Protecting Yourself Online

Seven Top Tips

A guide by the Law and Order Foundation

---

1 Never give out your personal details

If you are asked to enter your bank details or reveal your passwords via an email, pop-up window or by someone who has telephoned you, don't do it! Your bank will never ask you for any of your personal details or ask you to transfer money out of your bank account. Make sure you navigate directly to the website you want to visit. If you're unsure, you can always telephone your bank using the number on an official letter.

2 Use strong passwords

Make your password longer than seven characters and include a combination of letters, numbers and symbols. Don't repeat the same password across lots of different websites because if one site is hacked, all of your personal information could be compromised. Change your passwords frequently and never share your passwords with other people.

3 Only access secure websites

If the address for the website you are using does not start with https, or if the site asks you for your credit or debit card details when it doesn't seem necessary, then do not enter any of your details.

Who can I contact if I have been a victim of cyber crime?

If money has been taken out of your bank account or a credit card has been used without your authority, contact your bank and/or card provider immediately. For all forms of online fraud, contact Action Fraud for a crime reference number, which you can then use when you contact the police. If there is a crime being committed right now, or you are in danger, you should contact the police by telephoning 999 immediately.

4 Install anti-virus software and updates

Make sure you install an anti-virus programme onto your computer. This will help you spot unsafe websites and get rid of any viruses if your device is infected. Never open any attachment you are not expecting, or those sent from email addresses that do not look official, or if the accompanying email has spelling or grammatical errors.

5 Backup your files

Some viruses will deliberately damage the files on your computer and then demand money for them to be restored. To protect against this, you can back-up important computer files onto an external hard drive or memory pen, or a computer that is not connected to the internet.

6 Secure your mobile phone

If you have a mobile phone, make sure you have a pin code for your memory card and a pin or password for your phone. Try not to leave yourself logged into your social media and email accounts on lots of different devices. If someone gains access to your phone or computer, they could then have access to all of your accounts and information.

7 Be aware of major security breaches

Online security breaches are sometimes reported in the news, so keep an eye out for information. It may be that a company or service you have used has been attacked. There is usually some advice about the steps you can take to secure your personal information. This might include installing a recommended software update and/or changing your password.

Please visit www.getsafeonline.org for further tips on how to stay safe online

If you are victim of cyber crime or fraud even after following the advice in this guide, we regret that the Law and Order Foundation cannot accept any liability.

LAW AND ORDER FOUNDATION

Voice for Victims | Communities against Crime

DONATE NOW

The Law and Order Foundation can only continue to do its work with your support

www.lawandorderfoundation.co.uk/donate

Contact

Law and Order Foundation
PO BOX 999
Twickenham
Middlesex
TW1 3TB

Email: info@lawandorderfoundation.co.uk

Twitter: @lawandorderfoun
Facebook: /lawandorderfoundation

LOF-CC1-18