The Latest Scams You Need to Be Aware of in 2025

QUICK ANSWER

Scammers often use new technology, such as AI, to enhance tried-and-true scams. Learn about the latest twists and types of attacks, and what you can do to stay safe in 2025.

The new year doesn't necessarily bring about a shift in scam tactics. In fact, over the years, many scams have slowly evolved as scammers incorporate new technology and play off of the most recent major events.

But there is a general sense that scams and fraud have become increasingly common around the world. The Global Anti-Scam Alliance (GASA) reports that over $1.03 trillion was lost to scammers in 2024.

Scammers almost always have the same goal—to get your personal information or money. Learning about the latest developments will hopefully help you stay one step ahead. The latest scams to watch out for in 2025 include AI-powered scams, imposter scams and investment scams.

1. AI Scams

The clearest example of scammers using new technology comes from the explosion of artificial intelligence and thus AI-powered scams.

In December 2024, the FBI posted a public service announcement listing some of the ways that criminals use generative AI to trick victims. The GASA also highlighted the increasing role of generative AI in scams around the world and noted that deepfake-related crime increased by more than 1,500% in the Asia-Pacific region from 2022 to 2023.

Generative AI tools generally get classified by the type of content they generate, such as text, images or videos. Scammers can use them to enhance different types of popular scams:

- **Phishing and smishing:** Scammers can use AI to write more convincing and natural-sounding phishing emails and text messages.

- **AI images:** Scammers can use AI-generated images to quickly create eye-catching websites, social media ads, fake identification documents, explicit photos and fake headshots for social media profiles.
- **Deepfake videos:** AI-generated videos might be created to promote fake products, services or investments. Scammers also might use deepfake recordings or real-time face- and body-swapping tools to trick victims into thinking they're someone else.
- **Fake and cloned voices:** Scammers also use AI-generated or altered voices for their videos and for phone-based scams. Some AI tools can even mimic real accents.

The potential to create an image, video or voice of someone can make many existing scams more believable, and it opens up new opportunities for scammers.

Learn more: Who Gets Scammed the Most?

2. Imposter Scams

Scammers almost always hide their identity, and imposter scams are one of the most common types of scams or fraud because the category is fairly broad. These happen when the scammer pretends to be a friend, relative, celebrity, politician, businessperson, government agent, delivery person or company representative.

Some types of imposter scams are so prevalent that they have their own name, such as the grandparent scam (which doesn't actually always involve a grandparent) and romance scams (which sometimes involve platonic rather than romantic relationships).

According to the Federal Trade Commission's (FTC) 2023 Consumer Sentinel Network Data Book, about 20% of people targeted by an imposter scam in 2023 lost money, and the median loss was $800. The FTC also reported that government imposter scams in particular led to a massive increase in losses during the first three months of 2024, with median losses of $14,740.

Now that scammers can use AI, it's more important than ever to be skeptical when someone contacts you, especially if they try to scare you or offer you a gift or investment opportunity.

2025 Spotlight: Email and Text as Preferred Contact Methods

The FTC reports that the percentage of imposter scams that start with a phone call has decreased from 67% in 2020 to 32% in 2023. Text messages and email are becoming a preferred method of first contact.

For example, the scammers might impersonate a company and send a message or email about a fake security alert, renewal, invoice, discount or tracking error. There are even multi-party scams, where the first scammer directs you to an accomplice who poses as a government agent or bank employee.

Learn more: Different Types of Identity Theft and Fraud

3. Sextortion Scams Targeting Children and Teens

One disturbing scam that's become more prevalent in recent years is a financial sexual extortion, or sextortion, scam.

The scammers often pretend to be young girls or women who are interested in a romantic relationship. They may send stolen or AI-generated explicit photos and trick victims into sharing explicit photos or videos. Alternatively, scammers sometimes trick victims after forming a friendship and then offering money, gift cards or something else in exchange for images or videos.

Victims are told that the images or videos will be sent to family, friends and classmates if they don't pay the scammers. Often, this all happens very quickly—sometimes in less than an hour—and victims may be too embarrassed to ask for help.

The FBI and the National Center for Missing and Exploited Children's CyberTipline have more resources. You can also report the scam to the CyberTipline and get help taking down explicit content.

Learn more: Common Scams Targeting Children and Teens

4. Romance Scams

While romance scams aren't new, they remain a popular scam and are a prime example of how scammers can use generative AI to trick victims.

Scammers often steal someone's identity or create fake profiles on dating and social media apps to meet victims. There's no surefire method to detect a fake. Some will use AI to deepfake video calls, and some crime

organizations even force people or hire models to conduct romance scams.

After gaining your trust, the scammer might ask you to buy them something, ask for money or give you an investment "tip" that's part of the scam. Or, the person may "mistakenly" send you money and ask you to send it back or forward it to someone else. If your bank later determines that their payment was fraudulent, the sum of the payment will be subtracted from your account.

Many romance scams start with text messages, private messages on social media or in dating apps. And they can target anyone—some scammers even seek to form platonic rather than romantic relationships.

2025 Spotlight: "Accidental" Text Messages

Have you gotten a text message that seems genuine, but it also appears to be intended for someone else? It might say something like, "Sorry I'm running late, I'll be there in 15 minutes." Not wanting to be rude, you respond to tell the sender they've got the wrong number.

These wrong number texts are often the first step in a romance or employment scam. Although there's sometimes a scammer on the other end from the start, scammers can also use AI messaging bots to target thousands of people at a time.

5. Phone-Related Scams

Scammers may contact you by phone, and some phone scams rely on smartphones' capabilities to access the internet and install malware. These phone-related scams include:

- **Robocalls:** Robocalls have people's phones ringing nonstop with increasingly natural-sounding recorded voices. They may offer everything from auto warranties to vacations, or issue a threat to try and get your attention. Some robocalls can even respond to your questions using prerecorded or AI-generated messages.
- **Malicious apps:** Scammers may try to get you to install a malicious app to steal your information. Or, they might create a nearly identical copy of an existing app and then make money from in-app purchases. Recently, there were reports of malware that could infect your phone and trick you into calling the scammer when you try to call your bank.

- **QR codes:** These convenient codes have gained popularity as a touchless option to do things like read a restaurant menu or make a payment. However, scammers place their QR codes in inconspicuous spots, and scanning the code could prompt you to make a small purchase or enter your credentials on a lookalike website. Some scammers even go as far as printing QR codes on letters that appear to come from government agencies and then mailing them out.
- **SIM swapping:** This technique is used by a thief to reassign your number to a SIM card in a phone they control. They can then try to log in to your accounts using codes or links sent to your phone number. Contact your carrier to see if there are any security measures for stopping SIM swapping. Also, see if your accounts let you use a non-SMS multifactor authentication option, such as an authenticator app that the scammer can't steal or access.
- **One-time password (OTP) bots:** Some scammers use so-called OTP bots to trick people into sharing the authentication codes. The scammer might try to log in, prompting the bank to send you a one-time code. At the same time, the bot imitates the company and calls, texts or emails you asking for the code. The timing might convince you that the bot's request is legitimate. However, if you respond, it sends the code to the scammer, who can now log in to your account.

Learn more: Ways to Protect Your Parents From Phone Scams

6. Cryptocurrency and Investment Scams

Cryptocurrency prices rocketed after the presidential election, and cryptocurrency scams are sure to follow. These have taken different forms over the years, including scams involving fake prizes, contests, giveaways or early investment opportunities.

The scammers may impersonate celebrities or popular websites to lure victims into sending them money, sharing login information or "investing" in a project. Crypto exchange accounts have also been the target of the OTP bot attack technique described above to prevent you from getting your crypto back while the scammer drains your account.

Investment scams often rely on similar techniques, but without the crypto spin. The Better Business Bureau (BBB) considered the combined crypto and investments scam to be the riskiest scam in its 2023 BBB Scam Tracker Risk Report. Although it didn't have the highest median losses at $3,800, over 80% of people who were targeted reported a loss.

7. Online Purchase Scams

Online purchase scams continue to be one of the riskiest types of scams, according to the Better Business Bureau. Although median losses were relatively low at $100, over 40% of the scams reported to the BBB were online purchase scams and over 80% of people report falling for the scam.

Some scammers set up fake e-commerce stores and buy ads for the website on social media. Alternatively, scammers might list items for sale on online marketplaces, including social media platforms' marketplaces.

The scammers might take your money and never send anything in return. Or, they might be committing triangulation fraud and purchasing the item you bought with someone else's stolen credit card. You might not realize you were part of a scam unless you try to return the item or use a warranty.

Always look for red flags such as too-good-to-be-true prices, lack of details or high-pressure sales tactics. Paying with your credit card can also help you limit potential losses, as you can initiate a chargeback if you don't receive a product or service.

2025 Spotlight: Refund Phishing

Some scammers figured out a new way to profit from stolen credit card information. Rather than focusing on stealing money from the card, they make a fraudulent purchase from a fake merchant whose name is a phone number or email. Victims call or visit the site to dispute the transaction, but they're phished—tricked into sharing personal and account information with the scammer.

Learn more: What Is Social Engineering and How Can You Protect Yourself?

8. Employment Scams

Employment scams use enticing, and hard-to-detect, lures to target people who've been out of work. Some scammers take a slow approach with interviews and a legitimate-seeming operation. They then collect personal information from your employment forms, or tell you to buy equipment or training.

Other scams get right to the point and promise guaranteed or easy income—if you purchase their program. Sometimes, a fake employer sends a large paycheck and asks you to send the "extra" back—a play on the popular overpayment scam.

The FTC says reports about task scams, when you're hired to repeat simple tasks online, increased from about 5,000 during all of 2023 to 20,000 during the first half of 2024. You might be able to withdraw small amounts at first. But the scam occurs when you're told you can pay to increase your earning rate and that you have to deposit money to unlock larger withdrawals. You make the payments, but you can't get any of the money—or your supposed earnings—out.

You may also come across job opportunities that involve receiving money and sending funds to another account, or receiving and reshipping packages. These "money mule" and "reshipping mule" jobs are often part of an illegal operation, and you could be personally liable.

Learn more: How to Protect Your Bank Account From Fraud

9. Check Fraud

Criminals have been breaking into mailboxes and robbing mail carriers to steal mail and look for checks. If you mail a check and it's stolen, they might create a counterfeit check and use it to withdraw money from your account.

Your bank or credit union will often reimburse you, but it could take a long time and cause money problems while you wait. It might be best to avoid writing and mailing checks altogether. If you have to send a check, some pens, such as Uni-Ball pens with Super Ink, claim to stop check washing. That still won't protect against some other types of check fraud, though.

Learn more: What Is Check Fraud?

How to Avoid a Scam

While scammers' delivery methods and messaging can quickly change, a few basic security measures can help protect you from the latest and most common scams:

- **Be skeptical when someone contacts you.** Scammers can spoof calls and emails to make it look like they are coming from different sources, including government agencies, charities, banks and large companies. Don't share personal information, usernames, passwords or one-time codes that others can use to access your accounts or steal your identity.

- **Don't click unknown links.** Whether the link arrives in your email, a text or a direct message, never click on it unless you're certain the sender has good intentions. If the message says it's from a company or government agency, call the company using a number that you look up on your own to confirm its legitimacy.
- **Be careful with your phone.** Similarly, if you suspect a spam call, don't respond or press a button. The safest option is to hang up or ignore the call entirely. You can look up the organization and initiate a call if you're worried there may be an issue.
- **Update your devices.** Software updates may include important security measures that can help protect your phone, tablet or computer.
- **Enable multifactor authentication.** Add this feature to any accounts that offer it as an option, and try to use a non-SMS version to protect yourself from SIM swapping.
- **Research companies before taking any actions.** Before you make a purchase or donation, take a few minutes to review the company. Do a web search for its name plus "scam" or "reviews" and research charities on Charity Navigator and CharityWatch.
- **Don't refund or forward overpayments.** Be careful whenever a company or person asks you to refund or forward part of a payment. Often, the original payment will be fraudulent and taken back later.
- **Look for suspicious payment requirements.** Scammers often ask for payments via cash, wire transfer, money order, cryptocurrency or gift cards. These payments can be harder to track and cancel than other forms of payment, which can leave you stuck without recourse.
- **Create a family password.** Create a family password that you can all use to verify that it's really one of you on the phone, and not someone who created a deepfaked video or cloned voice.

Learn more: How to Identify a Scammer

What to Do if You Fall Victim to a Scam

Although there are some exceptions, you often can't get your money back if you fall for a scam. There's also no way to take back any personal information that you sent. But there are a few steps you can take that might help prevent additional fraud and protect other people:

- **Report the scam and scammer.** You can report scammers to the BBB and the FTC online. Additionally, report the scam and related message to any relevant parties, such as your bank, credit card issuer, social media platform, email provider, phone carrier or the USPS' Postal Inspection Service. You can also file a police report, which might help with recovering your identity or lost funds.
- **Scan your devices.** If you clicked on a link or attachment, you may want to run an antivirus scan to check for malware.
- **Change your passwords.** Change the passwords on any accounts that use a password the scammer might know. Use this as an opportunity to create stronger passwords or try out the newer passwordless option called passkeys that are available on some websites.
- **Protect your credit.** You may be worried about identity theft if you gave the scammer your personal information. You have the right to add fraud alerts and security freezes, also called credit freezes, to your credit reports for free. These can help keep someone else from opening an account using your information.

Monitoring Your Credit and Identity

Following basic safety strategies and reviewing the latest scam alerts can help you stay safe. But mistakes can happen, particularly when you're stressed or overwhelmed. Even if you're doing everything right, your information could be compromised in a data breach.

Sign up for free credit monitoring with Experian to get alerted when there are unexpected changes in your credit report, which could help you quickly respond to some types of fraud. Additionally, a paid premium membership could offer additional types of monitoring, identity theft insurance and fraud resolution support.

Original Source:

Article on Experian.com/Blog

Author: Louis De Nicola, 20/12/2024