Private Clients

Fraud prevention and digital security

Keeping your business safe

Keeping you and your business safe from fraud and scams is our priority at Barclays. Understanding how fraudsters operate can help protect you and your money.

Fraud or scam – what is the difference?

'Fraud' and 'scam' are often used interchangeably, but there's a key difference: fraud happens without your participation, while a scam relies on your involvement.

Examples of fraud include identity theft or card skimming, where your card information is copied or altered by the fraudster. Victims are unaware of this activity, and haven't given any authorisation or permission for it.

Scams are usually a direct request for money and can seem extremely plausible. You might think the request is from a supplier and authorise the payment. Sometimes these scams go unnoticed until the real supplier asks when their payment will be received.

Knowing the common risks

Social engineering: phishing, smishing and vishing

Fraudsters manipulate victims into providing confidential information or other actions that will compromise their security. Phishing involves emails which seem legitimate, but direct you to bogus websites or phone lines to capture your confidential information. Vishing and smishing are similar techniques where contact is made, respectively, by phone or text. There are other types of social engineering that specifically target businesses, such as CEO impersonation.

How to stay safe

- Have a digital safety policy in place that includes what to do if people receive unsolicited or suspicious emails, calls or texts – for instance, ignoring links and informing your IT team
- Make sure unsolicited or unexpected requests are verified using a publicly available number or contact form. Don't use numbers or links provided by the contact
- Make sure all requests for payments, donations, contributions or other financial commitments are thoroughly checked before action is taken
- Be careful with publicly available company information as fraudsters are skilled at gathering what they need to make their requests appear genuine
- Remember that reputable organisations will never ask you for passwords, PINs, payment authorisation codes or access to your systems.

CEO impersonation scams

Fraudsters can pretend to be a senior person in an organisation – generally the CEO – to persuade an employee, particularly those in accounts, to make a payment. This usually takes the form of an urgent payment request from a third party, and may also say that the transaction is confidential and/or sensitive to prevent attempts at verification. This most often happens when the apparent sender is actually out of the office.

How to stay safe

- Have a strict payment process in place and make sure everyone adheres to it
- Don't allow staff to be pressured by urgent requests, even if they appear to be from someone senior
- Any payment requests with new or amended bank details received by email, letter or phone should be independently verified. This includes internal emails from senior management that contain payment requests
- Don't reveal sensitive company information on publicly available platforms like websites, social media and out-of-office emails.

Invoice scams

Fraudsters can pretend to be a supplier you legitimately owe money to, such as your insurance provider, office landlord or broadband provider. They send an invoice or bill either requesting payment or asking you to change the details of the account you pay into.

How to stay safe

- Always verify details of any new/amended payment instructions verbally by using contact details held on file, and not on the instruction
- Set up designated points of contact with companies or people you pay regularly
- Set up procedures for changes of payment information so more than one person must approve them
- Check invoices for irregularities, particularly in bank account details, wording and company logos
- Use technology that matches invoices with purchase orders
- Be aware that testimonials on your own or supplier websites could reveal information about your payee relationships
- Conduct regular audits on all payment accounts.

Cyber attacks

A cyber attack occurs when hackers illegally access your company's IT systems to obtain confidential/financial information or to disrupt your business by taking control of its systems and holding them to ransom. System access is often gained via malicious software, known as malware, sent to you via email, encouraging you to click on a link or open an attachment.

How to stay safe

- Implement a cyber security policy – if you don't know where to start, seek professional advice
- Keep your firewalls and security software updated, setting auto-updates where possible
- Ensure important files are backed up on external devices disconnected from your network
- Make sure your digital safety policy advises never to open links or attachments unless they are from a trustworthy source
- If your computer becomes infected, disconnect from the network straight away and seek professional assistance.

Remote working and public Wi-Fi

Today's working culture increasingly sees people operating outside the office. That can create security risks, particularly when using public, shared or unsecured Wi-Fi to access company information or files. There's also the risk of someone simply looking over a shoulder to access information they shouldn't have.

How to stay safe

- Give remote workers a safe way to access the information they need, like a VPN connection or secured dongle that gives them a safe connection every time
- Prohibit using public, shared or unsecured Wi-Fi to access confidential business information.

Investment or boiler room scams

Fraudsters can pose as sales people, offering investment opportunities such as shares, gold, carbon credits or vineyards at a discounted price. They often use hard-selling tactics to persuade you, suggesting the offer is time-limited. Scammers may praise your understanding of risk and say you've been selected for an 'exclusive' chance. The high-pressure nature of this tactic is why they're often referred to as 'boiler room' scams.

The shares they're pushing may be listed on an illiquid market so can't be sold, or may be a small unquoted company that, the fraudster claims, is planning to list. In other cases, the company may not exist or the share certificates are fake.

How to stay safe

- Any so-called 'investment opportunity' you receive out of the blue is likely to be very risky or a scam
- If you're considering an investment, do plenty of research including consulting with your local financial regulator for trustworthy or suspicious firms before you invest
- In India, the National Stock Exchange publishes lists of companies you should be watchful for at https://www.nseindia.com/corporates/content/compliance_info.htm.

Fraud prevention is a team effort so please share this guide within your company to raise awareness.

We are here to help

If you think your business has fallen victim to a scam or fraud, please contact us immediately:

+91 22 6000 7888

customerservices@barclays.com

Received a suspicious email? Forward it to: internetsecurity@barclays.co.uk, then delete it.

privatebank.barclays.com/fraud

IBIM9035_PC July 2019

BARCLAYS

Refresh your knowledge at any time by visiting privatebank.barclays.com/fraud for our latest advice