

Cyber Crime and Staying Safe Online

Reporting Fraud

Fraud and Cyber crime is reported nationally to **Action fraud**.

Via phone **0300 123 2040**

Or online

<https://actionfraud.police.uk/>

Feedback Survey

<https://www.smartsurvey.co.uk/s/Individual-MET2021>

Be Cyber Aware

1. **Create a separate password for your email**
2. **Create a strong password using three random words**
3. **Save your passwords in your browser**
4. **Turn on two-factor authentication**
5. **Update your devices**
6. **Turn on backup**

Resources & Advice

www.met.police.uk/littlemedia

Electronic copies of our leaflets and links to our animations

Email:

cyberprotect@met.police.uk

<https://takefive-stopfraud.org.uk>

"National campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud"

<https://www.getsafeonline.org>

"UK's leading source of unbiased, factual and easy-to-understand information on online safety"

www.haveibeenpwned.com

Enter your email to see if it's ever appeared in a breach.

<http://cyberaware.gov.uk/>

The UK Government's advice on how to stay secure online. Includes advice around activating 2FA.

Creating Strong Passwords

1. Three random words
grinning skydiving otters
2. Capitalise some letters
GrinningSkydivingOtters
3. Add some numbers & characters to make it even stronger.
GrinningSkydivingOtters£33



**METROPOLITAN
POLICE**

10 Tips to avoid Cyber crime

Have a strong password

To create a strong password simply join three random but memorable words together. To make it stronger add numbers & symbols.

For example: GrinningSkydivingOtters£33

GrinningSkydivingOtters



Have an (up to date) anti-virus

Download updates and scan your devices regularly (once a week at least).



Update software – install patches

Always update or patch your software as soon as you're prompted to ensure that it remains safe and secure.

UPDATE COMPLETE



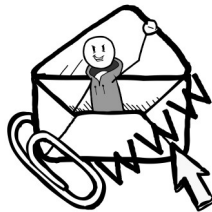
Back up your data regularly

Regularly copy your important information to external storage like external hard drives, USBs or cloud storage.



Don't click on links/open attachments (unless verified) in emails or texts

Clicking on unverified links or attachments in emails or texts can give criminals access to your devices.



Avoid public Wi-Fi for personal activities

Never use free Wi-Fi for anything you don't want a stranger to see, and consider keeping Wi-Fi turned off



Report all fraud and cyber crime to Action Fraud.

Even if you didn't lose money, you should still report every instance of fraud or cyber crime you're targeted by. Every report assists police investigations, disrupts criminals, and reduces harm.



Turn on two factor authentication.

Where available turn on 2FA on any accounts that contain important or personal information. Go to <http://cyberaware.gov.uk> for instructions on how to set up 2FA across popular online services.



Always challenge requests for personal information.

Criminals will try all sorts of stories to get you to part with your money or data, Never give information to anyone who contacts you out of the blue.



Set privacy settings on social media

Be careful who can see what you share online, ensure your privacy settings are set to a high level. Never share private information or any pin codes on social media.

