DCPCU
Dedicated Card and Payment Crime Unit

Financial Fraud Action UK
Working together to prevent fraud

Neighbourhood Watch SCOTLAND

DO YOU KNOW WHO'S CALLING YOU?

People are not always who they say they are...

CITY OF LONDON POLICE

EVERY YEAR,

people fall victim to fraud following a phone call. Fraudsters are posing as bank staff, police officers and other officials or companies in a position of trust. Often the fraudster will claim there has been a fraud on your account and that you need to take action. This type of fraud is called Vishing and it's becoming more sophisticated and widespread.

Vishing – how it works

You'll get a call, claiming to be from your bank, the police or other officials or companies, informing you that a fraudulent payment has been spotted on your account and this needs to be resolved, or that someone has been arrested for using your card. The caller may even claim to be from a service provider, informing you that you're due a rebate, or you've overpaid on your account and they'd like to refund you.

You may be asked to call back using the phone number on the back of your card – this further convinces you that the caller is genuine. However, the fraudster keeps the line open at their end therefore when you make the call, you are unknowingly connected straight back to them or their accomplices.

They may ask for your 4-digit PIN or ask you to key it into your phone's handset. Once the fraudster has your PIN, bank details and/or online banking passwords, they have access to your money.

Hang up, wait 5 minutes to clear the line, or where possible use a different phone line, then call back on an advertised number. If you don't have another telephone to use, call someone you know first to make sure the telephone line is free.

Variations of this type of fraud include:

- asking the victim to assist in a police investigation against corrupt bank staff giving away counterfeit currency. The victim is requested to withdraw a large sum of cash and take it home, where it is then collected by a courier
- being told that your computer has a virus and that you can pay to have it removed. The fraudster may also take control of your computer and add software to obtain your data

Investment Fraud – what you need to know

Generally speaking, cold calling for investment business is prohibited by law.

Investment fraud can take many forms, with fraudsters commonly using wine investments, share sales, land banking, rare earth minerals and carbon credits to target potential investors. Recently, criminals have tried to scam their victims using "pension release" frauds where a lifetime's savings can be lost in a moment.

Anyone can become a victim of this type of crime, which often starts with a call from someone claiming to be a financial services professional and offering an investment opportunity which sounds too good to be true. Thousands of people have been left devastated by this type of crime – don't let this happen to you, see our advice and information overleaf on steps you can take to protect yourself from this type of fraud.

Telephone scams – what you need to do

The police are actively targeting fraudsters and organised criminal gangs but you need to be mindful of unsolicited calls and emails. Follow our advice to help protect you from this type of crime.

Protecting your card and personal details is vital.

- Be wary of all unsolicited calls and emails
- Never reveal personal or financial information, including your PIN or bank card details to anyone
- Don't be pressured into making important financial decisions, if an offer sounds too good to be true it probably is
- In order to clear your line from the fraudster, wait at least five minutes before making any calls
- Your bank will never ask you to check the number showing on your telephone display matches their registered telephone number. This display cannot be trusted, as the number showing can be altered by the caller
- Remember – the police and banks will never ring you and ask you to verify your PIN or online banking passwords, withdraw cash, transfer money to another "safe" account or purchase high value goods
- If you believe you have had one of these calls or know someone who has, get in contact with your bank straight away or, if you feel in immediate danger, call 999

BE FIRM, SAY NO AND HANG UP ON FRAUD.

If you've been a victim

It is distressing to learn or think that you have been a victim of this type of crime. If this has happened to you, then please report it to Action Fraud in the first instance. Action Fraud is the UK's national reporting centre for fraud and internet crime where you should report fraud if you have been scammed, defrauded or experienced cyber crime.

You can call Action Fraud on **0300 123 2040** or report via their website reporting template at **www.actionfraud.police.uk**

Further information and advice about this type of fraud and others can be found at:

www.cityoflondon.police.uk

www.actionfraud.police.uk

www.financialfraudaction.org.uk

www.ourwatch.org.uk

www.neighbourhoodwatchscotland.co.uk