Gift Card Fraud

There are a variety of different ways this scam operates, but normally it will be either stating that a bill needs to be paid or someone in difficulty who would like you to purchase a gift card for them and they will pay you back later.

No genuine government department or company would make this type of request.

Check with the source 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.

Courier Fraud

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'. Of course, the new account is operated by the scammers, who then steal the remaining funds.

Your bank will not send a courier to your home.

Your bank and the police will never collect your bank card.

Your bank and the police will never ask for your PIN.

If you receive one of these calls, end it immediately.

Privacy Settings

Always 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.

Over Sharing

Every social media app works by allowing you to upload pictures and personal views in an easy/seamless manner. Think before posting.

Think of your safety and the safety of your possessions - criminals use social media as a research tool!

Think about who can tag you in posts and also the possible repercussions of posting inflammatory or embarrassing content - what would happen if a prospective employer was to see it when searching your profile during a job interview?

1872 PRIFYSGOL ABERYSTWYTH UNIVERSITY

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:

01970 622400 / is@aber.ac.uk

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
&
1872 PRIFYSGOL ABERYSTWYTH UNIVERSITY

Staying Safe Online

Passwords
2FA
Money Muling
Romance Fraud
Sextortion
Crypto Currency Scams
Investment Scams
Software Updates
Links
Webmail Rules & Filters
Invoice & Mandate Fraud
Anti Virus Software
Gift Card Fraud
Courier Fraud
Privacy Settings
Over Sharing

Passwords *****|

Passwords 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.

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

2FA

Adding Two-Factor Authentication 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.

Money Muling

Criminals may contact you in person or via social media. They will ask you to receive money into your bank account and transfer it into another account, allowing you to keep some for yourself. If you let this happen, you're a money mule. If you're involved in money laundering, it is a crime.

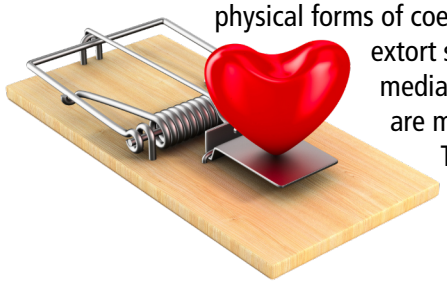
Romance Fraud

This 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 ask you for money or enough personal information to steal your identity.

Romance fraudsters are masters of manipulation and will go to great lengths to create a false reality in which an individual feels that they are making reasonable and rational decisions.

Sextortion

Sextortion is a form of sexual exploitation where non-physical forms of coercion are used to extort sexual favours. Social media and text messages are most commonly used. The contact often starts on a social networking site.



The victim is then encouraged to move to another platform that allows a video messaging facility.

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.

Cryptocurrency Scams

Bitcoin, Ethereum, Doge, XRP and thousands more crypto currencies may seem like a great way to make quick money, but be careful. 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.

Investment Scams

If it seems too good to be true it normally is.

Why isn't everyone else investing in this opportunity if it is so good?

Scammers will use impressive looking websites and offers of huge returns for small investments to lure you in. Always seek independent financial advice and check the advice on the Financial Conduct Authority website. (www.fca.org.uk)

Keep Devices 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.

Be aware

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

Webmail Rules & Filters

If a criminal gains access to your email account (by using a hacked or leaked password) they will often use the webmail facility to copy contacts and relevant data that they can then use.

They can send sound convincing emails due to the detailed and specific information they have from your account. This is another reason passwords should be strong and unique and why 2FA should be implemented as this will stop criminals being able to access your email account in the first place, even if your password is compromised.

Invoice & Mandate Fraud

Criminals use compromised email accounts to send genuine looking invoices. (For example; an email appearing to come from the Uni asking to pay fees or accommodation).

The recipient doesn't realise that the account number and sort code have been changed and often pays the money without realising they have sent it to a different account. It may not be until weeks later that they become aware as they are contacted by the person or company, they still owe money to.

By this time, the money is long gone and unable to be traced or reclaimed. 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 – back of bank card etc.)

Anti-Virus Software

Remember - Anti Virus Software is only good if it is kept up to date. Anti-Virus software will not protect you from your own actions – so always think before you click!