Fraud and Scams Frequently Asked Questions

What is **Fraud**? What is **Cyber Crime**?

Fraud is when somebody lies, or deceives you, in order to cause harm, usually by stealing your money. Cyber Crime is when fraudsters target computers, tablets or phones or use the internet to swindle you. Increased use of electronic devices for everyday activities means that cyber criminals have a wealth of opportunity to commit crime.

What are **Phone and Text Message Scams**?

Fraud over the phone, or vishing, is when a fraudster calls claiming they're from your bank or another organisation that you trust, often under the pretence there has been fraud on your account. A text message might not be from who you think it is. Smishing is when fraudsters pretend a message is from someone you trust.

What is **Pension Fraud**?

Pension fraud is when a fraudster tries to con you out of your pension money. They will often start by contacting you unexpectedly about an investment or other business opportunity to persuade you to transfer your pension pot to them or release funds from it. It is often invested in unusual and high-risk investments like overseas property or renewable energy bonds or simply stolen outright.

What about **Bogus Tradesmen**?

Bogus tradesmen try to scam you after knocking at your door. Buying on your doorstep can be convenient, however, a salesman who uses clever tactics can pressure you into buying something you actually don't want or something that is poor value for money. Door-to-door fraud includes pressure selling, unfair contracts, overpriced or substandard home maintenance or improvements, phoney consumer surveys and bogus charity collections.

What can I do to stop fraudsters catching me out?

- Never give money, bank details or personal information to someone you do not know or trust
- Make sure you check a person's identity before handing over money or signing anything
- Don't be pressured into making a decision you are uncomfortable with; discuss it with someone you trust
- Be suspicious of phone calls, texts or emails which come out of the blue asking for personal or financial details or asking you to withdraw cash
- If a phone call raises your suspicions, hang up the phone and allow at least five minutes for the line to clear

For Cyber Crime:

- Use strong passwords and use different passwords for each account
- Install trusted security software and keep software and apps up to date
- Don't send sensitive information over public Wi-Fi
- Check the security settings of your Social Media accounts and make sure they are set to private. Once information is on the internet, it is there forever!

For door-to-door fraud:

- Always ask for identification before letting anyone you don't know into your house
- Check credentials, including a permanent business address and landline telephone number
- Don't sign on the spot, get more quotes to make sure you are not being ripped off
- If in any doubt, ask the person to leave or call the Citizens Advice consumer helpline on 03454 04 05 06.

Who can **Help**?

If you've been the victim of a scam, don't be embarrassed to report it. It can happen to anyone. Report it to your bank immediately and report it using the Action Fraud Online Reporting Tool or contact Action Fraud on 0300 123 2040. Fraud and cyber crime is reported to Action Fraud instead of the police as Action Fraud takes reports from victims nationwide providing a clear picture of the scale of fraud and cyber crime, allowing law enforcement to link crimes which happen across the country. This kind of intelligence is the key to disrupting cyber crime. When you have made a report to Action Fraud you will be given a National Fraud Reporting Centre number and you will receive an update within 28 working days.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

What should I do if I receive a suspicious email?

Fraudsters contact people by email usually saying that they need you to verify something. This is phishing, If you have received an email which you're not quite sure about, forward it to: report@phishing.gov.uk It might be from a company you don't normally receive messages from, or someone you do not know. If you are suspicious, you should report it. Your report will help the National Cyber Security Centre to act quickly, protecting many more people from being affected.

Website: www.oldhamsafeguarding.org
Email: OldhamSafeguardingAdultsBoard@Oldham.gov.uk