Common Scams:

Recognizing and avoiding fraud

Consumer Action Managing Money Project

www.managing-money.org

Common Scams: Recognizing and avoiding fraud

It's impossible to be aware of all the different types of scams being perpetrated. However, there are certain scams that are carried out far more often than others, due in large part to their success rate. Here is a rundown of some of the most widely perpetrated scams. Although we organize the scams by target group, scammers can expand their target audience and will not hesitate to reel in anyone who will take the bait, so check out the scams in all the categories (general, seniors, veterans/servicemembers, immigrants and students) to be better prepared to avoid them. As you read about the scams, look for the warning signs that would alert you to similar ploys. And make note of the "What to know/do" section for each, which provides effective tips for spotting, dodging and dealing with scam attempts.

Note: This publication is intended for use with **Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks**, which has been written to help you understand how crooks reel in their prey, recognize potential scams, know what to do to avoid becoming a victim, and find scam prevention and reporting resources. **Just Say No to Scams** is available for free download at Consumer Action's website (https://www.consumer-action.org/english/articles/scams_guide).

Table of Contents

General scams

These ploys typically don't target a specific demographic (seniors, veterans, immigrants, etc.); virtually everyone is fair game. In many of these scams, victims are found by chance (for example, when the scammer places calls to random numbers or promotes a bogus tech support service online). In others, the crook works off of a "lead" (for example, your name on a "sucker" list—a list of people who have fallen for scams in the past and are believed to be more likely to be cheated again—or your profile on a dating website).

Tax scams

How they work: An imposter claiming to work for the Internal Revenue Service (IRS) threatens you with arrest, deportation or other action if you don't immediately pay taxes you supposedly owe, typically via wire transfer, prepaid card or gift card (including iTunes). Another approach is to request "verification" of personal or account information, supposedly for the purpose of processing your tax return or refund.

What to know/do: The IRS will always contact you by mail first. If you haven't received a letter, be suspicious of a call or other communication claiming to be from the agency. Be particularly wary if you are asked for immediate payment, or if the person insists you use a particular payment method (wire transfer, prepaid card, gift card or cashier's check, for example). Also be suspicious if the person asks for personal data such as your Social Security or other account number, or your PIN or password. And remember: A legitimate IRS employee will never threaten you with arrest, a lawsuit or deportation for not paying your taxes. Read the "Tax Scams/Consumer Alerts" page on the IRS website to become familiar with these and similar tactics (https://www.irs.gov/newsroom/tax-scams-consumer-alerts).

If you think the call might be legitimate, ask for the caller's name, badge number and callback number. (Don't trust caller ID, which is often rigged by scammers.) Then hang up and call the U.S. Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484 to verify that the person is really an IRS employee with a valid reason to contact you. If you receive a questionable letter, you can verify the notice type and contact information on the IRS website (https://www.irs.gov/individuals/understanding-your-irs-notice-or-letter). Do not reply to or click on links in email or text messages claiming to be from the IRS. Do not ever pay anything until you have verified beyond any doubt that you owe the money *and* are paying it to a legitimate IRS representative.

Debt collection scams

How they work: A scammer impersonating a legitimate debt collector contacts you about a debt you supposedly owe, requiring immediate payment, often in the form of a wire transfer, prepaid or gift card number, or cashier's check. If you don't pay up, the "collector" threatens you with jail or other legal action. In other cases, the collector is legitimate, but the debt is not valid (too old, or already paid

or settled), is for the wrong amount, or is being collected from the wrong person (because you have the same name as the real debtor, for example).

What to know/do: If a debt collector contacts you, proceed with caution, particularly if the contact is unexpected. Collecting a valid debt is not a scam. However, there have been cases where scammers have accessed consumers' credit reports and, armed with accurate information about account names, balances and payment history, were able to convince the accountholders to pay them. Threats or disclosure of confidential information (like your Social Security number) is illegal and should raise a red flag, as should demand for payment via a particular method (wire or gift card, for example).

Anytime you are contacted by a debt collector, you should request that a "validation notice" be mailed to you. This notice includes detailed information about the debt and your rights, and, by law, must be sent within five days of initial contact. Refuse to discuss the debt until you receive it. In the meantime, ask for the collector's name, agency name, address, phone number and website address, and then do some research. But remember, just because you confirm someone is a legitimate debt collector doesn't mean they have the right to collect the debt from you. Do not pay anything until you have verified the legitimacy of the collector *and* the validity of the debt. Learn more in Consumer Action's **When a Collector Calls** (https://www.consumer-action.org/english/articles/when_a_collector_calls_an_insiders_guide_to_responding_to_debt_collectors) and at the Federal Trade Commission's (FTC) "Fake Debt Collectors" webpage (https://www.consumer.ftc.gov/articles/0258-fake-debt-collectors).

Counterfeit check scams

How they work: Someone gives you a (counterfeit) check and asks you to deposit it and then return part of the money to them. It is often cloaked as an accidental overpayment for something they are purchasing from you, though sometimes it's related to a "secret shopping" gig, work-at-home pitch or similar scheme. When the fake check bounces, you are out whatever money you gave to the scammer plus a returned check fee.

What to know/do: The best policy is not to accept a check or money order unless you know and trust the person you're dealing with and/or the bank confirms that the check has cleared (though it can take a while to be sure the payment isn't counterfeit or forged). If you decide to call and confirm the validity of a check with the bank it is drawn on, find the bank's phone number on your own; don't trust a phone number or website address printed on the face of the check or provided by the person giving it to you. Don't believe contrived excuses for an overpayment; only accept the exact amount due you. Never wire money to strangers; the funds are untraceable and unrecoverable. Learn more at the FTC's "Fake Checks" webpage (https://www.consumer.ftc.gov/articles/0159-fake-checks).

Advance fee scams

How they work: Someone contacts you offering help dealing with your finances—for example, getting out of debt, reducing payments on your student loans, avoiding foreclosure, getting a lump sum out of your pension, tapping the equity in your home, negotiating a tax settlement or erasing negative information in your credit report. You pay the scammer's fee upfront, but the help doesn't materialize.

What to know/do: Be skeptical if you didn't initiate contact. If you are interested in an offer, first verify the business's legitimacy, check customer satisfaction ratings, compare prices, etc. Also look into the value of the assistance you would be paying for. In many cases, the service being offered for a fee is actually available free of charge. For example, federal student loan borrowers can reduce or defer payments through the U.S. Department of Education at any time for free (https://studentaid.ed.gov/sa/repay-loans); homeowners can apply for a loan modification or forbearance through their mortgage servicer at no charge (https://www.consumer.ftc.gov/articles/0187-when-paying-mortgage-struggle); taxpayers can set up a payment plan (https://www.irs.gov/payments/payment-plans-installment-agreements) or try to negotiate a settlement (https://www.irs.gov/payments/offer-in-compromise) directly with the IRS for free; and it costs nothing for consumers to try to negotiate a settlement with their creditors (https://www.consumerfinance.gov/ask-cfpb/what-is-the-best-way-to-negotiate-a-settlement-with-a-debt-collector-en-1447/) or correct errors in their credit reports (https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports). It's also important to know that, at least in the case of credit repair, federal law prohibits companies from collecting fees until *after* certain services have been delivered (https://www.consumer.ftc.gov/articles/0058-credit-repair-how-help-yourself#croa).

Avoid anyone who promises you will qualify for a loan or credit card before you even apply, particularly if you have a low or no credit score. Learn more at the FTC's "Advance-Fee Loans" webpage (https://www.consumer.ftc.gov/articles/0078-advance-fee-loans).

If you have a problem with a company, report it to your local consumer affairs office or to your state attorney general (AG) (http://www.naag.org/).

Windfall (sweepstakes, inheritance, etc.) scams

How they work: Someone informs you that you've won a prize, received an inheritance, gotten a grant or are entitled to some other windfall—*but*, you must first pay a fee or provide personal information to collect it. In some cases, scammers place ads offering grants and then will request that victims wire money for processing fees or taxes before the grant money can be sent to them (of course, it never is).

What to know/do: Assume that anyone who contacts you to say you have won a prize, received an inheritance or are entitled to some other windfall but demands

a fee or personal information before you can collect it is a scammer. Learn more at the FTC's "Prize Scams" webpage (https://www.consumer.ftc.gov/articles/0199-prize-scams).

While the promise of a jackpot is enticing, steer clear of any contest that requires you to reveal sensitive data (Social Security number, etc.) to enter. Don't click on links in email or text messages announcing you've won—they could install malware.

Ignore any communication requesting help to get a fortune out of another country and into the U.S. (known generally as "Nigerian Prince" scams). If you're the victim of an international scam (many originate overseas), you can report it to eConsumer.gov (www.econsumer.gov), a site run by the International Consumer Protection and Enforcement Network (ICPEN).

Recovery/refund scams

How they work: Someone contacts you promising to recover money you've lost—for a fee.

What to know/do: Assume that anyone who contacts you to recover lost money—missing prize winnings, undelivered products, fraud losses, etc.—is trying to scam you. Scammers often share "sucker lists" containing the contact information of consumers who have fallen for scams in the past. The idea is that someone who has been scammed before is more likely to fall for another scam—in this case, believing that someone will help recover your losses. Legitimate agencies, like the FTC and CFPB, that work on consumers' behalf never call victims to promise a refund in advance and never ask for a fee or personal information before helping.

If you get a communication that you think might be legitimate, get the person's name, company or agency name, contact information and tax ID number, and then do your own independent research. (Don't believe that a phone number, address or website the person provides is trustworthy.) Learn more at the FTC's "Refund and Recovery Scams" webpage (https://www.consumer.ftc.gov/articles/0102-refund-and-recovery-scams).

Charity scams

How they work: You are contacted by a charity (maybe even one with a familiar name) requesting an immediate monetary donation. The representative dissuades you from thinking about it or researching the organization. These scams happen year-round, but are particularly prevalent after a natural disaster or other tragedy, or during the holidays, when people are eager to help and donation requests are expected.

What to know/do: Rather than donate in response to a random request, be proactive and research the causes and charities you want to support. Charity

Navigator (https://www.charitynavigator.org/) and Give.org (http://give.org/) are just a couple of the online tools available for finding a legitimate charity that meets your goals. After a disaster or other tragedy, local news outlets often compile lists of reputable charities helping victims—check out those websites or contact the station.

If you think you might be interested in supporting a caller's charity, ask the person to provide the organization's website address. But be aware that a scammer could set up a bogus website, so you'll still want to verify legitimacy using one of the charity research websites. When donating, use a credit card, which offers strong consumer protections under the law, rather than cash, wired funds, prepaid or gift cards, or a cashier's check. And don't give an unknown caller access to your account by providing an account number.

The Do Not Call Registry (https://www.donotcall.gov/), which allows you to opt out of telemarketing calls, doesn't apply to charities, but you can ask an organization not to contact you again if you don't want to hear from them. If the charity is legitimate, it will likely comply with your request. If it's bogus, you can expect future calls. The FTC offers additional information at its "Before Giving to a Charity" webpage (https://www.consumer.ftc.gov/articles/0074-giving-charity).

Pyramid schemes

How they work: This type of investment scam (also known as a Ponzi scheme) lures victims through the promise of very attractive and/or guaranteed returns. Early investors tout the too-good-to-be-true opportunity to friends and family members, unwittingly recruiting new victims. Once the supply of new investors dwindles and/or existing investors want to cash out, the scheme falls apart and everyone (except the originator) loses (think Bernie Madoff, whose elaborate Ponzi scheme was discovered in late 2008: https://en.wikipedia.org/wiki/Madoff_investment_scandal). Multi-level marketing (MLM) schemes are similar, but are organized as businesses where recruits are required to buy a large inventory and/or recruit new distributors.

What to know/do: Don't put your money into any investment not registered with the Securities and Exchange Commission (SEC) and/or state regulators, or invest with anyone who isn't a licensed investment professional or employed by a registered investment company. Tools for researching investment companies and professionals include FINRA's BrokerCheck (https://brokercheck.finra.org/ or 800-289-9999); the SEC's Investment Adviser Public Disclosure program (https://adviserinfo.sec.gov/IAPD/Default.aspx); and your state's securities regulator, which you can find through the North American Securities Administrators Association (NASAA) website (http://www.nasaa.org/about-us/contact-us/contact-your-regulator/). Be particularly suspicious of any investment that *guarantees* positive returns, promises unusually high returns or pays positive returns even when similar investments are not doing well. Check your account statements and follow up on errors. Be suspicious if you meet with

resistance when trying to withdraw money, or you don't receive a payment you're expecting.

One of the best ways to protect yourself and find legitimate investments is to learn about investing from reputable sources, including Morningstar (http://www.morningstar.com/cover/Classroom.html), 360 Degrees of Financial Literacy (https://www.360financialliteracy.org/Topics/Investor-Education/Investing-Basics), The Motley Fool (https://www.fool.com/retirement/2017/08/19/our-guide-to-investing-for-beginners.aspx) and E*Trade (https://us.etrade.com/knowledge/education).

Multi-level marketing (MLM) schemes are similar, but are organized as businesses where recruits are required to "buy in," sometimes through the purchase of a large inventory of product they then have to sell to recoup their investment. Often, recruits earn money by signing up new distributors, whose investment is used to pay off the earlier participants. While not always illegal, the FTC offers tips for steering clear of questionable multi-level marketing schemes (https://www.ftc.gov/tips-advice/business-center/guidance/multilevel-marketing). Learn more in The Balance's "10 Signs It Is an MLM Scam" (https://www.thebalance.com/business-is-an-mlm-scam-1794756).

Affinity fraud

How it works: Someone offers you an attractive (but fraudulent or questionable) investment or business opportunity specifically because of your affiliation with a particular demographic or community.

What to know/do: Affinity fraud exploits the trust that exists among members of a group (those who share a common religion, language, ethnicity, culture, profession, financial status, age, etc.). The fraudster might be a member of the group, or may just pretend to be. In some cases, the organizer befriends prominent members of the group in order to gain entry and legitimacy. The scam typically takes the form of a fake investment or business venture. Money given to the organizer by new investors is used to pay off earlier investors. Eventually the scheme collapses when there are no new investors to fund it, existing investors suspect foul play (sometimes because they are met with resistance when trying to get their money out) or the perpetrator vanishes with the money. While affinity fraud hits virtually all demographics, immigrant communities can be particularly attractive targets because they may not speak English well, could be economically marginalized, might not be aware of their rights, or may fear deportation or other consequences if they report the crime.

Do not let your guard down just because of a common background, or because someone you trust vouches for the organizer or touts the investment (that person might be fooled too). Go through the same steps to verify the individual, company and investment that you would if there were no personal connection (see "Pyramid schemes" on page 7). Be aware that social media has made it easier

for scammers to find their victims and infiltrate a group or community. The SEC warns that even if an actual investment exists, it typically makes little or no profit—the fraudster simply uses investors' money until the scheme collapses. If you are a victim of affinity fraud, report it to law enforcement. While there are no guarantees, your report could help prosecute the perpetrator and result in restitution (as in the Bernie Madoff case: http://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7). At the very least, reporting it to the SEC or the Federal Trade Commission could help prevent other consumers from falling prey to the same scam.

Sales scams

How they work: Scammers want your money, and one of the best ways to get it is to try to sell you something. Often, the item is counterfeit, invalid or nonexistent. Cases include counterfeit luxury goods, duplicate concert/event tickets, invalid gift cards, leases on homes the scammers don't own, undelivered goods sold through a website, supplies or training for bogus work-at-home jobs, or puppies that don't exist. In the case of health and cosmetic products, what is being sold may be ineffective or even dangerous.

What to know/do: It's wise to do business only with merchants you know and trust, or ones that you have at least had an opportunity to investigate through online reviews, the Better Business Bureau, etc. When conducting a peer-to-peer transaction (buying from or selling to an individual), try to do it through an intermediary that offers some protections (PayPal, eBay and Airbnb, for example). If a buyer or seller tries to persuade you to do the deal "off the record" (outside the site's normal, tracked process), it's a sign that you could be dealing with a scammer and you should probably walk away. Always beware of offers, claims and prices that appear too good to be true, and be suspicious of unlikely or convoluted stories (for example, the landlord working overseas who needs to rent his home out from afar).

If you run into a problem, try to resolve it first with the individual that you made the purchase from. However, if it's an intentional scam and/or you paid with cash or the equivalent, you have little hope of recovering your losses. If you made the transaction through an intermediary, find out what protections it offers. If you paid by credit card, contact the card issuer to dispute the charge. If you paid by debit card or check, you may be out of luck, but it's worth contacting the bank to see if there's anything they can do. If you believe a crime has been committed, report it to the police. If the scam took place online, report it to the Internet Crime Complaint Center (https://www.ic3.gov/default.aspx) as well.

When shopping online—even with legitimate businesses—take precautions to avoid problems and be prepared to deal with issues that might arise. Consumer Action's free *Savvy online shopping: Tips for trouble-free transactions* (https://www.consumer-action.org/modules/articles/savvy_online_shopping_tips_for_trouble_free_transa

ctions) and *Savvy online shopping: How to resolve a dispute* (https://www.consumer-action.org/modules/articles/savvy_online_shopping_how_to_resolve_a_dispute) guides can help you stay safe and resolve problems.

Tech support scams

How they work: Someone claiming to be from a well-known tech company notifies you (typically by phone or email, or through a pop-up window in your browser) that there is a serious technical problem with your computer that he can fix if you pay a fee or give him remote access to your computer. (Victims sometimes unwittingly initiate contact with the scammer themselves after finding a bogus tech support number online.) The scammer takes your payment and provides worthless services and/or downloads malware that locks your computer files until you pay a ransom. Sometimes the scammer agrees to provide the victim with a refund of any fees paid but claims to need a bank account number to do so. Then, instead of putting money *into* the account, he takes money *out* of it.

What to know/do: Assume that any unexpected call claiming to be aware of your computer problems is a scam and hang up; Microsoft, Apple and similar companies are not actively tracking your computer looking for problems and then contacting you to fix them, and neither is your internet service provider (ISP). You should also assume that emails and pop-up windows saying there is a problem with your computer are malicious.

Even finding tech support through an online search can be risky since fraudsters often buy ads and pay search engines to have their info come up in search results for key words such as “tech support,” “virus removal,” “Norton support,” etc. When you need to contact tech support, conduct your search carefully and verify that you are contacting a legitimate business. (Tip: Spoofed sites typically have a URL close to, but not the same as, the real one—for example, www.microsofthelp.com or www.micosoft.com instead of the correct www.microsoft.com.) Never provide your credit card number, account information or personal data to someone claiming to be from tech support unless you initiated the call, are absolutely certain who you’re dealing with and have thoroughly researched the product, service or subscription you’re being sold.

Never click on links in unsolicited email messages or texts, and never click on pop-up ads, warnings or other messages. Doing so can initiate the installation of damaging software onto your computer or device.

Don’t give someone you aren’t 100 percent sure you can trust remote access to your computer to “fix” it, since that provides them with the opportunity to steal your data and/or cause damage and then charge you a fee to undo it.

For many reasons, it's a good habit to back up your computer files regularly and install software that protects you against viruses, spyware and malware. Learn more about computer and online security at the FTC's OnGuardOnline (https://www.consumer.ftc.gov/features/feature-0038-onguardonline). And if you think only older generations fall for tech support scams, you're wrong—millennials may be the hardest hit (http://abcnews.go.com/US/tech-support-scams-hit-millennials-hardest-realize/story?id=51743331).

False health claims

How they work: Hucksters market weight loss, medical and youth-preserving treatments and products that turn out to be ineffective or even harmful.

What to know/do: Read the FDA's "Health Fraud Scams…Are *Everywhere*" (https://www.fda.gov/downloads/forconsumers/protectyourself/healthfraud/ucm302359.pdf), which provides tips for recognizing these types of scams. Consult with your general physician regarding any specific medical issues you experience. And remember: There's no quick and easy way to lose weight, no "miracle" cures, and no fountain of youth.

The Red Flags of Quackery (viewable at https://blogs.agu.org/wildwildscience/2013/04/30/the-red-flags-of-quackery/) is an entertaining illustrated guide to pseudo-science and the bogus claims that lead consumers to spend, collectively, billions of dollars each year on ineffective and even dangerous health treatments and products.

Whatever the product or program you are considering, beware of "free" trial offers, often hawked through television infomercials. Trial offers of any kind can be costly because many, if not most, people who accept the offer forget to cancel before the trial period ends and wind up paying for something they don't want.

Romance scams

How they work: Often perpetrated online through dating websites or social media, this ruse involves tricking the victim into believing the scammer has romantic intentions or is a true friend. Once he or she has gained the target's confidence and emotional commitment, a request for money is made, often under the guise of wanting to purchase a ticket to come visit the victim. In some cases, the money is needed to resolve a nonexistent emergency.

What to know/do: Scammers prey on the vulnerable, so always have your guard up when you put yourself out there as someone looking for a relationship. Before becoming involved with someone new, do some background research. Scammers often create fake online profiles and use stolen photos. Search the person's name, try to verify that they live and work where they say they do, and do an image search of their photo using a tool such as Google Images (https://images.google.com/). (Click the little camera image to paste in the photo's URL or upload the photo you want to compare.) If the photo appears under several different names, it's a scam.

Don’t ignore the little signs that something isn’t right. For example, scammers often proclaim deep feelings very quickly, ask their target to communicate off the dating site (to avoid being detected by the site moderator), or claim to be American, yet their communication style doesn't match that of a native speaker. They tell stories that tug at your heartstrings, use a lot of endearments (“babe” and “darling,” for example), often are traveling or working abroad (providing an excuse not to meet in person), and eventually ask for money (or make you believe you chose to offer it to them). Don’t ever send money to someone you met online or enter into any other transaction with them (opening a bank account and wiring money, forwarding a package or making an online purchase, for example).

Learn more at the FTC’s “Online Dating Scams” webpage (https://www.consumer.ftc.gov/articles/0004-online-dating-scams). AARP’s article “Are You Real?—Inside an Online Dating Scam” (https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html) is a detailed account of how one scammer broke his victim’s heart and stole $300,000 from her. The U.S. Army Criminal Investigation Command, which receives hundreds of allegations a month from victims who state they got involved in an online relationship with someone claiming to be a military servicemember, offers a webpage full of red flags to look for and tips for avoiding an imposter (http://www.cid.army.mil/romancescam.html). While you should report the scam to the website where it began as well as to the FTC (https://www.ftccomplaintassistant.gov/), the FBI’s Internet Crime Complaint Center (https://www.ic3.gov/default.aspx) and your state attorney general (http://www.naag.org/current-attorneys-general.php), the odds of you recovering your financial losses are slim to none.

Blackmail schemes

How they work: You do something that you wouldn’t want a spouse, parent, employer, school administrator, law enforcement officer or anyone else to find out about, and someone photographs or records you, or gets hold of a sensitive email or text message, and then demands money to keep your secret.

What to know/do: Since virtually everyone around you has a smartphone and the ability to photograph or record whatever you do, and email and text messages are not always secure, don’t put yourself in a compromising position. As you make choices, ask yourself how your actions could be construed and what the consequences might be. If you submit to someone’s demands for money in exchange for their silence, be aware that there’s no guarantee your secret will remain private even after you have met the blackmailer’s demands.

Senior scams

While consumers of all ages should be on guard against scams, seniors can be particularly vulnerable to fraud. This can be because of changes in the brain that make it harder for the elderly to detect suspicious body language and other warning signs that someone might be untrustworthy (http://news.usc.edu/135031/senior-scams-and-fraud-due-to-aging-brain/). Or it can be because they are isolated, are more likely than young people to be home (and available to answer the phone or door), are inexperienced in managing their finances (a deceased spouse may have been the primary household money manager) or don't have access to the internet and the tools it offers for verifying claims and identifying scams. The elderly are also more likely to be financially scammed by someone they know and trust—a friend, family member, caregiver or other helper.

All states have laws to protect older people from abuse. In addition to reporting suspected elder fraud to the local adult protective services agency (https://eldercare.acl.gov/Public/Index.aspx) and law enforcement, notify any financial institution holding an account that has been fraudulently accessed. Learn more about the following scams and others in the National Council on Aging's (NCOA) list of the top 10 financial scams targeting seniors (https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/).

Medicare/Social Security scams
How they work: A scammer posing as a Medicare or Social Security Administration representative provides a bogus reason why he needs your Medicare or SS number and/or financial account information (and then uses your Medicare benefits or steals your money or identity). In another scenario, someone sells you a cheap Medicare-covered medical device such as a back brace. Using your account information, they bill Medicare for a device worth many times more than what you received. Or they sell you discounted prescription drugs that might be fake or even harmful.

What to know/do: Government agencies typically initiate communications via mail, not by phone, so don't ever give your Medicare, Social Security or other account numbers or your personal data to an unexpected caller. Only provide your Medicare number to healthcare providers or facilities at the time you are actively seeking service. Call Medicare (800-633-4227) or Social Security (800-772-1213) to verify a request.

Never respond to open solicitations for Medicare-covered supplies or services. If there is something you need, ask your healthcare provider for referrals to suppliers, or ask your doctor if the supplier you are considering doing business with is reputable. Be very cautious about ordering medication online or in response to a call or other unsolicited communication. Confirm with your

physician that the company you are considering ordering from is reputable. Consistently monitor your Medicare statements. Look for any claims for services or supplies billed to you that you didn't receive or that are more expensive than expected. You can set up an account at MyMedicare.gov (https://www.mymedicare.gov/) and access your claims information online at any time.

If you suspect you have been contacted by a Medicare scammer or are the victim of Medicare fraud, report it to the U.S. Department of Health and Human Services Office of Inspector General by phone (800-HHS-TIPS/800-447-8477) or online (https://forms.oig.hhs.gov/hotlineoperations/report-fraud-form.aspx). Learn more at Medicare's "fighting fraud" webpage (https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud).

Home equity scams

How they work: A lender offers you a loan against the equity in your home—money you could use to make needed repairs or just make ends meet. But the loan turns out to have high fees added. Or, the lender encourages you to refinance repeatedly to pull more money out of your home, each time adding additional fees to your debt. These loans typically have variable interest rates, which means your payments fluctuate and may become unaffordable, and many are "interest only," which means you never pay down your debt and your payments will eventually increase. In some cases, the loan has a balloon clause requiring full repayment in just a few years. If you can't keep up, the lender forecloses on the property and you lose your home.

What to know/do: Seniors aren't the only victims of home equity loan scams, but they can be particularly attractive targets because they are more likely to have a lot of equity in their property and to live on a fixed income that makes it difficult to pay for repairs or property taxes. Before using your home as collateral for a loan, consider other options, like taking in a boarder or reducing your living costs in some way.

Do not respond to unsolicited loan offers. Borrow only from a reputable lender that you contact after shopping around and doing some company research. Get advice and assistance from someone you can trust. A HUD-certified housing counselor can offer guidance about loan terms, affordability, lender reputation, your rights and alternatives to borrowing. Find one at the U.S. Department of Housing and Urban Development website (https://www.hud.gov/i_want_to/talk_to_a_housing_counselor).

Have someone knowledgeable look over the loan papers with you. Be sure you understand the terms of the loan, including what the monthly payments will be; whether they can fluctuate, and by how much and how often; whether the payments include principal or are interest-only; and whether there is a balloon payment. If you find yourself in over your head, don't wait—get assistance

immediately. If the loan violates federal credit laws, you may be able to save your home. Contact a HUD counselor or an attorney for guidance. If you are of low income, find local legal aid at the Legal Services Corporation website (https://www.lsc.gov/what-legal-aid/find-legal-aid).

Grandparent scams

How they work: A scammer pretending to be a family member—often a grandchild—calls and claims to need money urgently, typically for something like emergency medical care or bail in another country. Sometimes pairs of scammers work together, with one claiming to be an arresting officer, lawyer, doctor or other authority figure and the other impersonating the grandchild pleading for help (briefly enough to evade detection as an imposter). The scammer demands payment, usually via wire or a prepaid or gift card, to avoid some unwelcome consequence (jail, withheld medical care, etc.).

What to know/do: As with other scams carried out by a caller demanding immediate payment, just hang up. If you are concerned about the person who is supposedly in trouble and in need of money, try to contact him or her directly, or verify with another family member or anyone else likely to know if the story is true (even if the scammer tells you not to).

You can avoid a lot of scam attempts simply by screening out callers you don't know. Ask your phone service provider if it offers the option to block unrecognized and unwanted calls.

Funeral and burial scams

How they work: In one approach, the scammer reads obituaries and funeral notices and then contacts the grieving spouse or family members (often by attending the funeral!) claiming the deceased died with an outstanding debt and coercing them to pay it off. Another type of scam is the sale of fake burial plots, often discovered by the victim or family members only when the plot is needed. And, while not technically a scam, some funeral homes try to oversell products and services in violation of the law.

What to know/do: If you are contacted or approached by someone you don't know claiming to be a friend or lost family member of the deceased, be skeptical. Don't be convinced just because the person can produce some accurate details about the deceased—there is a lot of information online, in public records and even in an obituary that can help someone piece together a convincing story. Don't ever give anyone money under pressure. If you think their claim might be legitimate, take time to verify it. Ask for help from people you trust—your lawyer, if you have one, would be a good resource because he or she could also tell you what your rights are related to any debts the deceased left behind. Learn more at the FTC's "Debts and Deceased Relatives" webpage (https://www.consumer.ftc.gov/articles/0081-debts-and-deceased-relatives).

If you decide to pre-purchase a burial plot or crypt, do so through a reputable cemetery, and get a written receipt. If you will be making payments rather than paying in full at the time of purchase, read the agreement so that you understand any fees or hidden costs, such as interest or other charges.

While not a scam in the strictest sense, a tactic of disreputable funeral homes is to capitalize on family members' unfamiliarity with the considerable cost of funeral services. For example, some funeral directors will insist that an expensive casket is needed for a direct cremation (untrue), or will try to upsell and overcharge you. Don't be pressured into spending more than you want or need to. The Funeral Rule (https://www.consumer.ftc.gov/articles/0300-ftc-funeral-rule), enforced by the Federal Trade Commission, gives you many rights, including the right to buy funeral goods and services separately rather than as a package that includes things you might not need or want; the right to get price information over the phone and a written, itemized price list when you visit a funeral home; and the right to provide the funeral home with a casket or urn you purchase elsewhere. (*Note:* The Funeral Rule doesn't cover cemeteries and mausoleums unless they sell both funeral goods and funeral services.)

Veteran and servicemember scams

Instead of receiving deserved respect for their service to our country, veterans, and even active duty servicemembers, are instead often targeted by scammers. In fact, a late-2017 AARP Fraud Watch Network survey found that more than twice as many veterans as nonveterans lost money to scam artists during the previous five years. Below are a few of the most prevalent veteran/servicemember scams. Read the *AARP Watchdog Alert Handbook: Veterans' Edition: 9 Ways Con Artists Target Veterans* (http://action.aarp.org/site/DocServer/Watchdog-Alert-Handbook-Veterans-Edition.pdf) to learn more about how to avoid becoming a scam victim.

Veteran charity scams

How they work: A scammer appeals to your loyalty to the military by requesting a donation to a charity that purports to help veterans and/or servicemembers. In some cases, the charity doesn't exist. In others, a charity is established legally, but all or most of the donated funds go into the pockets of the fundraisers.

What to know/do: Don't judge a charity by its name. Before responding to a donation request, research the organization on one of the websites listed under "Charity scams" on page 6. As with any donation request, never feel pressured. You can call the charity directly or visit its website to make a donation if you are satisfied with what you find out from your research. If you make a donation, use a credit card—never cash.

Military benefits schemes

How they work: In one scenario, a veteran is offered a cash buyout of his or her future pension or disability benefits. The buyout is typically a fraction of the value of the benefit, leaving the veteran in financial straits after the lump sum runs out. Or, the veteran is persuaded to take out a pension advance loan at an exorbitant cost with unaffordable payments. In another scenario, the veteran is persuaded to put his or her assets into an annuity or trust in order to qualify for the Aid & Attendance Benefit, reserved for those with few liquid assets at their disposal. The veteran ends up paying high fees for the advice and financial products, and also may jeopardize their eligibility for Medicaid, lose access to their money for a long time or have to repay the benefits after an investigation.

What to know/do: Don't take a buyout of, or a loan against, your VA pension or other benefits, move your assets around to qualify for benefits, or pay someone to file a claim. Call the U.S. Department of Veterans Affairs (VA) National Pension Hotline at 877-294-6380 to speak to a counselor about any investment or other pitch that requires you to pay for it out of your pension or sign over your benefits. For more information about VA pension, visit www.benefits.va.gov/pension or call 800-827-1000. Learn more at the FTC's "Pension Advances: Not So Fast" webpage (https://www.consumer.ftc.gov/articles/0513-pension-advances-not-so-fast).

The VA also warns against working with anyone who tries to persuade you to move assets around or who charges you for help filing a claim for pension or Aid & Attendance benefits (https://www.benefits.va.gov/PENSION/Pensionprograminfo.pdf). Learn more at the Federal Trade Commission's "Veterans' Pensions" webpage (https://www.consumer.ftc.gov/articles/0349-veterans-pensions).

If you are having trouble making ends meet, look into other options that don't put your future income at risk. Read Consumer Action's 15-page *Servicemembers and Veterans Financial Empowerment Resource Sheet* (https://www.consumer-action.org/english/articles/servicemembers_and_veterans), which provides information about dozens of government and non-profit resources and programs that you might qualify for, from housing assistance and emergency grants to food programs and utility discounts. This is a companion to, and should be used in conjunction with, the general *Financial Empowerment Resource Sheet* (https://www.consumer-action.org/english/articles/financial_empowerment_resource_sheet), which includes dozens more resources that do not require military or veteran status. Also read Consumer Action's *Economic survival guide for servicemembers and veterans* (https://www.consumer-action.org/english/articles/economic_survival_guide_for_servicemembers_and_veterans), which can help you recognize scams, protect your benefits and know your rights.

VA records/assistance scams
How they work: Someone attempts to charge for military records that are available free or at a low cost directly through the VA or other agency. Or, they offer to assist you with filing for your VA benefits, for a fee.

What to know/do: Contact the VA or your service unit directly to request copies of the records you need. They are provided free or for a very small fee. (Visit https://www.usa.gov/veterans-documents for links to records sources.) The FTC warns veterans not to pay for benefits application forms—they are available free—and wants you to know that the people who are accredited through the VA to provide assistance are not allowed to charge you for help completing and submitting VA paperwork. To find an accredited adviser (attorney, claims agent or Veterans Service Organization representative), use the VA's online search tool (https://www.va.gov/ogc/apps/accreditation/index.asp). You also can contact your state Veterans Affairs office (https://www.va.gov/statedva.htm) for information and referrals. Do not assume that an adviser is accredited, qualified or honest just because the business has "veterans," "military" or similar terms in its name.

GI Bill schemes
How they work: Recruiters convince veterans to use their GI Bill benefits at their shady for-profit school. In many cases, the school requires the veteran to take out expensive private student loans to cover all the tuition and expenses, yet provides a sub-par education that leaves the student unprepared to earn a living. In other cases, veterans are the victims of bait-and-switch scams, where they use their benefits to enroll in one type of schooling and receive, instead, low-cost correspondence courses that aren't even covered by the GI Bill.

What to know/do: Before choosing a school or training program, visit the Know Before You Enroll website (http://knowbeforeyouenroll.org/), developed to protect veterans and their GI Bill benefits. Consumer Action's *A Guide to Finding the Right Job Training School* (https://www.consumer-action.org/modules/articles/job_training_schools) presents the pros and cons of different education options and helps you vet schools and job training programs.

VA phishing attempts
How they work: Someone contacts you claiming to be with the VA and says that your personal data is needed to "update" your records, be considered for a job (through the Vets.gov career site), proceed with a benefits claim or for some other reason. Once you give up your information, the scammer steals your money or your identity.

What to know/do: The VA and related agencies will never ask you for your sensitive data by phone or email; requests and other communications come via regular mail. If you get a call or message that you think might be legitimate, call the VA (800-827-1000), agency or business directly to verify. If you confirm that the call or email you received was a phishing attempt, report it to the VA's Identity Safety Service (https://www.va.gov/identitytheft/ or 855-578-5492).

Immigrant scams

The vast majority of scams targeting immigrants in the U.S. use either the promise of achieving the victim's desired immigration status or the threat of deportation to persuade him or her to give the scammer money or disclose personal information. These schemes become more widespread in a political climate that is unfriendly toward immigrants because it is easier to exploit their fears. In such an environment, it's particularly important to verify claims and vet the agencies and individuals who offer services and assistance.

Immigration assistance scams

How they work: Businesses and individuals claiming to have special expertise or influence charge you for help filling out immigration forms, getting a visa, renewing a green card or applying for citizenship. In most cases, the fee is unnecessary because free assistance is available. In many cases, the person providing the "service" is unqualified and actually does more harm than good. In some cases, the perpetrator takes your money and does nothing at all.

What to know/do: Don't rely on a *notario* for legal advice. These people often represent themselves as qualified to offer legal advice or immigration services, but in the U.S. *notarios* are not lawyers and are not authorized to provide any legal services related to immigration. In fact, the "help" they offer might actually hurt you. Get immigration assistance only from those authorized by the U.S. government to provide it. Find an authorized immigration service provider at the U.S. Citizenship and Immigration Service (USCIS) website (https://www.uscis.gov/avoid-scams/find-legal-services).

Don't believe someone's claim that they can get you special treatment or a change to your immigration status. Do not pay for blank government forms; get free forms at www.uscis.gov/forms or by calling the USCIS (800-870-3676) or visiting a local USCIS office (https://www.uscis.gov/about-us/find-uscis-office/field-offices). Don't let anyone keep the originals of your official documents, such as your passport or birth certificate. A scammer might do this to ensure you pay them. USCIS will never ask you to transfer money to an individual, or to wire money via Western Union or use PayPal for immigration fees. The State Department will never email you about receiving a visa.

The USCIS offers tips for avoiding scams and finding legitimate, qualified assistance on its website (https://www.uscis.gov/avoid-scams). The FTC offers additional information at its "Scams Against Immigrants" webpage (https://www.consumer.ftc.gov/articles/0141-scams-against-immigrants).

Deportation scams

How they work: The scammer threatens to arrest or deport you or your family members if you don't pay a fee. Sometimes he or she impersonates an

immigration official or Homeland Security officer, other times a debt collector or the IRS—anyone who can make the threat of deportation convincing.

What to know/do: Immigration, Homeland Security and other agency officials will not call you, threaten you or demand payment. Even if a fee were required, these agencies don't collect payments by phone, or by wire transfer, prepaid card or gift card. They also don't ask immigration applicants to confirm personal information (such as passport number) that they should already have. If you have applied for a visa and believe a call or other communication could be legitimate, call back using the contact number you were given at the time of your application. Or find it on the legitimate agency's website (beware of spoofed—fake—sites, and don't trust Caller ID).

Student scams

Students can be attractive targets for scammers because they are easy to find (college campuses), have some money (from parents, student loans, part-time jobs, etc.), are away from home for the first time (so not under parents' watchful eyes) and probably inexperienced with money management. The best protection for college students is to learn, before heading off to school, how to recognize and avoid scams.

Tuition scams

How they work: Someone claiming to be from the college registrar or other school office contacts you to say that your tuition is late and you'll be dropped from your classes if you don't make the payment immediately.

What to know/do: As with other scams requiring immediate payment "or else," contact the office the caller claims to represent at a number you find yourself and know is legitimate and ask what the status of your account is. If the original contact was legitimate, you can pay the office when you contact them.

Advance fee scams

How they work: Someone contacts you offering help to get a scholarship, complete your FAFSA (Free Application for Federal Student Aid) or get an internship. You pay the scammer's fee upfront but don't get the help or results you expected.

What to know/do: You can do all these things yourself at no cost (it's not called a **"**Free**"** Application for Federal Student Aid for nothing). The U.S. Department of Education even offers free application assistance at its website (https://studentaid.ed.gov/sa/fafsa/filling-out) and by phone (800-433-3243). However, if you are interested in paying for assistance or guidance, do some research on the company or individual first—verify legitimacy, check customer satisfaction ratings, compare prices, etc.—and get guidance from a counselor at the school you are, or will be, attending. If you have a problem with a company,

report it to your school as well as to your local consumer affairs office and/or state attorney general (AG) (http://www.naag.org/).

Online textbook scams
How they work: A website offers textbooks at "unbeatable" prices, but the books you ordered never arrive.

What to know/do: Generally speaking, unusually low prices for anything should raise a red flag. Don't do business with an online retailer until you have verified that the website and merchant are legitimate. Check online reviews and ratings, and ask around to find out if other students at your school have had a good experience with the merchant. If you do buy, use a credit card so that you have recourse if your order is not fulfilled or the items you receive were misrepresented.

Check-cashing scams
How they work: Similar in most ways to other counterfeit check scams (see page 4), this one is carried out by someone posing as a fellow student, perhaps claiming to have lost their ID/debit card or not having an account established yet. The scammer typically offers to let you keep a portion of the check in exchange for your cashing it. Their check later bounces and you're out the cash you gave them plus a returned check fee.

What to know/do: Simply don't deposit or cash a check from someone you don't know and trust.

Protect yourself!

Being able to recognize common scams is a good way to avoid them and other types of fraud. Learn more about how crooks reel in their prey and what you can do to avoid becoming a victim in ***Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks***, available for free download at Consumer Action's website (https://www.consumer-action.org/english/articles/scams_guide).

About Consumer Action

www.consumer-action.org

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their rights and financially prosper.

Consumer advice and assistance: Submit consumer complaints to www.consumer-action.org/hotline/complaint_form or 415-777-9635 (Chinese, English and Spanish spoken).

About this guide

This guide was created by Consumer Action's Managing Money Project (www.managing-money.org). It is part of a free, comprehensive educational module on scams, including training materials to be used by community educators, available online (https://www.consumer-action.org/modules/module_scams).