SKIPTON INTERNATIONAL

Skipton International Fraud Prevention Guide

At Skipton International we take the security of our customer's very seriously.

Fraudsters have been getting more sophisticated over recent years and are increasingly targeting individuals whilst purporting to be from their bank, police or another credible agency. Fraudsters even copy bank or government agency logos and other information to make their emails or postal communications look official. You can no longer solely rely on a communication looking like it has come from the bank to be sure it is genuine.

If you are the slightest bit concerned please call us on

+44 (0) 1481 730730.

It is imperative that together we are vigilant and keep up to date with the latest developments so that we are wise to the Fraudsters methods in order to protect ourselves. If you hear of a new fraud being discussed on the TV, Radio, Newspapers or other media Skipton International would always recommend that our customers take a keen interest in these reports to avoid falling victim themselves.

Below we have provided some notes which we hope you will find of interest.

Please remember that Skipton **will never**:

Ask you to transfer funds into a different or 'holding' account for any reason.

Request your Skipton account details or password by email.

Pass secure details onto a third party (particularly your password).

What to do if you think you are a victim of fraud

Stop payments - Contact Skipton International immediately as we may be able to help stop the payment.

Report to the police - Contact your local police force and provide as much information as you can about what's happened.

Beware of ongoing scams - If you have been targeted by fraudsters be especially vigilant, it is possible you might be approached again.

Skipton International Online Security

We are committed to ensuring your information is safe when using Skipton International Online.
We will do everything we can to help reduce the risk of fraud and protect you and your money when online.

In conjunction with the below, we recommend you view the UK Government-sponsored website called Get Safe Online and Staying safe against scams on moneyadviceservice.org.uk

Our Responsibilities

You will receive a unique User ID and Activation Code from us when you register for Skipton International Online. On the initial registration you will need to enter these details, create a password and register a device (which will be used to generate additional one-time passwords for each subsequent logon).

We will disable access after 3 failed attempt login attempts. You will need to call Skipton International Limited to reset your account.

Your session will time out after a period of inactivity.

We will never send documents relating to your account as email attachments. We will instead always direct you to log into Skipton Online to access your information.

Your Responsibilities

Do not reveal your security details (including your password) to anyone. Skipton International will never ask you to disclose this information to us.

Choose strong passwords with a mix of letters, numbers and special characters.

If you suspect someone knows your password, change it immediately.

Always log in via the Skipton International Limited website www.skiptoninternational.com

Log off when you have finished your session.

When you log in, you will see your last session details so you can keep a regular check on your activity.

Your Responsibilities (continued)

Ensure you have installed the latest security updates on the device you log in on.

Check your transaction history to detect any irregularities. If you have any doubts please let us know.

Be aware of spam emails.

If you are selling or giving away your device, please ensure that is properly wiped or factory reset.

Contact us as soon as possible if you think your log in details have been compromised.

Scams that could affect Skipton Customers

Phishing

Be aware of any unexpected emails that claim to be from Skipton International that ask you to click on a link to an external website and will attempt to get personal details from you. The email and site may look authentic but they are fraudulent.

If you have any suspicion, do not open the link, and delete the message.

If you have provided any of your personal details then let us know immediately on +44 (0) 1481 730730.

Vishing

Similar to Phishing but the fraudster makes contact over the phone. They may appear to be very credible and already have some information about you. They could pose as Police, Government officials or even Skipton employees. They will try to persuade you to transfer money into another account for any number of reasons.

Be aware that Skipton (or the police) will never ask you to transfer funds into a different or 'holding' account. Remember, if a fraudster stays on the line after you hang up the line will remain open, when you pick the phone back up you will be speaking to the same person – Ideally call Skipton using another phone line or wait a few minutes before making the call.

If you are contacted out of the blue and are in any way concerned, end the call and contact us securely on +44 (0) 1481 730730.

Mishing

Like Phishing/Vishing but contact is made via text message that is amended to look official. Skipton International rarely use text messages and would never request any personal information via this medium.

Do not respond and contact us immediately on

+44 (0) 1481 730730.

Postal Fraud

Only ever send documents/letters to our registered address of :

Skipton International Limited
PO Box 509
Tudor House
The Bordage
St Peter Port
Guernsey
GY1 6DS

Never reveal your Skipton password to anyone, except to a Skipton International employee whom you have called on +44 (0) 1481 730730 (or on a previously confirmed direct dial line) who may ask for certain letters/digits from your password to confirm identity.

If you have any concerns that your mail has been intercepted or tampered with then contact us immediately on

+44 (0) 1481 730730.

Computer Software Scams

Similar to Phishing scams, a fraudster will attempt to coerce you into downloading an app or software onto your mobile phone or computer which will allow them to gain access.

Posing as a representative from a genuine organisation (e.g. the police, tax office, telecommunications company) the fraudster could use a range of methods to make contact (e.g. text message, email, phone call). They will try to get you to act, they could claim that there is a security threat and your details have been compromised or that there has been suspicious activity on your bank account. Once the app/software has been downloaded the fraudster will trick you into logging into your bank account giving them the access they need to take over the computer and steal money.

If you think you may have been a victim of any type of scam then contact Skipton immediately on

+44 (0) 1481 730730.

Money Mule Scams

Money Mule scams are a type of money laundering used by criminals and fraudsters to move around and legitimise their proceeds of crime. A money mule is a person who receives money into their bank account from a third party and then transfers it onto someone else, often obtaining a commission. Even if the Money Mule is not directly involved in the crimes that generated the money or claim that they did not know they were being used by criminals, they are still accomplices and could face prosecution by the police if they are caught.

Fraudsters will often recruit Money Mules through seemingly legitimate job offers advertised via online job forums, email, social media or online pop-up ads. Common job titles and positions advertised include 'Accounts Manager', 'Money Transfer Manager' or 'Local Agent/Representative'. Posing as employers they can offer the chance to make easy cash from home with no experience necessary. The types of work being advertised can vary but it will always include using your own bank account to transfer money.

Whilst those under 35 years old or those suffering financial hardship are the most likely targets, anyone could be approached or fall victim to Money Mule fraudsters. To protect yourself you should:

- be wary of unsolicited offers to make easy money;
- never give out your bank details to anyone unless you know and trust them;
- never use your own bank account to transfer money;
- carry out research into any company that makes you a job offer, ensuring you check that contact details are genuine.

If you think you may have been a victim of any type of scam then contact Skipton immediately on +44 (0) 1481 730730.

COVID-19 Fraud Scams

Skipton would like to warn you that there are fraudsters using the Covid-19 pandemic as a cover. There have been multiple cases worldwide of fraudsters using coronavirus-themed phishing emails to attempt to trick people into opening malicious email attachments or revealing sensitive personal and financial information. For example, UK Action Fraud have advised that a common tactic being used by fraudsters is to contact potential victims over email purporting to be from research organisation's affiliated with the Centres for Disease Control and Prevention (CDC) and the World Health Organisation (WHO).

They claim to be able to provide the recipient with a list of coronavirus infected people in their area. In order to access this information, the victim needs to click on a link, which leads to a malicious website, or is asked to make a payment in Bitcoin.

Other Covid-19 scams relate to online sales of items that are perceived to be in short supply across the country, such as personal protective items (PPE) and medical supplies. If you are shopping online it is always important to stop and think about who you are buying from, do your research and look for reviews of the sites you are using.