Our top 10 tech tips

Originally published March 2020

The internet has opened up new opportunities to shop, bank, research, work and connect whenever we want to and wherever we are. But we could all be unwittingly giving criminals many opportunities to steal directly from us or to steal our identities and commit fraud against ourselves or others.

Here are our top tips to help make you safer online.

1. Set strong passwords

Current advice is to use a paraphrase of three or four unconnected words, which others would find hard to guess, comprising at least 13 characters, for example 'candleshipmonkey'.

To make it even more secure, include random capital letters and replace some of the letters with numbers or special characters. Like using '!' instead of 'I', '4' instead of 'A', or '#' instead of 'H'.

And of course: avoid using the same password for more than one account.

2. Protect your hardware

Always set a password, Personal Identification Number (PIN), or passcode. Not just for your mobiles and tablets but also for all your 'smart' devices. That includes TVs, voice assistants, and even refrigerators. All can offer ways for cybercriminals to enter your home. Your Wi-Fi router will also have a factory-set password that you should change.

The cameras in your smart devices could also be used to spy on you so cover the webcams of your laptops, tablets and TVs when not actively using them.

You should also back your devices up regularly either on the cloud or to an external hard drive.

3. Secure your connection

We've recommended changing the password on your home WiFi network but when out and about think twice before using public WiFi unless it is password protected. Always wait until you're able to connect to a secure Wi-Fi network before providing sensitive data such as your bank account details. Or use your mobile contract's data allowance.

4. Secure your software

Update all your software regularly, especially when prompted to. Updates and upgrades often contain additional security features and 'patches' that fix security flaws in the original coding. Security software from a recognised company can provide a vital layer of defence.

Schroders
personalwealth

If your laptop uses Windows 7, upgrade to Windows 10 as Microsoft will no longer provide software updates and 'patches' for the older program. Some older machines can't run Windows 10 so you may have to replace your device.

5. Protect your identity

Be careful how much you reveal especially on social media posts. Sharing your address, phone number, birthday and other personal information can put you at a greater risk of identity theft, stalking and harassment.

Many pop quizzes are thinly disguised attempts to steal personal security information: such as the name of your first pet combined with your mother's maiden name, your middle name combined with the street where you live or grew up, or the make and model of your first car. These are all security back-up questions.

6. Protect your reputation

Once online, always online: the Internet does not have a delete key. There is no way for you to take back a comment you wish you hadn't made, or get rid of that embarrassing drunken selfie you took at a party. It's out there for everyone to see. Don't put anything online that you wouldn't want to see on the front page of a national newspaper. One way to protect yourself is to use a nickname and a profile picture that does not give away who you are.

7. Buy securely

Any time you make a purchase online, you need to provide credit card or bank account information. Only supply this to sites with secure, encrypted connections. Look for an address that starts with https: (the 's' stands for secure) rather than simply http: They may also have a padlock icon next to the address bar.

Finally, set up two-factor authentication wherever you can. For example, always elect to receive a text message or email from your bank or credit card provider with a single use passcode.

8. Download securely

If a cybercriminal can get you to download an app carrying malicious software ('malware') that can take over your device or steal information they have struck gold. This could be disguised as anything from a popular game to something that checks traffic or the weather

Always download from an official app store and avoid installing apps from links in emails, social media, text messages or websites that look suspicious. Uninstall apps when you no longer need them.

9. Email securely

Email remains the easiest and most successful approach for cybercriminals to attack unsuspecting users*. Known as phishing, predators disguised as plausible businesses or individuals send links to non-legitimate websites that steal your information.

Never click on suspicious or unknown links or attachments. Spelling errors, poor grammar, email addresses that don't seem quite right, and out-of-the blue messages from friends should be treated with utmost caution. So, think before you click.

10. Dispose of your old technology safely

It is very important to make sure you delete all your personal information and account details before retiring and disposing of your old equipment. Even ‘deleted’ data can be retrieved with relative ease by criminals.

Disposing of your tech through a recognised disposal facility will also ensure the minimum environmental impact and prevent you from breaking the law. Some retailers will transfer your data.

Conclusion

We are living and sharing more and more of ourselves in very public ways. Ways that didn’t exist as recently as ten years ago. How many of are really trained or even educated to understand the threats and pitfalls that lie in wait for us? Always stay vigilant and never give away sensitive information unless you can verify that the source is legitimate.

In the end, good security is about being vigilant and keeping yourself abreast of how technology is changing our lives. For today's security might not be tomorrow's.

If you think you have been the victim of online fraud, report the incident to your local police.