

According to various Government and financial industry bodies, there has been a significant increase in fraudulent activity in recent years.

Fraudsters have many sophisticated ways to carry out their crimes and some of these are used to target victims through the internet. We are all potential victims of fraud and whilst we may not be able to stop this crime entirely we can all take steps to help prevent it from happening to us.

This leaflet has been produced to illustrate the common types of internet fraud and provide guidance on the steps you can take to protect yourself and your business.

For further information about online security visit our website at:

www.bankofscotland.co.uk/corporate/onlinesecurity



! PLEASE READ THIS INFORMATION CAREFULLY AND MAKE SURE THAT ANYONE IN YOUR BUSINESS WHO USES INTERNET BANKING IS AWARE OF ITS CONTENT.

For more information, contact our Helpdesk on:
0845 604 4267[†]
Lines are open 24 hours, 7 days a week.
Or visit our website at:
www.bankofscotland.co.uk/corporate/ib

Data Protection Notice: To see how we use your information and how to give your consent, please read the Data Protection section on our Group website <http://www.bankofscotland.co.uk/dataprotection> or ask for a printed copy. We will use your information to contact you by mail, telephone, E-mail, SMS or otherwise about other products and services that may be of interest to you. If you do not wish to receive this information please visit <http://www.bankofscotland.co.uk/dataprotection> for details on how to opt out of this service.

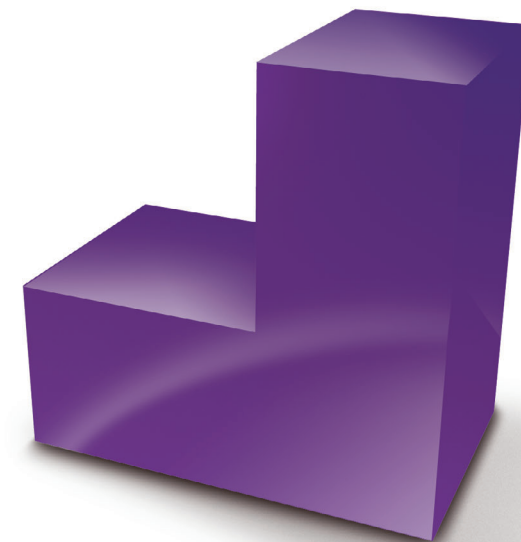
[†]Telephone calls may be recorded for security purposes and monitored under our quality control procedures.
Bank of Scotland plc. Registered in Scotland number SC327000. Registered Office: The Mound, Edinburgh, EH1 1YZ.

You may contact us using Type Talk. Information is available in large print, audio and Braille on request.

 **BANK OF SCOTLAND**
CORPORATE

Business Internet Banking

**SIMPLE
STEPS TO
PROTECT
YOUR
BUSINESS**



[ONLINE SECURITY]

 **BANK OF SCOTLAND**
CORPORATE

WHAT ARE THE COMMON TYPES OF ONLINE FRAUD?

Email Scams

- You are sent a fraudulent email claiming to be from your banker or another financial institution.
- This will ask you for your account details or request for your assistance to move money that requires your account details.

Phishing

- Someone disguises themselves as being from a bank or financial institution.
- They contact you by email, in which you are invited to go to an official looking (but bogus) website via an attachment or link.
- You are then misled into providing financial or personal information, which they require to commit a fraud against you.
- Bank of Scotland would never ask for your confidential information in this way or any other method (see **Physical Security**).

! IF YOU RECEIVE ONE OF THESE EMAILS, YOU SHOULD FORWARD IT TO onlineinvestigations@bankofscotland.co.uk AND DELETE THE EMAIL WITHOUT RESPONDING, OPENING ANY ATTACHMENT OR CLICKING ON ANY LINK.

Pharming

- These attacks are initiated by criminal hacker's compromising the Domain Name Server and redirecting traffic from a legitimate website to a bogus address.
- As far as your browser is concerned you are connected to the correct website.
- The aim of these attacks is to obtain financial or personal information from you.
- These attacks are a variation on Phishing and are aimed at the Domain Name Server not directly at you or your PC.

! WHEN ACCESSING A WEBSITE EXAMINE YOUR BROWSER'S ADDRESS BAR WHERE YOU MAY NOTICE THAT THE WEBSITE NAME IS NOT EXACTLY AS YOU TYPED IT. IF THIS IS THE CASE YOU SHOULD EXIT THE WEBSITE IMMEDIATELY.

Trojan Horse Attacks

- A Trojan Horse is a malicious software programme, which has been designed to disrupt the operations of a computer.
- You may download a file which, when activated will run a programme, that will capture details such as passwords and account details for fraudsters to use.

Spyware

- Spyware is technology that gathers information about you without your knowledge. Spyware is similar to a Trojan Horse in that you can unwittingly install it when installing other software on your PC, or even browsing on the Internet.

! BE AWARE OF THE CONTENT OF ELECTRONIC FILES AND WHO IS SENDING THEM BEFORE THEY ARE DOWNLOADED.

WHAT ACTIONS SHOULD I TAKE TO PROTECT MY BUSINESS?

PC and Laptop Security

- We strongly recommend that you have firewall technology, anti-virus and anti-spyware software installed on any computer that has internet access.
- Ensure that your anti-virus and anti-spyware programmes are updated regularly and that you have the latest security patches installed.
- Keep your operating system and browser up to date as newer versions have higher levels of internal security.
- Do not download files from an unknown source or open emails from unknown senders; they may contain viruses.
- Only use trusted PCs or Laptops, at home and work.
- Be aware of the fraudulent communication scenarios and check independently with service providers at known contact numbers if in doubt.
- Do not write down or divulge personal or security information to a third party.
- Always remember to change your password at regular intervals, at least once a month.

Physical Security

- Internet Banking uses the very latest Token technology. These compact Tokens generate a unique six digit code which changes every sixty seconds, making an already secure-environment even safer. For more information on Tokens please see www.bankofscotland.co.uk/corporate/knownyourtokenguide

- ! Never let any other person use your personal Token.**
- ! Never write down or divulge your Password for Internet Banking to anyone, including Bank of Scotland staff.**
- ! Make sure you have logged off properly by selecting the 'Log off' button when you have finished using our service.**
- ! Bank of Scotland, in line with all major banks, would not contact you and request your security information either electronically, online or by phone. This information should never be divulged. If in any doubt contact the Internet Banking Helpdesk.**

WHAT IF I SUSPECT I AM A VICTIM?

If you notice suspicious activity on your PC or Laptop, such as rebooting, running slowly, displaying unexpected or strange messages, have it checked by a technically qualified person to identify whether or not a virus is present. Until you are confident that there are no viruses on your PC or Laptop, do not access Internet Banking.

If you are concerned that your Internet Banking login details may have been compromised, please contact the Internet Banking Helpdesk immediately on:

0845 604 4267⁺

Lines are open 24 hours, 7 days a week.

