Dyfed Powys Police have joined forces with Get Safe Online to bring you some expert, easy-to-follow tips on protecting yourself, your family, your finances and connected devices whilst using the internet.

To get the full picture, please visit **www.getsafeonline.org**

Always remember that if something seems too good to be true, it probably is.

Please pass on our advice to others.

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.

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 expert, impartial, up-to-date advice and best practice that's easy to understand and act on
- Supported by the government, law enforcement agencies, regulators and private sector companies in internet safety, technology, retail and financial services

www.getsafeonline.org

Stay safe

Stay secure

Heddlu Police
DYFED-POWYS
Diogelu ein cymunedau, gyda'n gilydd Safeguarding our communities, together

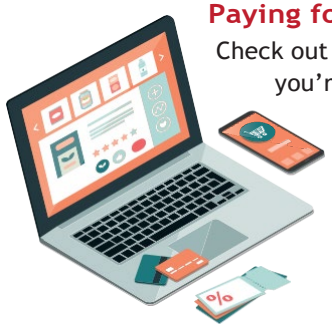
Stay safe, stay secure – read these top tips:

Passwords & PINS

PINs and passwords are your first line of defence on your computer, mobile device, apps, online bank accounts and social media. Create passwords that are strong, don't share them and use a different one for every online account in case one or more gets hacked. A secure password manager will help you to remember them all.

Protect your privacy

Don't overshare personal or financial details on social media, websites or on the phone. Check privacy settings on your social media accounts. Your details can be pieced together by criminals to defraud you or steal your identity.



Paying for goods or services

Check out the company or person you're buying from – whether it's tickets, goods, a car, a flat, flight or the other things you buy online. Make sure what you're buying actually exists. Never pay by direct transfer and don't hand over any personal details.

Ransomware, spyware & other malware

Malware can cause many problems including locking your access until you've paid a ransom, monitoring your keystrokes or being spied on via your webcam. Protect all devices with security software and install updates to all programs, apps and operating systems when prompted. Never pay or respond to ransoms: it's unlikely your device will be unlocked.

Out & about

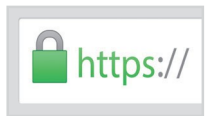
Never use Wi-Fi hotspots for anything confidential as they may not be secure and your information or transactions could be at risk. Instead, use your data, a broadband dongle or VPN, or wait until you get home. Don't leave mobile devices unattended.

Links & attachments

Don't click on links in emails, texts or on social media, nor open email attachments, if the source isn't 100% known and trustworthy, or they're random and unexpected. They may be 'phishing' for information or result in you downloading malware.

Secure web pages & payments

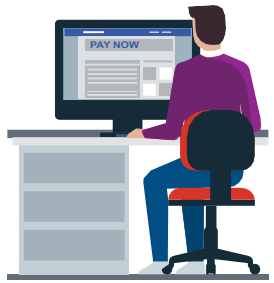
When shopping or banking online, check that the page address is spelled correctly, as criminals can create fake sites with similar addresses to the authentic one. It's best to type the address in rather than follow links.



Before clicking 'pay', check there's a closed padlock symbol in the browser window and that the web address begins with 'https://' … the 's' stands for 'secure'. Do bear in mind, however, that a secure site can still be a fraudulent site. Physically log out of accounts when you've finished your transaction.

Payment update requests

If you get an email, letter or call asking you to change payment details for an online account, subscription or perhaps solicitor's fees, always call the company or organisation on what you know to be the correct number to ensure it isn't a scam.



Payment by voucher scams

Remember that HMRC, the police, DVLA, courts or similar organisations would never request or accept payment using iTunes, STEAM or similar vouchers/gift cards. Any requests for payment in this way are fraudulent.

Blackmail emails

A lot of people have received emails threatening extortion for accessing adult content online. Some even quote a current or old password. These are opportunistic, so don't contact the sender or pay a ransom. However, you should think about changing that password. Also, don't remove your clothes in front of your webcam, you never know where the images will end up.

Online abuse

If you're a victim of online trolling, threats, stalking or blackmail, ignore the abuser and report it to the police, social network or your internet service provider as appropriate. And, of course, it's completely unacceptable for you to abuse others.

Safeguarding children

Work with your kids to keep them safe, talk about what they do and who they talk to online. Use your ISP's content filters and install parental software.