- Computer crimes / Computer viruses

How you're most likely to be HACKED/ SCAMMED/ INFECTED in 2024

Nik Rawlinson explores how to protect yourself from the most common attacks and exploits



PRINTED FROM PRESSREADER
COMMERCIAL DISTRIBUTION IS STRICTLY PROHIBITED
NOT FOR SALE
PERSONAL COPY

It might be a while since you last experienced a major malware attack – but the threat hasn't gone away. Cybersecurity specialist SonicWall reports that there were more than 5.5 billion malware attacks recorded in 2022. And simply keeping your security software up to date may not keep you safe: cloud solutions provider Mimecast found that more than 90% of successful hacking attacks are now enabled not by traditional malware, but by someone unwittingly clicking on a phishing email.

If you want to minimise your risks, you need to recognise the biggest threats, and know how to avoid them – whether that's via your computer, your mobile devices, your website or your smart devices.

YOUR COMPUTER

If it seems like the days of major virus outbreaks are behind us, that's because operating systems have got much better at blocking this type of threat. Windows and macOS both have built-in safeguards to prevent applications from performing dangerous actions such as meddling with your system settings and replicating themselves – at least without your permission. This is what's happening when Windows asks "Do you want to allow this app to make changes to your device?"

However, the effectiveness of these safeguards depends on the user paying attention, and not reflexively clicking "Yes" on apps they don't know to be trustworthy. If you've downloaded an installer from an official store or the original manufacturer, the risk may be minimal, but if you get apps from sketchier sites – or via BitTorrent – they could be bundled with a malicious payload. At its most benign, this might be some unwanted utility or browser toolbar; at the opposite end of the scale, it could be a Trojan or even ransomware.

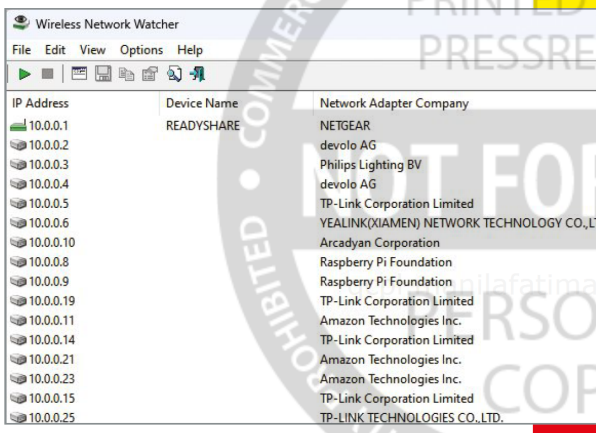
However, while installing untrusted downloads is a sure way to compromise your own security, it's not the most common. Hackers and other malicious actors increasingly take a sneakier approach: in 2021, three-quarters of hackers said that traditional firewall and antivirus protections were obsolete in an age when they could instead use social engineering to gain access to privileged accounts.

Verizon's 2023 Data Breach Investigations Report found that 74% of breaches "involved the human element, which includes social engineering attacks". The UK government's latest cybersecurity breaches survey confirmed that 79% of businesses and 83% of charities had experienced phishing attacks over the previous 12 months. By contrast, viruses, spyware and malware accounted for just 11% of business-focused attacks and 9% of attacks on charities, while ransomware affected 4% in each category.

Your best defence, therefore, isn't technical but mental: you need to be suspicious of anything that arrives by email, and very wary of sharing personal information that could be exploited. You might also choose to use a VPN to encrypt your communications: this won't prevent you from inadvertently entering sensitive information into a phishing site, but it will block snoopers from spying on your network traffic or your Wi-Fi connection.

There are lots of VPNs to choose from; our A-List pick NordVPN (**nordvpn.com**) costs £86 for two years, but if that's too much for you, our second choice ProtonVPN has a free tier (**protonvpn.com/free-vpn**), which can be used with a single device connecting through servers in the Netherlands, US and Japan. Both NordVPN and ProtonVPN maintain a no-logs policy, and they're based in jurisdictions that further protect your privacy (Panama and Switzerland respectively). Opera also offers a free VPN service for in-browser use (**opera.com/features/free-vpn**).

There are plenty of other VPN services to choose from, but treat unfamiliar brands with scepticism: all of your network traffic will be passing through their servers as you browse and work online, so it's essential that you trust them and understand what they're doing with your data.



ABOVE Wireless Network Watcher can log and list your network devices



KEEP YOUR COMPUTER SAFE

- Be alert to social engineering and phishing attacks
- Employ multiple lines of defence, including a VPN
- Keep watch for unfamiliar devices on your home and business network

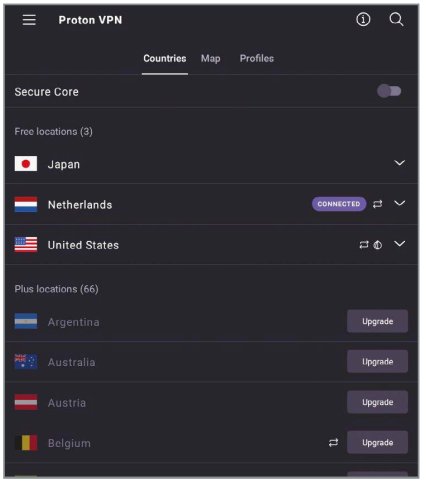
Depending on your network hardware, it may be possible to set up a VPN on your router. This protects every device in your home, without your having to configure each machine individually. However, the VPN can impact on your connection speed – and remember that once you take your phone or laptop outside of your home network, it will no longer be protected.

Another network-oriented measure you can take is to keep an eye out for unfamiliar or unauthorised devices – in truth this is an unlikely avenue of attack, but if a rogue device gets onto your LAN it could harvest data for nefarious purposes, or distribute malware across your devices. An app such as Wireless Network Watcher (**pcpro.link/352watcher**) can alert you to the arrival of new clients on your network, and your router will normally allow you to block any devices you don't recognise.

YOUR MOBILE DEVICES

Smartphones hold a significant quantity of personal data. Many of us use them as payment devices, they can track our movements, and they have access to our contacts, texts, photos and emails. This makes them a prime target for attack.

The most common way in which smartphones and tablets get compromised is via dodgy software installed from outside of the official app stores. In 2016, the European Union Agency for Cybersecurity (ENISA) warned that users should avoid third-party sources to minimise the risk of installing a malicious



LEFT ProtonVPN's free tier is ideal for a single device

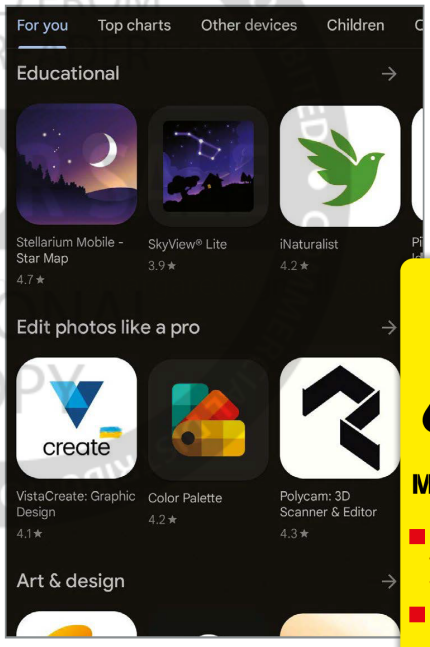
application; the following year, the US Department of Homeland Security issued a report affirming that "users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorised app stores".

To be fair, sideloading doesn't always have to be problematic – both Apple and Google permit large companies to distribute their own in-house apps on company devices, but this requires special corporate configuration and managed accounts.

For individuals, sticking to the official stores lets you avoid a lot of bad stuff. In 2020, Apple removed or rejected close to a million apps and updates from its App Store; almost a quarter were found to be violating privacy guidelines, while more than 150,000 were banned for being spam, copycat applications or misleading users. Apple also expelled 470,000 teams from its developer programme for fraud-related reasons, and rejected 205,000 enrolment attempts, again over fraud concerns.

Historically Google hasn't been quite so strict about what gets into the Play Store, but the tech giant has recently stepped up its efforts to crack down on malware (see **pcpro.link/352appmalware**), and its Google Play Protect technology automatically scans apps for potentially malicious behaviour. "Play Protect can't keep all malware off of Android phones," noted security consultant Joel Snyder, writing for Samsung, "but the risk is much higher when users install apps from the internet or hacker-specific app stores. For this reason, most Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD) policies prohibit sideloading."

Even with these safeguards in place, you should still check the reputations of the apps you download, and be cautious about anything unfamiliar. Researchers at VPN Check last year found that 84 potentially deceptive apps remained on sale through Apple's App Store, 12 months after they'd been logged as malicious by antivirus firm Avast. "These apps are not necessarily malware, or viruses," explained *PC Pro*'s sister site TechRadar Pro. "They might not try to steal data, damage, or destroy the endpoint they're infecting. But they do try to incur extra costs for the victims (either via hidden fees, premium subscriptions, or other similar mechanisms), and are relatively hard to eliminate from the devices."



LEFT Downloading from official app stores gives you extra protection



KEEP YOUR MOBILE DEVICES SAFE

- Only download apps from official stores where possible
- Don't sideload apps unless through certified channels
- Don't trust apps from unrecognised sources

YOUR WEBSITE

If you have a website, it's probably hosted remotely, but that doesn't mean you can afford to neglect its security. If your site is hacked via an unpatched exploit, it could be wiped – or encrypted by ransomware, leaving you with no good options if you don't have an up-to-date backup.

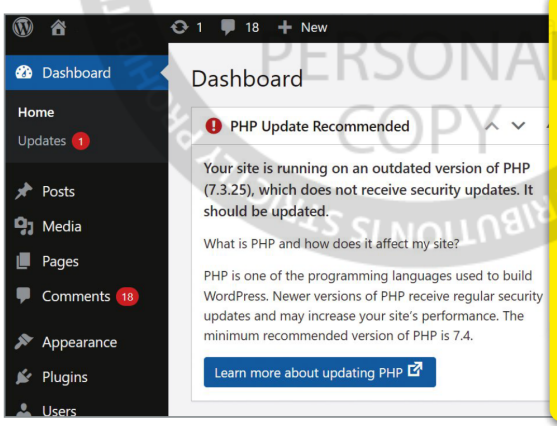
To a certain degree, the security of your site and your online data is in the hands of your hosting provider. If they're slow to update key web technologies, you'll become more and more vulnerable as time goes on. Those technologies might include software and frameworks such as PHP, WordPress, Joomla and Drupal, plus any plugins you're using. Check that your site is using the latest versions – and if it's not up to date, either patch the software yourself or demand that your provider updates it on your behalf.

Realise, too, that it's not just your own data you need to worry about: you also have a responsibility to your website visitors to keep your site secure. A hacked server could be used as a launch point for attacks on other servers or services, and if you're storing sensitive data on your server – or in a linked database – this could leak, exposing you to potential legal action. One of the most common ways that this happens is via a SQL injection attack, where a malicious actor enters deliberately crafted code into an input box, which is interpreted by the underlying database as a query or instruction, rather than data. It's your responsibility to make sure any input fields on your site aren't susceptible to this type of exploit.

Another popular type of attack is cross-site scripting (XSS for short), in which hackers embed malicious content on your pages, which is then executed in the visitor's browser. It may be possible to defend against XSS content using JavaScript, or by disabling scripts altogether where this is practical.

If you're looking to tighten up your website security, a good start is to install an SSL certificate, which you can do for free via Let's Encrypt (**letsencrypt.org**). This won't protect against the types of attack above, but it does provide encryption between your site and the visitor's computer, making it harder for snoopers to steal sensitive information.

If you're running WordPress, we'd also recommend using a tool such as Wordfence (**wordfence.com**). This guards against unauthorised logins with IP banning, rate limiting and

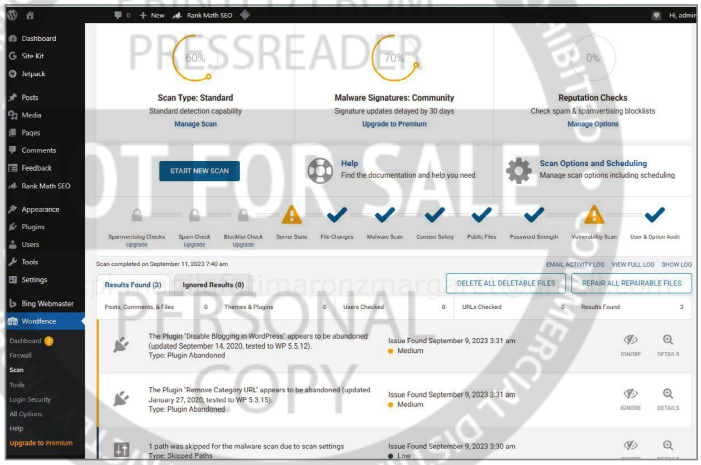


BELOW This server is running an old version of PHP, increasing risks



KEEP YOUR WEBSITE SAFE

- Keep all software, databases and plugins up to date
- Guard against SQL injection, cross-site scripting and other vulnerabilities
- Consider installing additional security software



ABOVE Wordfence can block unauthorised users and monitor your site for changes

easy 2FA – and, more than this, it checks your site against other exploits seen on the Wordfence network and monitors files on your server for unauthorised or unexpected changes. It's easy to install from the WordPress repository, and the free tier will go a long way towards hardening an entry-level or personal site. For the full feature set you can sign up for the $119 per year Premium plan, which includes real-time firewall rules, malware signature scanning and a dynamically updated IP blocklist.

YOUR SMART DEVICES

Smart home devices from big-name manufacturers shouldn't normally be a major security concern – but don't be complacent. Doorbell manufacturer Ring found itself the subject of a class action lawsuit after hackers took over users' devices. According to *The Guardian* (**pcpro.link/352ring**), one Ring user claimed that, while he was watching TV one night, his camera asked "What are you watching?" Another alleges that his children were addressed by an unknown hacker through the device, who commented on their basketball play and encouraged them to approach the camera.

As for doorbells from rival Nest, *Which?* found that "hackers were able to exploit a Denial of Service (DoS) attack, which effectively is a way to spam the device with requests so that it goes offline. An attacker could use this to stop your doorbell from recording if they want to approach your home" (**pcpro.link/352which**).

It goes without saying that, to minimise the chances of exploits such as these, you should ensure your smart devices are running the most recent firmware available. Frequently, they'll update themselves automatically, but it's often possible to perform a manual check through any associated smartphone apps. Once a smart appliance is no longer supported by the manufacturer, consider replacing it.

Aside from firmware updates, settings and options on IoT and smart home devices are normally fairly minimal, so if you want to improve their security you'll need to do it at the network level. You should of course change the default passwords on any smart devices you're using, and ensure the wireless network has strong encryption – ideally the latest WPA3 standard. If your ISP router doesn't support this, you can pick up a cheap WPA3-compliant router for under £100, which you can connect to your existing router to broadcast a secure wireless network – just be sure to turn off Wi-Fi on your old router.

For maximum safety, it's a good idea to connect your IoT devices to a guest network, rather than the main one that handles your computers and phones. This ensures that even if a smart appliance is completely compromised, it's isolated from any devices that might contain personal information or exploitable software. ●

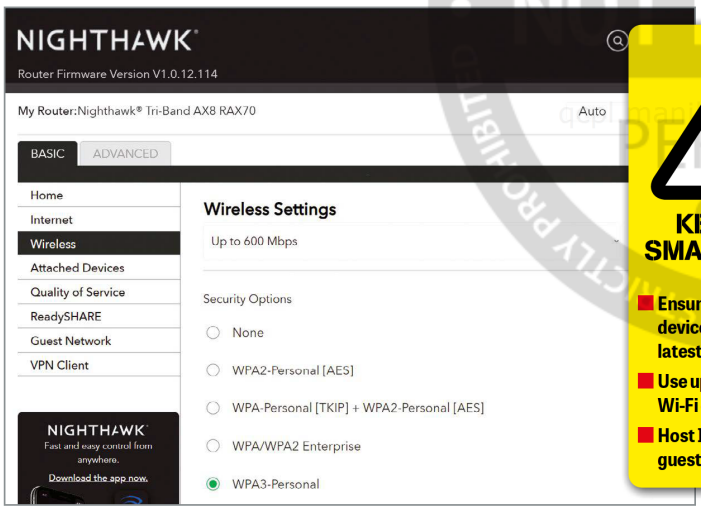
CLOUD SERVICES

When it comes to online services such as Gmail or OneDrive, privacy and security are generally handled entirely by the provider: you'll get little or no visibility or control over the technical or architectural side of things. This is because the resources that power your cloud account are almost certainly shared with thousands or millions of other users; it's simply not practical for the vendor to leave security up to individual users.

If you're buying into a software-as-a-service product, therefore, it's critically important to do your due diligence, especially for businesses (*see p104*). Check for compliance with the ISO 27000 family of standards for information security management, and in particular ISO 27017 and ISO 27018. The former is a code of practice that aims to reduce the risk of security problems in cloud environments; ISO 27018 is concerned with privacy and minimising risk when handling personally identifiable information in cloud environments.

Although it's not exactly a security concern, you should also consider how you're going to get your existing data into a cloud service – and how you might get it out again at the end of a long-term contract. Moving accounts or databases between online services may be difficult or even impossible: your best option might be to start from scratch at the start of the next financial year, after exporting historic records as PDFs, spreadsheets or an alternative interchange format. Consider, too, how you'd continue to function if the service suffered an outage, or even unexpectedly went out of business: keeping local copies of your data can reduce your exposure.

For businesses that have multiple users accessing SaaS platforms, accounts must be regularly audited, to ensure no-one can access anything they shouldn't be able to; where possible you should also check login times, locations and activities. One of the most common ways that businesses are exploited is via employees abusing their access, or being tricked into giving away passwords or other sensitive information. Implement 2FA where possible, mandate the use of strong, complex passwords on all accounts – and it goes without saying that access must be promptly revoked when someone leaves the organisation.



BELOW LEFT Use WPA3 encryption across your network if your router supports it

KEEP YOUR SMART DEVICES SAFE

- Ensure that all smart devices are running the latest firmware
- Use up-to-date, robust Wi-Fi encryption
- Host IoT appliances on a guest network