A guide to internet security

Print this guide

Whilst the overall benefits of using the internet can be huge, security should be a concern for everyone. When using the internet you need to accept certain risks, but this should by no means put anyone off. With the right knowledge and sensible precautions any risks can be minimised.

What you will learn in this guide:

- Definitions of the most common online security threats.
- key steps you should take to protect yourself when online.

What is internet security and the most common online attacks?

Internet security describes the efforts and precautions we take to keep ourselves safe from malicious online attacks — which usually involve some kind of illegal breach of our web accounts, programs or connected devices.

Some of the most common types of so-called cyber attacks we should all be aware of include:

- **Hacks**: This basically describes the unauthorised access to a secured system by individuals or groups, commonly referred to as ‘hackers’. Common targets of hackers are websites, email accounts and large commercial or public databases.
- **Phishing scams**: One of the most common (and easy to fall for) form of online scam, this is where an individual (usually a hacker) masquerading as an established company such as a bank or well-known retailer, emails individuals asking them to hand over private data such as their email login or bank details. The scammer masquerades under some kind of bogus premise (such as ‘we need to update your details’ or ‘we’re updating our systems and need you to complete this form’). At first glance, these emails can be pretty convincing and it’s not hard to see how so many people can fall foul of them.
- **Viruses**: computer viruses are one of the longest and well-known of computer pests. They are essentially files or mini programs that can ‘sneak’ onto computers within wider files downloaded by users, with malicious intent — ranging from significantly slowing down your computer, to spying on or even controlling your computer, and extracting sensitive information for personal gain.

How to stay safe: top internet security tips

- **Always use antivirus software**: This is an absolute essential if you want to avoid having your devices compromised. There’s a range of options out there at various price points — but you needn’t fork out a fortune to protect your computer. There are actually quite a few cheaper or even free antivirus programs out there that are rated highly, and these days both Microsoft and Apple offer built-in protection with many of their devices. Mobile security shouldn't be overlooked either. Apps such as Lookout, can help protect your phone. Here's a useful list of free antivirus apps for ipads and iphones.
- **Never trust unfamiliar email addresses or links**: If you receive an email address out of the blue from a bank or retailer that asks for any personal details, treat it with extreme caution. A tell-tale sign of a phishing hack is that the email address (whilst in many cases can be impressively similar to the genuine brand’s) won’t be the real thing. If you suspect malicious intent, report the address to your email provider and delete. Phishing attacks and scams are becoming increasingly common on social media, too. Quite simply, if you don’t trust a link, never click on it.
- **Secure your web browsers**: All the common web browsers (Internet Explorer, Mozilla Firefox and

Google Chrome) will have various security setting that can help minimise risk to your online accounts and data. For instance, you could switch off the option for your browser to remember your login details for email accounts and social media, set the security options to 'high' and regularly clear the browser's cache (or even disable all together) so that your browser doesn't cling on to too much potentially sensitive data.

- **Regularly change your passwords**: Make a rule to update all your passwords every few weeks. This might seem like a hassle, but if it significantly reduces risk of hacks and security breaches (which it does) then it's worth the effort. Make sure you opt for a memorable yet secure password (many accounts advise on the quality of your selected password).
- **Regularly update your software**: This is a really basic one, but many people tend to ignore alerts from programs advising them to update to their latest version as 'there are more important things to be getting on with'. However, the exact reason for many software updates can be to strengthen a recent security vulnerability.
- **Always check site security levels before trusting**: We often need to enter personal details on a website. As a general rule of thumb, all websites that ask for these details should be using an additional level of security to protect your data via an 'https' address (the 's' stands for 'security' and websites that don't have this, will be missing the 's').
- **Use Two-factor authentication** (sometimes referred to as 2FA) which provides your accounts with an extra layer of security and can stop cyber criminals accessing your account – even if they have your password. You'll be asked to verify a second piece of information after entering your password, this could be digits from a code sent via a text message (SMS), a notification in your app or providing fingerprint or facial recognition.

  This type of security means that your account can't be accessed directly from just entering your password, adding another barrier between your personal details and cyber criminals. You can read our guide on how to set up 2 factor authentication for Gmail at this link.
- **Back up your personal data** - It's a good idea to back up your personal and valuable data you have stored on your devices to an external source such as an external hard drive or cloud storage service. This creates a copy that can be accessed easily if you become the victim of a malicious attack.

  Hopefully you'll see that there's lots of things you can do to keep safe when accessing and using the internet, by taking precautions and following sensible guidance and best practices, you can keep your devices and personal information secure.
- When using **public wifi be more cautious** about the sites you visit (for example, don't log into your online bank account), as not all wifi hotspots are secure.
- **Use common sense**: At the end of the day, the reality of online security threats are not much different to the offline world. Simply be alert to unusual behaviour or practices, don't trust strangers and be wary of unsolicited approaches for your information.

The internet, just like the 'real' world, is full of both potential opportunities, as well as dangers and risks. Hopefully this guide has made you aware of what those risks are and the steps that both you and your community should be taking to avoid becoming a target of cyber attacks.

Further reading:

- Comparitech's Internet Security guide to help you stay safe online.
- Virgin Media's great guide: Cybercrime: What is it and how can you stay safe online?, includes a test, to help you remember what you've learnt.
- Which? guide to How to keep your data safe when using public wifi.

Last update July 2024

Next steps

- A guide to cyberbullying
- How to set up and run your Facebook page
- How to shop safely online

- Email safety tips
- Keeping your children safe online

How do digital skills change lives?

Find out about Digital Inclusion

Digital Unite

0800 228 9272

du@digitalunite.com

Get in touch

Privacy policy/ Equality and Diversity Policy

Terms of use/ Cookie policy

Our learning platforms

Digital Champions Network

Inspire

Our newsletter

Research, resources, insights and offers.