Keeping one step ahead of fraud

Vishing (telephone fraud)

Royal Bank of Scotland

We know how important it is to keep your business secure against fraud and scams. Vishing is a threat you need to be aware of. Read on to discover what to look for and what you could do to protect your company.

Vishing

Vishing is the name given to telephone fraud. The fraudster usually impersonates a member of bank staff over the phone, generally claiming that there is an issue with your account that requires urgent attention. Be aware that fraudsters may also impersonate other third parties (such as representatives of telecommunications or utilities companies).

What to look for (some or all of the below may be present)

- You receive an unsolicited telephone call where the caller generally advises they are from the bank, usually the fraud or security team. As above, the fraudster may also claim to be from any known and trusted company
- You are advised there is a problem with your account that requires your urgent attention. For example; suspicious transactions have been identified, malicious software has been detected on your profile, or there is an internal investigation

The caller could then ask you to ...

- Identify yourself by providing full or part of your PIN, passwords or smartcard codes
- Follow instructions for you to key a test payment, reverse or cancel a transaction
- Download screen sharing software to diagnose or remedy the problem
- Avoid contacting the bank or relationship team as there is an internal investigation
- Check your caller ID as the number displayed will be a number you know and trust, this has however been 'spoofed'

Don't forget

Failure to take adequate security precautions could ultimately leave your business liable for any losses which arise from fraud.
The Bank will **NEVER** ask you for your full PIN and password online, **NEVER** ask for your PIN, password or smartcard codes over the telephone and will **NEVER** ask you for smartcard codes at log in.

What to do

- Never be afraid to terminate a call. Hang up and call The Royal Bank of Scotland on a number you know and trust
- Do not assume a call is genuine just because the caller knows information about you or the business
- Remember, we will never ask for PIN, passwords or smartcard codes over the telephone
- We will never ask you to key or authorise test payments, reverse transactions or ask you to download screen sharing software

Get in touch

If you suspect fraudulent activity on Bankline, call: **0800 161 5157**

To report other suspicious activity, call: **0800 161 5150**

If you need any other help, please call your Relationship Team.

116650 Apr 2018