WEATHERBYS
PRIVATE BANK

YOUR GUIDE TO FRAUD PROTECTION

YOUR GUIDE
TO FRAUD PROTECTION

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, don't take any action until you have been able to confirm its source. It's better to do nothing than risk your account being compromised.

If you are concerned you may have provided your bank details to a fraudster, please call us immediately on **+ 44(0)1933 543543.**

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

In this guide we have outlined current best practice for IT security. Implementing our advice will 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 password
- Log any incidents accurately and keep any evidence which might aid any subsequent investigation

VITAL READING

These are the four most prevalent types of fraud. If you don't have time to read this guide from start to finish, please read this quick summary:

1. Please **do not ever reveal any personal information,** PINs, passwords or bank details to anyone over the phone. If you feel at all suspicious, end the call.
2. Please 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.
3. 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 at all don't do anything and call us.
4. Invoice fraud, whereby fraudsters issue genuine-looking invoices which have altered bank payment details, is very common. **Check their information before you pay a new supplier** or if the bank details of an existing supplier have changed.

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:

- at least 8 characters long
- 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.

CHEQUE PAYMENTS

Never accept a cheque or a banker's draft from someone you don't know.

Or at the very least don't release any goods until six days after you pay 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 a CHAPS payment.

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

PHONE CALLS

Never reveal your personal details, PINs or passwords over the phone.

Beware of calls claiming to be from your bank or the police saying your account has been targeted by fraudsters. Avoid taking any unsolicited calls from someone trying to sell or offer you advice on pension 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, call back the number from a different line, or call us and we will check it out for you.

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, PIN numbers or bank account numbers in an email. Legitimate companies and banks will never ask you for these details.

It is safer to use a paid-for email service which will have better security features than a free one, such as Gmail or Hotmail.

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

TEXT MESSAGES

Ignore and delete any suspicious text messages.

These days 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 ones.

If you are unsure, contact us and we will check it out for you.

FACE TO FACE

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

Fraudsters have been known to pose as couriers commissioned by the customer's bank to collect their bank card from them.

Please never hesitate to call us if you have any concerns at all. We are here to help and would much prefer to check and double check than let any of our customers 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.

Check with a phone call before you pay a new supplier or if the bank details of an existing supplier have changed.

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, 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 yellow padlock symbol in the browser window shows the payment process is secure.

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 or a VPN, especially when accessing private or sensitive information.

MOBILE DEVICES AND COMPUTERS

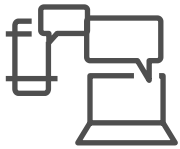
Do not leave mobile devices and computers unlocked or unattended.

Some simple safeguards will prevent your devices from being hacked.

- Use a passcode lock with six to eight mixed characters.
- 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 to 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 and avoid it

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.



Do not install ‘free’ software without knowing its provenance 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 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 your computer, especially remotely.**

WEATHERBYS PRIVATE BANK

London Office:
22 Sackville Street
London
W1S 3DN
Telephone: + 44 (0)20 7292 9029

Wellingborough Office:
Sanders Road
Wellingborough
Northamptonshire
NN8 4BX
Telephone: + 44 (0)1933 543 543

Edinburgh Office:
2 Rutland Square
Edinburgh
EH1 2AS
Telephone: + 44 (0)131 285 2020

privatebank@weatherbys.bank

www.weatherbys.bank