Christmas is a time when many of us will be spending more money and possibly letting our guard down as we think we have found a bargain.

Remember, criminals don't take a Christmas break.

Criminals love this time of the year – they use the combination of lower prices and the sense of urgency to trick you into parting with your money on items that don't even exist!

Dyfed Powys Police Cyber Crime Team have put together this handy guide to help you have a safer cyber Christmas.

Treat yourself to a privacy pamper at this time of year…

Relax and take some time to check the privacy settings on your applications - often the developer has left them to share everything by default, as this is in their interest. Make sure you check the settings on each of your apps to ensure you are not giving out data you were unaware of, especially if you are setting up a new device you received for Christmas.

Share responsibly this Christmas…

Every social media app works by allowing you to upload pictures and personal views in an easy/seamless manner. Think before posting your Christmas capers - some things are best left unseen!

Think of your safety and the safety of your possessions. Burglars use social media as a research tool.

Think about possible repercussions of posting details of your lovely gifts - criminals love you to advertise your expensive possessions, along with where you live!

Don't get a virus this festive season

Remember - Anti Virus Software only works if it is kept up to date.

Anti-Virus software will not protect you from your own actions – so always think before you click!

Stop:

Take a moment to think before parting with your money or information - it could keep you safe.

Challenge:

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect:

Contact your bank immediately if you think you've fallen victim to a scam and report it to the Police.

Report:

You can report suspicious emails to:
report@phishing.gov.uk

You can also report suspicious texts by forwarding the original message to **7726,** which spells SPAM on your keypad.

Heddlu Police
DYFED-POWYS

Heddlu Police
DYFED-POWYS

Wishing you a safe and merry Christmas

Top tips for a happy & cyber-safe Christmas

Heddlu Police
DYFED-POWYS

Keep your digital front door locked this Christmas…

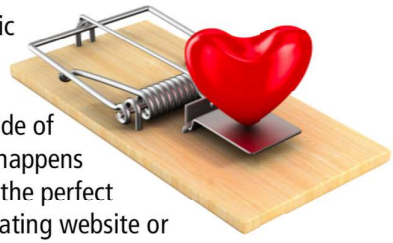
Don't be a statistic this Christmas, make sure your passwords are strong and unique.
Passwords may seem boring, but they are the key to your digital front door. Choose a strong password and make sure each online account has a different password. If not, criminals may be able to gain access to your other online accounts if your password becomes known, ruining your Christmas!

Consider the use of a Password manager app to ensure you can maintain multiple strong passwords safely.

Give yourself the present of peace of mind:
Adding Two-Factor Authentication (2FA) is a far more secure solution than relying on passwords alone.

2FA works by requiring two different methods to authenticate yourself - so if your password is compromised, your account is still protected by 2FA.

Love is in the air, but beware of a Christmas Romance Fraudster



Christmas may be a romantic time of year, but be careful to make sure you really know who is on the other side of the screen. Romance fraud happens when you think you've met the perfect partner through an online dating website or app. But criminals use a fake profile to form a relationship with you. They gain your trust and then start to ask you for money or gather enough personal information to steal your identity.

Keep your clothes on this Christmas – don't become a victim of Sextortion!

The contact often starts on a social networking site. Once on video messaging, the victim is enticed into committing a sexual act, often in response to something displayed by the suspect.

This act is recorded by the suspect who then threatens to release the video unless money is paid.

The suspect states that the recording will be released on YouTube or to specific friends and family on the victim's social media friends list.

The safest way to avoid sextortion is to never take your clothes off in front of a webcam.

Christmas Crypto – is it safe?

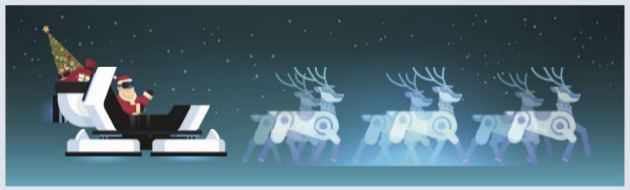
Cryptocurrency is not regulated and if you lose money by investing via a fake platform, or lose access to your private wallet, you will have no recourse to your funds. Cryptocurrency is still a gamble, despite it gaining popularity in mainstream media.

Bills, bills, bills – be careful of Invoice & Mandate Fraud

Be careful as criminals often use authentic looking invoices.

Always query change of account details and always check by ringing the person or company (using a number you know, or have obtained by a trusted method.

Click to see where Santa is?



Be aware - when you click on unverified links or download suspicious apps you increase the risk of exposure to malware (malicious software / viruses).

Keep your new device and software up to date

Criminals make use of known security vulnerabilities in software and hardware.

Manufacturers and App developers patch their software and issue security updates to prevent criminals from exploiting these loopholes. If you don't run the most up to date operating system or software version, you are putting yourself at risk of compromise.

Has a friend said they need a Gift Card, but no time to buy one?...

Check with the sender of the request before purchasing a gift card - phone them or ask a trusted friend of theirs - sometimes social media accounts are hacked to carry out these scams, so be careful which medium you use to contact the individual to check.

The police or bank will not ask you to help catch a criminal this Christmas… don't fall for a Christmas Courier Fraud scam.

The criminal often pretends to be from the police or a bank and state that they require your assistance to trap a rogue employee that is putting counterfeit cash into the ATM.

They ask you to withdraw money and then state that a courier will collect the cash as well as your bank card and you will be re-imbursed. They often continue the scam by stating that your bank account is in danger and you need to transfer all the funds into a 'safe account'.

The new account is operated by the scammers, who then steal the remaining funds.

- **Your bank won't send a courier to your home.**
- **The bank or police never collect your bank card.**
- **The bank or police will never ask for your PIN.**

If you receive one of these calls, end it immediately, wait two minutes and then call the police on **101**.