FRAUD AWARENESS

Raising your awareness is the first step in keeping yourself safe and secure from potential fraudsters

Websites

Scam websites are fraudulent sites designed to deceive users for various purposes, including financial gain, identity theft, or malware distribution. These sites often impersonate legitimate businesses, organisations, or government entities to gain users' trust and exploit their personal information or device vulnerabilities.

Social Media, Messaging Platforms and Apps

All of these can be used to facilitate fraud. The scammer often creates fake profiles, becomes friends with innocent people, and then sends spam messages or links that lead to malicious sites. Scammers can also learn a lot about you from details you share on your social media accounts. They create quizzes or posts designed to deceive you into sharing personal information, which they use to try and guess account passwords or target you with other scams

Advance Fee- This is when fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise.

Bogus Invoice/Debt – This is when fraudsters send an invoice or bill to a company requesting payment for goods or services that haven't been ordered or received. The invoice might say that the dye date for the payment has passed or threaten that non-payment will affect credit rating.

Counterfeit Cheques – This is when a cheque has been made or tampered with in a way that the bank will reject it. You're left out of pocket for whatever you gave away for the cheque.

Foreign Money Exchange - This is when scammers promise unrealistic returns on foreign currency schemes and trick people into investing in them. They use high-pressure tactics to convince investors to deposit large sums into a trading account..

Impersonation of Officials – This is when fraudsters impersonate officials to make false promises about tax rebates, or to demand fees, 'customs payments' or 'VAT payments'.

Phishing – This is where scammers deceive people into revealing sensitive information or installing malware such as ransomware.

Debt Management – This is when scammers prey on people who are in financial distress and struggling to make ends meet. The scammers promise to help consolidate your debt or negotiate lower payments, but instead end up stealing your money. They may even guarantee that they can get your debt reduced or eliminated.

Romance / Dating – This is when people are duped into sending money to criminals who go to great lengths to gain their trust and convince them that they are in a genuine relationship.

Technical Support - This is when a scammer claims to offer a legitimate technical support service. Victims contact scammers in a variety of ways, often through fake pop-ups resembling error messages or via fake 'help lines' advertised on websites owned by the scammers.

Energy Scam – This is when scammers may contact you pretending to be from a utility company, offering you better rates for your energy, suggesting that you switch to them, and then they ask for your bank details.

DO

- Use strong passwords, with a number of capital letters, numbers and special characters.
- Set up two-factor authentication.
- Secure your personal information.
- Stay informed on the latest cyber threats.
- Be careful with links and new website address.
- Check the senders email address before clicking on any links within an email.

DO NOT

- Respond to messages asking for personal or financial details.
- Click on links or attachments in suspicious emails or text messages.
- Open email from people you don't know.

Types of Contact Methods

- **BANK:** Watch out for calls supposedly from your bank about fraudulent use of your bank account or bank cards. Scammers might ask you for your PIN and tell you to give your bank card to a courier. Your bank will never do this.
- **COMPENSATION CALLS:** This is a call from a company asking about a car accident you've supposedly had, claiming you may be entitled to compensation. Don't engage in these calls. If you've had an accident, call your own insurance company on the phone number provided on your policy.
- **COMPUTER OR MOBILE REPAIR SCAMS:** The person may call and tell you that your device has a virus, and that you need to download software to fix it. This is actually spyware – an unwanted programme that runs on your device and can give scammers access to all your online information.
- **COUNCIL TAX:** Calls claiming to be about correcting your Council Tax band or giving you a calls claiming to be about correcting your Council Tax band or giving you a Council Tax rebate. Your council would never call you about a rebate out of the blue.
- **FAKE CALLER ID:** Scammers can mimic an official telephone number, which can trick you into thinking the caller is from a legitimate organisation, such as a bank or utility company.
- **HMRC:** You may get a call from someone claiming to be from HM Revenue & Customs (HMRC) saying there's an issue with your tax refund or an unpaid tax bill. They may leave a message and ask you to call back. HMRC would never contact you in this way and would never ask you to reveal personal financial information such as your bank account details.
- **SALES AND INVESTMENT CALLS:** These are unwanted or pushy sales calls, or investment opportunities that seem too good to be true.
- **TEXTS WITH FAKE LINKS:** You might receive a text asking you to follow a link to fix a problem with one of your accounts or to track a parcel. These links will often take you to a fake website and get you to log in, which scammers can then use to access your information.
- **UNDERCOVER POLICE SCAMS:** Calls from someone claiming to be 'undercover police', claiming that they're investigating a member of staff at your bank and asking for your card details. The police would never ask you to take part in this.
- **PENSION OR DEBT MANAGEMENT OFFERS:** Be wary of cold calls or texts from strange numbers offering products or services, such as pension or debt management.
- **TELEPHONE PREFERENCE SERVICE:** Watch out for calls asking you to pay to renew your membership of the Telephone Preference Service. The service is free and any calls asking you to pay for it are scams.

Email

Scammers will send bogus emails in the hope that people will enter their personal details. They may direct you to a fake website, trick you into thinking you've won the lottery or a prize, or pretend to be someone you may know who has been stranded somewhere and needs money.

Some emails may also have a link or file attached for you to click on or open. These are sometimes called spam or junk emails. Opening these links or downloading the files may be harmful to your computer.

If you see a suspicious email, don't reply with your details or open any links or documents. Delete the email straight away. If the email claims to be from an organisation, phone them directly using the phone number found on their official website and ask them.

What to do if you suspect you have been a victim of a scam

If you believe you've been the victim of a scam, fraud, or online crime (cybercrime) you can report it to Action Fraud:

- www.actionfraud.police.uk
- 0300 123 2040 (Monday to Friday 8am to 8pm)

If you have any concerns about fraud in the NHS or require any further advice, you can contact:

- **Your Anti-Crime Specialist: Sarah Pratley Email:** spratley@nhs.net **Phone: 07769 640781**
- **Alternatively, call** the 24-hour Fraud and Corruption reporting line on **0800 028 4060** or use the online reporting form: www.cfa.nhs.uk/reportfraud

tiaa

www.tiaa.co.uk | 0845 300 3333