BROWN SHIPLEY
A QUINTET PRIVATE BANK

HOW TO PROTECT YOURSELF FROM FRAUD

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.

Contents

HOW TO PROTECT YOURSELF FROM FRAUD

EMAIL 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.**

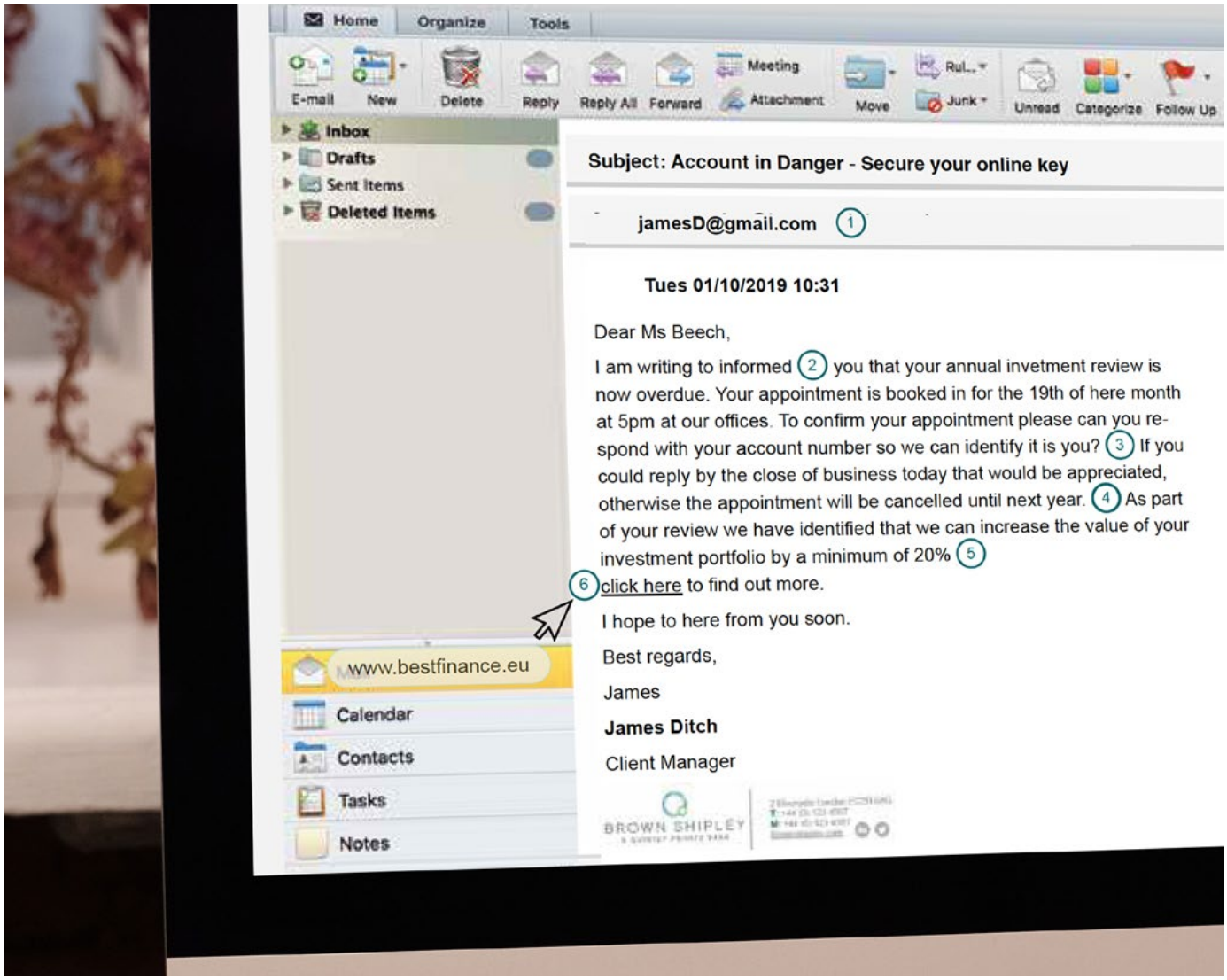
The email may request that you provide sensitive information within a given time period or your account may be closed. Threats and tight time frames are often used to pressure you to act quickly. Instead, you should check that the information is legitimate and contact your provider directly to confirm 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. The best way to get in touch with a company is to use a known email or phone number, such as the one on the back of your bank card.
- 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.

HOW TO PROTECT YOURSELF FROM FRAUD

TELEPHONE FRAUD

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...

They have identified fraud on your account and need you to complete an urgent security check.

There's an incredible offer available but you have to act now to qualify for it.

They're the police calling to tell you that you've been a victim of fraud and that you need to transfer your funds to a 'safe' account.

They're from a government agency telling you that you're due a refund and they need your bank account details to process the payment.

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.

HOW TO PROTECT YOURSELF FROM FRAUD

KEEPING YOUR DIGITAL DEVICES SAFE

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.

Malware

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 https://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.

HOW TO PROTECT YOURSELF FROM FRAUD

INVESTMENT FRAUD

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.

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.
- Too 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.

How to protect yourself

- Know your Financial Adviser / Client Advisor – this might sound obvious but you should always consult your usual Financial Adviser / Client Advisor 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 or PRA – all UK 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.

Official - NFIB Fraud and Cyber Crime Dashboard for October 2023 - October 2024 have shared that there were **279,680** reports of fraud received:		
Cheque, Plastic Card & Bank Account	**28,968 Reports**	**£145.4m Reported losses**
Online Shopping and Auctions	**60,981 Reports**	**£108.7m Reported losses**
Consumer Fraud	**126,450 Reports**	**£482.7m Reported losses**
Investment Fraud	**27,516 Reports**	**£563m Reported losses**
Banking Fraud	**35,765 Reports**	**£569m Reported losses**
This equated to **279,680 Reports** and **£1.868bn Reported losses**.		

In terms of Cyber Crime a total of **54,096** reports were received:		
Hacking Social Media & Email	**35,862 Reports**	**£1.1m Reported losses**
Computer Virus\Malware\Spyware	**4,456 Reports**	**£904.1k Reported losses**
Hacking Personal	**10,208 Reports**	**£411.4k Reported losses**
Hacking Extortion	**3,570 Reports**	**£3.6m Reported losses**
This equated to **54,096 Reports** and approx **£6.01m Reported losses**.		

Source: https://www.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46

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.

HOW TO PROTECT YOURSELF FROM FRAUD

PENSION FRAUD

Pension fraud

When you've worked hard all your life, you deserve to enjoy your 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 provide the following guidance.

Do:

- Treat all unexpected calls, emails and text messages with caution. Don't assume they're genuine, even if the person knows some basic information about you.
- Hang up on calls and ignore messages if you feel pressured to act quickly. A genuine bank or business won't mind waiting if you want time to think.
- Check your bank account and credit card statements regularly.
- Consider getting independent financial advice or guidance before a big financial decision (MoneyHelper has information on how to find a financial adviser).
- Check overseas regulators if you're dealing with an overseas firm (you should also check the list of scam warnings from overseas regulators).

Don't:

- Give out your bank account or credit card details unless you're certain who you're dealing with.
- Share your passwords with anyone (including your social media passwords).
- Give access to your device by downloading software or an app from a source you don't trust. Scammers may be able to take control of your device and access. your bank account.

HOW TO PROTECT YOURSELF FROM FRAUD

INVOICE FRAUD

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.

HOW TO PROTECT YOURSELF FROM FRAUD

ARTIFICIAL INTELLIGENCE FRAUD

Artificial Intelligence fraud

Artificial Intelligence (AI) is transforming every sector, including the financial services sector. However, AI has also opened the door for criminals to misuse its capabilities, making fraud and scams far more sophisticated and difficult to spot. To protect yourself, it is essential to understand the common types of AI fraud and how to safeguard against them.

What is AI?

Artificial Intelligence (AI), broadly defined, involves the use of digital technology to create systems that are capable of performing tasks, including complex tasks, commonly thought to require human intelligence.

Types of AI fraud

Deepfake scams

AI can create convincing fake audio, video or images that impersonate individuals. For example, scammers may use deepfakes to impersonate someone from Brown Shipley or other businesses you trust to deceive you into transferring money or sharing sensitive or confidential information.

Sophisticated phishing

AI can create sophisticated personalised phishing emails or calls, making it more difficult for you to tell whether communications are legitimate or fraudulent.

Identity theft

AI can gather and misuse your personal data from social media or other sources to create fake identities for financial fraud and other illegal activities.

Automated fraud

fraudsters can use AI to automate attacks by using stolen usernames and passwords to gain unauthorised access to your accounts.

What should I look out for?

- Unexpected communications – emails, messages or calls from unknown or unexpected sources that seem unusually urgent or request sensitive information.
- Too good to be true – fraudsters may use AI to create highly convincing scams that promise high returns on investments or big rewards.
- Inconsistencies – deepfakes or AI-generated communications often have subtle inconsistencies in tone, language or visuals. This can include unnatural speech patterns, unclear or pixelated images or mismatches in behaviour.

How to protect yourself

- Stay a step ahead – keep yourself up to date on the latest AI fraud techniques, so you are more likely to recognise suspicious activity.
- Double check who you're talking to – always confirm the identity of individuals or organisations. For example, call the person/your Brown Shipley Client Advisor on their known contact number or the number on the organisation's website before sharing sensitive information or transferring funds. For more reassurance, consider having a safe phrase that only friends and family know.
- Strengthen your online passwords – use strong unique passwords and multi-factor authentication (MFA) for all your accounts to limit the risk of unauthorised access. Don't use the same password for all of your accounts.
- Protect your personal information – take care over what personal information you share online and use the privacy settings on your social media accounts for additional security.
- Use antivirus software and AI detection tools – ensure you update your antivirus software to the latest version. You can also use AI tools that are designed to detect fraud, such as deepfake detection software, to stay ahead of potential threats.
- Report suspicious activities straight away – if you suspect you have been targeted by AI fraud, report it immediately to your financial institution, service provider or relevant authority.

Protection starts with awareness

With the reach of AI growing, it's crucial to remain vigilant against its misuse. By staying informed and proactive, you can protect yourself, friends and family from becoming victims of AI fraud.

HOW TO PROTECT YOURSELF FROM FRAUD

KEEPING YOURSELF SAFE FROM FRAUD

Keeping yourself safe 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 works 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 you should follow the below steps immediately.

First steps

The first thing you should do if you've been a victim of fraud is to contact Action Fraud. You can report a fraud via:

- The Action Fraud website - https://actionfraud.police.uk/
- The Action Fraud online fraud reporting tool - https://actionfraud.police.uk/reporting-fraud-and-cyber-crime
- or by calling Action Fraud on 0300 123 2040, Textphone 0300 123 2050 (Monday to Friday 8am to 8pm).

If there is a crime being committed right now or if you are in danger you should call the police on 999.

If debit or credit cards, online banking or cheques are involved, your first step should be to contact your bank or credit card company.

If you suspect you have become a victim of fraud, you should also contact your usual Brown Shipley Client Advisor.

Useful links

The Financial Conduct Authority (FCA) plays a key role in the prevention of fraud. They are raising awareness through a range of initiatives that can help protect you against fraud:

- FCA ScamSmart campaign raises awareness of investment, pension and loan scams.
  https://fca.org.uk/scamsmart
- FCA's Warning List of unauthorised firms where you can check whether a firm is regulated by the FCA before you invest.
  https://fca.org.uk/consumers/warning-list-unauthorised-firms
- InvestSmart
  https://fca.org.uk/investsmart

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:

- Take Five - takefive-stopfraud.org.uk
- Get Safe Online - getsafeonline.org
- ICO (Information Commissioner's Office) - ico.org.uk

BROWN SHIPLEY
A QUINTET PRIVATE BANK

Talk to us

Please contact us to discuss your particular requirements.

Visit brownshipley.com/contact.

UK_HOW-TO-PROTECT-YOURSELF-FROM-FRAUD_02/25