The 15 most dangerous places on the Internet

By Jon Martindale,Contributor, PCWorld May 27, 2025

Don't want to catch malware or get hacked by cybercriminals? Take extra care when visiting these sites—or just avoid them altogether.

The internet might be more sanitized than it was in decades past, but it's still plenty dangerous. You've been warned that the web is a security minefield—that it's easy to get in trouble. You can do everything right and still be taken by a malware infection, a phishing scam, or an invasion of online privacy. We want to help.

Here are some of the most dangerous threats on the internet and what you can do to stay out of harm's way. Not all web dangers are created equal, though. Indeed, some threats will actively come looking for you while others you may never see if you don't seek them out. Let our threat level indicator be your guide:

Foundry

Threat 1: Misinformation

Where it happens: Social media

Foundry

You know this one already, but we're all as susceptible as ever. As social media algorithms continue to curate content, create bubbles, and spur echo chambers, they've become better at pushing misinformation in stories and images that seem like they *could* be true—and that's often all it takes. Once you've clicked through, you'll be susceptible to further misinformation that reinforces the faux story that caught your interest, and it'll tell the algorithms to keep pushing more of that kind of content that interests you, sending you down the wrong path.

How to stay safe: While cutting out social media altogether is the best answer, it just isn't practical for most of us. You can protect yourself against social media misinformation by actively analyzing all stories, images, and links you come across. If it seems designed to provoke an emotional response in you, pause and reconsider. Double-check all stories with trusted third-party sources. And lastly, think about leaving certain social media sites that are inundated with misinformation and move towards ones that are better moderated and more open.

Threat 2: Deepfakes and AI scams

Where it happens: Just about everywhere

Foundry

This one's tricky because you're just as likely to find deepfakes and AI scams in your email inbox as you will on social media, on YouTube, and ads all across the internet. The dangers are equally varied. A deepfake (which is a video or audio that's been digitally altered to appear as someone else) can damage someone's reputation, lead you to believe misinformation, or incite you to feel negatively towards certain groups, countries, or organizations. Meanwhile, AI scams can catch you off guard and hack your data or steal your personal information.

How to stay safe: Deepfakes and AI scams are by nature hard to spot, which is why you need to develop a healthy skepticism towards everything on the internet. Remember that disinformation campaigns, hackers, and bad actors are all trying to prey on you in some way. Always question any video or audio that seems alarming or sensational.

Threat 3: Lookalike URLs

Where it happens: Your browser's address bar

Foundry

With phishing scams on the rise, you're likely to encounter lookalike URLs in fraudulent emails, but you're also likely to run into this if you often type URLs directly into your browser's address bar. If you mis-type a popular website—for example, goggle.com instead of google.com—you could end up on a fake site that *imitates* the one you meant to visit. It doesn't happen all the time, but when it does, it's because the fake site's owner wants you to input your login credentials so they can steal them.

Similarly, you may run into scam links on the web that replace certain mundane characters with lookalike letters, such as from the cyrillic alphabet. When you're in a rush, you may not easily spot the difference between realsite.com and rẹalsite.com.

How to stay safe: Double-check every URL you type into a browser, and double-check every link you click on by hovering your mouse over it and looking at the URL preview at the bottom of the browser. When in doubt, it's safer to type in a URL than it is to click on a link.

Threat 4: QR code scams

Where it happens: The real world

Foundry

QR code scams are particularly nefarious because they can follow you into the real world. They're commonly found on parking meters, restaurant menus, bulletin boards, or outdoor venues that offer Wi-Fi access. Scammers and criminals stick their own fake QR codes on top of the original ones—often with a literal sticker—and it sends you to an imposter site that steals your logins, details, and/or financial information.

How to stay safe: Before scanning any QR code, double-check that it's from a legitimate organization. When scanning QR codes in public, make sure it isn't a sticker. Also, remember that QR code scams simply take you to fraudulent sites, so double-check that you've arrived on a legitimate page that doesn't have any red flags. If it seems off, close the tab.

Threat 5: Malvertising

Where it happens: Streaming sites

Foundry

Who hasn't visited ad-infested streaming sites to watch TVs shows without suffering Netflix's or Disney's increasingly expensive paywalls? Doubly so for live sports! If you've ever pirated a soccer stream or boxing pay-per-view, then you know the kinds of sketchy sites I'm talking about. The risk here is that these sites are funded via ads, but most ad sellers don't want to be associated with such illegal activity—so these streaming sites have to be less scrupulous with which ads they accept, and that means their ads can contain malware. This is known as "malvertising."

How to stay safe: Not only should you *never* give these sites your personal or financial information, you should *never* click on any of their ads. Also, make sure your antivirus software is up-to-date and working properly before visiting such sites. (You *are* using antivirus, right?) Consider using a VPN, too. These sites are illegal, after all.

Threat 6: Dangerous ideologies

Where it happens: Discord, Telegram, WhatsApp, other modern communication apps with weak moderation

Foundry

Modern communication apps are great for staying in touch with friends and family, but they're also hotbeds of nefarious activity. Terrorists, white supremacist groups, illegal pornographers, and militant groups have all been known to use such apps for organizing, recruiting, and spreading dangerous ideologies and unlawful material. Some groups use these apps to operate slowburn pipelines of propaganda, disinformation, and indoctrination to radicalize susceptible people.

How to stay safe: "Just say no" is useless advice most of the time, but it's entirely apt here. You just need to avoid such groups and communities. In fact, when you see them, consider reporting them. If you're part of an online community that has devolved into espousing dangerous, derogatory, or distasteful ideas that make you uncomfortable, steer clear and leave. Delete. Block. Report. Move on.

Threat 7: Crypto scams

Where it happens: Social media, user comments

Foundry

Cryptocurrency and blockchain technology have some legitimate uses and could still impact the future of financial institutions, but we're still in the get-rich-quick, anything-goes era—and that means scammers love using crypto to part those who don't know any better from their money. Such scams

include fake celebrity accounts that promise a big return on your investment of just a few fractions of Bitcoin, and crypto wallet transfer services that try to steal your private key and/or recovery phrase.

How to stay safe: Not your keys, not your coins. If you own cryptocurrencies, keep your keys private and *never* share them with anyone. Get your crypto off of exchanges and into cold wallets where you are the only master of your coins. You probably aren't going to be one of those who get rich quick, so play it safe, invest only what you can afford to lose, never panic, and keep your FOMO in check.

Threat 8: Fake app stores

Where it happens: APK download sites

Foundry

Every so often, Google might ban a game you really want to play or an app that you depended on. When this happens, you can usually sideload those apps and games via APK download sites—but if you aren't careful, you could fall victim to fake apps that are loaded with malware. It may seem fine and proper when you launch it, but in the background it could be stealing your passwords, credit card info, etc. The locked-down nature of the Google Play Store and Apple App Store can be annoying, but part of it is done for your protection. Going outside puts you at risk.

How to stay safe: For best results, avoid sideloading apps that aren't available through official app stores. But if you simply *must* download an app that isn't available, make sure you 100% trust the creator of the app and make sure you *only* download the app with their official links. Meanwhile, install anti-malware on your device for an extra layer of protection, and consider backing up your device just in case you catch ransomware that blocks you from accessing your data.

Threat 9: Man-in-the-middle attacks

Where it happens: Public Wi-Fi

Foundry

Public Wi-Fi is super convenient, but remember: if you have free access to a public Wi-Fi network, then so do scammers and hackers. Some hackers are able to eavesdrop on public Wi-Fi and tap into your online activity. Scammers can set up imitation Wi-Fi access points that *seem* like they belong to that cafe you're in, except it's a fake. Lastly, even without any scammers or hackers involved, do you trust whoever is providing you with free Wi-Fi? Perhaps *they're* the ones spying on you and stealing your personal data as it flows through the network.

How to stay safe: Always use a reputable VPN before connecting to public Wi-Fi. The VPN will encrypt your online activity and hide what you're doing so it's useless to anyone eavesdropping. But as a rule of

thumb when using public Wi-Fi, don't log in to online accounts and don't type your banking details or any other sensitive information that you wouldn't want to share publicly. Assume everything you do on public Wi-Fi is being monitored, as it may well be.

Threat 10: Search engine poisoning

Where it happens: Search engines

Foundry

Search engine optimization has ruined search engines—in more ways than one. The first page of Google's search results is often filled with not-so-high-quality content, but I'm talking about something else: the fact that scammers and hackers can *also* poison the search results by pushing their malicious websites to the top of the list, either via manipulative SEO techniques or paid ad positions. You might think you're clicking on a link to a well-known and reputable brand, but it could be an imposter site that tries to steal your sensitive data or infect you with malware.

How to stay safe: It's near impossible to avoid search engines altogether, so it behooves you to pay extra attention before clicking on links in the search results. Avoid clicking on the paid ad links, and always double-check the URL before clicking on an organic link. If it looks off, don't click it. Lastly, make sure you're protected by antivirus software.

Threat 11: Scam and malware emails

Where it happens: Your inbox

Foundry

The "Nigerian prince" scam email has been the butt of jokes for decades now, but the rise of generative AI has made these scams way more effective *and* overwhelming to deal with. Scam and malware-infested emails are trickier than ever as they now incorporate personal details to surgically target individuals. This can make them much harder to spot and easier to trust, lulling you into their carefully laid traps.

How to stay safe: There's no good replacement for email just yet, so we all need to keep using it for now. But you can be more careful by never clicking links in emails and never opening unsolicited attachments. If you didn't request it, don't bother with it. And as with other scams, be wary of any email that sounds alarming, urgent, or scary, especially if it seems to want you to act fast within a time limit.

Threat 12: Physical attacks in person

Where it happens: eBay, Craigslist, Facebook Marketplace, Vinted, Mercari, any used marketplace with local pickup options

Foundry

As the cost of living crisis chomps down on victims across the world, second-hand marketplaces have boomed in popularity. They're great for scoring deals *and* for limiting your environmental impact as a consumer. But they have their risks. You can be scammed, of course, but you can also be attacked if you pick up your purchases in person. Just a few months ago, a woman in Pennsylvania was robbed while test driving a used car she planned to buy.

How to stay safe: This problem isn't common enough to avoid second-hand marketplaces altogether, and you don't have to avoid local pickups either. But *always* meet in a well-lit, public space. Ideally, take a friend with you to the meet; if you have to go alone, *always* let someone know where you'll be, who you're meeting, and when you'll be home. And if possible, skip the cash and pay for your purchase digitally—after inspecting the product's condition, of course.

Threat 13: Lies and hallucinations

Where it happens: AI chatbots, search engines

Foundry

The rapid growth of AI is both exciting yet terrifying. One of the scariest aspects of modern AI chatbots and assistants is how easily they make things up and confidently present them as fact. At best, you ask a simple question and get the wrong answer; at worst, you get a complex answer that *sounds* right but is full of falsehoods and non-existent entities. The danger is when you don't know enough yourself to fact check the AI's response. These "hallucinations" appear in everything from ChatGPT to Copilot to Google's AI Overviews and more—and as more sketchy websites use AI to create their content, the entire web is barreling towards a future where it becomes one giant hallucination.

How to stay safe: Never take AI entirely at its word. Ask for citations. Use other non-AI sources to double-check its statements. If you really want to be safe, avoid using AI for anything that hinges on factual accuracy and only use AI for fun or creative tasks. Once you start assuming that everything AI tells you is suspect, you'll be ahead of curve.

Threat 14: Criminal content

Where it happens: Onion sites, porn sites

Foundry

The cleartext (i.e., non-encrypted) internet that we all use every day is much cleaner than it once was, but illegal content is still always one click away. Some unsafe porn sites have illegal content hiding in their video libraries, and it gets even worse once you start dabbling with the Tor Browser and "onion sites" (i.e., the dark web). On the dark web, you can encounter all kinds of dubious, dangerous, and detestable things—hitmen for hire, illicit drug sales, outlawed pornography, other stuff that will scar your mind and can never be unseen. The kind of stuff that you can actually be arrested and charged with real crimes for.

How to stay safe: Using the Tor Browser to hide your identity online is a good start, as is using a VPN to further obfuscate your online activity. But your best bet is to steer clear of the dark web altogether. A strong antivirus might help protect you against malware, but it won't do anything for the illegal content you might come across. If you *must* use the dark web, be extremely careful. But seriously, don't.

Threat 15: Copyright infringement

Where it happens: Torrent sites, illegal download sites

Foundry

Any time you download something illegally, you put yourself at risk. If you aren't careful, you can be caught by law enforcement and copyright holders. That popular torrent might seem innocent enough, but it could be a honeypot set up to trap unsuspecting downloaders. On top of that, ISPs like Comcast and Verizon monitor internet activity and can easily tell when you're pirating digital content. All that to say, you could get slapped with a copyright infringement notice—and if that happens, you could lose your internet access and/or face legal consequences.

How to stay safe: Always use a reputable VPN to mask your identity when you download torrents and visit illegal download sites. A VPN covers up your tracks, so to speak, by preventing ISPs from spying on your traffic and making your internet activity impossible to trace back to you. But again, you need a *reputable* VPN that doesn't store your internet activity. Look for one with a no-logs policy.