Avoiding Scams and Fraud

Resources

Scams and Fraud:

- AARP
- FBI.gov
- FTC (Federal Trade Commission)
    - ReportFraud.ftc.gov
- AAA
- Better Business Bureau
- USPS.com (Informed Delivery)

- **Helpline**: AARP Fraud Watch Network Helpline: **877-908-3360** (Trained fraud specialist that provide support & guidance for victims and families.)

- **Victim Support** (AARP): aarp.org/VictimSupport (This online program provides a safe place for victims and their families to address the emotional impact of fraud.)

Credit Report

Many credit card companies provide credit reports for free. If not, go to AnnualCreditReport.com, or call 877-322-8228.

Identity Theft

- IdentityTheft.gov
- www.USDOJ.gov
- US Dept of Justice: 202-514-2000

7 Tactics Criminals Use to Perpetrate Fraud

Scammers have learned how to manipulate people's emotions and take advantage of their trust in others

By: Christina Ianzito,
AARP

November 10, 2022

Many people believe they are too smart to be taken in by a scam. But they miss the key point: Scammers mostly bypass your intellect and rely on sophisticated psychological and emotional manipulations to get you to say yes. "You don't have to be a fool to be fooled," says Robert Cialdini, author of *Influence: The Psychology of Persuasion.* "These people are using tactics and strategies that all of us are susceptible to." Specifically, he explains, they weaponize universal human instincts such as fear of loss, love and trust in others. Here are some of their techniques.

1. Scammers establish camaraderie

"So sorry to hear about the loss of your husband. You know, my own wife passed away last year as well. It's been hard."

The Trick: Scammers will parrot back the target's religion, political affiliation, military background or life situation to get the target to feel "he's just like me," Cialdini notes. "Then we tend to lower our defenses and are much more likely to follow their lead."

2. Scammers play on your aversion to loss

"You've won the sweepstakes! You are now rich! But if you don't act fast ..."

The Trick: Many people have a deep-seated fear of missing out (FOMO, in internet jargon) on good opportunities, given how infrequently they appear. The criminal encourages that FOMO, Cialdini says. "They do it in terms of the uniqueness of the idea, or the dwindling of availability of the product or service. This spooks people into choices."

3. Scammers flatter you

"I can tell you know a lot about finance, so you know how much money you can make in cryptocurrency if you manage the risks."

The Trick: "Usually, at the beginning, it's a lot of love bombing," says Anthony Pratkanis, emeritus professor of psychology at the University of California, Santa Cruz. They'll frequently praise the victim, Cialdini says. "That lends itself to a sense of connection and trust. 'If this person likes me, well, then I can trust this person.' "

4. Scammers make you feel anxious

“This malware means your bank account has been compromised. Someone could steal from it very easily now.”

The Trick: “We live in this age of anxiety, where there are so many actual existential fears,” AARP fraud expert Doug Shadel says. “It’s pretty easy to get people to say, ‘All right, what do I have to do to make this one go away?’ ”

No matter where you live, fraud is never far away. Report a scam or search for existing scams near you.

5. Scammers create instant terror

“Grandpa, help! I’ve been arrested and need money for bail right away!”

The Trick: “When you’re afraid, the emotional part of your brain takes over the cognitive part of your brain,” Shadel says. “That’s what they want. When your emotions kick in, it swaps out the logic.” In such moments of powerful emotion, you are far more likely to think you hear a loved one’s voice and to fall for a scam.

6. Scammers seduce you

“I love talking to you. I have not felt so close to someone in so long.”

The Trick: In a romance scam, as in a [real] love relationship, you’ll have reciprocating self-disclosures,” Pratkanis explains. “I’ll tell you a little bit about me. In return, you tell me a little bit about you. And as we go further down the path, we say more intimate things, and that creates a sense of closeness, even love.”

7. Scammers intimidate you

“I’m with the police; you’ve missed jury duty again. Either pay a $900 fine now or go to jail.”

The Trick: They present themselves as a feared authority (say, a cop, IRS officer or Medicare rep). “Technology makes it so easy now to pretend to be someone you’re not,” Shadel says. “Criminals can program their caller ID so it says ‘San Diego Sheriff’s Office.’ ”

How to stay rational when scammers rattle you

Monitor your reactions to calls from strangers. Do you feel heated? Is your pulse rising? Are you getting angry or anxious?

If the answer is yes, get out of the situation immediately. Simply say, “I won’t do this by phone. Send a letter. Goodbye.” Then hang up.

Recenter yourself: Leave the room, take 10 deep breaths and ask yourself questions that you know the answers to, such as “What color is grass?”

Look at the situation like a scientist, as though you’re observing someone else in the same position.

Never make an immediate impulse-buying decision. Wait at least 24 hours to allow emotions to subside before making a purchase.

Get advice from a person you trust and respect. Merely discussing the situation out loud helps bring rationality back.

Christina Ianzito covers fraud and breaking news for aarp.org and is the books editor for aarp.org and AARP The Magazine*. Also a longtime travel writer and editor, she received a 2020 Lowell Thomas Award for travel writing from the Society of American Travel Writers Foundation.*

Avoiding Scams and Fraud

10 Common Phone Scams

(US News)

1. Scammers sometimes offer free gifts as rewards to consumers that actually are efforts to take your money and information. Vacations and travel are among the most common offerings by scammers seeking your address, credit card number, credit information, while asking for a shipping and handling fee or similar fee to send the gift.

2. 'You've won the lottery' scams often come from outside the United States, thus making law enforcement's job all the harder. Scammers ask their victims to pay a fee, buy tickets, and/or provide personal information. The Federal Trade Commission (FTC) estimates that Americans lose up to $120 million to the schemes.

3. 'I'm calling from the IRS' scams are particularly common before April 15, when Americans file their income tax statements or near the end of the fiscal year. Typically, scammers claim that the victim owes taxes or has another problem. They mimic caller IDs, and may even have acquired victims' social security numbers. But the IRS will never phone taxpayers nor request an immediate wire transfer of money. IRS contacts taxpayers by mail.

4. 'I'm calling from the bank' schemers contact victims about alleged problems with a bank account or funds, sometimes originating as text messages asking for contact via telephone. The scam is looking for personal information, including bank account and credit card information, to take your money.

5. Charity scams can happen at any time, but are frequent after disasters when generous people want to help others; the funds wind up in the scammers' pockets. While some charities do accept donations via telephone, when in doubt, call them back on a verified line to make a donation.

6. Debt scammers use fear to trick victims into forking over money. Sometimes posing as collection agencies, they urgently request payment of a supposed debt and even threaten legal action should victims fail to pay. They may also offer to write off supposed debt, which does not exist, in exchange for a smaller payment. In this case, demand the name, address, and phone number of the caller, as well as the exact amount of the debt, the name of the creditor, and a validation notice that collection agencies are legally required to provide. If the caller cannot provide this, it's a scam.

7. In family emergency schemes, scammers try to impersonate family members requesting money, claiming poverty or legal trouble. Seniors should be aware that a common scam is pushed by scammers claiming to be a grandchild. In these cases, disconnect and call the real relative, who will probably know nothing about the claim.

8. In jury duty scams, schemers exploit fears of legal consequences for failing to heed a court summons. In these scams, scammers claim to be calling to ascertain your eligibility for jury duty. Usually, they want your social security number or they demand immediate payment of a fine for supposed failure to show up for jury duty while threatening jail time. Courts and jury commissions will not contact you by telephone to demand immediate payments.

9. Small businesses, or sometimes individuals, are often targeted by utility scams when schemers claim to be calling from an energy company to demand payment of a supposed outstanding bill in order to avoid shut-off. Utility bills normally are not paid over the phone, and utilities offer videos on their websites about making a secure payment.

10. In recovery scams, victims are called by unknown parties claiming to have recovered stolen funds. The scammers ask for personal information and/or payment of a small fee for recovery of the funds. Lists of scam victims are valuable to criminals, who sell and trade the lists to other scammers. Be careful if you are a scam victim.

Other schemes include offers of business coaching, investment opportunities, student debt forgiveness, extended car warranties, and "free" trials of products that wind up as monthly payments.

Things To Watch Out For:

Be wary if any caller asks for passwords. Policies are in place at reputable organizations which never ask for passwords or personal identification numbers (PINs) over the phone. Instead, they will provide links at websites where consumers can enter the information.

Scammers don't answer questions while reputable organizations will provide information and proof, and allow speaking with supervisors.

Scammers use recording technology to record victims saying "yes" when the scammers ask "Can you hear me?" They use the recording as proof of victims' agreement to a purchase, for example. Avoid saying "yes."

Scammers threaten account disruption or legal action, while legitimate callers rarely do so.

If callers discourage calling them back on an official number, they are probably illegitimate.

Older people can fall victim to family emergency schemes in which scammers try to impersonate family members requesting money, claiming poverty or legal trouble.

How To Avoid Telephone Scams:

To reduce the chances of being scammed, minimize your reliance on phones. If family members, friends, and frequently consulted organizations contact you through other platforms, you will thus be likely to identify phone scams.

Block unwanted calls.

Screen calls that you do not recognize, let them go to voicemail. Legitimate calls will probably leave a voice message, but scammers will probably hang up.

When receiving a call from an unfamiliar number, Google the caller's number to reveal where it came from. Many websites list scammers' numbers.

If your cell phone plan includes scam filters, enabling it will reduce exposure to scams.

When in doubt, hang up. Legitimate callers will contact you again or another way, thus providing an opportunity to verify their identity before contacting them again.

Never follow instructions unknown callers give before verifying their legitimacy. Scammers want your information and/or money.

If in doubt about a caller, note the caller's name, organization, and other information (e.g. date and time), which can be useful in investigating the call.

Finally, to reduce the number of unwanted calls, register your phone number with the FTC's National Do Not Call Registry. You may register online at donotcall.gov or by calling 1-888-382-1222 (TTY: 1-866-290-4236)

Cellphone, Bluetooth, and Wi-Fi Protection

Avoiding Becoming a Victim

Cybersecurity attacks can happen anywhere, so a few simple precautions can help prevent you from becoming a victim.

Wi-Fi:

Do NOT Use publicly available Wi-Fi, that does not have a unique password that was issued specifically to you. Specifically to you really means a one of a kind, hard to guess password. For example, a unique password does NOT include the "password of the day" for the coffee shop that is provided to every customer, or a password such as "password".

Public Wi-Fi is just that, and anytime you connect to public Wi-Fi 100% of your information that is broadcast and/or stored on your device (laptop, tablet, phone, etc.) is now available to any hacker that is monitoring that Wi-Fi.

Remember the Rule: If it is free, then you and your information are what is being sold – You Are for Sale!

Bluetooth:

Do Not Use publicly available USB charging ports and/or stations. When you need to charge your phone only use an electrical wall outlet with your own plug and charging cable.

Criminals have the ability to hijack any device connected to a Bluetooth charging station and download all of the device's files and information.

Cellphone:

Do not accept roaming charges pop-up notifications, or any other pop-up notifications on your cell phone.

Avoiding Scams and Fraud

Did You Receive a Text Message From Yourself? You're Not Alone.

(NY Times: Brian X. Chen - April 6, 2022)

Text spam is on the rise. The latest version involves scammers sending messages to you seemingly from your own phone number. Here's what to do.

A few weeks ago, I woke up to an early morning text message on my smartphone. It wasn't my editor or a needy friend in a different time zone. It was a message from myself.

"Free Msg: Your bill is paid for March. Thanks, here's a little gift for you," the text from my own phone number read, pointing me to a web link.

In the last month I've received a handful of such texts. In online forums, many Verizon customers have reported the same experience.

It was clear to me what was going on. Scammers had used internet tools to manipulate phone networks to message me from a number they weren't actually texting from. It was the same method that robocallers use to "spoof" phone calls to appear as though they are coming from someone legitimate, like a neighbor. Had I clicked on the web link, I most likely would have been asked for personal information like a credit card number, which a scammer could use for fraud.

Consumers have struggled with cellphone spam for years, primarily in the form of robocalls with scammers incessantly ringing to leave fraudulent messages about late payments for student loans, audits by the Internal Revenue Service and expired car warranties.

Only recently has mobile phone fraud shifted more toward texting, experts said. Spam texts from all sorts of phone numbers — and not just your own — are on the rise. In March, 11.6 billion scam messages were sent on American wireless networks, up 30 percent from February. That outpaced robocalls, which rose 20 percent in the same period, according to an analysis by Teltech, which makes anti-spam tools for phones.

- Dig deeper into the moment.

Verizon confirmed that it was investigating the text issue. On Monday, it said it had fixed the problem. "We have blocked the source of the recent text messaging scheme in which bad actors were sending fraudulent text messages to Verizon customers which appeared to come from the recipient's own number," said Adria Tomaszewski, a Verizon spokeswoman.

Representatives for AT&T and T-Mobile said they had not seen the same problem. But text spam affects all wireless subscribers, and carriers now offer resources online for how people can protect themselves and report spam.

Text scams vary widely but often involve getting you to cough up your personal data with messages disguised as tracking updates for phony package deliveries, or information about health products and online banking. Their rise has been fueled partly by the fact that messages are so effortless to send, Teltech said. In addition, industrywide and government efforts to crack down on robocalls may be pushing scammers to move on to text messages.

“Scammers are always looking for the next big thing,” said Giulia Porter, a vice president at Teltech. “Spam texts are just increasing at a much more drastic rate than spam calls.”

Here’s what to look out for with text scams — and what you can do.

What spam text looks like

By far the most common text scam is the message impersonating a company that is offering a shipping update on a package, such as UPS, FedEx or Amazon, according to Teltech.

In the last week, I have received messages that said a Samsung TV — a big-ticket item meant to get my attention — could not be delivered. Another advertised an anti-aging skin cream. Another message touted the benefits of a product that cured brain fog.

Be on the lookout for these telltale signs of a fraudulent text:

- Scam texts typically come from phone numbers that are 10 digits or longer. Authentic commercial entities generally send messages from four-, five- or six-digit numbers.
- The message contains misspelled words that were intended to circumvent the wireless carriers’ spam filters.
- The links in a scam text often look strange. Instead of a traditional web link composed of “www.websitename.com,” they are web links that contain sentences or phrases, like droppoundsketo.com. This practice, called URL masking, involves using a phony web link that directs you to a different web address that asks for your personal information.

How to protect yourself

First and foremost, never click on a link or file in a suspicious message.

Definitely don’t reply to such a message, either. Even typing “STOP” will indicate to a scammer that your phone number is active.

To report a scammy text, AT&T, Verizon and T-Mobile offer the same number to forward the messages to: 7726. After forwarding, the carrier asks for the phone number that the message came from.

If text spam is becoming overwhelming, spam-filtering apps like Teltech's TextKiller are meant to help. The app, which blocks spam texts for $4 a month, scans messages coming from phone numbers that are not in your address book. If the text is detected as spam, it gets filtered into a folder labeled "Junk."

TextKiller was thorough — perhaps too thorough. It successfully caught five spam messages in five days, but it also erroneously filtered two legitimate messages, including a response from Verizon thanking me for reporting spam and a message from an AT&T spokesman. So I wouldn't recommend paying $4 a month for this app, which is available only for iPhones, unless spam texts have become truly unbearable for you.

Teltech said that false positives for messages marked as spam happened in rare cases, and that customers could share feedback to train TextKiller's accuracy.

A more practical solution is to use free tools to minimize interruptions from spam texts. On iPhones, you can open the Settings app, tap messages and enable an option to "filter unknown senders." That places messages from numbers that are not in your phone book into a separate messages folder. On Android phones, you can open the messages app, enter the spam messages settings and enable "block unknown senders."

Finally, both iPhones and Android devices include the ability to open the settings of a message and block a specific number from contacting you.

Bottom line

There's a moral to this story: We can help prevent spam from flooding our phones if we stop sharing our phone numbers with people we don't fully trust. That includes the cashier at a retail store asking for our phone number to get a discount, or an app or a website asking for our digits when we sign up for an account. Who knows where our digits eventually end up after they reach the hands of marketers?

A better idea is for all of us to carry a second set of digits, which can be created with free internet calling apps like Google Voice, that we treat as a burner phone number.

That way, the next time a scammer tries to send you a text from yourself, it won't come from your own number.

Avoiding Scams and Fraud

How to Protect Yourself From Scams (Experian)

While it's true that phishers use increasingly sophisticated techniques to steal information, it's also true that you can avoid many of their attempts if you know what to look out for. Here's how to protect yourself from identity theft and reduce the risk of being targeted.

Guard Your Personal Information

Immediate requests for money transfers or for your Social Security number are a sure indication that you're dealing with a scammer. Avoid phishing scams by safeguarding your sensitive information.

Don't give out your Social Security number or bank account number to anyone who calls and asks you for it. A legitimate banker or government official won't call and request this information. If someone you think is official calls and asks you for identifying information, hang up and call back using the number listed on the organization's official website.

Set Up Strong, Unique Passwords

Using the same password across your devices and financial accounts places you at a higher risk of losing your key information to a fraudster.

Instead, use unique and complex passwords with a combination of letters and numbers. Using a password manager can be an easy way to securely keep track of your passwords.

Review Your Credit Reports Regularly

Make it part of your routine to regularly check your credit reports for discrepancies. You can get free copies of your credit reports from all three major consumer credit bureaus at AnnualCreditReport.com. You can check your Experian credit report and credit score for free through Experian.

If you encounter information you believe may be the result of fraud, dispute the information with the appropriate credit bureau right away.

Handle Sensitive Mail Responsibly

Check your mail every day and bring all letters inside to help prevent mail theft. Shred anything with personally identifying information on it before tossing it, and store documents you intend to keep in a secure place.

You can also opt out of credit offers and choose to receive electronic statements from your utility companies and credit issuers to limit the amount of sensitive mail you receive.

The Bottom Line

Scammers thrive on surprise—an alarming phone call, a confusing message, a threatening letter, a malicious link in an innocuous email. If you know what to expect and stay up to date on the tactics of scammers, you'll be much harder to target.

If you're worried a scammer has accessed your information, you can place a fraud alert on your credit reports. The alert asks lenders to confirm your identity before issuing you any new credit. If you've repeatedly been victimized by scammers, you might consider securing your credit with a credit freeze, which blocks access to your credit history.

Lastly, report any attempts at phishing using the Federal Trade Commission's official reporting site to help law enforcement track and prevent identity theft.

An official website of the United States government

Here’s how you know

.cls-1{fill:none;}.cls-2{fill:#1d3557;}.cls-3{fill:#065cb4;}.cls-4{clip-path:url(#clip-path);}.cls-5{fill:#fff;}.cls-6{fill:#003d79;}

Menu

CFG: Main Menu Mega

CFG: Main Navigation

- Identity Theft and Online Security
- Scams

Items per page
20
Filters
Fulltext search Enter a search term...

Search

Breadcrumb

1. Home
2. Articles

Vea esta página en español
Article

How To Stop Junk Mail

Tired of having your mailbox crammed with ads and other mail you didn't ask for, like preapproved credit card applications? The good news is that there are ways to cut down on how much unsolicited mail you get.

- How To Get Less Mail From Marketers
- How To Stop Credit Card and Insurance Offers

How To Get Less Mail From Marketers

To decide what types of mail you do and don't want from marketers, register at the Direct Marketing Association's (DMA) consumer website DMAchoice.org, and choose what catalogs, magazine offers, and other mail you want to get. DMAchoice will stop most, but not all, promotional mail. You'll have to pay a $4 processing fee, and your registration will last for 10 years.

If you do not have online access, register by sending your name and address (with signature), along with a $5 processing fee (check or money order payable to the Association of National Advertisers or ANA) to:

DMAchoice
Consumer Preferences
P.O. Box 900
Cos Cob, CT 06807

The site also offers the no-cost option to stop mail from being sent to someone who's deceased (Deceased Do Not Contact List) or to a dependent in your care (Do Not Contact for Caretakers List(link is external)). Registration for the Caretakers List will last for 10 years.

DMAchoice.org also has an Email Preference Service that lets you get less unsolicited commercial email. Registration is free and will last for six years. To learn more about what options you have for dealing with unwanted email, read this

article on email spam.

For comments or questions about DMAchoice, visit dmachoice.org/report/initReport.php(link is external).

Learn more about stopping unwanted calls at ftc.gov/calls.

How To Stop Credit Card and Insurance Offers

If you don't want to get prescreened offers of credit and insurance in the mail, you have two choices for opting out of those offers:

- opt out of getting them for five years
- opt out of getting them permanently

To opt out for five years: Go to optoutprescreen.com(link is external) or call 1-888-5-OPT-OUT (1-888-567-8688). The phone number and website are operated by the major credit bureaus.

To opt out permanently: Go to optoutprescreen.com(link is external) or call 1-888-5-OPT-OUT (1-888-567-8688) to start the process. **But to complete your request, you'll need to sign and return the Permanent Opt-Out Election form you'll get after you've started the process.**

When you call or visit optoutprescreen.com(link is external), they'll ask for your personal information, including your name, address, Social Security number, and date of birth. Sharing your Social Security number and date of birth is optional, but the website says that giving this information can help them ensure that they can successfully process your request. It says the information you give is confidential and will be used only to process your request to opt out.

Search Terms
mail
opt out
Topics
Unwanted Calls, Emails, and Texts
Unwanted Emails, Texts, and Mail
July 2022
Return to top
.cls-1{fill:none;}.cls-2{fill:#1d3557;}.cls-3{fill:#065cb4;}.cls-4{clip-path:url(#clip-path);}.cls-5{fill:#fff;}.cls-6{fill:#003d79;}
Menu

CFG: Footer Menu

- Feature Pages
- Articles
- Consumer Alerts
- Videos

CFG: Footer Menu Right

- Report Fraud
- Get Consumer Alerts

CFG: Footer

An official website of the United States government

Here’s how you know

.cls-1{fill:none;}.cls-2{fill:#1d3557;}.cls-3{fill:#065cb4;}.cls-4{clip-path:url(#clip-path);}.cls-5{fill:#fff;}.cls-6{fill:#003d79;}

Menu

CFG: Main Menu Mega

CFG: Main Navigation

- Identity Theft and Online Security
- Scams

Items per page
20
Filters
Fulltext search Enter a search term...

Search

Breadcrumb

1. Home
2. Articles

Vea esta página en español
Article

Lost or Stolen Credit, ATM, and Debit Cards

If your credit, ATM, or debit card is lost or stolen, federal law limits your liability for charges made without your permission, but your protection depends on the type of card — and when you report the loss.

- Report Loss Or Theft Immediately
- Watch for Fraudulent Activity
- How To Limit Your Losses
- How To Protect Your Account Information
- Avoiding Credit Card Loss Protection Scams

Report Loss Or Theft Immediately

If your credit, ATM, or debit card is lost or stolen, don't wait to report it.

1. **Call — or get on the mobile app — and report the loss or theft to the bank or credit union that issued the card as soon as possible.** Federal law says you're not responsible to pay for charges or withdrawals made without your permission if they happen after you report the loss. It's important to act fast. If you wait until someone uses your card without permission, you may have to pay some or all of those charges. Check your statement or online account for the right number to call. Consider keeping the customer service numbers for your bank or credit union in your phone's contacts, and keep them up to date.

2. **Follow up immediately in writing**. Send a letter to the card issuer and include your account number, the date and time when you noticed your card was missing, and when you first reported the loss. Keep a copy of your letter and your notes from calls with the bank or credit union.

Watch Your Accounts

1. Keep checking your account statements **and call to report fraudulent charges ASAP**. If you spot a charge you

didn’t make, call to report it immediately. If you wait, you may have to pay for the charges, or lose the money withdrawn from your account.
2. Follow up immediately in writing. Send a letter to the address used for billing disputes (credit cards) or errors (debit cards). Confirm that you reported the fraudulent charge or withdrawal. Include the date and time when you noticed your card was missing, and when you first reported the loss.
3. Check if your homeowner's or renter's insurance covers you for card thefts. If not, ask your insurance company to include this protection in your policy going forward.
4. Check your credit reports. Get copies of your free credit reports to monitor for accounts or charges you don’t recognize. If you suspect identity theft, visit IdentityTheft.gov to report it and get a recovery plan.

How To Limit Your Losses

Under federal law, you have protections that help limit what you have to pay if your credit, ATM, or debit cards are lost or stolen.

	Credit card	**ATM/Debit card**
You report your card’s loss **before** someone uses it	You aren’t responsible for any charges you didn’t authorize	You aren’t responsible for any transactions you didn’t authorize
You report your card’s loss **after** someone uses it	The maximum you might be responsible for is $50	What you’re responsible for depends on how quickly you reported it
Your account number is used but your card isn’t lost or stolen	You aren’t responsible for any charges you didn’t authorize	You aren’t responsible for any transactions you didn’t authorize if you reported the loss within 60 calendar days after your statement is sent to you

If someone uses your ATM or debit card before you report it lost or stolen, what you owe depends on how quickly you report it.

If you report your ATM or debit card lost or stolen…	**Your maximum loss is…**
…before any unauthorized charges are made	$0
…within 2 business days after you learn about the loss or theft	$50
…more than 2 business days after you learn about the	

loss or theft, but within 60 calendar days after your statement is sent to you	$500
…more than 60 calendar days after your statement is sent to you	All the money taken from your ATM/debit card account, and possibly more — for example, money in accounts linked to your debit account

How To Protect Your Account Information

- **Don't share your account information. Don't give your account number** over the phone unless you made the call — and know why you need to share it. Never leave your account information out in the open.
- **Protect your accounts by using multi-factor authentication, when available.** Some accounts offer extra security by requiring two or more credentials to log into your account. This is called multi-factor authentication — a security practice that makes it harder for scammers to log in to your accounts if they get your username and password. To log in to your account, you'd need either:
  - Something you have — like a passcode you get via text message or an authentication app.
  - Something you are — like a scan of your fingerprint, your retina, or your face.
- **Keep an eye on your accounts. Regularly check your account activity**, especially if you bank online.
  - Carefully check your ATM or debit card transactions because they take money from your account right away. Report any withdrawals you don't recognize to your bank or credit union immediately.
  - For your credit cards, open your monthly statements promptly. Compare the current balance and charges on your account with your receipts. Report any charges you don't recognize as soon as you discover them.
- **Keep your cards, PINs, receipts, and deposit slips safe — and dispose of them carefully.**
  - Carry only the cards you'll need. Don't carry the PIN for your ATM or debit card in your wallet, purse, or pocket. Never write your PIN on the card itself, or on any piece of paper that you could lose or someone could see.
  - Cut up old cards. Be sure to cut through the account number, the magnetic strip on the back, and the security code — before you throw the pieces away in separate bags. If your card has a chip, it may be difficult to cut. You may want to destroy the chip by smashing it into pieces with a hammer.

Avoiding Credit Card Loss Protection Scams

Scammers sometimes contact you — by phone, text, email, or by messaging you on social media — and try to trick you into thinking you need to buy "credit card loss protection insurance." They may say you need it because computer hackers can get into your credit card and charge thousands of dollars. Or they might say they're from your credit card company's "security department." They'll claim you just need to confirm your account number to activate your card's protection feature — but you'll end up getting charged. No matter the story, it's a scam and they're just after your account number. Reputable financial companies won't contact you like this, and there's no need to pay for this so-called protection. Federal law already protects you from unauthorized use of your credit card.

If you see a scam, fraud, or a bad business practice, tell the FTC. Go to ReportFraud.ftc.gov, the FTC's website that makes it easy for you to report.

Search Terms
ATM

credit card
debit
Topics
Credit, Loans, and Debt
Credit and Debt
January 2022
Return to top
.cls-1{fill:none;}.cls-2{fill:#1d3557;}.cls-3{fill:#065cb4;}.cls-4{clip-path:url(#clip-path);}.cls-5{fill:#fff;}.cls-6{fill:#003d79;}

Menu

CFG: Footer Menu

- Feature Pages
- Articles
- Consumer Alerts
- Videos

CFG: Footer Menu Right

- Report Fraud
- Get Consumer Alerts

CFG: Footer

- ftc.gov
- About Us
- Contact Us
- Privacy and Notices
- FOIA
- Office of Inspector General

(link is external)
(link is external)
(link is external)

Avoiding Scams and Fraud

Methods Used to Deceive and Defraud

(FBI – PSA: I-091919)

With the elderly population growing in the United States, it is likely perpetrators will find more and more victims. Elderly, as well as younger individuals, may encounter the following scams:

- **Romance Scam:** Perpetrators pose as interested romantic partners through dating websites to capitalize on their elderly victims' desire to find companions.
- **Tech Support Scam:** Perpetrators pose as technology support representatives and offer to fix non-existent computer issues—gaining remote access to victims' devices and, thus, their sensitive information.
- **Grandparent Scam:** Perpetrators pose as a relative—usually a child or grandchild—claiming to be in immediate dire financial need.

  Example: My dad losing money to this scam. Tell story.

- **Government Impersonation Scam:** Perpetrators pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- **Sweepstakes/Charity/Lottery Scam:** Perpetrators claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."
- **Home Repair Scam:** Perpetrators appear in person and charge homeowners in advance for home improvement services that they never provide.
- **TV/Radio Scam:** Perpetrators target potential victims using illegitimate advertisements about legitimate services, such as reverse mortgages or credit repair.
- **Family/Caregiver Scam:** Perpetrators are relatives or acquaintances of the elderly victims and take advantage of them or otherwise get their money.

Defense and Mitigation

Taking the following steps may help protect yourself from being victimized:

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Resist the pressure to act quickly. Perpetrators create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.

- Be cautious of unsolicited phone calls, mailings, and door-to-door services offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, or checks—or wire information or funds—to unknown or unverified persons or businesses.
- Ensure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- If you receive a pop-up or locked screen on your device, immediately disconnect from the internet and shut down the affected device. Pop-ups are regularly used by perpetrators to spread malicious software. To avoid accidental clicks on or within a pop-up, enable pop-up blockers.
- Do not open any emails or click on attachments you do not recognize and avoid suspicious websites.
- If a perpetrator gains access to a device or an account, take precautions to protect your identity; immediately contact your financial institutions to place protections on your accounts; and monitor your accounts and personal information for suspicious activity.

Filing a Complaint

If you believe you or someone you know may have been a victim of elder fraud, you should contact your local FBI field office. **You can also file a complaint with the Internet Crime Complaint Center at www.ic3.gov.** When reporting a scam—regardless of dollar amount—be as descriptive as possible in the complaint by including:

1. Dates the perpetrator had contact with you, and the methods of communication.
2. Names of the perpetrator and company.
3. Phone numbers, email addresses, and mailing addresses used by the subject.
4. Websites used by the subject company.
5. Method of payment.
6. Account names and numbers and the financial institutions to which you sent funds, including wire transfers and prepaid card payments.
7. Descriptions of interactions with the perpetrator and the instructions you were given.

Complainants are also encouraged to keep all original documentation, emails, faxes, and logs of all communications. Because scams and fraudulent websites appear very quickly, individuals are encouraged to report possible internet scams and fraudulent websites by filing a complaint with the IC3 at www.ic3.gov.

Phishing

Updated: 10/18/2022 by Computer Hope

Pronounced like *fishing*, **phishing** is a malicious individual or group who scam users. They do so by sending e-mails or creating web pages designed to collect an individual's online bank, credit card, or other login information. Because these e-mails and web pages look legitimate, users trust them and enter their personal information. The information below shows examples of phishing attempts and ways to avoid a phishing attack and threats.

Example of phishing e-mail

```
Dear eBay customer,

Your Account is Suspended. We will ask for your password only once. We will
charge your account once per year. However, you will receive a confirmation
request in about 24 hours after the make complete unsuspend process. You have
24 hours from the time you'll receive the e-mail to complete this eBay
request.

Note: Ignoring this message can cause eBay TKO delete your account forever.

To make unsuspend process please use this link:

http://fakeaddress.com/ebay

eBay will request personal data(password;and so on) in this e-mail.

Thank you for using eBay!

http://www.ebay.com

---------------------------------------------------------------------

This eBay notice was sent to you based on your eBay account preferences. If
you would like to review your notification preferences for other
communications, click here. If you would like to receive this e-mail in text
only, click here.
```

To those who frequently use online services, these e-mails may appear as if they have come from the company. However, these e-mails are designed to make a user want to click a link that helps them steal personal information such as usernames, passwords, credit card, and personal information. Below are some helpful tips on identifying these e-mails and how to handle them.

How to identify a phishing e-mail

Identifying a phishing e-mail is key to avoiding a phishing attack. Here are some things to look out for when reading e-mail.

1. *Wrong company* - These e-mails are sent out to thousands of different e-mail addresses and often the person sending these e-mails has no idea who you are. If you have no affiliation with the company the e-mail address is supposedly coming from, it is fake. For example, if the e-mail is coming from Wells Fargo bank but you bank at a different bank.
2. *Spelling and grammar* - Improper spelling and grammar are often a dead giveaway. Look for obvious errors.
3. *No mention of account information* - If the company were sending you information regarding errors to your account, they would mention your account or username in the e-mail. In the above example, the e-mail says "eBay customer." If this was eBay, they would mention your username. However, be cautious of spear phishing, a type of phishing where the attacker knows some personal information.
4. *Deadlines* - E-mail requests an immediate response or a specific deadline. For example, in the above example, the requirement to log in and change your account information within 24 hours.
5. *Links* - Although many phishing e-mails are getting better at hiding the true URL you are visiting, often these e-mails list a URL that is not related to the company's URL. For example, in our above eBay example, "http://fakeaddress.com/ebay" is not an eBay URL, only a URL with an "ebay" directory. If you are unfamiliar with how a URL is structured, see the URL definition for additional information.

What to do if you are unsure if an e-mail is official

- *Never* follow any links in an e-mail. Instead of following the link in the e-mail, visit the page by manually typing the address of the company. For example, in the example above, instead of visiting the fake eBay URL, you would type: https://www.ebay.com in your web browser and log into the official website.
- *Never* send any personal information through e-mail. If a company is requesting personal information or says your account is invalid, visit the website and log into the account as you normally would.
- Finally, if you are still concerned about your account or personal information, contact the company directly, either through their e-mail address or over the phone.

Issues commonly contained in phishing e-mails

Below are some issues a phishing e-mail may inquire about to trick users.

- *Account issues* - account or password expiring, account being hacked, account out-of-date, or account information needing to be changed.
- *Credit card or other personal information* - credit card expiring or being stolen, incorrect social security number or other personal information, or duplicate credit card or other personal information.
- *Confirming orders* - a request for you to log in to confirm recent orders or transactions.

Common companies affected by phishing attacks

Below is a listing of companies phishers often try to attack.

- Any major bank.
- Popular websites, such as Amazon, Facebook, Gmail, MySpace, PayPal, eBay, Microsoft, Apple, YouTube, etc.
- Government: FBI, CIA, IRS, etc.
- Internet service providers, such as AOL, Cox, MSN, XFinity, etc.
- Casinos and lottery.
- Online dating or community websites.

I've fallen for a phishing attack, what should I do?

If you've read this page too late and have already fallen for a phishing attack, log into your account from the company's page and change your password immediately. Also, it is a good idea to scan your computer for malware, in case the site has infected your computer. Finally, if the company supports two-factor authentication, it is also a good idea to enable this feature on your account.

If you believe personal information was stolen, it is also a good idea to watch all your accounts for suspicious activity.

Avoiding Scams and Fraud

Scam Glossary - FCC

COVID-19 Scams

Phone scammers are preying on consumer fears over the novel coronavirus (COVID-19) pandemic, calling and texting with scam offers for free home testing kits, bogus cures, fake health insurance, and more. Learn more and listen to scam call audio.

The FCC scam glossary describes robocall scams, spoofing scams and related consumer fraud, which the FCC tracks through complaints filed by consumers, news reports, and notices from other government agencies, consumer groups and industry sources. Glossary entries include links to more detailed information posted in the Consumer Help Center and to trusted external sources.

#	
809 Scam	A scammer leaves an urgent voicemail and a call-back number with an 809 area code. While it appears to be a three-digit U.S. area code, it's actually an international number. If you call, you'll be charged international rates while the person answering tries to keep you on the line as long as possible. Similar to the "One Ring" Scam.
90# Scam	Someone impersonating a telephone company employee calls your landline phone and asks you to dial 90# to connect to an outside line. This enables them to bill their calls to your account.
A	
Appliance Repair Scams (Better Business Bureau)	Scammers post fake customer-service numbers that show up in web search engine results. When you call, a "representative" asks for your personal info and a deposit. But instead of fixing your appliance, they steal your money and sell or keep your personal info for future scams.
Auto Warranty Scam	A scammer calls you with a sales pitch for renewing your auto warranty or insurance policy. The scammer may have acquired information about your car and its existing warranty to make the offer seem more credible.
B	

Back-to-School Scams	Calls or messages to college students may offer what seem to be official scholarships, house rentals, roommate arrangements, loans or tech support, with the aim of maliciously acquiring sensitive information or money.
Banking/Credit Card Scams (USA.gov)	Scammers sometimes pose as bank or credit card representatives calling about an unauthorized withdrawal from your account or suspicious use of your card. They may spoof the number of your bank to fool you, then ask you to confirm your account info, password or security information to steal your money.
Bank Account Smishing	You get a text message that seems to be from a bank, telling you a hold has been placed on an account in your name and providing a link to reactivate it. Selecting the link may download malicious software, giving scammers access to banking and other information on your phone.

C

Callback/Voicemail Scams	Scam callers leave voicemails threatening legal action if you don't call back. Our guidance is: Never call back an unfamiliar number, because it may lead to a scam.
"Can You Hear Me" Scam	Scammers open by asking a yes-or-no question, such as: "Can you hear me?" or "Is this X?" Their goal is to record you saying "yes" in response. They then may use that recording to authorize charges over the phone.
Catfishing/Online Dating Scams (FBI)	Catfishers create fake identities on dating apps and social media to coax you into fake online relationships. They often quickly move to personal channels such as phone or email, using your trust to acquire money or personal info, or help you hide their criminal activities. You'll probably never meet them in person.
Cellphone Cloning	Scammers illegally monitor radio wave transmissions to intercept unique identifying numbers that cell phones transmit. They then modify their own phones to broadcast these numbers, cloning the legitimate phone ID, so their calls and data use are charged to the cloned account.

Cellphone Subscriber Fraud	If scammers already have some of your personal information, they may use it to sign up for cell phone service in your name. That way, while they make the calls, you pay the bill.
Charity Scams	Scammers call asking for charitable donations, often after large-scale disasters. They may make up phony charities or spoof a real charity to trick you out of your money.
Chinese Consulate Scam	Scammers, speaking Mandarin, pose as Chinese consulate employees. They may request money for a family member who they say is in trouble or ask for personal information for a parcel delivery. Sometimes they claim the call is related to a criminal investigation.
Collect Call Dialing Scam	By buying up toll-free numbers a few digits away from well-known carriers, some companies try to profit from collect call misdials. They often charge higher fees than the carrier you intended to use.
COVID-19/Coronavirus Scam	Phone scammers are preying on fears over the novel coronavirus (COVID-19) pandemic, calling and texting consumers with scam offers for free home testing kits, bogus cures, fake health insurance, and more. Learn more and hear audio from real scam calls.
Cramming	Cramming is when phone companies or third-party billing companies place misleading, unauthorized, deceptive or poorly explained charges on a phone bill.
Credit Card/Interest Rate Scams	Scam callers pretending to represent banks and credit card companies use a variety of tactics, such as bogus fraud alerts or promises of lowered interest rates, to steal your personal information and your credit.
Cryptocurrency Scams (Federal Trade Commission)	A crypto scammer may call claiming to be from the government, a local utility company, or even a romantic interest directing you to withdraw money from your bank account.

D	
Department of Homeland Security Scam (DHS.gov)	Scammers spoofing the DHS number call people to falsely claim that they are victims of identity theft or, in a variation, to threaten arrest. The scammers request payment or personal information to resolve the issue.
Disaster Relief Scam	After disasters, some callers may impersonate charities, seeking disaster aid. Before giving money, verify that you're talking with a real charity.
E	
Email/Phishing Scams (Federal Trade Commission)	Scammers often use email "phishing" to hook unsuspecting fraud victims. Treat all unsolicited email and spam as suspicious: Do not open or reply. To avoid loading malicious software onto your computer or device, never click a link – even from a trusted source – unless you've verified its authenticity. Be especially wary of emails asking for emergency funds or help from friends, family and colleagues. Their email accounts may have been hacked. Scammers will also pretend to be government agencies in scam emails.
Employment Scam (Better Business Bureau)	Bogus job postings, recruitment emails and online ads - often illegally using legitimate company names – are all tools scammers use to defraud people seeking employment. Always be suspicious of quick offers with high salaries or pre-payment requests for coaching, training or certifications, and never share personal information until you're certain a job posting is legitimate. Many employment scams also offer advanced payment for supplies. These checks will often bounce, costing you money.
F	
FBI Arrest Scam (FBI.gov)	Scammers spoof FBI field office numbers and call claiming that they have a warrant for your arrest. They then demand payment to rescind the warrant. An alternate version of this scam threatens international students with deportation.

Free Trial Scams (Federal Trade Commission)	Free-trial product offers you receive over the phone may be too good to be true. You may be asked to pay a small fee by credit card, which can lead to other unwanted fraudulent charges, or you may be unable to cancel after the trial runs out, forcing you to pay for the product in question.
Flood Insurance Scam	After floods, scammers may target hard hit areas with fake calls about flood insurance to steal private information or money. They may spoof a legitimate flood insurance company to appear more convincing.
G	
Gift Card Scams (Federal Trade Commission)	A telltale sign of phone scams is if the caller asks you to make a payment with a gift card. Many scammers prefer this non-refundable and hard to trace form of payment.
Google Listing Scams (Google My Business Help)	Some scammers claim that they can add or remove you or your business from Google searches or similar services. These callers, unaffiliated with Google, seek payment for services they can't deliver.
Government Grant Scam (Federal Trade Commission)	Scammers claim that you are eligible for a government grant and offer to forward it to your checking account as soon as you give them your account information, which they sell or use to steal your money. The scammer may spoof the number of the government agency they claim to be representing.
Grandparent/Family Emergency Scam	Scammers sometimes prey on grandparents by claiming their family members are in jail or in trouble and need money quickly. They use stolen personal information such as family member names and hometowns to seem more convincing.
H	
Health Insurance Scam	Scammers call peddling phony health care coverage at discounted rates. Callers sometimes use spoofing to impersonate government officials or insurance companies. Often the products they sell are medical discount cards that end up not being accepted anywhere. While fraudulent solicitations occur year-round, be especially vigilant during open enrollment season.

Holiday Charity Scams	Don't let scammers stifle your charitable spirit. A little advanced research can ensure your contributions are reaching the intended recipients. Learn how to avoid becoming a victim of holiday charity scams.
I	
Identity Theft Scams (USA.gov)	Callers posing as government officials, often from the Social Security Administration, claim that you've been a victim of identity theft. These scammers ask for personal information or payment of some kind, or access to your bank account.
Imposter Scam (Federal Trade Commission)	A caller poses as someone you know or trust in order to obtain money or personal information. They often spoof a legitimate caller's number to appear more realistic.
Interest Rate/Credit Card Scams	Scam callers pretending to represent banks and credit card companies use a variety of tactics, such as bogus fraud alerts or promises of lowered interest rates, to steal your personal information and your credit.
Investment Scams (Securities and Exchange Commission)	When a caller claims to have a promising investment opportunity that will help you get rich quick, it's likely a scam.
IRS Call Scam	Scammers sometimes pose as IRS agents, threatening legal action and demanding money or personal information over the phone. To appear legitimate, imposters may attempt to spoof an IRS number.
J	
Juice Jacking	When traveling, don't get juice jacked when charging your device at public USB ports found in airports, trains, hotels and elsewhere. Reports say charging ports and cords can be hacked to infect devices with malware.

Jury Duty Scams (U.S. District Court, Washington D.C.)	Callers pose as local law enforcement, claiming they have a warrant for your arrest because you missed jury duty. They may instruct you to pay a fine by wiring money or using gift cards.
K	
Kidnapping Scams (National Institutes of Health)	Scammers may call you claiming to have kidnapped family members. They often use stolen information and spoof the family member's phone to make the scenario seem more realistic
L	
Lottery/Sweepstakes Scams (Federal Trade Commission)	These scams involve someone claiming you won a prize. However, they say you must pay a fee or provide sensitive banking information in order to get it. They keep the money, and you get nothing for it.
Low Power FM Radio Scam	LPFM Radio applicants may receive phone calls or messages offering to help with the application process or prompting them to buy a "Part 15" device for a fee. Their expertise or expensive devices aren't needed. The FCC authorizes all licenses for LPFM radio stations.
M	
Medical Device Scams (Health and Human Services)	Calls or ads offering free services or medical devices purportedly covered by Medicare – such as an orthopedic back, neck or knee brace – are mostly likely scams. If you don't need or qualify for such devices or services, either you or Medicare gets bilked. This scam is often just a ruse to steal your Medicare account info.
Medicare Card Scam	With the rollout of new Medicare cards, scammers may pose as Medicare representatives who say they need payment or personal info before the cards can be issued. They may also ask for the number on your new Medicare card in order to activate it.
Mexico Collect Call Scam	Operators say you have a collect call from a family member in Mexico, sometimes even providing the family member's name. You accept the call, but it's from a stranger who offers no information about family members. You end up being billed regardless.

N	
Nanny/Care Giver Scam (Federal Trade Commission)	Sometimes scammers post fake job listings for nannies or care givers. They offer a job but ask you to buy supplies or other equipment upfront. They may send you a post-dated check and ask you to purchase gift cards or transfer money to a vendor. The check inevitably bounces.
Neighbor Spoofing	Scammers spoof caller ID information that displays the same initial digits as your own phone number (usually the first six), making it seem like someone else with a local number is trying to reach you.
O	
One Ring/Wangiri Scam	When your phone rings only once, late at night, you may be tempted to call back. But the call may be from a foreign country with an area code that looks deceptively like it's in the U.S. If you dial back, international calling fees may wind up on your bill. Such cons are also known by the Japanese term "Wangiri."
Online Dating Scams/Catfishing (FBI)	Catfishers create fake identities on dating apps and social media to coax you into fake online relationships. They often move quickly to personal channels such as phone or email, using your trust to acquire money or personal info, or help you hide their criminal activities. You'll probably never meet them in person.
Open Enrollment Scams	During the yearly health-care open enrollment season, scam callers may offer fake insurance plans to swindle you out of money. They may spoof a legitimate insurance company's phone number so you'll think the call is authentic.
P	
Phishing/Email Scams (Federal Trade Commission)	Scammers often use email "phishing" to hook unsuspecting fraud victims. Treat all unsolicited email and spam as suspicious: Do not open or reply. To avoid loading malicious software onto your computer or device, never click a link – even from a trusted source – unless you've verified its authenticity. Be especially wary of emails asking for emergency funds or help from friends, family and colleagues. Their

	email accounts may have been hacked. Scammers will also pretend to be government agencies in scam emails.
Porting	A scammer gets your name and phone number, then gathers other identifiable information that can be used for identity theft. Pretending to be you, they then contact your mobile provider to report your phone as stolen or lost, and ask for the number to be "ported" to another provider and device. They can use your number to gain access to your financial accounts and other services with two-factor authentication enabled.
R	
Recovery Scams (Federal Trade Commission)	If you've already fallen for a scam, another scammer may call you and offer to get you your money back for a fee. Their goal is to double dip and steal more of your money.
Romance Scam	Romance scammers contact you through dating apps or social media to try to establish a romantic relationship with you in order to access your money or personal information. Scammers use fake identities and back stories to gain your trust.
S	
Slamming	Slamming is when a phone company illegally switches you from your existing phone service company to their own service without your permission, then bills you for service you did not request.
Smishing	Short for "SMS phishing," smishing often involves text messages claiming to be from your bank or another company. The message displays a phone number to call or a link to click, giving scammers the chance to trick you out of money or personal information.
Social Security Number Scam	Scammers may pose as government officials, often from the Social Security Administration, to request your Social Security Number or a payment of some sort. Sometimes, they claim your SSN is suspended. The call may spoof what appears to be a legitimate Social Security Administration number.

Spoofing	Spoofing occurs when a caller maliciously transmits false caller ID information to increase the likelihood that you'll answer. Scammers often spoof local numbers, private companies, government agencies and other institutions.
T	
Tech Support Scams	Phone scammers may masquerade as tech support employees for a major company in order to take your money or install a virus on your computer. They may call from what seem to be legitimate company numbers using caller ID spoofing.
Two Factor Authentication Scams (Federal Trade Commission)	Scammers call your carrier, asking them to port your number to their phone. They then use two factor authentication via text message to access personal and financial accounts, resetting your passwords and taking over the accounts.
U	
Utility Scams	Scammers posing as utility company employees warn that they need payment quickly, often with a pre-paid card, or else your service will be turned off. Businesses run by native Spanish speakers have also been targeted by this scam.
V	
Veteran Benefits Scam	These scams involve callers claiming that veterans are eligible for new benefits, often relating to home loans, to acquire personal and financial information. The caller may even spoof a legitimate benefits organization.
Voicemail/Callback Scams	Scam callers leave voicemails threatening legal action if you don't call back. Our guidance is: Never call back an unfamiliar number, because it may lead to a scam.

Voicemail Hacking Scam	Hackers guess default voicemail passwords (like "1234") and change voicemail greetings on phones to verbally accept collect call charges. They then use the phone to make international calls, costing you money.

W

Wangiri/One Ring Scam	When your phone rings only once, late at night, you may be tempted to call back. But the call may be from a foreign country with an area code that looks deceptively like it's in the U.S. If you dial back, international calling fees may wind up on your bill. Such cons are known by the Japanese term "Wangiri."

CREDIT CARD ALERTS TO PROTECT AGAINST FRAUD

How To Set Up Purchase and Fraud Alerts

Setting up alerts is simple and straightforward on any mobile app. Users can find notification settings either in the app's settings or in the user's profile. Below are instructions for setting up purchase and fraud alerts for the most popular credit card mobile apps.

Make sure your phone allows notifications from the credit card banking app of choice. To double-check, go to the phone's settings and search for the specific banking app to enable push notifications.

American Express Mobile App

1. Tap "Account" on the bottom-right corner of the screen
2. Tap "Notifications"
3. Turn on "Purchase Alerts" and enable "Account Protection" to receive alerts

Chase Mobile App

1. Enter profile by tapping the profile icon on the top-right corner of the screen
2. Under "Alerts," tap "Manage Alerts"
3. Select an account to edit alerts for
4. Tap "Balance & Spending" to set up purchase alert push notifications
5. Or, tap "Security alerts" to set up fraud alert push notifications

Citi Mobile App

1. Head to your profile and select "Account Alerts" (or Search "Account Alerts")
2. Go to "Spending"
3. "Transaction Amount Exceeds" turn on, and set to $1.00
4. "Card Not Present" turn on
5. International Transaction turn on
6. Set all of the above to "text" or "push text"
7. Pick which alerts you would like to set notifications for, including "Account Balance," "Balance Amount Exceeds," "Approaching Credit Limit" and "Over Credit Limit."

CAPITOL ONE

Instant purchase notifications

Keep track of your spending in real time. When you set up instant purchase notifications in the Capital One Mobile app (steps below), you can receive an alert any time a transaction is approved on your card.[1] You can enable notifications that include the amount of the purchase and information about the merchant.

CREDIT CARD ALERTS TO PROTECT AGAINST FRAUD

To enable notifications, follow these steps:

1. Log in and tap on the “Profile” tab.
2. Tap on “Alerts & Notifications.”
3. Select the card you want to set up alerts for.
4. Tap on “Instant Purchase Notification.”
5. Select your alert preference: push notifications, email or SMS.
6. Choose a desired dollar amount minimum. (Tip: Choosing $0 is great for tracking all purchases.)
7. Tap “Save,” and you’re all set!

Avoiding Scams and Fraud

Tips That Can Help You Avoid Texting Scams

Keep your guard up by:

- Do not respond to texts from unknown numbers, or any others that appear suspicious.
- Never share sensitive personal or financial information by text.
- Think twice before clicking any links in a text message. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they weren't hacked.
- If a business sends you a text that you weren't expecting, call them to verify its authenticity using the number on your bill or statement, or look up their number online.
- Remember that government agencies almost never initiate contact by phone or text.
- Report texting scam attempts to your wireless service provider by forwarding unwanted texts to 7726 (or "SPAM").
- File a complaint with the FCC.
- If you think you're the victim of a texting scam, report it immediately to your local law enforcement agency and notify your wireless service provider and financial institutions where you have accounts.

AARP - 14 Top Scams to Watch Out for in 2023

Criminals are quick to exploit current events and add new twists to well-known ruses

By: Patrick J. Kiger and Sari Harrar,

Published January 04, 2023 / Updated April 12, 2023

Scammers are like viruses: They continually evolve in response to the latest news and trends, using them for new ways to separate us from our cash.

These criminals "are so adaptable, they're going to just follow the headlines," says Amy Nofziger, director of fraud victim support for AARP. As she and other anti-fraud experts note, scammers have proved ingenious when it comes to updating traditional criminal operations such as the romance scam or the Ponzi scheme with new twists to make them more convincing and effective. And like the rest of society, scammers are increasingly going online.

"Most con artists have taken a digital-first approach to scamming," says Josh Planos, vice president of communications and public relations for the Better Business Bureau (BBB). He notes that the vast majority of today's scams originate through a digital on-ramp, such as social media or email.

Here are 14 emerging scams that anti-fraud experts are tracking in 2023, along with tips on how to thwart the crooks.

1. Cryptocurrency-romance scam

Crooks combine crypto scams with old-fashioned romance scams, posing as internet love interests so they can cajole their targets into downloading an app and investing in fake crypto accounts. "They claim that they're even putting some of their own money into your fund," explains former Federal Trade Commission official Steve Baker, who publishes the Baker Fraud Report. While the app displays data that seems to show your wealth growing, criminals are just taking your money.

How to stay safe: Carefully scrutinize any investment opportunity, even if you think you're a sophisticated investor. "People think it's not going to happen to them, but it is happening to many, which is why you have to keep your guard up," Nofziger says.

No matter where you live, fraud is never far away. Report a scam or search for existing scams near you.

2. Payday loan scam

Criminals exploit the inflation squeezing workers by offering fake payday loans that they claim will help people settle their bills, according to Nofziger. Loan applicants are told they'll need to prepay a fee. The money goes into the crooks' pockets, and the applicant gets nothing.

How to stay safe: Be wary of anyone who asks you to pay any sort of loan fee with a gift card or some other nontraceable form of payment.

3. One-time password (OTP) bot scam

Credit reporting company Experian warns that scammers utilize bots — automated programs — to deceive people into sharing the two-factor authentication codes sent to them via text or email from financial institutions (or from companies such as Amazon). The bot will make a robocall or send a text that appears to come from a bank, asking you to authorize a charge, then it asks you to enter the authentication code you've just been sent if the transaction isn't yours. It's actually the bot that's trying to log into your bank account, and it wants the code that the bank sent to you as a precaution, so it can get in.

How to stay safe: Never share authentication codes, or provide other information, in response to an unsolicited phone call or text.

4. Student loan forgiveness scam

The Biden administration's plan to forgive student loans faces an uncertain future after being tied up in the courts, but that hasn't stopped scammers from trying to take advantage of people who may not have heard it's on hold. They've built phony application sites aimed at stealing applicants' Social Security numbers and bank information, and sometimes they contact targets by phone, pressuring them into applying and charging a fee for their help. The scam still has legs, "because there's so much debt that people are carrying and they're looking for a way to get rid of it," explains Michael Bruemmer, vice president of the data breach group and consumer protection at Experian.

How to stay safe: Go to the Department of Education's student aid website to keep track of the proposed forgiveness program's status.

5. Puppy purchase scam

Scammers try to exploit dog lovers by offering cute puppies for sale on the web. In one instance documented by the BBB, a woman paid $850 for a Dalmatian puppy, only to receive additional requests for money — first $725 for travel insurance for the dog, then $615 for a special crate. In the end, the buyer lost $2,200 and never got the puppy — which didn't actually exist.

How to stay safe: Go to an animal shelter and check out the dogs available there, before you search online. If you spot a puppy you like on a website, do a reverse image search to make sure

it's not a photo stolen from some other site. Insist on seeing the pet in person before paying any money.

6. Check washing scam

Though other payment modes are replacing them, checks are still used often enough for scammers to exploit. One trick is "check washing," in which crooks steal checks from mailboxes and bathe them in household chemicals to erase the original name and dollar amount, leaving blank spaces they can fill in. It's possible to convert a $25 check to one for thousands of dollars.

How to stay safe: The U.S. Postal Inspection Service recommends depositing your outgoing mail in blue collection boxes before the day's last pickup, so it doesn't sit for as long. At home, avoid leaving mail in your own mailbox overnight, and have your mail held by the post office or picked up by a friend or neighbor if you're going to be away.

7. Free-gift QR code scam

This is a variation on a basic QR code scam that the FBI warned about: Scammers put fake codes over real ones to exploit the convenience of the barcodes people scan into their phones to see restaurant menus or make payments. Experian's Bruemmer says scammers may call and say they're going to send a QR code to your phone, so you can receive a free $100 gift card. In reality, the QR code may take you to a malicious website.

How to stay safe: If you receive a QR code out of the blue, contact the person or company that supposedly sent it, to make sure it is for real. Use a phone number you know is authentic.

8. `Oops, wrong number!' texts

Seemingly misdirected messages are increasingly the start of a scammer's ploy. A text message addressed to someone else pops up on your phone. It seems urgent — a rescheduled business meeting, or maybe a romantic get-together. You text back, "Sorry, wrong number!" The scammer keeps up the friendly texts, and may eventually invite you to join an adult website to see revealing pictures so you hand over credit card info and money, or try to convince you to make a cryptocurrency investment (and take your money).

How to stay safe: Don't respond to texts from numbers you don't recognize. Don't click on links in them or respond with "STOP" if the messages say you can do this to avoid future messages. Block the phone numbers they come from.

9. Fake barcodes on gift cards

Law enforcement agencies warn that nimble-fingered crooks affix fake barcode stickers over the real ones on the back of gift cards in stores. When you purchase the card, the cashier scans the fake barcode at checkout — directing your money into the scammer's gift card account.

How to stay safe: With some gift cards, you can make sure the number of the barcode matches the number on the packaging. Or feel or gently scratch the barcode on a gift card before buying. Don't purchase if the barcode is on a sticker, or if the package is ripped, wrinkled, bent or looks tampered with.

10. Crypto refund swindles

Beware if you've lost money in a cryptocurrency scam: Criminals set up fake "get your crypto cash back" websites, including one that looks like it's from the U.S. Department of State. After luring targets, they contact those who respond by phone, email or social media and ask for personal ID information, including account numbers and passwords, plus an advance fee for their services payable by gift card, cryptocurrency or wire transfer. You get nothing, warns the FTC.

How to stay safe: Crypto investments aren't insured by the government the way bank accounts are. For the most part, funds lost to crypto scammers are gone. Don't trust anyone who contacts you saying they can get your money back, says Frank McKenna, chief fraud specialist for the fraud detection company Point Predictive.

11. Bank impersonator racket

Let's say you've set up your bank or credit card online accounts so you can access them only with a live code sent from the institution. And let's say a criminal has your bank or credit card username and password login and wants to steal from you. What would he or she do? In this increasingly common fraud, they call you, claiming to be from your bank and warning about a problem with your account. The caller tells you they're emailing or texting you a "onetime passcode" for logging in and asks you to read it back to them for verification. In reality, the scammer's login attempt triggered your bank to send you the passcode. Handing it over gives criminals full access to your account.

How to stay safe: Never give your onetime passcode to anyone who calls you. Hang up, find your institution's phone number on a bank statement or on your credit card, and call. Ask if there really is a problem and report the con to the bank's fraud department, McKenna recommends.

12. LinkedIn relationship fakes

A criminal might send you a message on LinkedIn, claiming to be just starting out in the same industry you're in, seeking advice from a more experienced colleague. It's flattering and fun to be a mentor, so you agree. You get to know each other, and eventually they ask to move your conversation onto a personal device, then lure you into a scam.

How to stay safe: A request to continue your chat on a more private channel is a warning. So is talking up crypto. LinkedIn may flag requests to go off-platform as it tries to remove fake accounts. But you should end the conversation and block the scammer.

13. ‘I’ve got your package, where’s your house?’ hoax

New package delivery scams include texts and phone calls purportedly from a professional-sounding delivery driver who can’t find your house. Didn’t order anything? They may try to convince you someone’s sent a gift. Or you may receive an email about rescheduling a drop-off or a fake “package delivery attempt” sticker on your front door. Their goal? To get you to provide personal information or simply click on a link they provide. That link then downloads malware that will harvest passwords and account info from your computer.

How to stay safe: Contact the seller or delivery service using a verified phone number, the FCC recommends. Don’t use numbers or links provided by potential scammers.

14. Out-of-stock item scam

Scammers often place fake ads on social media sites for products at too-good-to-be-true prices, take your order and payment info, then tell you the item’s not available right now. Your refund is on the way, they promise, but it never arrives. And you can’t reach anyone at the company about it.

How to stay safe: Research businesses online before you buy, and only shop on secure websites with a lock symbol in the browser bar and an internet address that begins with “https.” And pay by credit card, the FTC recommends. That way, you can withhold payment pending an investigation.

Patrick J. Kiger is a contributing writer for AARP. He has written for a wide variety of publications, including the Los Angeles Times Magazine, GQ *and* Mother Jones*, and for websites of the Discovery Channel and National Geographic.*

Sari Harrar is a contributing writer to AARP The Magazine *and writes frequently for the* AARP Bulletin *and others on fraud, health and consumer affairs.*

HARVARD UNIVERSITY EMPLOYEES CREDIT UNION

Understanding the Difference Between Frauds and Scams

May 10, 2021 3:25:07 PM

There are plenty of similarities between frauds and scams, and probably the biggest similarity is – you don't want to be a victim of either! However, when it comes to protecting yourself and your finances, it's also important to understand the differences between the two. What's a fraud and what's a scam? How are they similar and different, and how can you avoid them?

Definitions: Fraud vs. Scam

Colloquially, the terms "fraud" and "scam" are used interchangeably to refer to any kind of financial wrongdoing. Legally speaking, fraud usually refers to a broader and more serious crime, with scams representing one type of fraud.

A good example is elder fraud, which unfortunately continues to be a major problem affecting millions of Americans every year. Under the broad category of elder fraud, specific scams include lottery scams, in which victims are asked to pay a fee to access their windfall; romance scams, capitalizing on victims' desires to find a companion; and tech support scams, wherein criminals attempt to gain remote access to a computer or cell phone.

Other types of fraud include charity and disaster fraud, credit card fraud, impersonation fraud, investment fraud, and more. In order to protect ourselves and our loved ones, it's a good idea to speak up about the overarching problem of fraud in general, as well as to discuss specific scams to look out for – while keeping in mind that scammers are revising their strategies all the time.

Common Frauds and Scams

Sadly, the coronavirus pandemic has led to a number of new scams. Watch out for funeral expense scams where criminals pose as officers from the Federal Emergency Management Agency (FEMA) and request personal details to help you register for funeral expense benefits; vaccine scams claiming to offer early access to the inoculation for a fee; and Social Security scams in which the scammer will falsely say that benefits can't be paid out during the pandemic unless they receive personal information or a mailed-in fee.

Digital fraud is a broad category encompassing many of the most common types of scams, such as phishing emails, malware, and identity theft via a compromised email account. While not all internet fraud can be avoided – especially where large-scale data breaches are concerned – it is

possible to protect yourself from internet scams by taking a few simple precautions. Don't open emails or online messages from senders you don't recognize, and beware of sender addresses that look official but include one or two odd characters or a spelling mistake. If you receive any digital communication asking for money, personal information, or directing you to download an attachment – proceed with caution and don't act in haste. Scammers rely on victims' panic to cloud their judgement, so if you feel any kind of pressure, this is a good sign that a scam might be afoot.

While online fraud is a common way for scammers to find new victims, it's equally important to be on the lookout for scams taking place on more traditional communication channels. Whether it's a telephone call from a strange number or a piece of snail mail from an organization that sounds legitimate, the best course of action is almost always the same: don't act fast, don't share personal or financial information, take the time to verify who's contacting you, and if you need, re-initiate the conversation through an official channel to get more information.

What Happens Next?

When you're impacted by a fraud or scam, call up your credit union, bank, or credit card issuer to confirm if any money has been stolen and to get their assistance in blocking access to your accounts. If you suspect identity theft, you can request a free security freeze to prevent the scammer from opening any lines of credit in your name. No matter what kind of fraud or scam you're facing, it's always a good idea to say something to someone you trust, as soon as possible.

You can help other potential victims by reporting the fraud to the Federal Trade Commission (FTC) at https://reportfraud.ftc.gov. The FTC also publishes information about fraud, unwanted calls, and other consumer issues currently affecting people in your state and around the country – a useful resource if you want to learn more about what scams to watch out for.

What To Know About Cryptocurrency and Scams

Confused about cryptocurrencies, like bitcoin or Ether (associated with Ethereum)? You're not alone. Before you use or invest in cryptocurrency, know what makes it different from cash and other payment methods, and how to spot cryptocurrency scams or detect cryptocurrency accounts that may be compromised.

What To Know About Cryptocurrency

What is cryptocurrency?

Cryptocurrency is a type of digital currency that generally exists only electronically. You usually use your phone, computer, or a cryptocurrency ATM to buy cryptocurrency. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrencies, and new ones keep being created.

How do people use cryptocurrency?

People use cryptocurrency for many reasons — quick payments, to avoid transaction fees that traditional banks charge, or because it offers some anonymity. Others hold cryptocurrency as an investment, hoping the value goes up.

How do you get cryptocurrency?

You can buy cryptocurrency through an exchange, an app, a website, or a cryptocurrency ATM. Some people earn cryptocurrency through a complex process called "mining," which requires advanced computer equipment to solve highly complicated math puzzles.

Where and how do you store cryptocurrency?

Cryptocurrency is stored in a digital wallet, which can be online, on your computer, or on an external hard drive. A digital wallet has a wallet address, which is usually a long string of numbers and letters. If something happens to your wallet or your cryptocurrency funds — like your online exchange platform goes out of business, you send cryptocurrency to the wrong person, you lose the password to your digital wallet, or your digital wallet is stolen or compromised — you're likely to find that no one can step in to help you recover your funds.

How is cryptocurrency different from U.S. Dollars?

Because cryptocurrency exists only online, there are important differences between cryptocurrency and traditional currency, like U.S. dollars.

- **Cryptocurrency accounts are not backed by a government.** Cryptocurrency held in accounts is **not** insured by a government like U.S. dollars deposited into an FDIC insured bank account. If something happens to your account or cryptocurrency funds — for

example, the company that provides storage for your wallet goes out of business or is hacked — the government has no obligation to step in and help get your money back.
- **Cryptocurrency values change constantly.** The value of a cryptocurrency can change rapidly, even changing by the hour. And the amount of the change can be significant. It depends on many factors, including supply and demand. Cryptocurrencies tend to be more volatile than more traditional investments, such as stocks and bonds. An investment that's worth thousands of dollars today might be worth only hundreds tomorrow. And, if the value goes down, there's no guarantee it will go up again.

Paying With Cryptocurrency?

There are many ways that paying with cryptocurrency is different from paying with a credit card or other traditional payment methods.

- **Cryptocurrency payments do not come with legal protections.** Credit cards and debit cards have legal protections if something goes wrong. For example, if you need to dispute a purchase, your credit card company has a process to help you get your money back. Cryptocurrencies typically do not come with any such protections.
- **Cryptocurrency payments typically are not reversible.** Once you pay with cryptocurrency, you can usually only get your money back if the person you paid sends it back. Before you buy something with cryptocurrency, know the seller's reputation, by doing some research before you pay.
- **Some information about your transactions will likely be public.** People talk about cryptocurrency transactions as anonymous. But the truth is not that simple. Cryptocurrency transactions will typically be recorded on a public ledger, called a "blockchain." That's a public list of every cryptocurrency transaction — both on the payment and receipt sides. Depending on the blockchain, the information added to the blockchain can include details like the transaction amount, as well as the sender's and recipient's wallet addresses. It's sometimes possible to use transaction and wallet information to identify the people involved in a specific transaction. And when you buy something from a seller who collects other information about you, like a shipping address, that information can also be used to identify you later on.

How To Avoid Cryptocurrency Scams

Scammers are always finding new ways to steal your money using cryptocurrency. To steer clear of a crypto con, here are some things to know.

- **Only scammers demand payment in cryptocurrency.** No legitimate business is going to demand you send cryptocurrency in advance – not to buy something, and not to protect your money. That's always a scam.

- **Only scammers will guarantee profits or big returns.** Don't trust people who promise you can quickly and easily make money in the crypto markets.

- **Never mix online dating and investment advice**. If you meet someone on a dating site or app, and they want to show you how to invest in crypto, or asks you to send them crypto, that's a scam.

Spot crypto-related scams

Scammers are using some tried and true scam tactics — only now they're demanding payment in cryptocurrency. Investment scams are one of the top ways scammers trick you into buying cryptocurrency and sending it on to scammers. But scammers are also impersonating businesses, government agencies, and a love interest, among other tactics.

Investment scams

Investment scams often promise you can "make lots of money" with "zero risk," and often start on social media or online dating apps or sites. These scams can, of course, start with an unexpected text, email, or call, too. And, with investment scams, crypto is central in two ways: it can be both the investment and the payment.

Here are some common investment scams, and how to spot them.

- **A so-called "investment manager" contacts you out of the blue.** They promise to grow your money — but only if you buy cryptocurrency and transfer it into their online account. The investment website they steer you to looks real, but it's really fake, and so are their promises. If you log in to your "investment account," you won't be able to withdraw your money at all, or only if you pay high fees.

- **A scammer pretends to be a celebrity who can multiply any cryptocurrency you send them.** But celebrities aren't contacting you through social media. It's a scammer. And if you click on an unexpected link they send or send cryptocurrency to a so-called celebrity's QR code, that money will go straight to a scammer and it'll be gone.

- **An online "love interest" wants you to send money or cryptocurrency to help you invest.** That's a scam. As soon as someone you meet on a dating site or app asks you for money, or offers you investment advice, know this: that's a scammer. The advice and offers to help you invest in cryptocurrency are nothing but scams. If you send them crypto, or money of any kind, it'll be gone, and you typically won't get it back.

- **Scammers guarantee that you'll make money or promise big payouts with guaranteed returns**. Nobody can make those guarantees. Much less in a short time. And there's nothing "low risk" about cryptocurrency investments. So: if a company or person promises you'll make a profit, that's a scam. Even if there's a celebrity endorsement or testimonials from happy investors. Those are easily faked.

- **Scammers promise free money**. They'll promise free cash or cryptocurrency, but free money promises are always fake.

- **Scammers make big claims without details or explanations.** No matter what the investment, find out how it works and ask questions about where your money is going. Honest investment managers or advisors want to share that information and will back it up with details.

Before you invest in crypto, search online for the name of the company or person and the cryptocurrency name, plus words like "review," "scam," or "complaint." See what others are saying. And read more about other common investment scams.

Business, government, and job impersonators

In a business, government, or job impersonator scam, the scammer pretends to be someone you trust to convince you to send them money by buying and sending cryptocurrency.

- **Scammers impersonate well-known companies.** These come in waves, and scammers might say they're from Amazon, Microsoft, FedEx, your bank, or many others. They'll text, call, email, or send messages on social media — or maybe put a pop-up alert on your computer. They might say there's fraud on your account, or your money is at risk — and to fix it, you need to buy crypto and send it to them. But that's a scam. If you click the link in any message, answer the call, or call back the number on the pop-up, you'll be connected to a scammer.

- **Scammers impersonate new or established businesses offering fraudulent crypto coins or tokens.** They'll say the company is entering the crypto world by issuing their own coin or token. They might create social media ads, news articles or a slick website to back it all up and trick people into buying. But these crypto coins and tokens are a scam that ends up stealing money from the people who buy them. Research online to find out whether a company has issued a coin or token. It will be widely reported in established media if it is true.

- **Scammers impersonate government agencies, law enforcement, or utility companies.** They might say there's a legal problem, that you owe money, or your accounts or benefits are frozen as part of an investigation. They tell you to solve the problem or protect your money by buying cryptocurrency. They might say to send it to a wallet address they give you — for "safe keeping." Some scammers even stay on the phone with you as they direct you to a cryptocurrency ATM and give step-by-step instruction on how to insert money and convert it to cryptocurrency. They'll direct you to send the crypto by scanning a QR code they give you, which directs the payment right into their digital wallet — and then it's gone.

- **Scammers list fake jobs on job sites.** They might even send unsolicited job offers related to crypto like jobs helping recruit investors, selling or mining cryptocurrency, or helping convert cash to crypto. But these so-called "jobs" only start if you pay a fee in cryptocurrency. Which is always a scam, every time. As your first task in your "job," these scammers send you a check to deposit into your bank account. (That check will turn out to be fake.) They'll tell you to withdraw some of that money, buy cryptocurrency for

a made-up "client," and send it to a crypto account they give you. But if you do, the money will be gone, and you'll be on the hook to repay that money to your bank.

To avoid business, government, and job impersonators, know that

- No legitimate business or government will ever email, text, or message you on social media to ask for money. And they will never demand that you buy or pay with cryptocurrency.
- Never click on a link from an unexpected text, email, or social media message, even if it seems to come from a company you know.
- Don't pay anyone who contacts you unexpectedly, demanding payment with cryptocurrency.
- Never pay a fee to get a job. If someone asks you to pay upfront for a job or says to buy cryptocurrency as part of your job, it's a scam.

Blackmail scams

Scammers might send emails or U.S. mail to your home saying they have embarrassing or compromising photos, videos, or personal information about you. Then, they threaten to make it public unless you pay them in cryptocurrency. Don't do it. This is blackmail and a criminal extortion attempt. Report it to the FBI immediately.

How To Report Cryptocurrency Scams

Report fraud and other suspicious activity involving cryptocurrency to

- the FTC at ReportFraud.ftc.gov
- the Commodity Futures Trading Commission (CFTC) at CFTC.gov/complaint
- the U.S. Securities and Exchange Commission (SEC) at sec.gov/tcr
- the Internet Crime Complaint Center (IC3) at ic3.gov/Home/FileComplaint
- the cryptocurrency exchange company you used to send the money