How to keep your identity safe online

Follow our advice and it's easy to be safe online.

Like the real world, the online realm has plenty of dangers. One of the most concerning is identity theft, where someone steals aspects of your life for their own nefarious purposes. Of course, identity theft can happen in the real world too but the nature of the web makes life that much easier for criminals.

From fake websites to dodgy software downloads that will secretly record your keystrokes, identify theft attempts are rife. The good news is that it is relatively easy to avoid becoming a victim – you just have to know how and where to tread carefully.

Step 1: Keep your security software up to date

Whatever device you use to get online, you should ensure that it has security software installed and enabled.

For Windows PC users, Microsoft Security Essentials is recommended, which is a free download from Microsoft. It protects against spyware and viruses, and works in the background, so it won't disturb your computer activities. It won't protect against all forms of identity theft but it is a reliable first line of defence. In addition, good anti-virus software is essential which must be maintained up to date.

Step 2: Be careful where and what you click

Deceitful web links get many web users into trouble. For example, clicking a link in an email message purporting to be from your bank could open a web browser to display a website that looks legitimate. But this is a widely practised scam known as 'phishing'. The seemingly correct appearance of the phishing website might trick you into logging in – and at that point, the fraud is complete. The perpetrator now has your bank-login details.

Few legitimate financial organisations actually send out emails like this, so the advice is to avoid clicking links in emails unless you're absolutely certain of the source. If you do need to visit your bank's website, do so by typing in the web address yourself, or use an existing, trusted browser bookmark.

Step 3: Use a password manager

It is very sensible to use a different password on every site which requires you to log in – but remembering all these codes is difficult. You can install a password-management tool allowing you to create and store lots of different login details securely, encrypted with a single password.

Step 4: Watch what you download

Tread very carefully when downloading and installing new software. This is particularly relevant when it comes to free programs, some of which may surreptitiously install privacy-invading tools at the same time.

This could be an annoying advertising add-on in your web browser, or something much more disturbing, such as a key-logging tool that will record whatever you type before sending this private information back to the program's author.

Of course, this does not mean that every free application is dodgy or that you should not trust any website offering free applications, but stick to well-known, trusted download sites such as **Download.com.** If you think you've installed something dodgy, delete it and perform a security scan.

Step 5: Shop on secure websites

When shopping online, always check that stores are genuine and secure.

Guard against phishing and check that the web address begins with 'https://' – the 's' being the all-important indicator that your computer connection to the website is secure, and that any transferred data will be encrypted en route.

For added security, use a credit card when and wherever possible, as this offers added legal protection against fraud (basically, the card's issuing bank will be jointly responsible for any problems for purchases above £100).

Step 6: Don't forget offline risks!

Remember that identity theft still happens in the real world. Tear up (or preferably shred) any sensitive printed documents before binning or recycling. Shredders start from around £20 online.

Never give personal details to unexpected callers, if the phone rings and you're asked to confirm your debit card details or account password, hang up – and then call the organisation back using a telephone number that you know to be correct.

If expected documents don't turn up in the post, contact the relevant company right away to find out why.