HOW TO PROTECT YOURSELF FROM FRAUD

BROWN SHIPLEY

A QUINTET PRIVATE BANK

IT’S BETTER TO BE SAFE THAN SORRY

HOW TO PROTECT YOURSELF FROM FRAUD

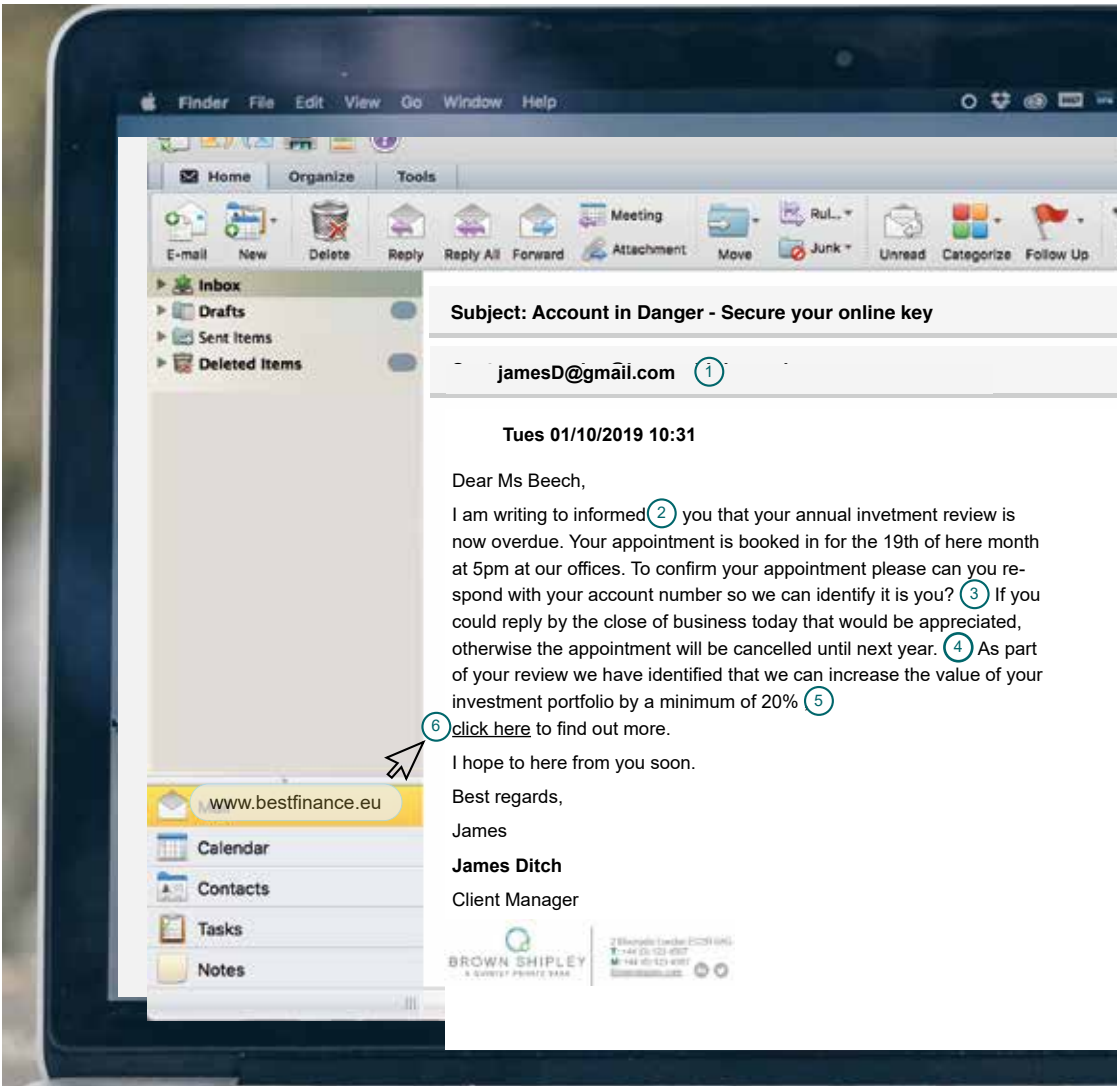
At Brown Shipley we take the safety of your money seriously. No matter how much you have, you should have the peace of mind that your money is safe and protected from fraud. Unfortunately, we live in a time where financial fraud is on the rise and fraudster tactics and techniques are becoming more and more convincing. So, to help you keep your wits about you, we’ve created the following guide to help you spot potential dangers, as well as the measures you can take to keep yourself protected from fraud.

EMAIL FRAUD

'Phishing', otherwise known as email fraud, is a popular tactic used by fraudsters to gain information, so be mindful about the emails that you receive. Although an email may look like it's from Brown Shipley, your bank or other well-known organisations, it may be a fraudster.

WHAT SHOULD I LOOK OUT FOR?

1. The email address is different from the organisation.
   If the email address is different from the organisation they say they are, this is a typical sign that the email is fraudulent. No respected business will send an email out from a personal email address such as @gmail.com or @hotmail.com.
2. The message contains poor spelling and grammar.
   Often fraudulent emails will contain spelling mistakes and poor grammar. If an email contains these types of errors it may be from a fraudster. Companies will always want to be professional, and check their emails over to ensure what they send you is correct.
3. The message asks for personal information.
   No company will ask you to provide personal information, account numbers or passwords via an email. If an email requests this type of information, it's most likely from a fraudster.
4. The email has a sense of urgency or a threat if you do not provide information in a given time period.
   The email may request that you provide sensitive information within a given time period or your account may be closed. Threats and tight time frames are often used to pressure you to act quickly. Instead, you should check that the information is legitimate and contact your provider directly to confirm the information.
5. The offer appears to be too good to be true.
   If the offer seems too good to be true, then it probably is, especially if this comes via an email. Trust your gut and treat these emails suspiciously, it's usually in your best interest to avoid acting on the message.
6. The email message contains mismatched website links.
   If the email contains any links to websites, make sure they are what they seem. It may be taking you somewhere different to where it says. Simply hover over the link. If the web address is different to the company claiming to contact you, it's not to be trusted.



HOW TO PROTECT YOURSELF

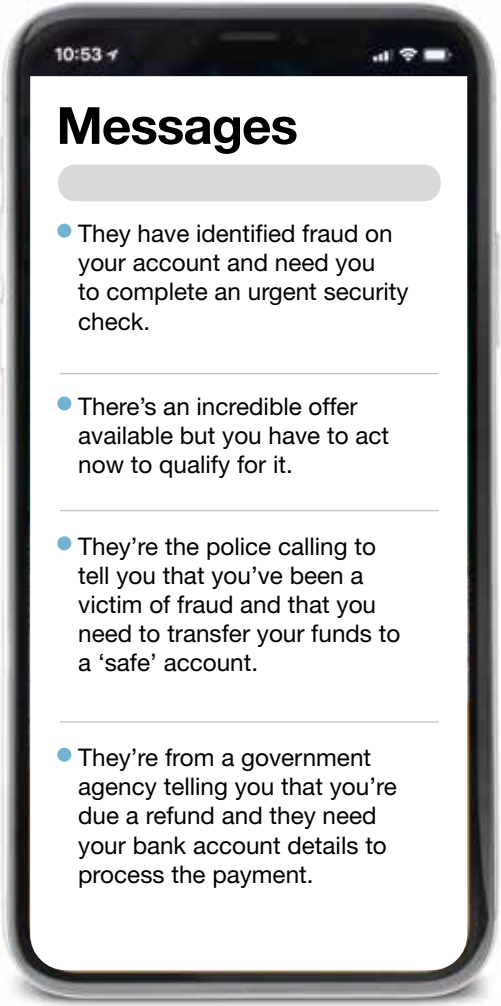
- Do not open, forward or respond to emails if you don't recognise the sender or you suspect it could be a scam
- Do not open up any attachments in emails sent to you from unknown sources. Contact the company first to check the email is legitimate
- Do not click on any links if you think the email is suspicious. Hover over the link to check the URL destination matches with the company who is sending it
- You can set filters to allow emails from a trusted source and likewise you can block any emails that may look suspicious.
- The National Cyber Security Centre have set up a Suspicious Email Reporting Service. To report a suspicious email, simply forward it to **report@phishing.gov.uk.**

TELEPHONE FRAUD

In addition to email fraud, people may also call you pretending to be from your bank or a legitimate organisation, or text you asking you to call a number. This is called 'vishing'.

WHAT SHOULD I LOOK OUT FOR?

A fraudster may tell you that...



HOW TO PROTECT YOURSELF

When dealing with any telephone calls or text messages from an unknown sender, just remember to stop and think first before sharing any personal information. Brown Shipley and other reputable organisations will never ask you to share your account details or any PIN codes. We will also never ask you to move your money to a ‘safe’ account. If in doubt, follow the below tips:

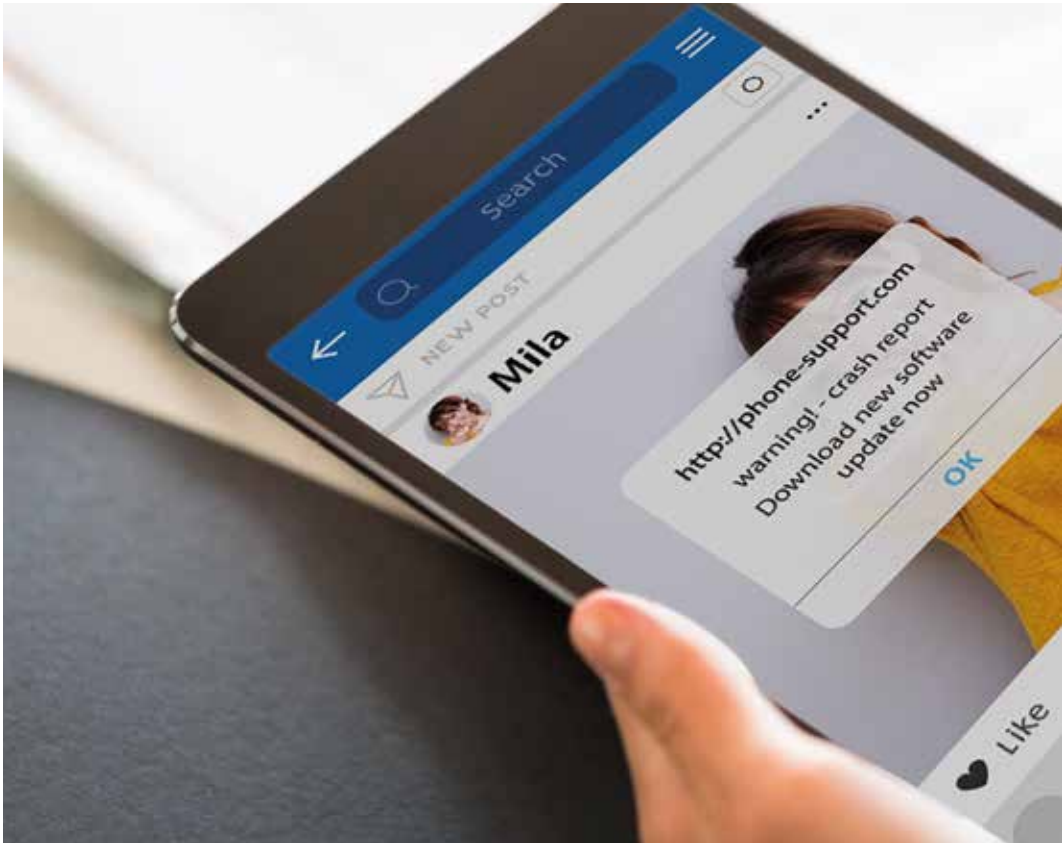
- **Stay alert when dealing with unsolicited calls** - remember they’ve called you without your request
- **Don’t reveal your personal details** - never give out your personal account information or PIN
- **Hang up** - if you’re not sure that a caller is genuine, end the call and call them back using the telephone numbers you know are correct for that organisation. Never use the call back facility on your phone. This way you can check that the call is legitimate for that organisation
- **Don’t feel rushed** - fraudsters often try and create a sense of urgency to try and get your personal details. Take your time and don’t let them rush you into giving information that you are not prepared to provide.

KEEPING YOUR DIGITAL DEVICES SAFE

Your devices contain lots of personal details. If fraudsters manage to hack your phone or laptop, they could get hold of your confidential information. Malware (malicious software) is any program or file that is harmful to your device. Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely.

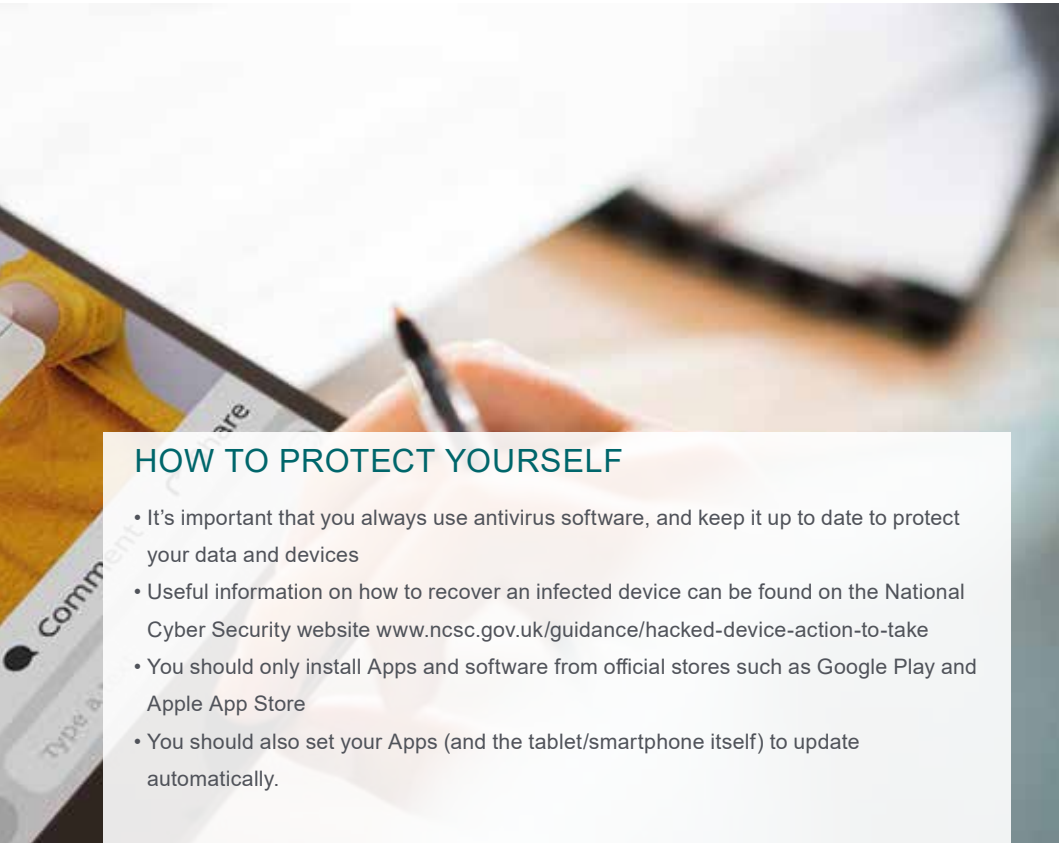
FRAUDSTERS MAY TRICK YOU INTO INSTALLING MALWARE ON YOUR COMPUTER, TABLET OR MOBILE BY:

- Encouraging you to open links or attachments in emails, texts or social media messages
- Creating a fake App that mimics a genuine banking or service App.



WHAT SHOULD I LOOK OUT FOR?

You may not realise that malware has been installed. You may be able to detect it if you notice unusual activity such as a sudden loss of disc space, unusually slow speeds, repeated crashes or freezes or an increase in unwanted internet activity and pop up advertisements. For this reason it's important that you always use antivirus software, and keep it up to date to protect your data and devices. An antivirus tool can also be installed on your device that detects and removes malware.



HOW TO PROTECT YOURSELF

- It's important that you always use antivirus software, and keep it up to date to protect your data and devices
- Useful information on how to recover an infected device can be found on the National Cyber Security website www.ncsc.gov.uk/guidance/hacked-device-action-to-take
- You should only install Apps and software from official stores such as Google Play and Apple App Store
- You should also set your Apps (and the tablet/smartphone itself) to update automatically.

INVESTMENT FRAUD

Investment fraud continues to be on the rise with the Financial Conduct Authority (FCA) warning investors to be extra vigilant to the ongoing threats of investment scams.

The FCA has shared data from Action Fraud showing that in 2018 there were over £197 million* of reported losses to fraud, with victims being scammed out of over £29,000 on average. In addition, the most commonly reported scams involve investments in shares, bonds, forex and cryptocurrencies by unscrupulous firms that are not FCA registered.
Fraudsters are increasingly using sophisticated tactics to persuade victims to invest, presenting a 'once in a lifetime opportunity' that's risk free. A seasoned investor like yourself should always be alert to these types of messages and remain particularly vigilant during the first quarter of the year, the peak investment season, as many look to invest before the end of the tax year.

WHAT SHOULD I LOOK OUT FOR?

When making investment decisions you should always be vigilant, although fraudsters will deploy a number of methods to trick investors, their tactics usually remain consistent. The below information provides you with the signs to look out for to help you identify the different types of investment scams:

- **Unsolicited calls or emails** – fraudsters will be extremely experienced and will remain very calm, often making repeat phone calls in the hope of wearing you down
- T**oo good to be true** – if an opportunity seems too good to be true, that's often the case. Fraudsters will also claim investment opportunities are 100% risk free and use technical and legal jargon to try and 'blind you with science'
- **Time pressured decisions** – fraudsters will often try to put you on the spot to get you to act immediately, and not give you the time to consider your actions or ask for other expert advice
- **False information** – don't think reviews from other clients prove anything, since they're easy to fake.

* Action Fraud data: Total amount lost during 2018 £197,465,740.12 from 6,759 reports.

HOW TO PROTECT YOURSELF

- Know your Financial Adviser / Investment Manager – this might sound obvious but you should always consult your usual Financial Adviser or Investment Manager where investment opportunities are concerned
- Don't be pressured into making a quick decision – make sure you take the time you need, ask plenty of questions and always do your homework
- If you are considering investing in a company take a look at their financial information
- Be vigilant, especially from unsolicited calls – never be afraid to say no. You can always then take the time to seek advice before moving forward
- Ask if they are authorised by the FCA – all financial organisations should be authorised and regulated by the Financial Conduct Authority (FCA) and be on their register. We suggest you check the company's website to confirm the individual works for the company.

PENSION FRAUD

When you've worked hard all your life, you deserve to enjoy you retirement. Pension scams are another area that fraudsters are focusing on. Although they can be difficult to spot, again, there are always tell-tale signs to look out for.

WHAT SHOULD I LOOK OUT FOR?

Like with other types of fraud, fraudsters can contact you out of the blue by phone, email or text. The below points help you to spot the signs and false claims that fraudsters could use:

- They could claim that they are authorised by the FCA or acting on behalf of the FCA or the government service Pension Wise
- They could offer a free pensions review
- They could claim that they can provide higher returns on your pension's savings
- They may say that they can help you release cash from your pension even though you are under 55
- They may also use high pressured sales tactics such as 'time-limited offers'
- The pension schemes offered may provide a longer-term investment period that means it could be several years before you realise something is wrong.

HOW TO PROTECT YOURSELF

To help protect yourself from pension fraud the FCA promote four simple rules:

- Reject unexpected offers – if you are contacted out of the blue about your pension, chances are it may be a fraudster. The safest thing to do is hang-up on any calls or ignore emails or texts
- Check who you are dealing with – The firm should be on the Financial Services Register and you can check the firms website to to check the individual works for them.
- Don't be rushed or pressured – take the time you need to undertake any checks and don't be pushed into making a decision quickly due to a time-limited offer
- Get impartial information or advice – you should seriously consider seeking financial guidance or advice before making changes to your pension. A Brown Shipley Advisor can support you with this or you can seek free independent and impartial advice from The Pensions Advisory Service.

INVOICE FRAUD

Whether you are an individual receiving invoices for work carried out within your property, or a business owner with multiple suppliers, invoice fraud is becoming increasingly common.

WHAT SHOULD I LOOK OUT FOR?

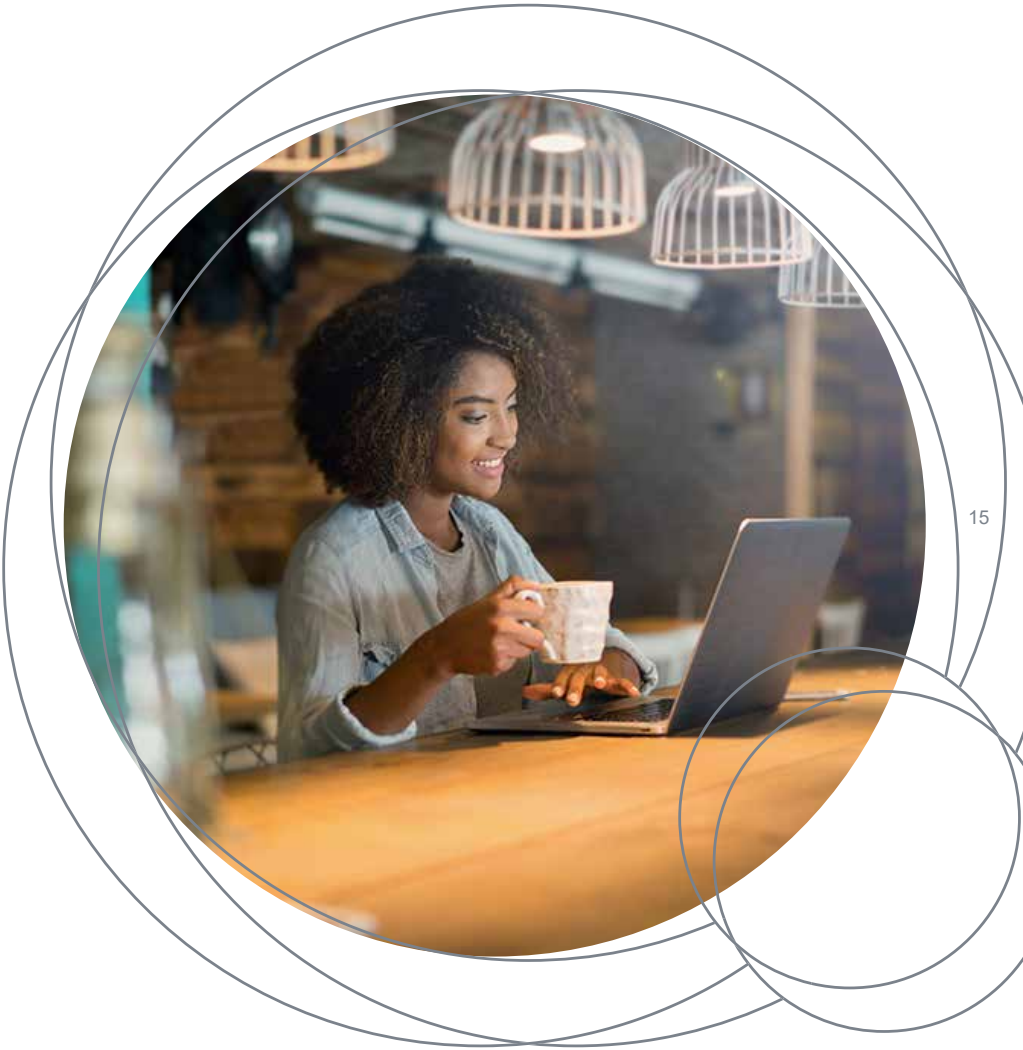
Invoice fraud occurs when an individual or a company is tricked into changing bank account payee details for a known payment. Fraudsters pose as regular suppliers and can either directly amend or make a formal request for bank account payee details to be changed. This can then result in a genuine payment instruction being sent to your bank.

Criminals who specialise in invoice fraud are often fully aware of the details and relationship between an individual or company and their suppliers, including when regular payments are due. Equipped with this information, they make contact with the individual or Finance team posing convincingly as a supplier. Payments are repeatedly made to them and the fraud is often only detected when the legitimate supplier chases for non-payment of an invoice. At this point it is extremely difficult to recover funds from the fraudulent account.

Individuals and companies are all vulnerable to invoice fraud and vigilance is the key to its prevention.

HOW TO PROTECT YOURSELF

- Always confirm the amount and beneficiary (account & sort code) of the payment directly and be satisfied the instructions are genuine and as expected by the recipient;
- Be vigilant when receiving invoices. Always check for irregularities including changes to supplier names and addresses and changes to invoiced amounts.
- Compare it to previous invoices received that you know are genuine – pay particular attention to the bank account details, wording used and the company logo.
- Changes to a supplier's financial details should always be verified with that supplier using their established on-file information. If you are suspicious about a telephone or email request, ask if you can call them back to establish if they are the genuine supplier.
- When a supplier invoice has been paid, it is good practice to inform them of the payment details made, including the account the payment was made to.
- Check your bank statements carefully. All suspicious debits should be reported to your bank immediately.
- Companies should consider removing information, such as testimonials, from their own or suppliers' websites or social media channels which could lead fraudsters to identify who your suppliers are.



PROTECT YOURSELF FROM FRAUD

If you've been a victim of fraud, the risk of having your identity stolen could be higher. You can add an extra layer of protection by signing up to Cifas (Credit Industry Fraud Avoidance System). This not-for-profit company work to protect businesses, charities, public bodies and individuals from financial crime. When you apply and pay for Protective Registration, they place a warning flag against your name. This prompts Cifas members to carry out extra checks to prove your identity and stop further fraud. Find out about Cifas Protect Registration for Individuals and how to apply at www.cifas.org.uk

YOUR SAFETY CHECKLIST

ALWAYS	NEVER
✓ Protect your mobile and computer with a passcode or password	✗ Install Apps from unknown sources – check they are legitimate before downloading to your device
✓ Protect your computer with a firewall and antivirus software	✗ Respond to a text message regarding a suspicious transaction without verifying the contact details are from a trusted source (not a search engine)
✓ Install the latest software and App updates as these often contain vital security updates	✗ Give out your bank details, PIN or passcode in response to a request by text message or over the phone
✓ Secure smartphones and tablets with a screen lock	✗ Never share updates about where you are and who you're with on social media
✓ Tell your mobile provider immediately if your phone is stolen or has been lost	
✓ Back up your most important data to an external hard drive or a cloud based storage system	
✓ Complete a factory reset if you sell your mobile phone or tablet	

WHO TO CONTACT

If you suspect that you have become a victim of fraud, contact Brown Shipley immediately on: 0800 916 6911* or email our dedicated fraud mailbox at: BSCO.fraud@brownshipley.co.uk

*Lines are open Monday to Friday - 9am to 5pm, local call charges apply. Telephone calls may be recorded for regulatory and legal purposes. If dialling from outside the UK please dial +44 207 320 3662.

The **National Cyber Security Centre** have set up a Suspicious Email Reporting Service to analyse and track phishing attacks and any malware involved. To report a suspicious email, simply forward it to report@phishing.gov.uk

If money has been taken from your account, this is fraud and illegal and you should also report the crime to the police through **Action Fraud**. They'll log it and give you a crime reference number.

Action Fraud - www.actionfraud.police.uk

Telephone: 0300 123 2040, Textphone: 0300 123 2050 (Monday to Friday, 8am to 8pm)

FURTHER INFORMATION

If you would like to find out more information about how to protect yourself against fraud, do take a look at the following websites which offer straight-forward and impartial advice to help protect you against financial fraud:

- Financial Fraud UK - www.financialfraudaction.org.uk
- Take Five - www.takefive-stopfraud.org.uk
- Get Safe Online – www.getsafeonline.org
- ICO (Information Commissioner's Office) - www.ico.org.uk