Current 2025 Top 10 List of Scams and Frauds

Top 10 List of Scams of 2025

Below is our list of the top 10, constantly updated. We have a side-by-side comparison of other reporting agencies top 10 scam lists here. The FTC's (Federal Trade Commission) data reported more than $5.8 billion in losses to 2.8 million consumers due to fraud in the last reporting year, which is an increase of more than 70 percent over the previous year.

The top categories are various imposter scams, followed by online shopping scams, then prizes, sweepstakes, and lotteries; internet services and fake job opportunities.

Medical scams of all types grew to become the largest category during COVID, but have overtaken by more traditional scams: phishing, spoofing, identity theft. For detailed explanations of each scam, how to report a scammer and how to protect yourself, click on the blue titles below for more information! To see federal and select state top 10 scam lists, click here. You can see state by state statistic (for states that report them) here.

Our list focuses on the scams that you could avoid, those reported to the CFR, FTC, Fraud.org and BBB (Better Business Bureau). For detailed explanations of each scam, how to report a scammer and how to protect yourself, click on the blue titles below for more information!

We have compiled other lists as well:

- FTC and national news and consumer organization top 10 consumer complaint scam lists.
- FTC, FBI, AARP, Arizona, Florida, Illinois, Ohio and Oregon
- Missouri, New York, Oregon, Ohio, Texas and Vermont

And to see a list of other type of top 10 scams, such as by category, or targeting specific groups, see this page.

For a quick look-up of new and current scams, see this alphabetized list of scams

Top 10 Scams

1. **Identity Theft, Phishing and Pharming**
   Usually a scammer sends an email, a text message or calls your phone and pretends to be some organization, company or person you trust. Scammers gain access to your confidential information, like social security numbers, date of birth and then use it to apply for credit cards, loans and financial accounts. Typically, the victim receives an email that appears to be from a credible, real bank or credit card company, with links to a website and a request to update account information. But the website and email are fakes, made to look like the real website. Here's a current example, the PayPal, "your account has been limited" scam.

2. **Phone scams**
   This includes telemarketers violating the Do Not Call list, Rob dialers, scammers calling up pretending to be from a bank or credit card company. The National Do Not Call Registry (U.S.) or the National Do Not Call List (Canada) offer consumers a free way to reduce telemarketing calls. Scammers call anyway, of course, and they've even found a way to scam consumers by pretending to be a government official calling to sign you up or confirming your previous participation on the Dot Not call list! A good example of this is the "Your Microsoft license key has expired" scam call - which you can hear and read about on this page. Medicare scam text messages

3. **Debt Collection**:
   Most of the complaints under this category involve debt collectors. Consumers tell of receiving calls from harassing collectors who are threatening and will repeatedly call attempting to collect a debt. Other complaints that fall under this category involved credit/debit card fees, pay day loans, credit repair companies and unauthorized use of credit/debit cards. Some of these complaints involved hidden fees and billing disputes as well.

4. **Fake Government Officials**
   If you received an email, letter or phone call from a government agency (typically the IRS or FBI) and it instructs you to wire, Western Union or MoneyGram money someplace, or follow a link and enter information - don't believe it! The U.S. government would never instruct anyone to use those methods to pay any bill or carry out a financial transaction, particularly with an overseas bank or agency.

5. **Scam Text Messages** - It looks like a text alert from your bank, asking you to confirm information or 'reactivate your debit card' by following a link on your smart phone. But it is just a way to steal personal information.

6. **Loans Scams / Credit Fixers**
   False promises of business or personal loans, even if credit is bad, for a fee upfront. Or a scam that promises to repair your credit for a fee.

7. **Fake Prizes, Sweepstakes, Free Gifts, Lottery Scams**
   You receive an email claiming you won a prize, lottery or gift, and you only have to pay a "small fee" to claim it or cover "handling costs". These include scams which can go under the name of genuine lotteries like the UK National Lottery and the El Gordo Spanish lottery. Unsolicited email or telephone calls tell people they are being entered or have already been entered into a prize draw. Later, they receive a call congratulating them on winning a substantial prize in a national lottery. But before they can claim their prize, they are told they must send money to pay for administration fees and taxes. The prize, of course, does not exist. No genuine lottery asks for money to pay fees or notifies its winners via email.

8. **Internet merchandise scams**
   You purchase something online, but it is either never delivered or it is not what they claimed it was, or is defective. Online shopping, and other shop from home, such as catalog, mail and phone shopping scams are on the rise. See this page about Facebook Marketplace Scams.

9. **Automobile-Related Complaints**
   Car loans, car buying, car sales, auto repair, fake or useless extended warranties. Some of the complaints alleged consumers paid for repairs and that services provided were shoddy. Consumers reported repair companies that return vehicles to the consumer in a worse condition than how it was initially given to them. Other complaints involved consumers not receiving title to their vehicles at the time of sale.

10. **Fake check payments**
    You sell something online or through Craig's List Consumers and you're paid with phony checks, and instructed to wire money back to buyer. The check looks real... but after you try to cash it, you find out it is a fake; and you're arrested for passing a counterfeit check! Read more about scam checks on this page and here about the EBay check scam.

And here are the next most common scams:

11. **Recovery/Refund Companies**
    A scammer contacts and claims you owe money on a debt or the scammer offers to recover money lost in a previous scam.

12. **Computer Performance Scams: Equipment and Software**
    Scammers claim to offer "technical support" for computer problems and charge a fee to fix nonexistent problems.

13. **Credit Bureaus and related credit scams**
    Credit/debit card fees, pay day loans, credit repair companies and unauthorized use of credit/debit cards. Some of these complaints involved hidden fees and billing disputes as well.

14. **Scholarship, Student Loan and Financial Aid scams**
    For a fee, a "search company" offers to conduct a customized search for scholarships or grants for students to apply for. Scammers take the money and run or provide a worthless list.

15. **Online Dating Scams**
    Fake profiles of scammers posing as attractive men and women, then claiming they need money to help in an emergency, typically when they claim to be out of the country on a business trip.

16. **Facebook Fake Friend Scam** - Did you ever get a Friend Request on Facebook from someone you already thought was your Friend? If you hit Accept, you may have just friended a scammer. Con artist nurtures an online relationship, builds trust, and convinces victim to send money.

17. **Click Bait Scam -** This one takes many forms, but many people may recall seeing those using Robin Williams death or the Malaysian Airline plane that went missing ("click here for video"). Other click bait schemes use celebrity images, fake news, and other sensational stories to get you to unknowingly download malware.

18. **Fake bills and invoices** - "Pro forma" invoicing: You get a bill that looks real, but either you never ordered the product or service, or they're not really the company you bought it from.

19. **Tech Support Scam:** You get a call or a pop-up on your computer claiming to be from Microsoft (or Norton, or Apple) about a problem on your computer. They say if you give "tech support" access to your hard drive, they can fix it. Instead, they install malware on your computer and start stealing your personal information.

20. **Medical Alert Scam** - This is a telemarketing scam that promises a 'free' medical alert system, that scam targeted seniors and caretakers. The robocalls claimed to be offering the medical alert devices and system free of charge because a family member or friend had already paid for it. In many cases, seniors were asked to provide their bank account or credit information to 'verify' their identity and, as a result, were charged the monthly $35 service fee. The system, of course, never arrived and the seniors were left with a charge they had trouble getting refunded. Easy rule of thumb - be wary of 'free' offers that require your personal information upfront and always verify with the supposed friend or family member that the caller says paid for the service.

21. **Ebay / Auction Reseller Scam** - Scammers posing as buyers convince sellers into shipping goods prior to receiving payment. Usually the fake buyer claims it's an 'emergency' like a child's birthday and asks the seller to ship the same day. The seller receives an email that appears as though it came from PayPal for the payment, but emails like that are easy for scammers to fake.

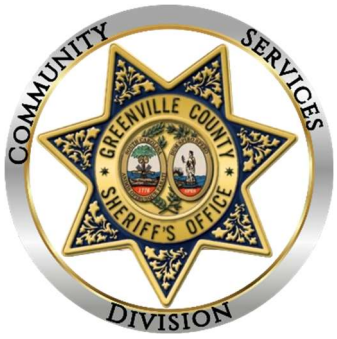
22. **Arrest Warrant Scam** - Scammers create a fake Caller ID, which allows them to call you and appear to be calling from a local police, sheriff or other law enforcement agency. They say there is a warrant out for your arrest, but that you can pay a fine in order to avoid criminal charges. Of course, these scammers don't take credit cards; only a Western Union MoneyGram, other wire transfer or pre-paid debit card will do.

23. **Invisible Home Improvements** - In addition to email, mail and phone, scammers now just show up at your door. Scammers posing as home improvement contractors come door-to-door sale and target seniors, those who live alone, and victims of weather-related disasters are common targets.

24. **Casting Call Scam** - Scammers pose as agents or talent scouts looking for actors, singers, models, reality show contestants, etc., and use phony audition notices to fool aspiring performers into paying to try out for parts that don't exist.

25. **Foreign Currency Scam** - Investments in foreign currency can sound like a great idea, and scammers frequently use real current events and news stories to make their pitches even more appealing. They advertise an easy investment with high return and low risk when you purchase Iraqi Dinar, Vietnamese Dong or, most recently, the Egyptian Pound. The plan is that, when those governments revalue their currencies, increasing their worth against the dollar, you just sell and cash in. Unlike previous hoaxes, you may even take possession of real currency. The problem is that they will be very difficult to sell, and it's extremely unlikely they will ever significantly increase in value.

26. **Affordable Care Act Scams (Obamacare) -** Scammers love the Affordable Care Act ('Obamacare'), using it as a way to fool Americans into sharing their personal information. **For guidance about health insurance see our sister website, ConsumersHealthcareGuide.org**.



Other common scams:

- **Internet Auction Frauds**
  Auction frauds (commonly called Ebay or PayPal scams, after the two largest venues) is a misrepresentation of a product advertised for sale through an Internet auction site or the failure to deliver products purchased through an Internet auction site.

- **Phishing/Spoofing Emails**
  Emails that pretend to be from a company, organization or government agency but ask you to enter or confirm
  your personal information

- **Nigerian Advance Fee Frauds (AFF)**
  These frauds take the form of an offer, via letter, e-mail or fax, to share a huge sum of money in return for using the recipient's bank account to transfer of the money out of the country. The perpetrators will often then use the bank account details to empty their victim's bank account. Often, they convince the victim that money is needed up front, to pay fees or is needed to bribe officials.

- **"PASSIVE RESIDUAL INCOME" SCAMS**
  Get rich scheme and scam websites - Make $$$ in your spare time! It so EASY once you get their free book or cd and learn their secrets! Sure... These websites are themselves scams; claiming to offer you a good deal, when at best, their products are worthless, they have no real secrets, and worse, some are identity thieves!

- **FreeCreditReport.com**
  What a scam this one is! The name of the website is freecreditreport.com, but you'll only get a credit report when you sign up for their paid service. And worst of all there IS a government mandated website where you CAN get a free credit report! Find out more here!

- **Work at Home Scams**
  Work-at-home and business opportunity scams are often advertised as paid work from home. After the would-be worker applies, they are asked for money up-front to pay for materials and, after paying, they hear nothing back. A variation of this is, people are asked to invest in a business that has little chance of success.

- **Matric and Multilevel Marketing** and **Pyramid Schemes**
  "MAKE MONEY NOW!" scream their websites! And do it in your spare time! Earn big bucks for almost no work. If that isn't enough to tell you it is a scam, let us explain why it is. These schemes are promoted through websites offering expensive electronic gadgets as free gifts in return for spending about $25 on an inexpensive product, such as a mobile phone signal booster. Consumers who buy the product then join a waiting list to receive their free gift. The person at the top of the list receives his/her gift only after a prescribed number of new members join up. The majority of those on the list will never receive the item.
  Pyramid schemes offer a return on a financial investment based on the number of new recruits to the scheme. Investors are misled about the likely returns. There are simply not enough people to support the scheme indefinitely.

- **Property Investment Scams**
  Investors attend a free presentation, which aims to persuade them to hand over large amounts of money to enroll on a course promising to make them a successful property dealer, usually involving "no money down".
  Schemes can involve the offer of buying yet-to-be built properties at a discount. Other variations include a buy-to-lease scheme where companies offer to source, renovate and manage properties, claiming good returns from rental income. The properties are generally near-derelict and the tenants non-existent.

- **900 Phone Number Scams**
  Postal notification of a win in a sweepstake or a holiday offer in this scam include instructions to ring a premium rate number. This is generally an 900 toll number. Calls to the number incur significant charges, the recorded message is lengthy, and the prize often does not exist. It is a scam that has been around a long time, but it is still in use.

- **Advance Fee Brokers**.
  Often these appear to be very professional operations with attractive websites and advertisements. However, it is illegal for a business to charge a fee prior to providing a loan. Typically, after wiring money to the scammer, the victim never receives the loan. These 'lenders' will use fake physical addresses or the addresses of real companies.

- **Credit Repair Services with Advance Fees**.
  Consumers with bad credit ratings are particularly vulnerable to this scam. Everything a credit-repair operation offers an individual can do personally at little or no cost. Credit repair operations cannot ask for money in advance and they cannot automatically remove legitimate negative reports from your credit history.

- **Foreign Lottery Scams**.
  Any lottery from a foreign country is illegal in the United States. Stating a person can win or is a winner already provides a strong incentive; however, people should never send money to obtain lottery money. Scammers using fictitious addresses will request you send 'fees and taxes' to them through a wire service, take the cash and never provide any winnings because there are no winners.

- **Office Supplies - Sale by Deceptive Telemarketing**.
  This scam features fake invoices for office supplies being sent to a business, often for only a couple hundred dollars. This relatively low amount makes it easier for company personnel to quickly sign off and feel it is not worth their time to check the invoice's validity, which would be done if it was for a larger amount.