Web of Deception: How to Prevent the Latest Online Scams

Get the latest statistics on “PayPal” scams, and learn to stay safe from phony job recruiters, fake charities, sextortion schemes, and even election scams.

Brett Cruz, Digital Security Expert

All of our content is written by humans, not robots. Learn More

The internet connects us with great people and helpful services 24/7. Unfortunately, it can also expose us to scams that threaten our personal information, privacy, and safety.

That’s why it is essential to stay informed about the latest scams. With that in mind, we’re bringing you new insights from nearly 1,100 American adults about their recent experiences with cybercriminals and the latest online schemes. We’ll also show you how to spot and stop fraudulent activity online and protect your data.

Here are the key findings from our research on online scams:

- 83% of people who use payment apps like PayPal or Venmo experienced some form of attempted or successful scams, up from 68% in 2023 and 42% in 2021.
- 50% of cryptocurrency owners have been targets of crypto scams. Most often, they took the form of “pump and dump” schemes, which involve artificially inflating the price of a cryptocurrency through misleading hype, and then selling off large holdings at the peak, causing the price to crash.
- Malicious links in text messages are becoming more and more common: 70% percent of Americans have received a text from someone they

didn't know, and 15% have clicked on links in texts from unknown senders.
- 1 in 4 adult social media users have been targeted by scammers, most often on Facebook and Instagram.
- Though tens of thousands of people have become victims of sextortion scams, and at least 20 people have died after being victimized, less than half of adults have heard of sextortion.

17 Scams To Be Aware of in 2024

1. Peer-To-Peer Payment App Scams
2. Malicious Link or Phishing Text Message Scams
3. Cryptocurrency Scams
4. Social Media Scams
5. Sextortion Scams
6. Election Scams
7. Gaming Scams
8. Investment Scams
9. Online Ticket Scams
10. Fake Charity Scams
11. Voice Cloning and Grandparent Scams
12. Deepfake Photo and Video Scams
13. SIM Card Scams
14. Fake Home Rental Scams
15. Survey and Quiz Scams
16. Fake Job Interview and Training Scams
17. Fake Subscription Renewal Scams

Peer-to-peer payment scams, phishing frauds, cryptocurrency schemes, and various gaming scams have become more sophisticated in recent years. Other new and timely scams include IRS impersonation scams and student loan forgiveness scams. The huge popularity of online shopping has also added fuel to package delivery scams.

1. Peer-To-Peer Payment App Scams

About 79 percent of Americans use peer-to-peer (P2P) apps, like PayPal, Venmo, or Zelle, at least once a week. These apps are convenient and easy to use, and scammers like them because it's typically the user's responsibility to ensure that transactions are legitimate.

According to our latest research, 83 percent of peer-to-peer payment users experienced some form of attempted or successful scamming activity while using the apps. That's up from 68 percent of users in 2023 and 42 percent of users in 2021.

According to our study, P2P app users most often experience attempted scams on PayPal. However, this could be due to PayPal's wide use—currently, the program has more than 400 million users!

Preventing Peer-To-Peer Payment App Scams

As long as you know the warning signs of peer-to-peer payment app scams, you can use the apps and safely enjoy their convenience. Follow these tips:

- Before sending money, verify a recipient's identity using phone numbers, email addresses, or QR codes.
- Activate all identity verification options available in an app. The recipient of any money transfers must undergo various steps to pass security.
- When paying a new recipient for the first time, send a $1 test payment and confirm the correct person received it. This step is even more critical when transferring large amounts of money.
- Move the money you receive in your P2P app to your bank quickly so that Federal Deposit Insurance Corporation (FDIC) insurance kicks in.
- Monitor your P2P accounts routinely. If fraud occurs, you may catch it early enough that the impact on you is minimal.
- Close accounts and delete all P2P apps you do not use.

While P2P apps are beneficial, you shouldn't use them for all types of transactions since fewer protections are in place in case of fraud. Instead, use credit or debit cards with built-in purchase protections whenever possible.

2. Malicious Link or Phishing Text Message Scams

Malicious link scams often involve deceptive emails, text messages, or advertisements that lure people into clicking on harmful links that can capture personal data. The risks include identity theft, financial loss, and the installation of malware on devices.

These scams can look like:

- "Oops, wrong number!" texts
- Emails and texts pretending to be from Amazon or other retailers
- Free-gift QR codes
- Tech support scams that gain remote access to your computer
- Late or failed package delivery messages

Unfortunately, malicious links in text messages are becoming more and more common. Seventy percent of Americans have gotten a text from someone they didn't know trying to make conversation (up slightly from 66 percent the prior year).

Preventing Malicious Link or Phishing Scams

These scams are so harmful in part because they can appear legitimate with messages featuring company logos, shipping notices, and the like. Here are a few ways to stop these scams before they impact you.

- Ignore emails and text messages from people you don't know, and block unknown senders.
- Ignore unexpected emails or texts, including those that claim failed log-

in attempts or suspicious activity.
- Watch out for messages with generic greetings such as, “Hello, Dear.”

Legitimate companies do not email or text you to update payment details. If you want to access your account to check on billing, never click on a link in a suspected scam message. Instead, type in the URL or Google the company if you don’t remember the URL. Thankfully, our research revealed that the number of people who said they have clicked on links in texts from strangers has declined year over year.

3. Cryptocurrency Scams

Cryptocurrency is an unregulated global digital currency that takes the form of “coins” or tokens. Some examples are Bitcoin, Ethereum, and Litecoin. While many crypto investors appreciate that the currency is unregulated, they are more susceptible to scams and fraud.

Our latest cryptocurrency report found that 40 percent of Americans in 2024 own cryptocurrency, up from 30 percent in 2023. Unfortunately, we also discovered that 50 percent of crypto owners were scam targets. The most common type was a “pump and dump” scheme, in which the price of a cryptocurrency is artificially boosted through false promotion, allowing the scammer to sell at a high point, causing the price to plummet and resulting in losses for other investors.

According to the Federal Trade Commission, if the following happens to you, it’s likely a scam:

- **Someone says you must pay in cryptocurrency (especially in advance):** Legit companies rarely require crypto payments as the only way to do business with them.
- **Someone guarantees huge profits:** No one can promise any type of return in the markets. A person who makes guarantees is a con artist.
- **If a person you’re dating online asks to show you how to invest in**

crypto or requests crypto, this is a sure sign of a scam.

Preventing Cryptocurrency Scams

- Remember that scammers often use social media to find victims through hacked or spoofed accounts or advertised advice and investment opportunities. Fake endorsements and giveaways are also relatively common. Your favorite celebrity may even seem to endorse a crypto opportunity on social media.
- Invest only through well-known, reputable platforms. Avoid those promising unrealistically high returns.
- Use two-factor authentication (2FA) and other security measures from your wallet or exchange. Regularly update your passwords and ensure they are strong and unique.
- Avoid opportunities that guarantee high returns with little or no risk. If an investment sounds too good to be true, it is.
- Avoid sharing private keys, seed phrases, or other sensitive information. Scammers often impersonate legitimate services to trick you.
- Research cryptocurrency projects thoroughly before you invest. Assess white papers, team members, and community feedback. Require verifiable information about the team or partnerships.

4. Social Media Scams

Of our study's adult social media users, 25 percent have been targeted by scams on social media platforms at least once. These scams can be fraudulent sales of items, event tickets, impersonations, phishing, giveaway scams, job offer fraud, and romance scams. The list goes on. Many of the scams that happened before the internet have been reinvented on social media. Shopping-related scams were most common among users in our study. More than one in 10 social media users said they'd purchased an item on social media they never received.

Nearly 70 percent of social media scam victims said they were scammed on Facebook, 47 percent on Instagram, and 18 percent on TikTok.

Preventing Social Media Scams

- When purchasing items on social media, check if the seller has a credible presence. Look for verified badges and read reviews or feedback from other shoppers.
- Steer clear of offers that seem too good to be true.
- Use secure payment methods rather than direct bank transfers, gift cards, or payment services that don't offer buyer protection.
- When clicking on links from social media profiles, ensure that the website or payment gateway uses HTTPS and has a valid SSL certificate. Look for a padlock icon in the address bar.

You can identify scam product listings if the content is poorly written, features generic or stock photos, and lacks contact information. In contrast, legitimate and professional businesses typically provide high-quality content and straightforward ways for customers to reach them.

5. Sextortion Scams

Though sextortion is an increasingly common and potentially deadly type of scam, fewer than half of the Americans in our study had heard of sextortion schemes.

In this type of fraud, scammers contact victims through social media or dating apps, pretending to be romantically interested. They build trust by sharing fake explicit photos and engaging in intimate conversations, eventually coercing the victim into sharing compromising material. The scammer then threatens to expose this content unless a ransom, usually paid in untraceable methods like cryptocurrency, is provided. Even after payment, the scam may continue with further demands.

People of any age can fall victim to this scheme, but often, teen boys are targeted. The FBI reported that from October 2021 to March 2023, there were around 12,600 victims, mostly boys, and at least 20 of these sextortion victims died by suicide. Shockingly, 65 percent of Generation Z says they or their friends have been targets in sextortion scams.

Preventing sextortion scams

- Do not share intimate photos or videos online with people you know and don't know. The person you think you're chatting with may be an impostor.
- Avoid people who push quickly for your intimate details, photos, or videos. With the rise of deepfakes (more on this later), even video chatting with someone might not be enough to verify that their photos match them.
- Beware if someone meets you on one platform and then wants to move to another and then perhaps another. This happens for encryption reasons, making it harder for authorities to track crimes.
- It's necessary to talk about sextortion with tweens and teens in an open, nonjudgmental way. Educate them on the red flags of sextortion and remind them to tell an adult they trust if they have concerns about people met online.

Being a victim of sextortion can be embarrassing and humiliating, but professionals can help. You can text "THORN" to 741741 to talk with a counselor. Consider reporting the scam to the police.

6. Election Scams

Election-related scams are a significant concern, especially during presidential election years. These scams can look like:

- **Fake donation requests:** Scammers can pose as representatives from political campaigns. They request donations via phone calls, emails, or

social media messages. They may use high-pressure tactics to get you to donate quickly, but the money never reaches the political candidate. Instead, scammers steal the donation for themselves.

- **Bogus voter registration services:** Scammers may call or text to say they can register you to vote or offer to update your voting information by phone. In 2024, California officials had to warn voters to exercise caution regarding text messages that prompted recipients to check their registration status, since this tactic could be used in scams. It's best to register in person at your local board of elections or through official websites like Vote.org.
- **Fake election surveys:** Scammers conduct fake election polls. Many offer rewards to get people to participate, but they aim to gather personal information, such as Social Security numbers, bank details, or credit card numbers.
- **Imposter scams:** Scammers pose as election officials or campaign representatives. They contact voters with "problems" about voter registration or absentee ballots. They may request personal information to "resolve" these issues.
- **Disinformation and deepfake campaigns:** Beware of bad actors who try to manipulate information related to candidates and elections in order to change the results of the vote. For example, in January 2024, some New Hampshire voters received a robocall that sounded like it came from President Joe Biden. The AI-generated voice told voters not to vote during the primary election, but to save their vote until the general election in November.

Preventing Election Scams

- Donate to candidates or political causes only through official campaign websites. Avoid making donations by phone unless you initiate the call.
- Register to vote or update your voter registration only through official channels. Avoid clicking on links from text messages regarding your voter registration. To register to vote, you can visit your local election

board in person, register online at government websites like www.usa.gov/register-to-vote, or fill out a form that you send by mail.

7. Gaming Scams

Fraud in video games spoils the fun for players. In 2023, we found that 37 percent of online or video gamers have been the target of a gaming scam at least once.

Scammers can trick gamers by selling fake in-game items and money on unauthorized websites and phony game codes. As gaming becomes more popular, players need to be careful. Knowing about fraud, protecting yourself, and keeping your gaming information safe is essential.

Preventing Gaming Scams

- Purchase games and in-game items only from official platforms and reputable retailers.
- Use secure payment methods. Do not pay through direct bank transfers.
- Beware of offers that are too good to be true. Common examples include free or extremely cheap game keys or in-game items.
- Avoid clicking on links or downloading attachments from unknown sources.
- Use secure passwords for your gaming accounts.
- Avoid sharing personal information such as your full name, address, or credit card details in chats or forums.
- Be aware of phishing attempts that trick you into providing personal or login information.

8. Investment Scams

Investing scams are common because they exploit people's desire for high returns, lack of financial knowledge, and fear of missing out. They are often

facilitated by sophisticated tactics. The internet provides endless opportunities for investment fraudsters: in some cases, unsuspecting users download fake investment apps that promise high returns.

Instead of becoming rich, investment scam victims have their personal and financial information stolen. Unfortunately, users often find these apps in legitimate app stores. More than 300 such apps may be in app stores at any time. Today, scammers also deploy deepfake videos featuring famous people to lend them more credibility.

Preventing App Investment Scams

- Avoid investments that promise high returns in exchange for no or little risk.
- Research a company or investment thoroughly before exchanging funds.
- Search the internet and BBB to see if other people have reported scams on the investment app you're considering.
- Invest only through trusted, known apps and platforms such as Fidelity, E-Trade, Acorns, Vanguard, or Ellevest.

9. Online Ticket Scams

Online ticket scammers use fake websites or social media listings. In a typical version of the scam, buyers fork over money but never receive the tickets. There are other versions, though, when buyers get significantly worse seats than what they paid for.

Over 90 percent of reported ticket scams in the U.K. begin on Facebook. For instance, unofficial groups selling Taylor Swift tickets are popular targets. Many fans were deceived while trying to purchase tickets for the Eras Tour, with average reported losses of £332. At least 3,000 fans were scammed, resulting in thefts totaling at least £1 million.

Preventing Online Ticket Scams

- Buy from official ticketing platforms or authorized resellers. Verify the website's URL, and look for secure payment options.
- Compare ticket prices with official sources. Beware of significantly cheaper offers.
- Avoid paying via gift cards or direct bank transfers. Instead, use credit cards or secure payment systems that offer protection.

10. Fake Charity Scams

Sadly, scammers exploit people suffering from global crises and those wanting to offer charity to needy people. For example, the FBI recently released a warning about charity scams popping up around the Israel-Hamas conflict. Helping people affected by natural disasters is another common fake charity scam the FBI warns about.

Scammers pose as charitable organizations to solicit donations that never reach the intended cause. The FTC is an excellent place to check for updates on this type of scam.

For instance, in March 2024, the FTC highlighted a particular cancer charity scam. Cancer Recovery Foundation, Inc. (CRFI) told donors their money would help cancer patients. The charity raked in $18.25 million in donations, with a tiny one percent going to cancer patients. Instead, Much of the money went to the fundraisers and the fake charity's executive director.

Preventing fake charity scams

- Research charities thoroughly before making donations. For instance, look them up on Charity Navigator, Guidestar, or the Better Business Bureau's Wise Giving Alliance to verify their legitimacy and financial health. You can also check the IRS to see whether a charity has tax-exempt status.

- Before making donations, check that the charity has a physical address and phone number. Avoid charities that provide only an email address or P.O. box.
- Double-check the charity's name to ensure you donate to the correct organization. Some fake charities use names similar to well-known organizations.
- If you have concerns, ask for specific details on how the charity plans to use your donation.
- Avoid charities that pressure you to donate immediately. Legitimate charities give you time to decide whether you want to donate.
- Avoid donating through unsecured websites or links from unsolicited emails. Do not donate via cash, gift card, wire transfer, or cryptocurrency. These methods are untraceable and offer no buyer protection.

11. Voice Cloning and Grandparent Scams

Scammers are using AI voice cloning technology to impersonate victims' loved ones and trick victims into sending money. Scammers need only a short audio clip to create convincing voice clones, and they can pull these samples from social media or other online sources.

With AI, they can create a good replica of a person's voice. This voice communicates with the victim, pleading for money to help with an emergency or, sometimes, asking for personal information that can lead to financial fraud or identity theft.

Older people may be at particular risk, and other types of 'grandparent' scams have been around for years. In this new iteration, scammers call an older person, pretending to be a distressed grandchild and needing money urgently for an emergency. AI voice cloning has made these scams more sophisticated and convincing.

Preventing AI Voice Clone and Grandparent Scams

- Create a secret code word with loved ones, including grandparents. Ask for it in an emergency if someone is begging for help.
- If someone claims to be a grandchild in distress, verify the caller by asking questions only your relative would know.
- If you have doubts about whether or not you're receiving a cloned voice call, hang up and call the person directly.
- Refrain from posting voice recordings online. These can be used to create cloned audio.
- Talk with older relatives about grandparent scams and how they should verify callers before sending payments or trusting their claims—scammers like to use pressure to create a sense of urgency. Remind your relatives to take a few minutes to double-check identities before sending money.

12. Deepfake Photo and Video Scams

Like with audio, AI can be used to create convincing video and photo impersonations. For example, scammers can use false images to make it appear as if someone is cheating on their spouse and threaten to release a video of the act. People have gotten into trouble at work and school for saying and doing things they never did, thanks to deepfakes.

You may be especially at risk if you own your own business, handle the finances at work, work in finance, or are wealthy. For instance, a finance worker thought he was on a video call with his company's CFO and several others, but they were deepfakes. The scammers ended up with $25 million.

Preventing Deepfake Photo and Video Scams

- Have secret code words to use with employees, supervisors, and others in a company to verify that they are who they say they are on video calls

where financial matters are discussed.
- Use digital watermarks in photo and video content you post online. This will reduce the chances of your images being used in deepfake content.
- If you are suspicious of photos you see online, you can check the images' metadata for inconsistencies.

13. SIM Card Scams

Scammers often research their victims thoroughly before carrying out this scam. They then convince mobile carriers to transfer the victim's phone number to a new SIM card, allowing them to receive the victim's calls and texts on a different device.

Scammers often obtain personal information by pretending to be smartphone carriers, tricking victims into clicking a link and providing details like their Social Security number or passwords. They may also use malware to capture passwords or buy personal info on the dark web. With this data, scammers can convince mobile carriers to swap the victim's SIM card, giving them control of the victim's phone number. This allows them to steal one-time passcodes needed to access bank accounts, crypto wallets, and other sensitive services.

Preventing SIM Card or OTP Scams

- Use authentication apps such as Google Authenticator instead of SMS-based one-time-passwords.
- Beware of unsolicited calls or messages requesting sensitive information.
- Contact your mobile carrier to add an extra layer of security to your account, such as a PIN or password, to prevent unauthorized SIM swaps.
- Be aware that scammers might use phishing emails, texts, or calls that look legitimate to trick you into providing your one-time passwords.

- Access your digital accounts through official websites or apps. Avoid links in emails or texts.
- Keep all phone software up to date.

Never share your OTP with anyone. Legitimate organizations will never ask for your OTP.

14. Fake Home Rental Scams

With rising housing costs and interest rates, people in some areas face tough competition to rent housing. This creates excellent opportunities for scammers who pose as landlords or property managers. Their goal is to trick potential renters into sending money to secure properties that don't exist or aren't available for rent.

Red flags for rental scams include rent much lower than market rates, pressure to act quickly, refusal to meet in person or show the property before committing, and demands for upfront payment. Poor grammar in ads can be a warning sign, but scammers may copy text and photos directly from other sites, only changing the contact information.

Preventing Fake Home Rental Scams

Before renting a new residence, keep these steps in mind to prevent scams:

- Get familiar with the typical rents in your area so you know when listings have unrealistic prices.
- Always view the property inside and out, and meet the landlord in person before signing a lease.
- Check ownership records to confirm the landlord's identity.
- Use trusted real estate websites such as Zillow to search for rentals.
- Only send a security deposit or rent payment after seeing the property and signing a legitimate lease agreement.

15. Survey and Quiz Scams

Fake surveys promise rewards while collecting victims' personal information for identity theft or selling on the dark web. Scammers lure victims with promises of rewards, such as gift cards or cash. These scams can take various forms, such as fake survey invitations, phishing links, and rewards that are never delivered.

Preventing Survey and Quiz Scams

- Take surveys only from reputable companies or websites. Don't click on survey links in unsolicited emails or messages. Instead, go directly to the company's website to find legitimate surveys. Also, legitimate surveys should have clear privacy policies about how your information will be used and protected.
- Avoid surveys that ask for sensitive information such as Social Security numbers, bank account details, and credit card information.
- Keep your computer and mobile device security current to block malicious sites and phishing attempts.

16. Fake Job Interview and Training Scams

In job scams, criminals often pose as potential employers to trick job seekers into providing personal information, paying upfront fees, or participating in fake employment activities. These scams can occur online, through emails, social media, job boards, and even in person.

Scammers often use AI to help write job listings so they seem more polished and legitimate, and the FTC explains that a typical job scam victim loses $2,000. Here are some common types of job scams:

- **Fake job listings:** Scammers post phony job ads on actual job boards or create counterfeit websites that look convincingly real. Phony job listings can promise high salaries, flexible working conditions, or other

benefits to draw in victims.

- **Phony recruiters:** Scammers pretend to be recruiters or hiring managers. They contact job seekers with interview requests or job offers via text, email, or phone calls.
- **Work-from-home or job training scams:** Scammers may ask victims to pay for training, equipment, or other upfront costs before hiring.
- **Reshipping scams:** Scammers hire people to receive, repackage, and ship goods, often stolen or bought with stolen credit cards. The victim could face criminal charges for unknowingly cooperating in this type of crime.

Preventing Job Scams

- Research the company thoroughly before you apply for a job. Check the official website, read reviews, and verify the contact information.
- Avoid job “opportunities” that require upfront payments for training, equipment, or uniforms, especially before hiring.
- See whether a job listing appears on multiple websites. If you see it in only one place, it may be a scam, especially if the role seems too good to be true.
- On job applications, wait to share personal information like your Social Security number until you verify the employer’s legitimacy.
- Be cautious if the hiring process is speedy and lacks thorough vetting. Scammers often hurry the process to obscure warning signs, while others might ask you to invest significant time, such as a lengthy interview, to lower your defenses.

17. Fake Subscription Renewal Scams

In this scheme, people get emails or texts claiming to be from services such as Netflix or Amazon urging them to click on links in order to renew subscriptions. These emails can appear legitimate, using genuine company logos and accurate renewal dates. However, this method can be used to

“phish” for credit card or other financial information and lead to identity theft.

Preventing Fake Subscription Renewal Scams

- If you receive an email claiming to be from a subscription service, check the sender’s email address for authenticity.
- If you have doubts about whether an email or text is authentic, you can always contact the business directly using their official contact information. Instead of relying on email links, type in the web address yourself or use mobile apps to update subscription billing details.
- Keep a record of renewal dates and charges for your subscriptions.
- Never give payment information for unsolicited requests.

Avoiding Scams in 2024

With online fraud rising, too many Americans are exposed to sophisticated scams. We’ve mostly seen many victims from peer-to-peer payment apps and unsolicited texts.

By recognizing the warning signs, being cautious with your personally identifiable information, and verifying the legitimacy of offers, you can safeguard your online security and financial well-being. Always remain aware – skeptical even – of random or too-good-to-be-true offers. Always verify who is contacting you, even if it takes a few extra minutes. Many times, it’s better to respond to the company directly by finding contact information on an official website.

Remember to conduct research, trust your instincts, and seek reputable sources when in doubt. With these precautions in mind, we can confidently navigate the digital realm, sidestepping the traps of new internet scams and ensuring a safer online experience for ourselves and others. Besides, you read this article, which means you are already several steps ahead.

FAQs

How common are online scams?

What are common scammer phrases?

What are the latest scams to be aware of?

What information does a scammer need to access my bank account?

How much information does a scammer need to steal your identity?