Microsoft, Apple, Dell, or Best Buy's Geek Squad. They may use tactics like falsely claiming that an individual's computer has been infected with a virus or requesting the individual provide them with personal information and/or remote access to their computer. They may also request an individual's credit card or bank account number to "bill" for their services.

In a similar scam, the intended victim may see a pop-up window on their computer screen describing a security threat and instructing them to call a number for a tech support agent who is a scammer. The FBI reports that in 2023, as in 2022, tech support scams were the top scam impacting older adult victims. Older adults reportedly lost nearly $590 million to tech support scams in 2023.[20]

### Reports from the Fraud Hotline

A woman from Georgia called the Committee's Fraud Hotline to report that she lost $25,000 in a tech support scam. The caller reported that her computer had frozen and a pop-up appeared, which prompted her to call, what she believed, was the tech support number for Microsoft. The caller dialed the number for assistance and scammers were able to steal thousands of dollars from her.

## RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive an alert saying there is a virus on your phone or computer and that you must call a number to resolve the issue.
- A scammer says that the only solution to protect your money or personal data from the "hacker" is to transfer your account funds to them while they get rid of the supposed virus.
- If you say that you would prefer to fix the issue by going to a physical store or calling a different company, the caller attempts to convince you that the virus is time-sensitive and only they can help you.

## STEPS TO PREVENT AND RESPOND

- If you receive an alert saying your phone or computer has a virus, do not call the number provided in the alert. Instead, call the official tech support number for your device (e.g., Apple or Microsoft).
- If a person calls you saying your device has been hacked or compromised by a virus, hang up and block their phone number.
- Never provide personal or financial information to an unexpected caller.
- Do not give remote access to a device or account unless you contacted that company first and know it to be legitimate.
- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

## MORE INFORMATION

- For more details about tech support scams, the Better Business Bureau has useful information at **www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams**.
- The FTC provides additional information on how to spot and avoid tech support scams at **consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams**.

# Government Imposter Scams

In government imposter scams, bad actors will pretend to be a representative of a federal agency, such as the Social Security Administration (SSA) or Internal Revenue Service (IRS). They may threaten a person's benefits, demand payment for "taxes" or "fees," or allege some problem in order to steal your money or personal information. They may also use documents or images, like a federal logo, when communicating with the intended victim to make their claim seem legitimate. Among the different types of government imposter scams, Social Security-related ones were the most common scam of this type reported to both the Committee's Fraud Hotline and the FTC in 2023. According to the FTC, victims lost over $126 million to Social Security imposter scams last year.[21]

**Reports from the Fraud Hotline**

A caller from West Virginia reported that he received a call from a scammer who claimed to be an employee of the federal government. The caller said he was told to send $900 to the scammer to erase his debt with the IRS.

## RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive a phone call, text, or email asking to confirm information that the government agency should already have, like an address or Social Security Number.
- The person contacting you threatens your benefits, asks you to wire money, put money on a prepaid debit card or gift card, or tells you to send cash or check using an overnight delivery service. They may also ask you to pay using cryptocurrency or via a P2P payment app.
- You are pressured to decide quickly and urgently, sometimes within a day or week.

## STEPS TO PREVENT AND RESPOND

- Hang up the phone or do not reply to the email or text message.
- Never give out or confirm financial or other sensitive information in response to unexpected calls, or if you are at all suspicious.
- Do not inherently trust a name or number. Scammers may use official-sounding names to make you trust them. To make their call seem legitimate, scammers may also use technology to disguise their real phone number.

- A government agency will never ask you to wire money, provide your Social Security Number, or send funds via gift card.
- Call the federal agency directly and wait to speak to a customer service representative to verify the call or email you received.
- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

## MORE INFORMATION

- The FTC provides tips on how to spot and avoid imposter scams at **consumer.ftc.gov/features/imposter-scams**.
- SSA has more information on how to protect yourself from Social Security Scams at **www.ssa.gov/scam**.

# Romance Scams

Romance scammers exploit an individual's desire for companionship and love by creating fake identities and forming emotional connections online. These scammers often pose as potential romantic partners, gaining victims' trust over time through frequent communication and declarations of affection. Once trust is established, the scammer typically fabricates a crisis or urgent need for money, such as medical expenses, travel costs, or investments, persuading the victim to send funds. Victims may be manipulated into keeping the relationship secret or rushed into making financial transactions before fully verifying the authenticity of their supposed partner.

Romance scams are pervasive across dating websites, social media platforms, messaging apps, and online forums. Awareness and caution are crucial in recognizing the signs of deception and protecting oneself from emotional and financial harm. The FTC reports that more than 64,000 consumers reported they were victims of romance scams in 2023, with reported losses totaling over $1.1 billion.[22]

**Reports from the Fraud Hotline**

A woman from Ohio called the Fraud Hotline to report that, for the past two years, she has been the victim of a romance scam where she lost $40,000.

## RED FLAGS

These are common signs that you may be facing this type of scam:

- The person never video calls you or meets you in person.
- You share no mutual friends with them on social media, and their identity is tough to trace online.
- They claim to be in love with you before meeting in person.
- They plan to visit you, but always have an excuse for why they can't that comes up last-minute.
- They request money be sent via cryptocurrency, wire transfer, P2P payment app, or gift card.

## STEPS TO PREVENT AND RESPOND

- If the person always refuses to video call or meet in person, block them.
- Never send money or gifts to someone that you have not met in person.

- Talk to your family and friends, or someone you trust, to get their advice.
- Contact your bank immediately if you think you sent money to a scammer.
- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

## MORE INFORMATION

- The U.S. Secret Service provides tips on how to avoid romance scams at **www.secretservice.gov/investigation/romancescams**.
- The FTC provides information and reporting resources at **www.consumer.ftc.gov/articles/what-know-about-romance-scams**.