AARP

Fraud Prevention

AARP Fraud Watch Network

Watchdog Alert Handbook:

Common Elements of Today's Scams — and How to Stay Safe

aarp.org/fraudwatchnetwork

INTRODUCTION

U.S. adults are collectively losing tens of billions of dollars every year. This may seem discouraging, but while criminals often use news headlines to inform their schemes, they do rely on elements that are common across scams. Knowing these common elements makes it easier to spot and avoid scams.

This booklet lays out the scam fundamentals. Spotting any of these tactics is a strong indication you are engaging with a criminal. If you find yourself in a scam situation, disengage immediately. If you have lost money or sensitive information, contact the police, tell them you are a victim of financial fraud and ask to file a report. Then file a report at **reportfraud.ftc.gov**. Though the chances of recovering losses is slim, your information will help investigators spot trends and possibly build cases. You can also turn to AARP's fraud support resources:

- If you or a loved one have been targeted by a scam or fraud, you are not alone. Our fraud specialists at the AARP Fraud Watch Network Helpline provide free support and guidance on what to do next. Call **877-908-3360**.
- If you've experienced fraud and are struggling in its aftermath, visit **aarp.org/fraudsupport** to learn about free, peer-led online sessions aimed at helping fraud victims begin healing emotionally.

ABOUT THE AARP FRAUD WATCH NETWORK

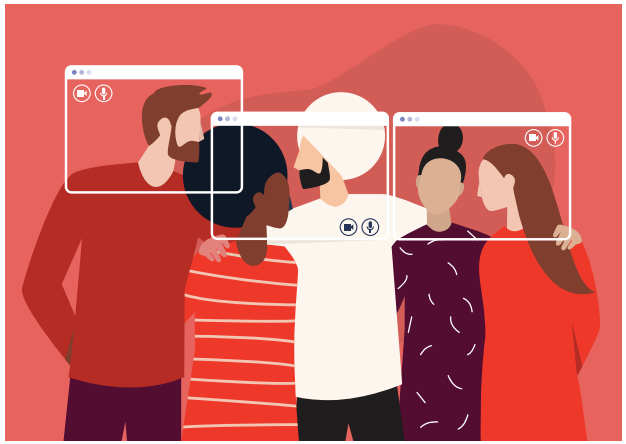
The AARP Fraud Watch Network is a free resource for all. With AARP as your partner, you'll learn how to proactively spot scams, get guidance from our fraud specialists if you've been targeted, and feel more secure knowing that we advocate at the federal, state and local levels to protect consumers and enforce the law.

To learn more, visit **aarp.org/fraudwatchnetwork**.

The Common Denominator: Using Our Emotions to Their Advantage

Perpetrators of financial crimes are adept at getting targets to believe they are someone they aren't, such as a government agency, a tech support provider, a retailer, even a relative in distress. And it can be hard to understand how victims accept a scammer's concocted story as true. But criminals have long known that the secret to their success is to use our emotions against us.

The first rule in the scammer's playbook is to get their targets into a heightened emotional state — what they call "under the ether." Once there, it's hard for us to access logical thinking, and we're in a place to believe just about anything they say. It's just how our brains are wired.



Under The Ether: Heightened Emotional State

DESIRED REACTION	THE CRIMINAL IMPERSONATES ...	THE PLOY
FEAR	Your utility company	Your power is about to be shut off.
	Social Security Administration	Your number has been suspended.
	Microsoft	You have a dangerous virus on your computer.
	A grandchild	I'm in trouble and need your help.
EXCITEMENT	Publishers Clearinghouse	You've won a million dollars and a car!
	Cold-calling investment broker	A can't-miss investment opportunity!
	Social media post from a friend	I applied for a free government grant and got $5,000. You should apply, too.
LOVE	Someone looking for a relationship online	I never thought I could love someone the way I love you.

CONTACT METHODS: HOW SCAMMERS SEEK TO REACH US

Phone

Despite — and maybe because of — technological advances, the telephone remains a hot method of contact for today's scammers. Phone scams often begin with a prerecorded robocall about some urgent matter that instructs you to stay on the line or press a button to speak to a representative.

*Add your numbers to the National Do Not Call Registry at **donotcall.gov** or **888-382-1222**. This will cut down on legitimate telemarketing calls, making it more likely that calls that do get through are scams. And when in doubt, let your answering machine or voicemail screen your calls.*

Email

Criminals are adept at making an email message look like it is coming from a trusted source, like your bank or a retailer you may do business with. The goal is for the message to instill urgency, to get you to take an action (click a link, call a phone number) without stepping back and considering whether the message is fraudulent.

Texts

Text messaging is one of the fastest-growing contact methods for today's scammers. As with phone calls and emails, the scammer impersonates a familiar or trusted source to get you to act immediately to address some urgent matter.

Avoid clicking on links in emails or texts. Instead, go to the website of the sender by typing the address into your browser, use the app for the sender (if you have one), or call them using a number you know to be legitimate (e.g., from a statement).

Online

The internet teems with fraudulent content. Criminal tactics include hacking social media accounts and sharing false information with the hacked person's contacts, such as how to sign up for free money from the government. Scammers also set up fake profiles – often by stealing someone's real identity — and then use charm to get targets to connect with them.

Criminals create legitimate-looking shopping sites online, and even create faux versions of the online stores of well-known retailers.

Criminals also buy ads that show up in web searches, linking you to a hot product at a great price — only clicking the link loads malicious software onto your device to steal usernames and passwords to your accounts, including your financial accounts. Or the fake ad includes a trusted retailer's customer service number and dialing it takes you right to the criminal.

Marshal your inner skeptic when online. Be wary of unbelievable deals, a push from a "friend" on social media to call a number or click a link for some deal or little-known benefit, websites with errors and limited contact information, and friend requests from celebrities.

In-Person

Plenty of crooked companies and outright scammers knock on doors to steal people's money or sensitive information or even to case the house for a later attempt at burglary. Criminals may claim to be from your utility provider or alarm service, or they may say they are selling subscriptions or seeking charitable donations. Following a major weather event, shady contractors and criminals will show up and offer to repair damages for cash up front, and then take the money and run.

Commit to not opening your door to strangers — that's the safest bet. If you do engage with someone at your door, be wary of pressure to make a quick decision or pay cash up front for work, and thoroughly read any contracts before signing.

PERSUASION TACTICS: HOW SCAMMERS SEEK TO CONVINCE US

Criminals use a variety of persuasion tactics to convince us of an untruth to steal our money or sensitive information — and they are good at it. Here are some of the tactics common to today's scams.

Phantom Riches

The prospect of wealth is behind many common scams, and the criminal's goal is to pressure the target into believing that a large bounty awaits. Fake lottery winnings and surefire investment schemes commonly use the phantom riches technique to coerce targets.

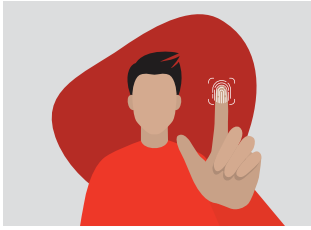
Criminals create legitimate-looking shopping sites online, and even create faux versions of the online stores of well-known retailers.

If you are told you've won a sweepstakes or a lottery, but you just need to pay some fees up front to claim your winnings, it is a scam. Full stop.

Profiling

The profiling tactic involves the criminal gathering key pieces of information about the target and using that information to establish credibility and elicit an emotional response. The goal is to get the target to act quickly to address an "urgent" situation. For example, today's scammer may peruse social media accounts to gather enough information to impersonate a family member in trouble.

Lock down your social media accounts to access only by friends and family. Follow the advice our parents gave us — don't talk to strangers. This includes strangers who reach us by phone.



Fear & Intimidation

Criminals commonly use fear and intimidation to get their targets under the ether. Many cases we hear about begin with inducing immediate fear, your grandson is in grave danger, the police have a warrant for your arrest, your computer has a deadly virus. And we've heard from victims that criminals will harangue them, calling dozens of times a day and leaving threats on their voicemail.

Scarcity

Criminals use the human impulse to stockpile limited supplies, alleging scarcity to convince us to act. Alleging scarcity to convince us to act now, before it's too late. , before it's too late. The early months of the coronavirus pandemic were replete with fake ads for much-desired personal protective equipment, while later it was about jumping the line to get the vaccine or quick access to in-demand testing.

Source Credibility

Impostor scams rely on getting the target to believe the contact is coming from a credible source — often a government agency, bank or major business. Common social media scams involve fake profiles that appear to be celebrities, or new "friends" with profiles that are a mix of invented and stolen information.

PAYMENT METHODS: HOW SCAMMERS GO AFTER OUR MONEY

> Cash

Offshore criminal operations often seek cash payments from people they target in the U.S.. Once the scammer convinces the target there's some fictional problem that can be solved with a payment, they may direct the target to fill a FedEx box with cash (with directions to wrap the dollars in a tea towel or aluminum foil) and overnight it to a U.S. address. A money mule (the person who transfers illegally acquired money or packages, sometimes not knowing they are involved in a scam) grabs the delivery and gets the money to the next step on its way back to the offshore criminals.

> Wire Transfers

Wire transfers are often requested as part of sweepstakes and lottery scams, where the target is asked to send money to help pay for processing big winnings — which never materialize. When a MoneyGram or Western Union transfer falls into the hands of a crook, it's untraceable, and protections are limited. If you wire money from your bank to someone who ends up being a criminal, your bank will call it an authorized transaction because you initiated it — even if under false pretenses — and you have no recourse.

Money Transfer Apps

Peer-to-peer (P2P) apps like CashApp, Venmo and Zelle allow you to send and receive money quickly and easily. However, the companies that offer these apps say they are intended to be used for splitting a dinner bill among friends or sending your grandchild money while she's off at college. They aren't intended to aren't intended for making purchases or other transactions with strangers or with businesses you have no relationship with. Once money is sent via a P2P app, it's next to impossible to claw it back if it was sent in error or to a criminal.

Cryptocurrency

As cryptocurrency becomes more accessible, crooks have grown more interested. In some cases, targets are directed to a "Bitcoin ATM" and told to insert cash. The scammer provides the target with information on where the cash-turned-Bitcoin should be deposited electronically. Once the cryptocurrency is transferred to the crook, it can't be traced. Cryptocurrency is also popping up in investment schemes.

Gift Cards

Con artists have latched on to gift cards as a convenient form of payment in their scams. The reasons are several: gift cards can be purchased just about anywhere, they are virtually untraceable, and criminals can drain the cards quickly. For example, the criminal convinces the target of an urgent matter that can be addressed with money, and says that the quickest way to remedy the problem is to go to a specific store, put a specific amount of money on one or more specific gift cards (sometimes referred to as electronic vouchers), and then share the activation information off the back.

Gift cards are not a legitimate form of payment. Anyone who directs you to pay for some obligation by purchasing gift cards and sharing the numbers off the back is lying to you.

A ROUNDUP ON HOW TO STAY SAFE

Beware the Faux Phone Call

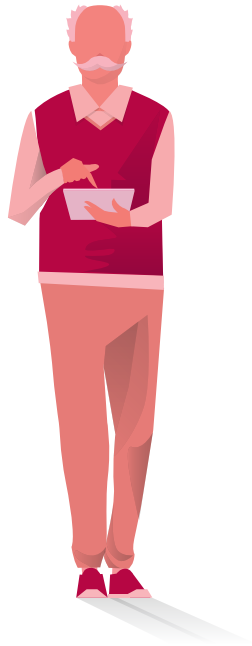
The phone is still #1 in the hearts of scammers. Use your voicemail or answering machine to screen incoming calls when you aren't absolutely certain who is calling. You can't trust caller ID because scammers use technology to hide their identity.

Listen to messages with intent. If the call induces a strong emotional response, pause. Ask a friend or family member what they think.

Stay safe by not providing sensitive information, like your social security number, Medicare number, or credit card or bank account information, to someone who calls you.

Know that federal, state and local government agencies will not call you out of the blue and demand money. Same with major retailers and utilities — calls from Amazon or from your power company out of the blue are most likely scams.

Add all of your phone numbers to the National Do Not Call Registry at **donotcall.gov** or **1-888-382-1222**. This will reduce the number of legitimate telemarketing calls coming in, making it easier to spot scam calls.



Don't Click Those Links

These days, it's so easy for criminals to send authentic-looking emails or texts that appear like they are coming from an entity you do business with. Skip the click! Instead, go to your web browser and type in the web address of who you think is trying contact you; if you have an app for them, log in to see if they are really trying to reach you.

Beware of online ads, too. A click on a scam ad could send you to a perfect copy of a legitimate retailer's site or could download malicious software intended to steal your credentials. Stick with retailers you have already done business with or that you trust.

Social Distance on Social Media

Every social media platform is swarming with scammers looking to score money or sensitive information. Keep your distance on social media and set your account to be open only to friends and family. Avoid accepting friend requests from strangers and know that accounts are easily hacked, so a message from a friend encouraging you to click a link for a free grant may actually be a criminal who has hacked their account.

Fortify Your Devices

Make sure your devices' operating systems are up to date and set updates to occur automatically. Often, updates are MEANT to patch a known pathway for criminal activity. Keep your protective software up to date as well, such as firewalls and antivirus tools. If you use your device in public, do not connect to free public Wi-Fi unless you enable a virtual private network (VPN). Options include ExpressVPN, NordVPN or Surfshark.

Pay Safely

Consider any request for an unusual payment method to be a red flag. These include money transfer apps, gift cards, cryptocurrency and wire transfers. The safest way to pay for purchases is with credit cards, because they offer consumer protections. Debit cards have similar protections, but if yours is compromised and money leaves your account, you have no access to that money until — and unless — the card issuer confirms fraud did occur. This could take weeks.

Be Reasonably Charitable

Sham charities abound, especially following natural disasters or other headline-grabbing events. Your best bet is to do your research and decide which charities you want to support — before an event happens. Make a list and stick to it. If you get a solicitation, simply say that you have made your giving decisions already. You can check out charities online at give.org or charitynavigator.org.

Don't Lose Yourself (or Your Identity)

Beyond stealing your money, some criminals specialize in stealing identities. Most of us have been notified that our sensitive information has been exposed in a data breach, a common means of identity theft. But identity theft can also involve stealing incoming or outgoing mail, rifling through garbage cans and recycling bins, or impersonating someone you would trust.

Identity theft becomes identity fraud when someone uses your identity for financial gain, such as by opening new accounts in your name, filing for government benefits in your name, filing false tax returns — or even taking over your accounts. This fraud can be committed by the criminal who stole your data or by the criminal who bought your data.

Steps to Protect Your Identity

To protect yourself now against future identity fraud, add a fraud alert to your credit reports, which requires a lender to contact you before opening a new account in your name (contact one of the three bureaus — Equifax, Experian or TransUnion — and the others will follow).

Or you can choose to freeze your credit. A freeze blocks lenders from opening new accounts in your name. You can freeze and unfreeze your reports at no cost, but you need to do it with each of the three bureaus.

Use strong and unique passwords for all online accounts. A password manager is a great tool great tool for setting and safely storing passwords; options include Bitwarden, LastPass, Dashlane or others.

Set up electronic access to all financial accounts. You can set alerts to text you with each transaction, so you can track activity, as well as other alerts. If app access is available, it has more encryption. Bonus: You don't have to wait a month or a quarter to review your account activity.

APPENDIX I: COMMON SCAMS

Scammers' keen ability to induce a strong emotional response — thus blocking our ability to access logical thinking — is their key to successful scams. Knowing about these scams before you are confronted with them is your key to avoiding a loss of money or sensitive information.

Business impostor: Contact from your bank, a shipping company, a retailer, tech support utility or other entity claiming there is a problem. They may also claim your auto warranty is about to expire or that they can help you resolve your debt. Options might include 1) press 1 to be connected to a representative, 2) call back a certain number or 3) click on a link to access your account.

> **Tip:** Do not press 1, do not call back a number given to you, and do not click on a link. If you think the call could be legitimate, find a number you know to be correct and call to inquire. And beware of searching online for a customer service number — you may end up calling a scammer directly.

Government impostor: Contact from a local state or federal agency claiming there is a problem and directing you to contact them immediately (in a manner akin to business impostors, above).

Government entities do not call out of the blue like this. If you have a concern, locate a number you know to be correct and call to inquire.

Can you do me a favor scam: Brief messages from someone you would normally trust, asking you to quickly purchase gift cards and share the number off the back. These typically occur in work settings, but also happen in communities of faith and elsewhere. The favor is a ruse and the money you use to buy gift cards is gone forever.

For example, you get a text from your boss explaining she's at a board meeting but needs gift cards for an employee appreciation event. She asks you to run to the store and buy five $100 Target cards and send pictures of the front and back of the cards. She says you can expense the cost.

In the faith community, the brief message is from your pastor or rabbi, who explains a family is in desperate need. He's out of town, so he asks you to buy a $250 Amazon card, snap pictures of the front and back of the card, and text him back. He'll pay you out of petty cash when he's back.

> **Tip:** You can avoid these by confirming any quick request for money or a gift card. Text your pastor, or email your boss or her administrative assistant; chances are high they never sent the request.

The grandparent scam: Someone claiming to be your grandchild, or representing your grandchild, calls claiming an urgent need for help: they've caused an accident and they've hurt someone badly, they were pulled over and the police found drugs in the car, or some similar scenario. They need you to send money right away with promise you won't tell their parents. They may ask for gift cards, wire transfer or cash.

> **Tip:** As hard as it may be, hang up on a call like this. Contact your grandchild or a family member who can confirm their whereabouts. The criminal will count on you staying on the phone to convince you of his lie.

Online romance scam: You meet someone on a dating site, simply playing an online game or perusing your social media feed. This person takes a quick interest in you, suggests you move to another platform to talk and turns on the charm. They will flatter you, ingratiate themselves and convince you that you belong together. Only you never meet in person — he's in the military abroad; she's on business in another country. Eventually, they will start asking for money. They may even show you they have a fat checking account in an American bank. The requests for money turn into demands, and they are relentless.

> **Tip:** Meeting someone online and not in person means you don't know them. Never send money to someone you know online whom you've never met in person.

APPENDIX II: AARP FRAUD WATCH NETWORK RESOURCES

AARP Fraud Watch Network online

aarp.org/fraudwatchnetwork

Get the latest news and information on scams, sign up for biweekly Watchdog Alerts, review more than 70 quick tip sheets on common scams, or report a scam on our scam-tracking map.

AARP Fraud Watch Network Helpline

877-908-3360

AARP's Fraud Watch Network Helpline is a free resource for AARP members and nonmembers alike. Trained fraud specialists and volunteers field thousands of calls each month. Report a scam or get guidance you can trust, free of judgment.

AARP VOA ReST Victim Support Program

aarp.org/fraudsupport

ReST stands for Resilience, Strength, and Time. AARP has joined with Volunteers of America to bring this helpful resource to victims of fraud and their families. This peer-led virtual session hosts up to five people and exists to address the emotional impact of your fraud experience.

AARP's The Perfect Scam Podcast℠

AARP's weekly podcast *The Perfect Scam*, tells the stories of people who find themselves the target of a scam. Host Bob Sullivan introduces listeners to those who have experienced scams firsthand, as well as to professional con artists and leading experts who pull back the curtain on how scammers operate. Find it at aarp.org/theperfectscam or wherever you listen to podcasts.

APPENDIX III: EXTERNAL RESOURCES

Annual Credit Report

This is the official site to get your free annual credit reports as guaranteed by Federal law. Be careful when typing this site name into your web browser. There are many look-alike sites with similar web site addresses.

Access online at: annualcreditreport.com

Charity Rating Sites

There are a number of websites that provide ratings and reviews of charities so that you can know if they are legitimate before you make a donation, including Charity Navigator and the Better Business Bureau's Wise Giving Alliance.

Access online at: charitynavigator.org and give.org

Federal Trade Commission (FTC) Consumer Help

Report fraud to the Federal Trade Commission. It won't help you recover your losses, but reported information is used to help with investigations.

Call toll-free 1-877-FTC-HELP (1-877-382-4357) or visit reportfraud.ftc.gov

National Do Not Call Registry

To help cut down on robocalls, add all of your numbers to the National Do Not Call Registry, operated by the FTC. It won't stop fraudulent calls, but it will make them easier to spot because most legitimate telemarketers won't call numbers on the registry.

Register your numbers at 1-888-382-1222 or donotcall.gov

Consumer Financial Protection Bureau (CFPB)

If you have a complaint about fraudulent activity involving a bank account or service, credit reporting and debt collection among other areas, contact the CFPB to file a complaint.

File online at: consumerfinance.gov/complaint

U.S. Postal Inspection Service

This site, sponsored by the U.S. Postal Inspection Service, has information about how to protect yourself from mail fraud and how to identify when you've been targeted.

Access online at: uspis.gov

FINRA Investor Education Foundation

This site, operated by the FINRA Investor Education Foundation, provides useful information about how to avoid investment fraud, including allowing you to check to see if a particular broker or investment adviser. It is particularly helpful in addressing a variety of frauds, including gold coins and oil and gas scams.

Access online at: saveandinvest.org

National Association of Attorneys General

The National Association of Attorneys General (NAAG) site provides contact information for all state attorneys general. Most state attorneys general welcome consumer inquiries and complaints about frauds occurring in the marketplace, and many offer complaint mediation services as well.

Access online at: naag.org

National Association of Insurance Commissioners

Visit the NAIC website to learn more about various types of consumer insurance products or to get helpful tips and tools for choosing an insurance provider.

Access online at: content.naic.org/consumer.htm

Customer Service Numbers for Commonly Impersonated Organizations

IRS (Treasury Inspector General): 800-366-4484

Social Security Administration: 800-772-1213

Medicare (HHS Office of Inspector General): 800-447-8477

Amazon Customer Support: 888-280-4331

Google: To report Google scams, visit support.google.com/faqs/answer/2952493

CREDIT BUREAU CONTACT INFO

Experian.com – 888-397-3742

Transunion.com – 888-909-8872

Equifax.com – 800-685-1111 (in N.Y., 800-349-9960)

Order free credit reports – annualcreditreport.com

NOTES

D19948 (0422)