Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks

Despite the best efforts of law enforcement agencies, businesses and government, scammers continue to rake in millions of dollars each year from unsuspecting consumers. While it's true that technology has opened up many new opportunities for crooks, in reality, the schemes employ many of the same old tricks. The good news is that regardless of the actual tactics used, a savvy consumer can spot a scam just by knowing the warning signs and being alert.

This guide will 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.

The signs of a scam

Scams are as varied as their perpetrators' imagination, but they all

7 things you must know about scams

1. Scams are always evolving, but you can spot—and avoid—a scam if you know what to look for.

2. An unexpected contact, a request for money or personal information, a sense of urgency, a threat or enticing offer, and pressure to use an unrecoverable payment method are some of the tip-offs of a scam.

3. The internet can be used by crooks to carry out their scams, but it also can be a powerful tool for you to detect and avoid them.

4. Credit cards offer strong consumer protections—using one, rather than other forms of payment, provides recourse if you do not get what you pay for.

5. A second opinion from a savvy and trusted person *before* you respond can be very helpful for avoiding scams and making wise choices.

6. Staying informed about the latest scams and newest tactics makes you better able to protect yourself.

7. Reporting a scam can help stop the perpetrators and also enable other consumers to avoid falling for the con.

have certain things in common. If you know what to look for—the telltale signs of a scam—you can spot a con long before the crook knows you're on to him or her. Not every scam raises all these warning signs, but all raise at least one.

It's probably a scam if:

- Someone contacts you unexpectedly and asks for something (money, personal data, account information or remote access to your computer, for example). The request might not come immediately, but it *will* come.

- You are promised something desirable (the ability to make big money working at home, the chance to get paid for cashing a check, help with a financial problem, or the immigrant visa you want, for example) or threatened with something unwelcome (arrest, deportation, forfeited lottery winnings, etc.).

- There is a sense of urgency to the person's request—they need your payment, personal information or computer access immediately for you to avoid some unwelcome consequence (arrest, account closure, computer crash, a lost investment opportunity, etc.).

- Payment is requested in a form that is untraceable or difficult to cancel or recover (such as a wire transfer or a gift or prepaid card).

- The message sent by a supposedly legitimate business or agency contains typos, unusual capitalization, non-native English use, bad grammar and other errors.

- The email address, phone number or website address (URL) provided in a communication supposedly coming from a well-known business or agency doesn't match the contact information found on its legitimate website, your account statement or another valid source.

Phishing

Phishing is one of the oldest and most widely used methods by scammers to get you to reveal sensitive information that can be used to steal your money, identity or security. In fact, as you will notice in the common scams described below, phishing plays a role in many different scams. Recognizing and avoiding phishing attempts is key to protecting yourself.

Whether delivered by email, phone, text message or social media, phishing messages attempt to scam you by pretending to be from a legitimate business, government agency or other trusted individual or entity that could believably have a need for your Social Security number, account numbers, passwords, birthdate or other sensitive personal information—to deliver a package, verify a transaction, send you a prize, fulfill an order, issue a refund, keep your account open, etc. Typically, there is a link to a website where you are asked to log in to

your account (if you have one) or enter other personal information, or where malicious software will automatically download. In many cases, the website is "spoofed"—designed to look just like the legitimate company or agency's website—to trick you into believing you are secure.

While many phishing messages appear to be from a company or agency, some look like they come from a friend (for example, "Check out the e-card your friend sent!") or a coworker ("I need you to send me the employee W-2s right away!"). Regardless of the purported source, all phishing attempts are designed to get you to act quickly and divulge sensitive information or open yourself up to malware (typically used to gain access to your data or to encrypt your files and demand ransom).

Phishing done by phone (sometimes called "vishing") enables the crooks to spoof, or rig, caller ID and use software programs to create phony automated customer service lines. In some of these scams, the perpetrator provides a phone number in an email, text message or website and requests your personal information when you call. In others, the initial contact is made by phone, by either an actual human or a recorded message. Often, the criminal already has some of your personal information, which he or she uses to create a sense of legitimacy. (For 2017, the FTC reported that scammers mostly contacted people by phone.)

Fraudulent text messages (smishing) often claim to be from the recipient's bank and request that the recipient respond (by text, phone or online) with account login/password to prevent their debit card from being deactivated or avoid some other unwelcome action. Clicking on a URL provided in a fraudulent text message can download malicious software that could allow your smartphone (along with all your contacts, logins and other data) to be hijacked.

Here are some tips for evading phishing attempts:

- **Pay attention to detail.** Most phishing attempts reveal themselves through spelling, capitalization and grammatical errors, non-native use of English (unnatural wording) and unprofessional presentation—things you wouldn't expect from a business or government agency. (View a phishing example in CNET's "How to spot a phishing email": *https://www.cnet.com/how-to/spot-a-phishing-email/*.)

- **Remember** that credit card issuers, banks and other financial institutions will never ask you to disclose your password. That is generally true for other businesses, too. Federal agencies will rarely call you or ask you to confirm personal information by phone. If they do, it is typically only regarding a matter you're already aware of.

- **Never respond directly** to an email or text message from a bank, business or agency, or trust the contact information provided in the message or call. Contact customer service via the known number, email address or website to verify that the request for your information is legitimate.

- **Don't trust the "From" field** in an email message. Reveal the sender's email address to see if it looks suspicious. Even if it doesn't look suspicious, it could be a forged address. (How-To Geek explains how to find out the real sender by digging into the email's "headers": *https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/*.) If either the sender or the subject looks suspicious, delete the email without opening.

- **Be equally critical of website URLs**; Techwalla explains the tricks you might come across (*https://www.techwalla.com/articles/how-to-recognize-a-fake-url*). To protect yourself, check the website address to see if it matches the known URL of the business or agency. Beware of lookalikes.

Type in the correct URL yourself rather than clicking a link. Look for the "s" in the address bar (in *https*) and the key or padlock symbol at the bottom of the browser, both of which indicate a secure website. If the website looks different from the last time you visited, or its appearance is in any way "off," leave—you may be a victim of "pharming." (Pharming refers to a fraudster installing malicious code on your computer that redirects you to a fraudulent website without your knowledge.)

- **Don't click links or open attachments** from unknown sources. Be cautious even with links and attachments sent from friends and other familiar sources, since email contact lists are often hijacked for the purpose of sending out phishing messages that are more likely to be opened.

- **Don't trust caller ID.** Technology has made it easy for scammers to block caller ID or to display a name or number you are likely to recognize and trust.

Learn more at Phishing.org (*www.phishing.org*). (Though the website is designed to help organizations and their IT professionals thwart phishing attempts, there are examples and tips useful for individuals, too.)

Report phishing attempts to the company, agency or organization impersonated in the message. Also forward phishing emails to the Federal Trade Commission (FTC) at *spam@uce.gov*, and file a complaint with the Internet Crime Complaint Center (IC3) (*https://www.ic3.gov/complaint/splash.aspx*).

Note: Check your financial account statements frequently for signs of fraudulent activity. (No need to wait for your monthly statement—you can check account activity online as often as you like.) If you find an unauthorized transaction, notify the bank or card issuer immediately. You have protections under the law, but there are deadlines you have to meet.

Common scams

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. Following is an overview of the types of scams that target the general public or, in some cases, particular groups of people. As you read about them, note what they have in common and look for the warning signs that would alert you to similar ploys.

For a compilation of dozens of common scams, including advice for avoiding each one, download the companion publication **Common Scams: Recognizing and avoiding fraud** from the Consumer Action website (*https://www.consumer-action.org/english/articles/common_scams*).

General scams

These ploys typically don't target a specific demographic; 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).

Some of the most widely perpetrated scams aimed at U.S. adults include:

- Imposters claiming to be from government agencies, debt collection companies or other "authorities" requesting your personal information or demanding money
- The passing of counterfeit checks
- Advance fees collected for worthless or undelivered services, or required before collecting a (non-existent) jackpot, inheritance, grant, etc.
- Requests for money or information in

exchange for (non-existent) help recovering money you've lost to a previous scam

- Requests for donations to bogus charities
- Pyramid/Ponzi investment schemes
- Sales of counterfeit or non-existent goods and services
- Bogus tech support offers and the installation of malware on victims' computers or smartphones
- Fake online romances and friendships that result in requests for money
- Blackmail (demanding money to keep photos or video of you from becoming public)

Senior scams

While consumers of all ages should be on guard against scams, research shows (*http://news.usc.edu/135031/senior-scams-and-fraud-due-to-aging-brain/*) that seniors can be particularly vulnerable to fraud 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. 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/*).

Some of the most widely perpetrated scams targeting U.S. seniors include:

- Imposters claiming to be from Medicare or the Social Security Administration requesting personal information or demanding money

- The sale of overpriced, worthless or dangerous medical devices or prescriptions
- High-fee, unaffordable and questionable home equity loans that often result in foreclosure
- Imposters pretending that a family member is in trouble and needs money immediately
- Imposters pretending that your deceased loved one owes them money
- The sale of fake burial plots, or high-pressure sales of overpriced funeral services
- The sale of ineffective or harmful anti-aging treatments and products

Veteran and servicemember scams

A late-2017 AARP Fraud Watch Network survey found that veterans are more likely than other Americans to be the victims of scams. In fact, more than twice as many veterans as nonveterans lost money to scam artists during the previous five years. Instead of receiving deserved respect for their service to our country, veterans, and even active duty servicemembers, are instead often targeted by scammers. Below are a few of the most prevalent veteran scams. Read the AARP Watchdog Alert Handbook: Veterans' Edition: 10 Ways Con Artists Target Veterans (*https://www.aarp.org/home-family/voices/veterans/info-2020/watchdog-alert-handbook.html*) to learn more about how to avoid becoming a scam victim.

Some of the most widely perpetrated scams aimed at U.S. veterans and servicemembers include:

- Requests for donations to bogus charities
- High-priced pension advance loans or offers to buy out future pension or disability benefits
- The sale of annuities or trusts to veterans in order to qualify for the Aid & Attendance Benefit
- High fees for military records or for assistance filing for veterans benefits
- For-profit schools that mislead prospective students into using their GI Bill benefits on a sub-par education
- Imposters claiming to be from the U.S. Department of Veterans Affairs (VA) and requesting personal information

Immigrant scams

The vast majority of scams targeting immigrants in the U.S. use either the promise of achieving a desired immigration status or the threat of deportation to persuade the immigrant 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 important to verify claims and get assistance from qualified agencies and individuals.

Some of the most widely perpetrated scams targeting U.S. immigrants include:

- Unqualified or worthless immigration advice and assistance
- Fees for forms and services that are available free
- Imposters threatening deportation if demands for money aren't met
- Bogus investments or business opportunities

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 may be inexperienced with money management. The best protection for college students is to learn, before heading off to school, how to recognize and avoid scams.

Some of the most widely perpetrated scams aimed at college students include:

7 ways to avoid a scam

1. **Be vigilant.** There are scammers and shady businesses around every corner, just waiting for their next victim. Keep your guard up.

2. **Maintain a healthy level of skepticism.** Scrutinize all unsolicited communications. If it sounds too good to be true, it almost certainly is.

3. **Beware of urgency.** Being rushed usually means someone doesn't want to give you time to do some research and make an informed decision.

4. **Guard your money and data.** If someone you don't know unexpectedly asks you for money or personal information, ignore them. Verify requests that might be legitimate *before* you act.

5. **Do your due diligence.** The internet is a great vetting tool. Use it to verify stories, names, phone numbers and other information you are given.

6. **Consult with someone you trust.** When faced with a request (or demand) for money, personal information or access to your computer or an account, get a second opinion from someone savvy and trustworthy.

7. **Pay with a credit card.** While other types of payment cards offer some protections, credit cards offer the strongest consumer protections under federal law—the right to dispute a fraudulent transaction, for example, and a $50 limit on your liability for unauthorized charges—and payments are traceable.

- School administration imposters demanding payment for tuition or other fees
- Fees for services that are available free (such as help filing a financial aid application)
- Online textbook sellers who take your money but don't fill the order
- The passing of counterfeit checks

Using the internet to avoid scams

While the internet is the tool of choice for many scammers, it is also a strong tool for identifying and avoiding scams.

Within minutes, a consumer with access to the internet can research an individual or company; verify a URL, phone number or address; check reviews and ratings; compare prices; and determine if a communication is questionable.

If you don't have internet access or are not comfortable online, get help at the public library, from a family member or friend, or from a local consumer protection office, Better Business Bureau or other trustworthy source.

Here are some ways to use the internet to protect yourself:

- *Check the validity of a threat, offer, claim or story.* A simple online search can reveal a scam. For example, the two top search results for "grandson call needs money for bail" are "How to Beat the Grandparent Scam – AARP" and "'Grandparent scam' explained: What you need to know – CBS News." Do this type of search, using at least a couple of different combinations of key words, whenever you need to verify what a potential scammer tells you.

- *Research an individual or company.* Type a name into the search bar of your browser and see what comes up (try it both with quotes around the name and without). Continue to dig

until you are satisfied. If there are no results for your search, that could be a red flag that the individual or company name is made up. If you find the company or individual's website, check it for professionalism. Typos, fuzzy images, stock photos, missing information and limited pages (no privacy policy, terms of use, etc.) can be a sign that the site was put together hastily, perhaps because it is a scam. Check the site's registration data—the name under which the website was registered and when it was created—at WhoIs.net (*www.whois.net*). Learn more about checking a domain's registration at *https://www.wikihow.com/Find-Out-Who-Registered-a-Domain*.

■ *Verify a company's web address, physical address and phone number.* Rather than trust the contact information you are given by a possible scammer, find it online, at the company or agency's legitimate website. Be sure you have spelled the name correctly—misspellings can take you to spoofed (fake) sites. Check the URL of the site you visit to be sure it isn't an adulterated version of the correct address (for example, www.microsofthelp.com or www.micosoft.com instead of the correct www.microsoft.com).

■ *Check ratings and reviews.* Do a search for the name of the company or individual along with the word "ratings" or "reviews" to see what customers and complaint handling and rating services (such as the Better Business Bureau) have to say. Check Facebook to see if the company has a page and if there are customer comments on it. If a company doesn't have any online reviews or ratings, or if they are all glowing, you might be dealing with a scam. Learn how to recognize fake reviews from Money (*http://time.com/money/4095258/fake-online-reviews-yelp-amazon-tripadvisor/*) and How-To Geek (*https://www.howtogeek.com/282802/how-to-spot-fake-reviews-on-amazon-yelp-and-other-sites/*).

Staying ahead of scammers

Scammers always seem to find new ways to find and trick their prey. Even consumers who consider themselves savvy can be caught off guard by a new twist on an old scam. The best way to avoid getting conned is to be aware of the latest scams making the rounds. That's easy to do thanks to a handful of newsletters and email alerts sent regularly by consumer protection groups and agencies to subscribers.

SCAM GRAM newsletter: SCAM GRAM is Consumer Action's monthly email alerting you to the dirtiest players in the world of tech fraud, credit card scams, ID theft and general con-artistry. Sign up to receive the SCAM GRAM each month in your inbox (*https://www.consumer-action.org/news/scam-gram*).

Fraud.org fraud alerts: Stay ahead of trending scams by signing up for Fraud.org monthly fraud alerts (*http://www.fraud.org/*). You can also

visit the website anytime to read about the latest tricks and tactics (*https://fraud.org/category/fraud-alerts/*).

Better Business Bureau (BBB) scam alerts: As the go-to for complaints against businesses, the BBB knows a thing or two about scams. The organization's Scam Tracker allows you to report a scam and read about other consumers' reported scams, all with the goal of foiling future attempts (*https://www.bbb.org/scamtracker/us/*).

Federal Trade Commission (FTC) scam alerts: Stay a step ahead with the latest information and practical tips from the nation's consumer protection agency. Browse FTC scam alerts by topic or by most recent (*https://www.consumer.ftc.gov/scam-alerts*), or sign up to have them sent directly to your inbox.

If you've been scammed

If you are the victim of a scam, you should report it. Where to report it depends on the type of scam. In virtually all cases, you should notify the Federal Trade Commission (*https://www.ftccomplaintassistant.gov*). The FTC collects information about current scams and frauds and directs it to law enforcement officials.

In most cases, you should also report it to your state attorney general (*http://www.naag.org/*). If the scam was a local job, notify your district attorney's office (*https://www.usa.gov/state-consumer*) as well. If you need a police report, contact local law enforcement.

If the scam was perpetrated via the internet, report it to the Internet Crime Complaint Center (IC3), an interagency website run by the National White Collar Crime Center and the FBI (*https://www.ic3.gov/complaint/default.aspx*).

If you believe it was an international scam, you can report it to eConsumer.gov (*www.econsumer.gov*), a site run by the International Consumer Protection and Enforcement Network (ICPEN), which is a partnership of 34 consumer protection agencies around the world.

If you received a scam letter or a fake check in the mail, report it to the United States Postal Inspection Service (*https://www.uspis.gov/report/* or 800-ASK-USPS).

IRS-related phishing attempts and other types of tax-related fraud should be reported to the Treasury Inspector General for Tax Administration (TIGTA) (*https://www.treasury.gov/tigta/contact_report_scam.shtml* or 800-366-4484).

If you are the victim of investment fraud, report it to one or more of the agencies that regulate the investment industry. This might include the Securities and Exchange Commission (*www.sec.gov/complaint/select.shtml* or 800-SEC-0330) and/or your state securities regulator (*http://www.nasaa.org/about-us/contact-us/contact-your-regulator/*). For reporting tips and additional contact information, visit the "Reporting Investment Fraud" page of SaveAndInvest.org (*https://www.saveandinvest.org/protect-your-money-report-fraud/reporting-investment-fraud*).

If the fraud was related to Medicare or Medicaid, report it to the U.S. Department of Health and Human Services Office of Inspector General (*https://forms.oig.hhs.gov/hotlineoperations/report-fraud-form.aspx* or 800-HHS-TIPS/800-447-8477). You can also report Medicaid fraud to your state agency (*https://www.cms.gov/About-CMS/Components/CPI/CPIReportingFraud*).

If you are a veteran who received a phishing call or email, report it to the U.S. Department of Veterans Affairs' Identity Safety Service (*https://www.va.gov/identitytheft/* or 855-578-5492).

If you received a suspicious call from someone alleging to be from the Social Security Administration (SSA), report it to the Office of the Inspector General *(https://oig.ssa.gov/report* or 800-269-0271).

Report credit and loan-related frauds, as well as scams related to money transfers, credit reports and other financial services, to the Consumer Financial Protection Bureau (*https://www.consumerfinance.gov/complaint/* or 855-411-2372). Find out where else to report different types of financial scams at the "Complaints About Banks and Lenders" page of USA.gov (*https://www.usa.gov/complaints-lender*). For tips on reporting mortgage and lending fraud, visit the "Reporting Mortgage and Lending Fraud" page of SaveAndInvest.org (*https://www.saveandinvest.org/protect-your-money-report-fraud/reporting-mortgage-and-lending-fraud*).

Notify your wireless service provider and/or your internet service provider of scam texts, emails and phone calls.

If you paid a scammer by credit card, dispute the charge with your card issuer. Contact your bank if you paid by debit card to see if you can stop payment or dispute the transaction. If you paid by prepaid card or gift card, contact the card issuer to find out if you have any recourse. If you paid via a third-party payment intermediary, such as PayPal or eBay, contact the company to see if you can dispute the transaction. If you paid the scammer via Western Union, call the company's fraud hotline (800-448-1492). If you used a different money transfer service, check its website for fraud reporting contact information.

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).

If you're an identity theft victim, visit IdentityTheft.gov (*www.identitytheft.gov*) to report the theft and create a recovery plan. If you think that your financial accounts were accessed or new accounts were opened in your name, request a free credit report (once every 12 months or whenever you're a victim of fraud) from each of the three major credit bureaus at AnnualCreditReport.com (*www.annualcreditreport.com*).

If you have low income and are the victim of a home equity, investment or similar financial scam, find local legal aid through the Legal Services Corporation website (*https://www.lsc.gov/what-legal-aid/find-legal-aid*). If you don't meet income guidelines, you can contact a local bar association to find an attorney (*https://www.americanbar.org/groups/legal_services/flh-home/flh-bar-directories-and-lawyer-finders.html*).

About this guide

This guide was created by Consumer Action's Managing Money Project (*www.managing-money.org*).

© Consumer Action 2018