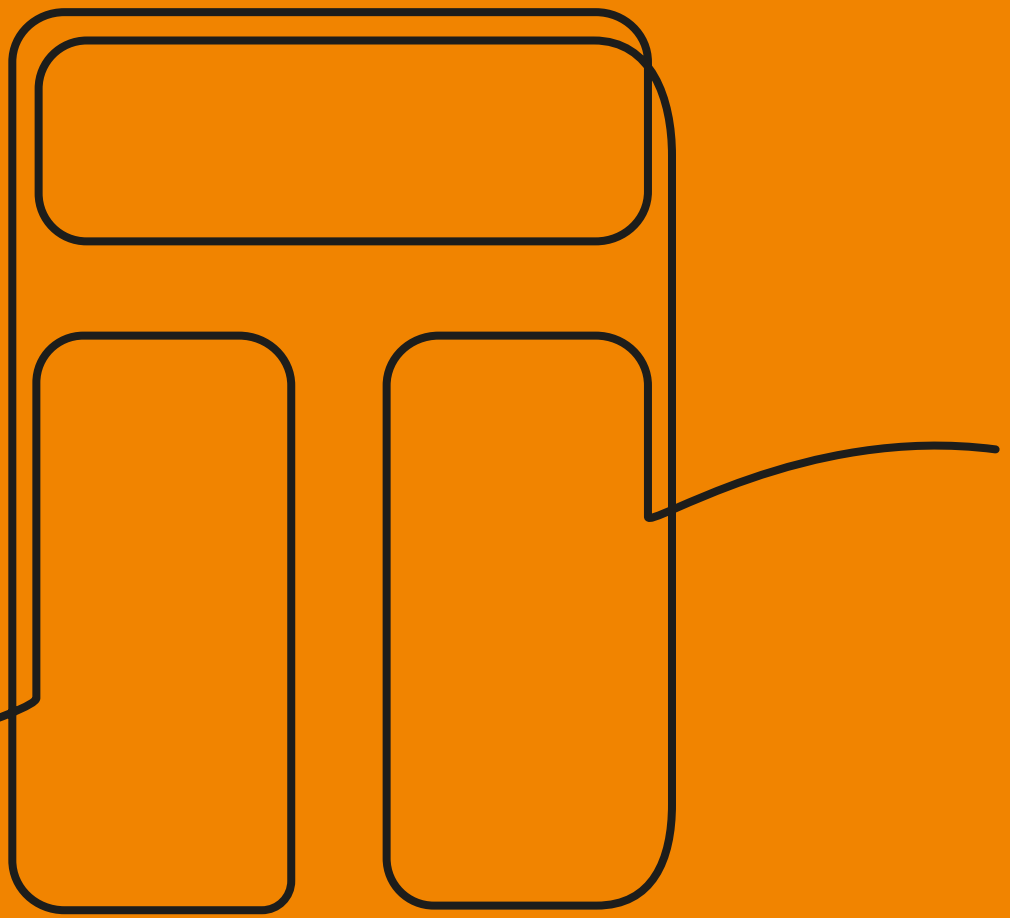
BE FRAUD AWARE



Teachers Building Society

BE FRAUD AWARE – STOP! THINK! ACT!

I THINK I MAY BE A VICTIM OF FRAUD OR A SCAM, WHAT DO I DO?

Please contact us as soon as possible if you spot suspicious activity on your account. You can contact us on telephone 0800 783 2367, or email us on memberservices@teachersbs.co.uk. Once you've contacted us, we recommend you report this to your local police station and get a crime reference number. You should also contact your local police station if your bank or building society debit card, credit card or cheque book has been stolen.

WHAT IS FRAUD?

Fraudsters will try every trick in the book to try and deceive you and take your well earned money. We've provided a list of the most common fraud and scams. If you think you have been a victim of this, contact Action Fraud on 0300 123 2040 or online at actionfraud.police.uk

FRAUD IS GETTING DIGITALISED

The digital age brings so many advantages, but it also brings challenges with it too. On average we spend more than 6 hours of our day online, so fraudsters will always be looking at ways of exploiting the time we spend online and work out new ways of conning us out of our money.

WHAT IS THE DIFFERENCE BETWEEN A SCAM AND FRAUD?

Fraud is a transaction on your account which you didn't authorise and didn't make yourself. A scam is where you make or authorise a payment from your account to somebody you believe is genuine, and later find out they weren't!

TYPES OF FRAUD AND SCAMS

CORONAVIRUS SCAMS

TEXT SCAMS:

A text purporting to be from the Government informs you that you have been issued a fine for leaving the house during the lockdown. You are told that if you don't pay immediately you will incur a heavier fine. You are encouraged to click on a link to make the payment which may deliver malware as well as taking the payment and your account details.

PHISHING SCAMS:

Cyber criminals are exploiting the Coronavirus by distributing emails posing as legitimate organisations such as the World Health Organization (WHO). You could receive an email purporting to be from the WHO with an attachment supposedly containing important information regarding the Coronavirus. This could lead to you opening the attachment causing various types of malware to infect your system, or prompt you to enter your email login and password to access the information. The criminals then have access to your email account.

SOCIAL ENGINEERING SCAMS:

Criminals use legitimate social media websites to seek donations from you for charitable causes related to the virus. Criminals will exploit your charitable spirit and seek donations to fraudulent causes surrounding the Coronavirus. You should exercise increased caution when donating to causes tied to Coronavirus relief.

NON-DELIVERY SCAMS:

Criminals are advertising in-demand medical supplies for sale to be used to protect against the Coronavirus, i.e. medical masks, hand gel, gloves etc. The criminal enterprise will demand upfront payments and then take your money and never deliver the items you have ordered. Increased caution and vigilance while purchasing these supplies should be exercised.

COURIER SCAMS:

Criminals may contact you offering to do your shopping whilst you're in isolation. They may trick you into handing over your bank or building society card and PIN. Never give your bank or building society bank card or PIN to a complete stranger. Your Local Authority may be able to support you or signpost you to reputable groups who can help you with your shopping if you are in isolation.

SAFE ACCOUNT SCAMS:

Criminals may call and claim that your money is at risk due to the possible collapse of the economy. They convince you to move your money to a 'safe account'. When you do, you realise you can't access it, and your money is gone. Genuine organisations will never ask you to move your money to a safe account.

ONLINE FRAUD

VISHING:

Vishing is when a fraudster gets in touch by phone, pretending to be from a company you have dealings with and trust. They may also send you a text, which asks you to call a number. They'll ask you to log in, move money or even want you to give them remote access to your computer or device.

If you're suspicious of the caller, end the call. Then find the number of the organisation from a trusted source (not a search engine) and call them from a different phone.

Don't be fooled by a caller who has your personal information.

PHISHING:

Phishing is when a fraudster gets in touch with you by email, text or social media messages. They'll try to trick you into giving away your personal or banking details.
They may write to you, posing as someone you know, or as a reputable organisation. They can seem very convincing. Sometimes they use logos, email addresses or contact names and details that are almost identical to those of a real organisation. They'll claim there's an urgent problem and ask you to login to your online account, update your details using a link they give you, and may ask you to transfer money as they may lead you to believe your money is at risk.

Phishing emails may not be addressed to you personally and the use of language or punctuation may be quite poor.

Avoid opening emails if you don't recognise the sender. Never click on links to log in or unlock your account.

ACCESSING YOUR DEVICE BY MALICIOUS SOFTWARE (AKA MALWARE):

Your mobile, tablet or computer contains a lot of your personal details. If a fraudster gains access to your device, it will be quite easy for them to obtain your personal information.

Malware is hostile software that buries itself in your device. It may spy on what you are doing online, including financial transactions. It could even prevent your apps or device from working unless a ransom payment is made.

The software can be installed by the fraudsters encouraging you to open links or attachments in emails, texts and social media messages. You might not even be aware that it has been installed.

Avoid being the victim of malware by regularly running a full check for malware once a week using your anti-virus software. Always use a firewall and reputable anti-virus software and run regular updates. Make sure that websites you visit are secure before you log in. Look for a padlock or key symbol and https in the address bar.

IDENTITY FRAUD

dentity theft can lead to fraud that can have a direct impact on your personal finances and make it difficult to obtain various forms of credit until the matter is resolved. Fraudsters can use your identity to obtain credit or open a bank account, order items in your name, take over your existing accounts and even obtain genuine documents like passports and driving licences.

To avoid identity fraud, keep important documents in a safe place and when disposing of them make sure you shred anything containing personal information. Never give out personal details like account numbers, PIN, passwords or one time passcodes to anybody. You can also regularly get a copy of your credit report from the various credit reference agencies. When your monthly statements arrive, ensure you review them to spot any unusual transactions.

COMMON SCAMS

ONLINE PURCHASE SCAMS:

You spot something for sale online, for example a car, concert tickets or tickets to a sporting event. The price seems to be too good to be true. The seller asks you to pay by a less secure method than the one the selling site recommends. You go ahead and transfer the money, to ensure you don't miss out on this bargain. However after transferring the money, you never hear from the seller again and the item you purchased never arrives.

Always ensure you use a reputable website or app to purchase goods online.

HACKED EMAIL ACCOUNT:

Fraudsters may send you an email that appears to look like it was sent from a trusted person or company. They tell you that you need to make payment and the companies bank information has changed. You may well owe that person or company money, so you think nothing of it and go ahead and transfer the funds.

This may be because the company or person's email account has been hacked. If you receive a request to make a payment, always get in touch with the requestor using the original contact information you received. Make sure the request is genuine before you make the payment.

Be careful - fake invoices sent by email can be very convincing!

ROGUE TRADERS:

A tradesperson knocks on your door, and informs you that you need urgent work doing to your home, for example a loose roof tile. The tradesperson goes ahead and does the work for you and overcharges you for work that wasn't needed. They may even ask you to make a part payment for materials and never return.

Don't rush into getting work done by a person knocking on your door. Get quotes from reputable tradesmen before committing to having the work done.

ROMANCE SCAMS:

You meet someone new online and they seem genuine. But can you be sure? They may be abroad and ask you for financial help to cover travel expenses to come and visit you. You trust them and you've developed strong feelings for them. You decide to transfer money to them to help them, but you never hear from them again.

Keep to conversation on a reputable dating agency site or app and never send money to a person you have only met online.

SAFE ACCOUNT SCAMS:

You receive a call from a trusted organisation such as your bank or building society, or even the police. They inform you that your money is as risk and that you need to move your money to a safe account that has been set up for you. You transfer the money in good faith, but your money is now gone and you later find out that your bank or building society never contacted you.

Never act on a phone call or contact out of the blue telling you to transfer funds. A genuine organisation will never ask you to do this.

ADVANCE FEE SCAMS:

A fraudster may contact you informing you that you need to make an upfront payment to them. They might tell you that you have won the lottery and have to pay a fee up front to release the funds. Or it may be about a loan you have enquired about, and they tell you to pay a fee up front before the funds will be sent to you. You make the payment but never receive the funds that were promised and never hear from them again.
If something seems too good to be true – it probably is! Never transfer funds without checking to ensure the request is genuine.

INVESTMENT SCAMS:

A fraudster contacts you informing you that they have investments available to you that will make you money. They ask you to transfer funds to invest in something like alternative energy or precious minerals. However the investment does not exist and after you transfer the money, you never get any returns and your money is lost forever.

The Financial Conduct Authority (FCA) have a website called ScamSmart which offers a warning list, to you can check the risks relating to potential investments. You can also see if the company that has contacted you is authorised by the FCA.

REMOTE ACCESS SCAMS:

A fraudster purporting to be from an internet provider contacts you and tells you there is a problem with your computer or device. They tell you they can access your device remotely to resolve the problem. You grant them access when the 'pop up' requesting access appears on your screen. They tell you that they have resolved the issue, and ask you to make payment to them by asking you to your online bank account. You make the transfer and they now also have your login credentials.

Don't allow yourself to be rushed into allowing remote access. Ensure you know who you are dealing with and if they can be trusted. Never log into your online bank account while someone is remotely accessing your device.

PENSION SCAMS:

You could be at risk from pension fraud even if you're not a pensioner. Unfortunately, following government reforms introduced in April 2015, pension scams have become increasingly common.

It's not just retirees who are affected, because defined contribution pension holders can now access their entire retirement fund from age 55. People are being encouraged to withdraw from their pensions and put money into schemes that offer large returns for a short-term investment. The 'investment' is actually deposited into a fraudulent account.

If you're under 55, you might be approached by someone promoting the benefits of early pension release schemes, and encouraged to access your pension early. The funds would actually be transferred into overseas schemes (with extortionate fees) or placed into high risk investments. And once money is transferred into an early release scheme, the scammers could take all of your pension pot.

Early pension release schemes are not authorised by HMRC and funds withdrawn will be charged anything from 55% to 70% in tax. The government only allows early access to pension funds in very limited circumstances. If you're considering entering a scheme to access your pension before 55, the Financial Conduct Authority (FCA) recommends seeking professional advice.

Firms, individuals and other bodies regulated by the FCA are unlikely to contact you unexpectedly or pressure you into making a decision. If they do, you should report them to the FCA straight away. If you've been approached by someone, you can check if they're regulated by searching the Financial Services Register online – there's no charge.

If you're approached about your pension, warning signs may include, being contacted out of the blue with cold calls, texts, emails or by door-to-door salespeople. Feeling pressured into making a quick decision by pushy sales techniques or being told you're being offered the best deals, like guaranteed returns.

CHEQUE FRAUD:

This is when someone gives you a cheque they know you can't cash. There are several variations of this scam, for example:

- Handing over counterfeit cheques, which are made to look real by the fraudster, or forged cheques, which are genuine but stolen from somebody else with the signature forged
- Altering or tampering with a cheque. It might not be noticeable or visible to the naked eye, but will be rejected by the bank
- Making an overpayment and then asking for the change. A fraudster will pay you using a fake cheque for more than the agreed value, with an excuse for the overpayment. They'll ask you to send back the difference, in cash or an untraceable money transfer. The cheque will bounce and you'll never hear from the fraudster again.

Keep yourself safe by:

- Only accepting cheques from people you know and trust
- Asking for a different means of payment if it involves a lot of money
- Use a pen when writing a cheque. Write clearly and put a line through empty spaces.

FURTHER HELP AND ADVICE

www.ActionFraud.Police.uk

www.Cifas.org.uk

www.CrimeStoppers-uk.org

www.Fca.org.uk

Teachers Building Society