

**My name is Adrian Lewis and I am currently employed by South Wales Police as a Financial Abuse Safeguarding Officer**, within the Economic and Cyber Crime Unit. Prior to this role I was a serving officer with South Wales, retiring from the force in February 2019.

I started my role in April 2019 and am one of two FASO'S employed by South Wales Police, the other FASO being my colleague Susan John, who has been employed as a civilian for a number of years, working in various departments, predominantly within the Swansea area.

Our day to day role is to support vulnerable victims of Fraud within the SWP force area and hopefully ensure that they are not a victim of Financial Crime in the future. We also do Presentations/Talks in the community giving Crime Prevention advice and how to prevent being a victim of Fraud.

Below are some helpful hints and tips on how to stay safe and not be a victim of a Fraud. I have also included numerous links and websites that provide valuable information on how to stay safe online and tips to prevent being a victim of Fraud.

I have also included our contact details should anyone require any advice/assistance in the future.

#### **Fraud Prevention Advice:**

**Things to consider to prevent fraud:**

- **Beware of unsolicited calls, emails and texts-never give out your personal information or click on the links, if you receive a call, email or text you are not expecting, your starting point should be that it is a fraud.**
- **Use internet security software to protect your devices**
- **Use a PIN/password on mobile devices**
- **Regularly check bank and credit card statements/online accounts**
- **Keep important documents and bank cards safe and when disposing make sure that any account/card numbers are not identifiable and (on cards) chip is fully destroyed**
- **Use the privacy settings and security available to restrict access to your information to unknown persons on social media**
- **Review online passwords to ensure they are complex and difficult to crack by fraudsters. See links below get safe online have a link to check how secure your password is.**
- **Only use public Wi-Fi for browsing, if you need to share personal or financial information ensure you are connected to a secure network or using a VPN (Virtual Private Network).**
- **If it seems too good to be true, it usually is!!**

- Always check that a caller is who they say they are, even if they say they are from your bank or the police. Be aware that fraudsters can keep the phone line open and then trick you into giving your details or transferring money into a fake account. Call back on a number you obtain from a trusted website, or your bill or bank statement-but wait 5 minutes and if possible use a different phone. Genuine callers will understand and respect that you want to be careful.
- Do some research before buying online or investing, read independent reviews of speak to an independent financial adviser.
- If sharing personal or financial details online check the website you are using is secure, the URL should start with https.
- Verify and check any text messages received before replying or clicking on links to ensure they are genuine.
- Never share your card PIN or passwords with anyone who contacts you by phone email or text
- Never share your personal or security information on a website that you have clicked to from a link in an email or text.
- Be cautious when clicking on links or downloading attachments in emails or texts. If in doubt delete it.
- Treat all unsolicited calls with caution—remember, banks and police will never contact you to ask you to transfer money to a new account, buy high value goods or hand over cards or money.

#### Things to consider:

- Do you really know who you are sending your money to? Are they genuinely who they say they are? Check the legitimacy of the person, company or organisation before sending your money or sharing personal details. Check on the FCAs list of regulated firms
- Always be suspicious of people contacting you unexpectedly or to offer you products of services or stating that they are from official organisations eg. The bank or the police.
- Be aware who you are receiving calls and texts from, always confirm their identity. The bank, police, and any company you may use on a day to day basis will never contact you saying they need personal details such as your PIN, passwords or security details.
- Remember—deals that seem too good to be true usually are.
- If you are asked to pay for a product or service upfront, take time to consider if the payment is genuine and if this is normal practice.
- Take care and read the small print when making a payment, sharing your personal details or signing up to a 'free' trial. Make sure you read the terms and conditions so you

understand how your details will be used/shared and if you are signing up to any further or future financial commitments.

- If you are contacted and told that you have won a competition, prize or lottery, think about whether you have even entered, especially "ID" you are being asked to part with money or personal details upfront-this is usually a scam.
- Review all your online passwords and ensure you have a unique and complex password across all your accounts.
- Don't ever feel pressured into making a rushed or on the spot decision about purchases or a request to make payments that you are not 100% sure about
- If you are uncertain, speak to someone you can trust, a family member or friend, bank staff or do some research online.
- Before entering payment details on a website ensure the link/site is secure by looking for the unbroken padlock or key symbol in the address bar.

Tell your bank straight away:

- If you don't recognise or didn't authorise a transaction that has gone out of your bank account or onto your credit card.
- If your card or account security details have got into the wrong hands and/or you feel that somebody may have wrongfully gained access to your bank account
- If your mobile is lost or stolen and you are registered for mobile banking services.

**Report to Action Fraud (the national fraud reporting body):**

- If you have been a victim of a scam and a fraudster has tricked you into parting with your money.

Everyone who reports to Action Fraud will be issued with a crime reference number and is also given the option to receive support from Victim Support. This can be done via their website (see links below) or telephone, contact number is 0300 123 2040

**Report to the Police:**

- If the crime is in progress, or about to happen, including where money is at risk.
- If there is an additional crime to report, such as a burglary or theft of your handbag, purse or wallet, or threat of physical violence.
- If the victim of a crime is elderly or vulnerable, the Police may be able to offer additional support or refer to partner organisations such as Trading Standards or Adult Social Services.

### Report to Citizens Advice/Trading Standards:

- If you have a dispute or complaint about something you have bought in a shop, by mail order or via the internet
- If you have been a victim of doorstep crime or a rogue trader.

### Useful links:

<https://haveibeenpwned> – Allows you to search across multiple data breaches to see if your email address or phone number has been compromised.

<https://www.security.org> – Password strength checker

[www.met.police.uk/globalassets/downloads/fraud/the-little-book-of-big-scams.pdf](http://www.met.police.uk/globalassets/downloads/fraud/the-little-book-of-big-scams.pdf) a booklet released by Met Police with details of current scams and how to avoid them.

[www.fca.org.uk/scamsmart](http://www.fca.org.uk/scamsmart)

[www.fca.org.uk/consumers/protect-yourself-scams](http://www.fca.org.uk/consumers/protect-yourself-scams)

[Financial conduct authority provides information on how to avoid and report scams.](#)

[www.getsafeonline.org](http://www.getsafeonline.org) Provides factual and easy to understand information on online safety, protecting your identity and keeping passwords secure

[www.actionfraud.police.uk](http://www.actionfraud.police.uk) you can sign up for free direct, verified accurate information about scams and frauds in your area by email, recorded voice and text message through Action Fraud Alerts and also report any scam/fraud through the online reporting tool or via their contact number [0300 123 2040](tel:03001232040)

[www.moneyadviceservice.org/en/articles/beginners-guide-to-scams](http://www.moneyadviceservice.org/en/articles/beginners-guide-to-scams) A beginners guide to scams from the Money Advice Service

<https://www.citizensadvice.org.uk/consumer/scams/scams/common-scams/common-scams/> Citizens Advice provide information on the most common scams

<https://www.ageuk.org/information-advice/money-legal/scams-fraud/report-fraud-to-action-fraud/> Guides to help spot fraud and scams from Age UK

### Citizens Advice Bureau (CAB) -

in partnership with Trading Standards.

Free, confidential and independent advice is provided to help people understand and overcome their problems. Issues range from money concerns, to housing and consumer rights.

Phone: 03444 111 444

[www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)

### **Royal Mail Scam Mail**

If you, or a family member, believe you are receiving scam mail, report it to the Royal Mail.

Phone: 0800 0113 466

Write to: Royal Mail, Freepost Scam Mail

**[Email: scam.mail@royalmail.com](mailto:scam.mail@royalmail.com)**

### **Telephone Preference Service (TPS)**

Individuals can register in order to opt out of receiving unwanted legitimate sales and marketing phone calls. Note: scammers do not 'work' in an environment which can be regulated.

Phone: 0345 070 0707

**[www.tpsonline.org.uk](http://www.tpsonline.org.uk)**

### **Stay Safe Online**

This organisation empowers home computer users with the information they need to keep themselves, their computer systems and their sensitive information safe and secure online.

**[www.staysafeonline.org](http://www.staysafeonline.org)**

### **Financial Conduct Authority**

Its aim is to make sure customers get a fair deal. It regulates the conduct of over 56,000 businesses. Their activities include making sure customers receive appropriate goods and services, and that the company puts the customer before its own profits and remuneration.

**[Phone: 0800 111 6768/www.fca.org.uk](http://www.fca.org.uk)**

### **Victim Support**

This organisation is an independent charity in England and Wales, providing specialist practical and emotional support to victims and witnesses of crime.

[Freephone: 080816 89 111](tel:08081689111)

[Takefive-stopfraud.org.uk](https://takefive-stopfraud.org.uk)



[Susan.John2@south-wales.police.uk](mailto:Susan.John2@south-wales.police.uk)

[07970165813](tel:07970165813)

[Adrian.Lewis2@south-wales.police.uk](mailto:Adrian.Lewis2@south-wales.police.uk)

[07584004224](tel:07584004224)

[Office Number 01639 889125](tel:01639889125)