Top Online Scams and How to Avoid Internet Scams

The internet is such an integral part of our lives that it can be easy sometimes to forget that not everyone we encounter online has our best interests at heart. Internet scams are an ever-present threat, with hackers and cybercriminals doing their best to stay one step ahead of internet users. Staying informed of the risks and how to combat them is the best way to keep safe. Here is a list of the top online scams and how to avoid getting duped.

1. Job offer scams

Job offer scams increased during the coronavirus pandemic. In this scam, you receive an unsolicited email offering a job, typically not in your area of expertise, often for a mystery shopper or similar position. When you accept, you are paid by check or money order for an amount greater than your "employer" offered. You are then asked to send back the difference, only to discover the original check or money order was fake, and you're out of the money you sent to your fake employer.

With the widespread use of professional networking sites like LinkedIn, unsolicited job offers are common, which means that anyone looking for work has to become savvy at sifting through the legitimate offers from the scams.

How to avoid job offer scams

If you decide to accept work, never cash suspicious checks without ensuring they are authentic. To be sure, ask your bank to place a hold on the funds until the check or money order is verified. Any time you are asked to send back the "difference," this is a sign that you are involved with a scam.

2. Lottery scams

Reportedly, lottery scams were the fourth most common type of scam in the US in 2020. You typically receive an email with these scams claiming you have won a little-known lottery, usually in another country and always with a substantial pay-out. To claim your prize, you will be asked to pay a fee. Scammers will often say these fees are for insurance costs, government taxes, bank fees, or courier charges. You are asked to send personal details for verification, and suddenly you're the victim of identity theft, and the money you sent is gone.

Another version of unexpected lottery or prize scams involves scammers gaining access to someone's social media account and contacting friends and family members and telling them that they have all won money. The scammer then provides an email address through which they will receive instructions on how to claim their prize. This is a particularly insidious version of the scam as it uses the trust between friends and family to trick people out of their money.

How to avoid lottery scams

Lottery scams have a few tell-tale signs:

The email is from a person, not a company.
You're not the only recipient.
You've never heard of the lottery.

If you receive an email like this, do a quick Google search to see if it's legitimate. (It never is.) We all want to find an easy windfall, but if you didn't buy a ticket, then it is extremely unlikely that you have won a lottery. Never send your personal information via email to anyone you don't know, and never trust anyone trying to give you money for nothing.

3. Beneficiary scams

You get an email from someone who is looking to move some money around quickly. These emails sometimes come from people claiming to be royalty – you've probably heard of the Nigerian prince scam – but more often, they're from a "businessman" who says he has millions to move out of the country and wants your help in exchange for a cut of the profits. The sender includes just enough details to make the offer seem legitimate. But the money is inevitably delayed, leaving you on the hook for a host of small payments to facilitate the transfer of funds.

How to avoid beneficiary scams

Falling for this scam is easy if you're down on your luck; however, you should look for a few signals that this is not what it seems. Poor grammar and spelling in the original email and a reply address that doesn't match the sender's prove that, especially on the internet, anything that sounds too good to be true always is.

4. Online dating scams

Romance scams are on the rise . You meet someone through a dating app or website, you start to get to know each other, and it can feel authentic. However, you can never be sure who is on the other side of your screen. If you find yourself in an online relationship with someone who begins to ask for money or asks you to redirect items they send you, then the person you've met is a scammer.

"Catfishers," as they are sometimes called, often use the identity of a real person to seem authentic and provide genuine details. However, they are sending fake photos and contact information to cover their tracks. Romance scams or dating site scams have a few key components:

Demonstration of strong emotions in a very short time.
A quick move from dating sites or apps into private channels.
Requests for money based on personal hardship—for example, for a sick

relative or a failed business.

How to avoid online dating scams

Avoiding romance scams means carefully scrutinizing any online relationship that develops too fast. Never give money to someone unless you also have a relationship with them offline. And if you do make a date with someone outside of cyberspace, be sure to let people in your life know where you'll be, to be on the safe side.

5. Charity fraud scams

After large-scale natural disasters or other high-profile public tragedies, you want to help any way you can, and scammers know to capitalize on this. They set up fake donation sites and accounts and then craft an emotional pitch email to solicit funds that never reach the victims. These scams are successful because they play on sympathy, but always make sure you do your research. Fact-check any donation sites and make sure they are affiliated with the issues they claim to represent.

How to avoid charity scams

To avoid a charity web scam, do not donate to any sites that look suspicious. Any actual charity will have a robust website with its mission statement and tax-exempt documentation. **To check if a charity is real or not, search for it on a public database**like Charity Check, CharityWatch, BBB Wise Giving Alliance, or Charity Navigator.

6. Coronavirus scams

The pandemic gave fraudsters the opportunity to devise new scams – although often these were variations on existing scams but repackaged with a fresh coronavirus angle.

For example:

Scammers posed as fake charities to solicit donations from the public.
They offered fake testing, vaccine, or treatment kits, sometimes targeting Medicare recipients in an attempt to steal personal information.
They created fake websites purporting to show maps displaying Covid infections, fatalities, and recoveries by country. In reality, scammers designed these websites to inject malware, spyware, and viruses onto users' machines.

How to avoid coronavirus scams

As with any charity scam, check that the charity is legitimate by using a known database. Never send money or provide personal information, credit card details, or online account details to anyone you do not know or trust. Check any website carefully to make sure it’s not a fake website. Don’t click on links or open attachments in any email you are unsure of. For more information on how to avoid coronavirus scams, read our article.

7. Repair scams

In a scam that starts in the real world and quickly moves into the online one, you receive a phone call from someone who claims to work for "Microsoft", or another large software company, claiming they can fix PC issues like slow internet speeds and loading times. It sounds helpful, and so when the email arrives in your inbox, you download a remote access program, which allows scammers to take control of your computer and install malware. Not all consumers are equally tech-savvy, so many don't know how their PC works and are easily deceived by scammers. Once they install malware, they have access to your files, data, and personal information.

How to avoid repair scams

Never accept any unsolicited repair advice, and do not purchase any repair

services unless you are sure who you are speaking with. Do not allow anyone remote access to your computer. If someone calls, ask for identifying information. The odds are that if you ask enough questions, the scammer will realize you can't be duped.

8. Social media scams

Social media scams are becoming increasingly more popular and come in many forms.

For example:

You might see a social media quiz that promises to tell you what personality type you are, or what celebrity you look like, or offers you an eye-catching prize. They usually include terms and conditions which allow the data you enter to be sold to third parties. The quiz developer can also obtain a lot of information about you from your profile, friends list, and IP address – which can be used to build up a picture as part of identity theft.
Or perhaps you receive a random friend request on Instagram from a fraudster posing as someone you may know, who then sends you a phishing link that takes you to a malicious site.
Perhaps you download an app on social media which you think is legitimate, but in fact downloads malware onto your device.

How to avoid social media scams

Avoid quizzes and never click on pop-up messages or posts that contain content that seems either shocking or else too good to be true. Don’t click on links or open attachments in unsolicited messages.

Beware of clicking on shortened URLs that hide the full location of the webpage. They are very common on Twitter, and while they could innocently direct you to the correct site, there’s always a chance they might divert you to one which installs malware.

9. Robocall scams

If you answer the phone and hear a recording rather than a live person speaking, that’s a robocall. Robocalls are sometimes used to deliver useful information, such as appointment reminders or flight cancellations. Mostly though, they are unsolicited marketing calls, and many of them are scams.

Robocall scams come in various forms – for example:

They may pretend to be from the IRS, asking you to pay a fake tax bill and saying that your Social Security number will be deleted if you don't.
They may pretend to be from a well-known technology company such as Apple, asking for customer information that a real company would not request over the phone.
They may offer a free trial for a product or service as a ruse to obtain your credit card information.

How to avoid robocall scams

The best thing to do is not to answer your phone if you suspect a robocall. However, you can’t always tell, so if you do answer the phone, hang up as soon as you realize it’s a robocall. Avoid following the bot’s instructions, such as "press 1 to speak to a live representative," etc. Avoid saying the word “yes” if you can – many robocalls start with the line “Hello, can you hear me?” to which users may reply "yes" without thinking. The scammers then store the recording and use it for fraudulent purposes.

Any interaction or positive engagement with a robocaller lets the scammers know that you are a potential prospect – so minimizing engagement is the best approach to take. **In the US, you can report robocalls** to the Federal Trade Commission at donotcall.gov.

10. Messaging scams

Fraudsters also use messaging systems and apps, such as SMS, WhatsApp, Facebook Messenger, Viber, Skype, Google Hangouts, and others, to scam you out of money. Phishing scams carried out via SMS are known as “smishing”.

There are various iterations of messaging scams. For example:

You might receive a text message telling you that you have a package or delivery pending, and you need to confirm your identity or pay a fee to claim ownership.
You might receive a message purporting to be from your bank, telling you that your account is being closed, or your debit card is being locked or charged, and to log in (to a fake website) to prevent that from happening.
Or perhaps the message tells you that you’ve won a huge prize, and to claim it, you need to submit your financial information.

How to avoid messaging scams

If an organization doesn’t usually contact you via a messaging app, that’s the first red flag. Genuine organizations won’t contact you out of the blue, asking you to divulge sensitive or personal information via a messaging app. Check for spelling errors or grammatical mistakes in the message – if it doesn’t look professional, that’s a giveaway that it’s a potential online scam. If you’re not sure, don't click on any links and avoid providing personal or financial data.

11. Online shopping scams

Scammers use the latest technology to set up fake retailer websites that look like genuine online stores, using stolen logos and copied designs. Many of these websites offer popular brands of clothing or jewelry, or gadgets at low prices. Sometimes you may receive the item you’ve paid for, but often you don't. A more recent version of the scam involves setting up a social media store, which usually disappears after a while to resurface again in another guise. For more information, read our article on Online Shopping

Safety.

How to avoid online shopping scams

If a product is advertised at an incredibly low price that seems too good to be true, that's a clear warning sign. Another sign is if the other party insists on immediate payment or payment by electronic funds transfer or a wire service. They may even ask you to purchase vouchers up-front to access a cheap deal or giveaway.

Tips: How to identify fake websites

A key aspect of online safety is being able to identify fake websites. To avoid website scams, there are several warning signs you can look out for.

Ensure you check the website's domain name, particularly if redirected to the website from another page or email. Scammers sometimes create websites whose domain names appear similar to well-known brands or organizations – for example, by changing a letter or adding a word.

You can look up additional information about a domain if you're suspicious. The Whois Lookup domain tracker gives you information about who a domain name is registered to, where they are, and how long the website has been active.

It's also wise to check the address bar of a website. Any website which invites you to submit personal information needs to be secure, which you can tell is the case if the URL starts with https:// instead of http:// - the "s" standing for "secure". Secure websites will also display a padlock icon in the URL address bar. This means the site has an SSL certificate.

Website content can give you an indication of trustworthiness. If the content is poorly written with numerous spelling or grammatical mistakes, this is a potential red flag. A shortage of information, such as a lack of terms and

conditions and privacy policy, or no returns policy on a shopping website, can also indicate that the website may not be legitimate.

Check for secure payment methods if making a purchase online. Legitimate websites should offer standard payment options, such as credit cards or PayPal. If a website asks you to use a wire transfer, money order, or other unsecured (and non-refundable) form of payment, then it’s best to stay away.

Reviews can be another helpful tool for checking out websites. You can search for the website at sites that aggregate online reviews. If reviews appear oddly similar or are all quite new, bear in mind they could be fake reviews. If no reviews exist, that is a cause for concern.

Tips on how to avoid internet scams

For those wondering how to avoid being scammed online, sensible tips you can follow to stay safe include:

1. Beware of any requests for your details or money

Avoid sending money or providing credit card details, online account details, or copies of personal documents to anyone you don't know or trust. Only use secure payment methods you are familiar with. Don't agree to transfer money or goods for someone else: money laundering is a criminal offense.

2. Be alert to phishing scams

A common theme amongst many online scams is phishing. Avoid clicking on links or opening attachments in suspicious emails or texts, and never respond to unsolicited messages and calls asking for personal or financial details.

3. Don’t respond to phone calls asking for remote access

to your computer

If someone claims to be from a well-known telecom or technology company and wants access to your computer to fix a problem or install a free upgrade, hang up immediately. Their real motivation is to take control of your computer to install malware on it so that they can gain access to your passwords and personal details.

4. Keep your mobile devices and computers secure

Use passwords to protect your devices and avoid giving access to others (including remotely). Protect your Wi-Fi network with a password and avoid using public computers or Wi-Fi hotspots to access online banking or provide personal information.

5. Use strong passwords

A strong password is not easy to guess and ideally made up of a combination of upper- and lower-case letters, special characters, and numbers. People often leave passwords unchanged for years, which reduces their security. A password manager tool is an excellent way to manage your passwords.

6. Review your privacy and security settings on social media

If you use social networking sites, be careful who you connect with and learn how to use your privacy and security settings to ensure you stay safe. If you recognize suspicious behavior, have clicked on spam, or have been scammed online, take steps to secure your account and be sure to report it.

7. Avoid streaming from unknown websites

Streaming content from unfamiliar and potentially inauthentic websites can

be a considerable risk for malware. Criminals behind digital piracy often make content free illegally to act as bait for a large number of visitors. Only stream content from sites you know and trust.

8. Resist the pressure to act immediately

Legitimate businesses will give you time to make decisions. Anyone who applies pressure on you to pay or disclose your personal information is potentially a scammer.

9. If it seems too good to be true, then it probably is

If a website or anyone you are communicating with online offers huge discounts or massive prizes that seem unreal or implausible, then exercise caution. As the old saying goes – if something seems too good to be true, it probably is.

In general: stay alert and be wary of people unexpectedly contacting you by email or phone and asking about personal information. If you fall victim to an online scam in the US, you can report it to the Federal Trade Commission. Other countries around the world have equivalent bodies.

The best way to protect yourself against internet scams is to install cybersecurity software on all your devices and keep it up to date. Avoid fake antivirus products – as these are usually scams and malicious code in disguise – by purchasing and downloading antivirus software from a legitimate website. For example, Kaspersky Total Security protects against hackers, viruses, malware, and more.

Related Articles:

Tips on how to prevent ransomware attacks
Spam and Phishing - What you need to know
How to Choose an Antivirus Solution

Ways hackers can violate your online privacy

Online shopping safety risks and how to protect yourself?