Report it!

If you are a victim of online fraud, report it to Action Fraud at **www.actionfraud.police.uk** or on **0300 123 2040**. If someone attempts to defraud you on a website, report it to the site. If someone's abused you, report it to the site or social network.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

About Get Safe Online

Get Safe Online is designed to help everybody safeguard against online fraud, identity theft, malware, abuse, device theft and other problems.

- Easily accessible on your computer or mobile device
- Packed with great advice and best practice that's easy to understand and act on
- Written and regularly updated by experts in online safety and security
- The UK government's default online security advice channel
- Supported by law enforcement agencies
- Backed by companies who are household names in internet safety, technology, retail and financial services

Get Safe Online

Stay safe, stay secure

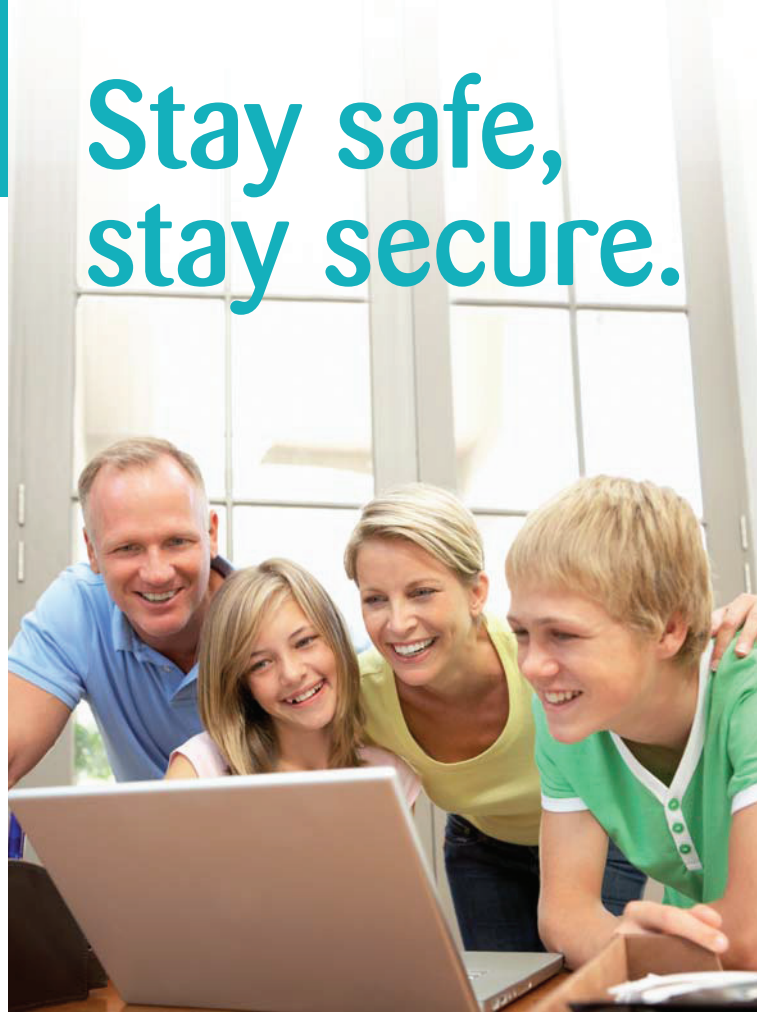
For more information and impartial advice on protecting yourself, your family, your business, your computer and mobile devices while online visit

www.getsafeonline.org

Gloucestershire Constabulary

OFFICIAL PARTNERS

LLOYDS BANK, HALIFAX, Experian, first direct, Standard Life, BARCLAYS, KASPERSKY, RBS, HSBC, Norton, NatWest, TESCO, PayPal, creativevirtual, Bob's Business, HM Government, Cabinet Office, Home Office, Department for Business Innovation & Skills, CYBER STREET, ASSOCIATION OF CHIEF POLICE OFFICERS, NCA National Crime Agency, CITY OF LONDON POLICE, METROPOLITAN POLICE, Ofcom, ActionFraud actionfraud.police.uk



Stay safe, stay secure.

With Get Safe Online
www.getsafeonline.org

Gloucestershire Constabulary

Get Safe Online is a unique resource designed to help you keep yourself, your family, your computer and mobile devices and your business protected against the many negative aspects of the internet.

This leaflet is designed to provide you with a few simple safety tips.

For more comprehensive guidance, please visit **www.getsafeonline.org**

It's easy to understand, offers practical, unbiased advice and is free to use.

Stay safe, stay secure – read these top tips:

PINs & passwords

Your first line of defence is a PIN or password – whether it's on your computer, mobile device, apps, online bank accounts or social media. Never use the same password for more than two things, make them as difficult as possible to guess and don't share them with anyone.

Viruses & other malware

Viruses and other malware can cause all kinds of problems – from simply making your device run slowly to locking it until you've paid a ransom, or letting someone spy on you through your camera. Protect all devices with security software and install updates to all your programs and apps when prompted.

Privacy

Don't reveal more private or financial details than is absolutely necessary – people aren't always who they seem and it might end up being pieced together to commit fraud or ID theft. Check the privacy settings on all your social media accounts.

WiFi

Make sure your home or business WiFi is set to 'secure' and protected with a strong and private password. When out and about never use a hotspot that may be unsecured, especially when what you're doing online is personal or financial.

Links and attachments

Don't open or forward emails from people or organisations you don't know, or those that seem to be from your bank or other official body that they just wouldn't normally send. Don't click on links in emails or social media posts, or open random attachments. They may be 'phishing' for information, or result in a virus or other malware.

Don't put up with abuse, or abuse others

Some people think hiding behind their keyboard makes it acceptable to abuse others … for example trolling, threatening, stalking or blackmailing. If you're a victim, ignore the abuser and report the abuse to the police, the social network or your internet service provider as appropriate. And, of course, it's completely unacceptable for you to abuse others.

Secure web pages

When shopping or banking online, before you enter your card details always check there's a padlock symbol in the browser window when you have logged in or registered, and that the web address begins with '**https://**'. The 's' stands for 'secure'. Log out of your accounts when you've finished with them – don't just close the window.

Paying for goods or services

Wherever possible, carefully check the company or person you're buying from – whether it's tickets, goods, a car, a flat, a flight or many of the other things you buy online. Make sure what you're buying actually exists. Never transfer money directly to a bank account or hand over any personal details.

Safeguarding children

Our kids may know their way around the internet, social networking and apps better than we do, but they're more vulnerable than we are, not having the judgement or maturity to cope with unexpected or threatening situations. Work with your kids to keep them safe, and use your internet service provider's content filters and some kind of parental software.