citizens advice North Hertfordshire

HOW TO PROTECT YOUR MONEY

PRACTICAL ADVICE ON HOW TO AVOID BEING THE VICTIM OF A SCAM

You receive a phone call telling you the caller is from your bank - "there's been some unusual activity on your account" this is the start of a common scam. They may tell you to check the caller display (if you have one) so that you can see that it matches the number on the reverse of your bank card and many fraudsters have the technology to be able to do this. This is all done to instill a sense of urgency and panic, they may well say to call them back on the number to show they are genuine. Always say that you will do this, however do not ring your bank number straight away, fraudsters can hold the line open and pretend that you are dialing your bank, call someone you know, a friend or family member, if the person you know answers then it is likely that the original call was from your bank however, if someone answers saying they are from your bank when you know you haven't dialed that number – IT IS A SCAM!

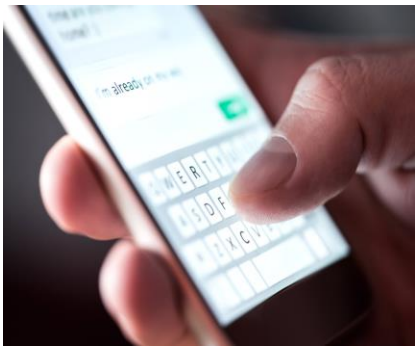
Remember:

- Your bank will **NEVER** ask you to withdraw money or move money. to another 'safe' account
- Your bank or the police will **NEVER** ask you to buy valuables, gift vouchers
- Your bank will **NEVER** ask you for your bank card PIN number
- Your bank or the police will **NEVER** come and collect your cards in person or ask you to deliver them somewhere 'safe'

COMPUTER SCAMS – THE FIXER

You receive a call from an internet provider such as BT, SKY etc. telling you that they have detected a problem with your computer which they are happy to fix for you. They will tell you they need to gain remote access to your computer or assist you in installing an anti-virus program to render your computer safe again. This is a common scam and a real provider on internet services would never call you to fix a problem, they wait for you to contact them to tell them you have a problem, not the other way around. This is the perfect way for a scammer to access your personal data for ID fraud, bank scams and passwords.

URGENT TEXT - THE FAMILY MEMBER:



You receive an urgent text from a loved one" *Hi Mum (Dad) I've lost my phone, this is my friend's number. Can you send me some money urgently I've got no means to pay for anything*". Stop and think, ask yourself a few simple questions: Why are they texting me? Why don't they phone me knowing I might be anxious? THIS IS A VERY COMMON SCAM. The text will ask for money to be sent to an account that might not be familiar, STOP, call either the number of the phone that's texting you and ask to speak to the person you know, or alternatively call them on the phone number you know to be theirs.

IDENTITY THEFT:

You receive an email from a well-known business such as BT, Amazon, a major delivery company, or perhaps TV licensing telling you your direct debit did not go through, they will ask you for information to confirm details, there is usually a link to click on or an attachment. Always check the email address of the sender, it may well be something very different from the name of the company they are pretending to be. Once you click on the link, they will ask for all sorts of information which may include bank details, NI number, name, address, date of birth etc. This information could be used to take out loans in your name, purchase goods and apply for benefits in your name. It may also be used and sold on to other scammers. Consider joining an organisation that will monitor your personal details such as Experian, or sometimes your bank may offer a similar type of service. You will then be informed if something unusual appears in your data eg. An application for a loan.

USEFUL INFORMATION

- **You receive a suspicious text – forward it to**:

  7726 – this spells SPAM on your keyboard. Telephone providers can investigate and block/ban the sender

- **You receive a suspicious email – forward it to:**

  report@phishing.gov.uk This will help to reduce the amount of scam communications you receive, making you a harder target for scammers

USEFUL WEBSITES

- **https://www.citizensadvice.org.uk/consumer/scams/get-helo-with-online-scams**

- **https://www.takefive-stopfraud.org.uk**

- **https://www.actionfraud.police.uk**