Private Clients

Fraud prevention and digital security

Keeping your money safe

Keeping you 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. Victims, thinking the situation is genuine, authorise a transfer of funds or provide personal information.

Knowing the common risks

Social engineering: phishing, smishing and vishing

Fraudsters manipulate victims into providing confidential information or other actions that compromise their security. Phishing involves emails which seem legitimate, but direct you to bogus websites or phone lines that capture your personal information. Vishing and smishing are similar techniques where contact is made, respectively, by phone or text.

How to stay safe

- Remember that reputable organisations will never ask you for PINs, passcodes, account information, or for access to your devices
- Don't click on links or open email attachments, even if they seem to be from a known sender like your bank or a government body. Verify that they are genuine first
- If you get a call you are not sure about, hang up and call back on a publicly available number or one you know you can trust
- Ignore any request to transfer money to a 'safe account', as no genuine bank would ask you to do this.

Invoice scams

Fraudsters can pretend to be someone you legitimately owe money to, such as a school, solicitor, holiday company or builder/decorator. 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

- If you receive an invoice asking for an unusual payment or a change of details, check with the apparent sender before you do anything else. Use a phone number, address or email address you know you can trust, like a publicly-available number or the online 'contact us' email address
- Check invoices and bills for irregularities, especially in the language, bank account details or company logos
- Don't action requests to amend payment instructions until you have verified that they are genuine
- Regularly review and check payments to make sure they are being received by the company
- Shred confidential information like bills and bank statements
- Keep a close eye on statements and report anything suspicious immediately.

Cyber fraud and public Wi-Fi

Cyber fraud involves malicious software, known as malware, that can infiltrate your computer system, smartphone or tablet, to access your logins and personal information. It might be sent in a link or software that seems genuine, or infiltrate your systems without you even knowing. Using public Wi-Fi can make it easier for fraudsters to gain access to your devices or access your information, because the network is less protected by security systems.

How to stay safe

- Keep your firewall and security software updated, setting auto-updates where possible
- Never click on links or attachments until you are completely sure they are legitimate
- Don't bank, shop or enter confidential information using unsecured or public Wi-Fi, unless you are on a network you know is secure, and always log out of any accounts you have accessed
- Back up sensitive information and files on external devices not connected to a network or the internet
- Create strong passwords for home Wi-Fi, devices and accounts, update them regularly and don't allow your web browser to remember them.

Card and cheque fraud

Card fraud can happen when debit or credit cards are lost or stolen, or copied when using payment devices or ATMs that have been tampered with. It may also happen when fraudsters have access to your information and open or access bank accounts in your name. Cheque fraud happens when someone steals or copies a cheque, often to buy high-value goods.

How to stay safe

- Check your accounts regularly, and report any suspicious transactions immediately
- When using an ATM, check for signs of tampering, shield your PIN and keep your card in sight when making payments
- Only carry cards or chequebooks if you need them and tell us right away if they have been lost or stolen
- If you're selling a high value item – a car, for example – to someone you don't know, ask for a cash or electronic payment rather than a cheque.

Investment or boiler room scams

Fraudsters can pose as sales people, offering cheap investments such as shares, gold, carbon credits or vineyards. 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 extremely hard to sell without losing money, or may be a small unquoted company that, the fraudster claims, is planning to list. In some 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.

Share this guide with any joint account holders so they are aware of potential risks.

We are here to help

If you think you have 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

IBIM9036_PC July 2019