BARCLAYS

Fraud and Security

If you think you are a victim to fraud or received a suspicious email that claims to be from Barclays please contact Barclays UAE Client Services at +971 (0)4 365 3030, from 9:00 am to 6:00 pm, Monday to Friday, and from 9:00 am to 3:00 pm, on Saturday or contact us on **uaefraud@barclays.com**.

Fraud Vs Scam – Understanding the difference
Fraud is a criminal act to deceive you and take your cash – it's a transaction that you didn't know about or authorise. For example, fraudsters may use your details to open accounts under your name or your business.

A scam is where you're tricked into making or authorising a payment to a criminal's account. Scammers impersonate banks and official organisations using emails, phone calls and texts that look and sound genuine.

In both instances it's important to trust your instincts and remember that if something appears to be too good to be true, it probably is!

General security tips

- Don't give anyone your Online Banking security PIN and make sure you change your security PIN on a regular basis.
- Remember to log out when you have finished using Online Banking services.
- Keep your Personal Security Token device secure. Never leave it on your desk where it can get into unsafe hands.
- Check your activity log on a regular basis to keep a track of your transactions. If you find anything suspicious, let us know straight away.

Suspicious emails, texts and calls

Fraudsters send e-mails (phishing) and texts (smishing) or make phone calls (vishing) to manipulate targets into revealing passwords and sensitive information or transferring money into other accounts. Phishing and smishing messages often contain links to fake websites that request password and account information or install viruses onto your devices. A common example of smishing is receiving a text message offering you the chance to win a prize by responding or inviting you to enter a competition by providing personal details.

Business email compromise (BEC) is a more sophisticated type of phishing where criminals gain access to an individual's email account and use their emails to pose as a trusted individual to try and trick you into sending money or divulging confidential information.

Fraudsters will also impersonate legitimate organisations including your bank. How to stay safe:

- Barclays will never contact you and ask for your password, PIN, payment authorisation codes, or full account details. Nor will we ask you to make a payment, move money to a safe account, send details of an account to wire money to or request access to your systems or PC
- Never respond to unsolicited emails requesting you to re-validate your Account & User information
- Caller ID can be faked, so don't rely on this as an indicator of legitimacy
- Never assume a caller is legitimate because they know information about you, your company, or your colleagues
- If you have received a scam text or phone call do not reply to it or call back. Scammers don't know your number is active until you use it, replying may trigger further smishing attempts
- If you get a suspicious call, end the conversation immediately and call a trusted contact at the organisation in question. Use a different phone as the fraudster can keep the original line open
- If you suspect you are a victim of smishing do a web search of the number and the content of the message to see if others have reported similar scams
- If you receive a suspicious email, forward it as an attachment to **internetsecurity@barclays.co.uk**, then delete it immediately

BARCLAYS

Invoice and CEO Fraud

Invoice fraud (also known as mandate or change of existing payee fraud) occurs when fraudsters impersonate new or existing suppliers in an attempt to redirect payments to accounts managed by them. They often state that their payment details have changed, provide new account details and imply urgency. The scam may only come to light when the genuine supplier seeks payment.

With **CEO Fraud** fraudsters will pose as senior management or other members of staff within your business and request urgent payments.

Fraudsters have been known to target businesses ahead of public holidays so be mindful of any last-minute requests, including end of day emails when staff are leaving the office.

These scams pose a constant threat and continue to contribute to devastating financial losses to businesses across the globe. Verbal checks are essential to protect your organisation from these scams. Below are some tips on how to carry these out effectively:

- Always conduct verbal checks over the phone for any new or amended payment instructions, and any requests to amend contact details
- Use contact details you hold on file, and apply the same principles to requests from within your organisation
- Don't use a number included within the request to make the call as this could result in you speaking with the fraudster
- Ask your contact to read the beneficiary bank details back to you - this will confirm whether they match the details provided to you in the instruction
- Never rely on an in-bound call for confirmation
- Don't rush - if you feel pressured to make a decision, take five minutes to stop and think about what is being asked of you, and follow the steps above
- Be alert to how much information is revealed about your company and key officials through your website, social media and out-of-office automated replies

Protecting your cards

If you are concerned about the security of your account, contact us immediately on **+91 22 6000 7888**. Card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. There are steps you can take to protect yourself from credit and debit card fraud.

To protect yourself:

- Always shield your PIN from any observers when using cash machines
- Only carry the cards you need
- Avoid placing cards in your pockets, where they can easily fall out
- Make sure that your cards fit snugly inside your wallet or purse
- Take precautions to avoid your card being stolen - for example, don't leave your handbag unattended or carry your wallet in your back pocket
- Do not hand-over your card to anyone even if they claim to be representatives from your bank and always cut the plastic in four pieces across the magnetic stripe before disposal
- Report any lost or stolen cards immediately

BARCLAYS

Malware

Are your devices protected from malware? Below are some guidelines which will help you to protect them:

- Keep all firewalls and security software regularly updated, consider using antivirus protection and run regular scans on all devices
- Install the latest updates for your internet browsers and keep both internet browsers and mobile devices updated to the latest operating systems (OS)
- Only download files and software from trustworthy sources
- Ensure any mobile apps you download have positive ratings and only use official marketplaces like the Google Store or the App Store
- Ensure all emails or texts you receive are from legitimate sources before opening any links or attachments, especially if they are pressuring you into taking urgent action
- Use complex passwords and multi-factor authentication to make it harder for criminals to access your accounts
- Educate employees on how to identify phishing emails and texts and what to do if they receive any
- Test and rehearse your disaster recovery plan to ensure your business is prepared for an attack

Ransomware

Ransomware is a type of malware that disables your IT system and prevents you accessing your data, usually by encrypting files. A criminal group will then demand a ransom in exchange for decryption. Ransomware is now the biggest cyber threat to UK businesses:

- Use layers of defence to help you detect malware and stop it causing harm
- Make regular backups of critical files. Store offline backups in a different location from your network and systems, or in a cloud service designed for this purpose
- Guard against malicious content reaching your devices, for instance by filtering file types and blocking malicious websites
- Prevent malware from running if it does reach your company devices by using up-to-date antivirus or anti-malware products and technologies on all devices, including mobile phones and tablets, such as AppLocker
- Ensure your suppliers have the right level of protection
- Train employees to be aware of the threat and vigilant about suspicious activity – malware is often delivered via email attachments

What to do if you're a victim:

- Be mindful that paying the ransoms demanded by cyber criminals only encourages further attacks. There is no guarantee it will get results.
- Disconnect infected devices from the network and turn off wi-fi
- Ensure you reset any compromised credentials, including passwords
- Safely wipe infected devices and reinstall the operating system
- Verify backups are free from malware before restoring

BARCLAYS

Investment Scams

Warning: Have you been approached with an Investment Opportunity? - Fraudsters are impersonating Barclays to scam individuals and businesses
Be alert for any investment opportunities (e.g. mortgage, investment bonds, online trading) offered to you by someone claiming to be a Barclays Representative – it could be a scam. Approaches have been known to be made via social channels including WhatsApp Groups, Facebook, Telegram, and Instagram and may reference genuine Barclays websites to try and convince you that the approach is genuine.

What to do if you are approached with an investment opportunity
If you don't already have an existing relationship with Barclays, be mindful that Barclays would not contact you offering investment opportunities. If you are an existing client, contact your Relationship Manager, or call the number on the back of your card, to verify if the request is legitimate.

What to do if you think you've been scammed
If you think that you have made a payment in relation to a fraudulent investment opportunity or scam, contact your bank to attempt retrieval of the payment and file a complaint with the local police as soon as possible. Barclays cannot accept responsibility for a payment made by yourself in good faith, which turned out to be a scam.

If you have been the victim of a fraud or scam (e.g. Investment/Romance/Inheritance/Marketplace scam) that isn't related to a Barclays product, but have made a payment to a Barclays account, contact your bank immediately. They will take steps to investigate the receiving accounts and retrieve funds wherever possible. You should also file a complaint with local police who will contact us directly should an investigation be launched. Barclays will fully co-operate with and assist Law Enforcement enquiries.

Remain vigilant for further approaches
If you have interacted with fraudsters, it is likely that they will attempt to contact you again, but through a different approach. This includes scenarios such as pretending to be a solicitor, law enforcement or the fraud department of your bank looking to retrieve any lost funds, therefore it is important that you maintain vigilance when being contacted by a third party.

Spotting digitally altered content or deepfakes

With the increased prevalence of misinformation and altered images online, it's important that you take steps to differentiate real content from AI-generated images and deepfakes to stay safe from fraud and scams.

What is a Deepfake?
A deepfake is a video, photo, or audio clip that looks and sounds real but has actually been created or altered using artificial intelligence.

Deepfakes can look exactly like real people, such as you, your friends, or famous people. While they can be fun, they can also be used to trick people, so you should always be careful and check if what you see or hear is real.

Examples include:

- **Fake Images**: These are pictures that look real but are made by a computer. For example, a picture of you flying like a superhero. Fraudsters may use fake images to create false statements from public figures
- **Fake Videos:** These are videos where people seem to be doing things they never did. Imagine a video of your favourite singer dancing in your living room, even though they never visited your house
- **Fake Audio:** These are sounds or voices that seem real but are made by a computer. Like hearing your friend say something funny, even though they never said it.

Spotting a deepfake or AI-generated images can be challenging, but there are several indicators that may help. The following are some tips to help you differentiate between real Vs fake:

Face and body movements don't match the words. This could look like:

- The lips slightly out of sync
- Smiles or expressions appear glitchy or stiff
- Strange blinking – too much or too little
- Unusual shadow or lighting that doesn't match the room#
- Blurry edges around the face or hair that looks fuzzy and melts into the background

Voices sound robotic or not quite right. They could appear to:

- Have strange phrasing or unusual pauses
- The tone doesn't match the emotion
- Words pronounced slightly off that may indicate a computer is in use

The message feels urgent or unusual - this is a major warning sign, especially for scams. Watch out for the person in the video or article:

- Asking for money, gift cards, crypto or banking information
- Is behaving in a way that doesn't fit their normal personality
- Says 'you must act know' and feels almost too good to be true

Staying safe:
If something feels suspicious, consider verifying the source by reaching out to the person or organisation only using a channel you know to be genuine, like a verified phone number, email address, or official website/social media account. For more information, see our advice under Suspicious, E-mails, texts and calls and Malware.

Staying aware of emerging detection tools and threats can also improve your chances of recognising and responding to potential deepfakes.