WEATHERBYS

PRIVATE BANK

YOUR GUIDE TO FRAUD PROTECTION

Criminals are finding increasingly sophisticated ways to part people from their money. The information in this guide will help you protect your personal information and wealth.

If any communication appears at all suspicious, do not take any action until you have been able to confirm its source. It is better to do nothing than risk your account being compromised.

In this guide we have outlined current best practice for IT security. Implementing our advice will help protect you from the vast majority of attacks.

However, there is always some risk, so the watchword is vigilance. This applies to you, members of your family and those closely involved with your affairs.

- Be alert if you are being pressured to reveal sensitive details
- We will never ask you for your debit card PIN, online banking password, transaction PIN or one-time passcode
- Log any incidents accurately and keep any evidence which might aid any subsequent investigation

Vital reading

If you do not have time to read this guide from start to finish, please read this quick summary:

1. Never reveal any personal information, PINs, passwords or bank details to anyone over the phone. If you feel at all suspicious, end the call.
2. Never disclose one-time passcodes (OTPs) which Weatherbys send you. Genuine entities will never need them, including Weatherbys staff.
3. Take the time to create different and secure PINs, passwords and reset questions to all your accounts and devices. An hour of your time spent doing this could save you thousands of pounds.
4. Even if the sender at the top of an email is a trusted household name – BT, the NHS, HMRC – think twice before you open it or click on a link. If in any doubt, do not do anything and call us immediately.
5. Invoice fraud, whereby fraudsters issue genuine-looking invoices which have altered bank payment details, is very common.

   Check their information verbally before you pay a new supplier or if the bank details of an existing supplier have changed.

If you are concerned you may have provided your bank details to a fraudster, please contact your private banking team or call the **Bank Helpdesk** immediately on **+44 (0) 1933 543 600**.

All instances of fraud and cybercrime should be reported to Action Fraud and the National Fraud & Cyber Crime Reporting Centre on **0300 123 2040** or telephone **101** if you are in Scotland.

PINs and passwords

Use different PINs and passwords for each account. Never share this information.

For the best security, use multi-factor authentication on all mobile devices and online accounts.

Passwords should be (where available):

- at least 8 characters long
- changed regularly
- contain at least one of each of
  - a capital letter
  - a number
  - a special character (e.g. $ or £)

Use answers that are hard to guess for password reset questions.

Debit card fraud

Always shield your PIN when using a cash machine and when making purchases.

Try to use cash machines inside bank branches where possible.

If your card is taken by a cash machine call us straightaway. Your card may have been taken by a cash machine due to a fault but occasionally fraudsters will attach card trapping devices to cash machines.

We can also set your debit card limit to align with your unique spending habits. By having a personalised limit, you are reducing your risk of fraud while continuing to use your card as you would usually.

If you are concerned about the integrity of your card, please block it immediately through the Weatherbys Card App, which you can download through the App Store or Play Store.

Cheque payments

Never accept a cheque or a banker's draft from someone you do not know.

Or at the very least do not release any goods until six days after you have paid in the cheque as then the money is yours and can't be reclaimed.

Ask for payment of high value items by internet or phone banking, or by a CHAPS payment.

Keep your cheque book in a safe place, report any missing cheques to us immediately and always check your bank statements thoroughly.

Phone calls

Never reveal your personal details, PINs, passwords or one-time passcodes over the phone.

Beware of calls claiming to be from your bank or the police saying your account has been targeted by fraudsters. Remember that the fraud team will never contact you directly; this will always be arranged through your private banking team or Relationship Manager.

Avoid taking any unsolicited calls from someone trying to sell or offer you advice on pensions or investments.

Do not assume you can trust the name or number on your phone display. Fraudsters can manipulate this to display an incoming call as a trusted organisation.

If you receive a suspicious call, phone back the number from a different line, or contact us and we will check it out for you.

You can also report it to **Action Fraud** on **0300 123 2040** or visit **www.actionfraud.police.uk**.

Email

Do not click on any links or open attachments within an email or on a website if you are unsure of the source.

Email scams are becoming increasingly sophisticated and could appear to come from someone you know and trust, such as your bank or HMRC.

Never put your passwords, PINs, card details or bank account numbers in an email. Legitimate companies and banks will never ask you for these details.

Be aware that using your name in your email address makes it easier for fraudsters to identify you.

Email phishing involves emailing and falsely claiming to be an established legitimate enterprise to deceive the recipient into surrendering personal information that will be used for fraudulent purposes, e.g. identity theft. Always ask yourself, does the subject make sense? Is an urgent response really required?

Cybercriminals can use lookalike email addresses or hide their true email address behind the display I.D. If you are suspicious, always check the sender's full email address.

Does the sender usually use a personal greeting or include some identifying information? Cybercriminals will use generic greetings, as it is likely the email has been sent to as many people as possible. Emails may include logos to try to create a sense of trust.

Never be hurried into clicking a link, opening an attachment, or replying with sensitive personal information. Cybercriminals want to create a sense of urgency and anxiety in the hope you will act immediately without thinking.

Phishing emails should be reported and forwarded on to **report@phishing.gov.uk**. If you are ever unsure if an email is legitimate, contact us and we will check it out for you.

Text messages

Ignore and delete any suspicious text messages.

Fraudsters can send text messages which at first glance seem genuine. They can appear in the same text thread as verified messages, making it very difficult to spot fake texts.

Cybercriminals will include text messages that contain a link or a downloadable file and encourage an urgent response.

Pay particular attention to text messages asking you to pay small fees to deliver a parcel, as these are almost always scams.

Phishing text messages should be reported and forwarded on to **7726** - it's free to do so. If you are ever unsure if a text message is legitimate, contact us and we will check it out for you.

Face to face

Always check the ID of tradespeople who solicit work or individuals asking to access your property.

Fraudsters have been known to pose as couriers commissioned by the client's bank to collect their bank card from them, which a bank will never do.

Please never hesitate to call us if you have any concerns. We are here to help and would much prefer to check and double check than let any of our clients risk being defrauded.

Invoice fraud

Many companies and individuals have fallen foul of fraudsters who issue genuine-looking invoices, by email or through the post, which have altered bank payment details. The victim is tricked into paying them rather than the actual supplier.

Before you pay a new supplier, or if the bank details of an existing supplier have changed, verbally check the details using a telephone number you know to be correct or one taken from their website, not from the invoice itself.

Social media

Restrict what you share on social media and what others share about you.

Fraudsters gather much useful information from careless use of social media.

Consider using a pseudonym instead of your own name on all your personal social media networks and do not share locations, names, ages, genders or phone numbers of anyone on social media.

Be aware that social media networks change their privacy rules frequently, so check regularly.

If you are no longer using a social media account, we suggest you delete the content and then deactivate the account.

Watch out for fraudsters who monitor posts and tweets and respond posing as a genuine company, perhaps including links to a compensation form (which is actually a fake link).

Online transactions

Always use secure sites with 'https' in the web address. This shows that the company has been independently verified.

A padlock symbol in the browser window should never be used to confirm a website is secure. Fraudsters have caught on to this and are increasingly securing their fake sites with digital certificates.

Using a domain checker like who.is can tell you when the website was created; a newly created website should raise alarm bells. We would also recommend reading reviews on websites such as Trustpilot before making purchases. Low star ratings should be a red flag, as should multiple similar reviews as this could be an indication of the reviews being written by the same person.

Never log in to your bank website through a link in an email, even if it appears to have come from your bank. Type the web address into the browser yourself.

When out and about and buying online, it is safer to access websites through your own network provider rather than public wi-fi. Some hotspots may not be secure.

Only use well-known reputable firms to transfer money and never transfer or receive funds for other people.

Genuine companies will be registered with Companies House or the Financial Conduct Authority. Check before making purchases and read their privacy and returns policy. Always check your bank statement against anything you buy online.

Wireless networks

Change any default passwords to wireless routers and networks.

Hide the SSID and change the default name.

Your router can provide a way for fraudsters to access personal information. Regard all unencrypted data sent over wireless networks as not secure.

Keep your router firmware up to date and use firewall settings. Make sure you recognise the wired and wireless networks you connect to.

Free public wi-fi is not secure, and your passwords and emails can be intercepted and captured by fraudsters close by. It is also possible to create fake wi-fi hotspots which look genuine. So, it is best to use 4G/5G or a VPN, especially when accessing private or sensitive information.

Mobile devices and computers

Do not leave mobile devices and computers unlocked or unattended. If you have to leave your device unattended for any reason, consider using a passcode lock with six to eight mixed characters.

Some simple safeguards will help prevent your devices from being hacked.

- Ensure it is set to auto-lock or log out after a very short period
- Set a unique password for your device that is different from your other accounts
- Regularly update your software, back-up your devices and configure their settings to allow you to wipe data remotely if it goes missing
- Restrict the information that can be synchronised with 'the cloud'
- Switch off services that are not needed (such as Bluetooth and GPS) and do not allow wi-fi to auto-connect to untrusted networks
- If the network is using WEP or no encryption, try to avoid it

In the unfortunate instance that your phone is stolen, please contact us immediately as your accounts and

cards may be at risk. Please visit our website for our guides on how best to configure your phone to minimise the impact of theft.

Private Bank | Protective yourself from phone theft

Racing Bank | Protective yourself from phone theft

We suggest you disable voice assistants such as Siri which can allow fraudsters with physical access to your device to circumvent security.

In general, we suggest you avoid accepting app requests for your location or access to your contact list.

Security

Do not install 'free' software without knowing its origin and do not try to access bootlegged music, films or live streams.

Make sure your computer is protected with security software and keep your operating system software and internet browser up to date.

Ensure that you restore the factory settings or remove the personalised information on devices you discard or sell.

Finally, be aware of remote access fraud. This is when scammers claim there is some kind of problem with your computer or internet service and ask for remote access to your device. Never let someone you do not know or trust have access to any of your devices, especially remotely.

Find out if your data has been included in a data breach

Use a data breach search tool such as **haveibeenpwned** to find if any known data breaches include online accounts you use or have been set-up using your email address.

- Visit **www.haveibeenpwned.com**
- Enter your email address or phone number to search for any linked data breaches (do not enter passwords)
- Visit any websites mentioned to close or secure your account

If you are concerned about identity theft as a result of a data breach or other data leak, visit **cifas.org.uk** for advice.

Examples of scams

Facebook and Instagram advertisements

Fraudsters are using social media to advertise fake websites selling 'too good to be true' offers. The website will prompt you to input your card details along with a one-time passcode to complete the transaction which fraudsters could then use to register for Apple and Google Pay using the stolen details.

Anti-virus pop-ups

False anti-virus pop-ups, particularly purporting to be McAfee, are being used by fraudsters to obtain card details or download malware onto devices. If you click the options in a fake pop-up or alert, the security of your device may be compromised.

Gift card scams

These scams usually start when someone asks you to purchase gift cards, and this can take place over a number of platforms including phone, email and social media. Fraudsters may impersonate a friend or colleague to obtain the redemption code/PIN. Once they have that number, they can redeem the card for its total value.

Compromised emails

Anyone who hacks your email account gains access to your contact list, which they can use for phishing attempts to carry out further fraud. From the content of your emails, they will have a good idea of which websites you have accounts with, including financial and banking sites. Once they know who you bank with, they will use your email account to send emails containing spoofed or modified invoices to redirect your funds to their own account. They can use your email to reset other account passwords, gain access to credit information, or even delete accounts. The information they uncover helps them to steal money or obtain personal data which they can sell on the dark web.

Investment fraud

Investment fraud comes in many forms but is typically when someone poses as an investment service provider, financial adviser or fund manager to convince you to transfer large sums of money into a company or service that doesn't actually exist.

They can create convincing-looking websites and adverts, and send you emails, texts and automated voice messages offering investments that sound too good to be true. They often are.

Fake holiday websites

Come summertime, fraudsters will promote fake holiday websites to steal personal information, including passport and card details. Perpetrators will convince victims further by sending fake reference and booking emails; you may not realise you have been scammed until you are unable to board the flight. The fake websites are very convincing – they sometimes fabricate ATOL (Air Travel Organisers' Licensing) protection numbers, something all credible holiday vendors use.

Useful information

- **cyberware.gov.uk**
- **ncsc.gov.uk/information/infographics-ncsc**
- **who.is**
- **haveibeenpwned.com**
- Report cybercrime and fraud to **actionfraud.police.uk**
- Forward phishing emails to **report@phishing.gov.uk**
- Forward phishing text messages to **7726** for free

You can also visit our website where we provide up to date information on the latest scams:

https://www.weatherbys.bank/help-and-support/latest-scams/

Your contact details

We hold up-to-date contact details for you so we can call you immediately if we see any suspicious activity on your account. Do not forget to let your private banking team know if any of your contact details change.

Time to take five

The first thing to remember is to take five and be fraud aware:

- If it seems too good to be true, then it probably is.
- Are you being pushed into making a hasty purchase or decision? This is a red flag that the situation is not right.
- Take another look. Is it likely that the tax office would send you a text asking you to make a payment?
- Check the facts. Call the organisation on their official number. Do not use the re-dial or call back function on your telephone.
- Take control. If you receive a call saying your bank has been compromised, hang up the telephone. Next, you can either log into your online bank account to check for yourself, or telephone the Bank Helpdesk using the number listed on your debit card to speak to someone about it.

Remember that we are here to help. If you have received an unsolicited approach and are concerned about it, please call your relationship manager for advice.

Contact

WEATHERBYS PRIVATE BANK

London

22 Sackville Street
Mayfair
London
W1S 3DN
United Kingdom

+44 (0) 20 7292 9029
privatebank@weatherbys.bank

Wellingborough

Sanders Road
Wellingborough
Northamptonshire
NN8 4BX
United Kingdom

+44 (0) 1933 543 600
privatebank@weatherbys.bank

Edinburgh

2 Rutland Square
Edinburgh
EH1 2AS
United Kingdom

+44 (0) 131 285 2020
privatebank@weatherbys.bank

Manchester

Orega, Arkwright House
Parsonage Gardens
Manchester
M3 2LF
United Kingdom

+44 (0)161 553 0600
privatebank@weatherbys.bank

If you are interested in finding out more about how Weatherbys Private Bank can help, **please get in touch or speak to your Private Banking team.**

WEATHERBYS
PRIVATE BANK