Jordan International Bank

How to protect yourself from fraud and scams

What is fraud?

Usually, fraud is suspicious activity on your account which you didn't know about or authorise. This means criminals have fraudulently gained access to a victims account and made payments without their knowledge.

This can include:

- Identity theft – when an individual illegally uses your details to open an account in your name.
- Unauthorised usage – when an individual uses your card without your consent for their financial gain.

Account takeover – when someone gains control of your account without your knowledge with the intent of making unauthorised transactions

What is a scam?

A scam usually means when you've authorised the payments because you've been tricked or persuaded by a criminal under false pretences.

This can include:

- Transferring money into a 'safe account' – tricked into transferring money into another account.
- Investment opportunities – fake investment opportunities to send money to the criminals.
- Romance – money sent to scammers when they've built up a 'fake relationship' by gaining their victim's trust.

For more information about Authorised Push Payment (APP) scams and how to protect yourself against these please visit our APP section on the website.

How to report fraud or a scam

If you feel that someone has authorised a transaction or accessed your account without your knowledge or consent, you must report this immediately. The same goes for a scam where you've been tricked into sending money to criminals.

You must contact us on privatebanking@jordanbank.co.uk or call us on +44 20 3144 0286. If your card is lost or stolen, then call our toll-free number on 0808 1961 700 or +44 204 5772 466 (if calling outside the UK). We will then talk you through the process of what to do next.

How you can protect yourself from fraud and scams

Whilst criminals continue to find new sophisticated ways to defraud its victims, there are ways you can remain vigilant and protect yourself. Here are some ways you can help protect yourself and your account from fraud and scams.

-Never share your personal details including your PIN, online banking, or username with anyone. Even if you believe it's the police or someone in authority.

-Never click on links from emails or SMS messages from unrecognised contacts. Always go to the website directly from your own browser if you believe it's a legitimate message.

-If you receive an unexpected call, email or an SMS message which relates to money or security details, do not respond to this. Contact your relationship manager. Unexpected correspondence can often be the first sign of a scam.

-Always read reviews of sites or companies you're dealing with and don't make payments unless you've checked the legitimacy of those companies you're dealing with.

-Please make sure you always tell us the real reason for the payment, especially if someone has told you not to tell us.

-When using Confirmation of Payee (CoP), ensure you use it correctly and if the details don't match do not continue with the payment unless you've checked this.

-Destroy statements, cards or any other documents with your account details on them.

-Do not give anyone remote access to your phone, computer or let them install any software to your devices.

-Your bank or police would never ask you to transfer money to a safe account or ask for your personal details including PIN or Passwords.

For full details about Authorised Push Payment (APP) Scams please see our website.

If you are ever concerned about fraud and scams, you can contact us for further information. Remember we won't ever pressure you into making a financial transaction, if something doesn't feel right, then you should rightly question this.

Take Five

To help everyone stay safe from fraud and scams, ***Take Five to Stop Fraud*** urges you to follow the following advice:

STOP: Take a moment to stop and think before parting with your money or information. It could keep you safe.

CHALLENGE: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT: Contact us immediately if you think you've been scammed and report it to Action Fraud at actionfraud.police.uk or on 0300 123 2040.

You can find more information on www.takefive-stopfraud.org.uk