COMMERCIAL BANKING

Fraud risk.
How exposed are you?

BANK OF SCOTLAND

An introduction

A message from our director

Police recorded crimes of fraud increased by 40% between 2014-15 and 2018-19*.

At Bank of Scotland Commercial Banking we are passionate about supporting our business clients and one of our key priorities is to help our clients stay safe from financial fraud. This booklet provides details of the latest scams impacting UK businesses and some very relevant ideas on how to avoid becoming a victim to financial fraud.

I lead a team of specialists across Fraud, Investigations, Financial Crime, Sanctions and Anti-Bribery and am very aware that fraud and cyber related fraud is on the rise, and that all businesses are vulnerable. It is essential that business leaders take the threat seriously and understand how they can reduce their business exposure.

In particular, impersonation fraud is on the rise in the UK and globally. Financial Fraud Action UK claims that "impersonation and deception scams continue to be one of the primary drivers behind business losses to financial fraud". In many cases where impersonation fraud takes place a cyber security attack may have occurred. The cyber breach can help fraudsters to conduct reconnaissance, research and harvest valuable information which is used to make their attack very convincing.

Please take some time to study this booklet and share it with everyone in your business who has a responsibility for making or authorising payments on behalf of the business. Afterwards, do take time to view our website for more information, details are provided further in this booklet.

Regards

Mark

Mark Brotherton, Director, Fraud & Financial Crime, Lloyds Banking Group, Commercial Banking

*Source: **https://www.gov.scot/publications/recorded-crime-scotland-2018-19/pages/4/**

Contents

Social engineering

The use of deception and manipulation to obtain confidential information or taking specific action.

What is social engineering?

Social engineering is the manipulation of individuals into performing actions or divulging confidential information. Fraudsters use social engineering tactics because it is usually easier to take advantage of your natural instinct to trust than it is to find ways of breaking into your systems. This could be persuading you to provide passwords and PINs or to transfer money.

The types of social engineering attacks currently being used by fraudsters to dupe businesses include phishing, vishing, smishing and spoofing – more on this later.

Your social media footprint

Social media has become a valuable tool for fraudsters in carrying out social engineering attacks because of the wealth of information that can be found on a victim. Fraudsters will often use personal information contained on social media platforms to target employees of a victim business by purporting to be a trusted person and encourage them into disclosing confidential information or to take specific action e.g. send a payment.

What is spoofing?

Spoofing is when a fraudster imitates genuine telephone numbers or the email addresses of financial institutions or other trusted people or organisations.

For example, the fraudster may alter the incoming number that appears on your phone's caller display, to one that you know is the genuine number for the Bank. Alternatively, they could send an email that appears to come from a senior person within the business, instructing an urgent payment to be made, usually via online banking; however the senior person's email account is either hacked or copied by fraudsters.

Implement a social media policy which helps employees understand their responsibilities when using social media both at work and at home

For further support, please visit:
www.getsafeonline.org/business

Protecting your business from social engineering

UK Finance urge you to Take Five to stop and consider whether the situation is genuine. Is this making sense?

1. **Requests to move money**

   A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

2. **Clicking on links/files**

   Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

3. **Personal information**

   Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

4. **Don't assume an email or phone call is authentic**

   Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Be mindful of who you trust – criminals may try and trick you into their confidence by telling you that you've been a victim of fraud. Criminals often use this to draw you into the conversation, to scare you into acting and revealing security details. Remember, criminals can also make any telephone number appear on your phone handset so even if you recognise it or it seems authentic, do not use it as verification they are genuine.

5. **Don't be rushed or pressured into making a decision**

   Under no circumstances would a genuine bank or some other trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons. Remember to stop and take time to carefully consider your actions. A genuine bank or some other trusted organisation won't rush you or mind waiting if you want time to think.

6. **Listen to your instincts**

   If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

7. **Stay in control**

   Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's okay to stop the discussion if you do not feel in control of it.

www.takefive-stopfraud.org.uk

Online fraud

Cyber enabled fraud.

What is malware?

Your systems can be infected by malware (malicious software) through viruses and Trojans which can then interrupt your online banking sessions and present you with a fake, but seemingly genuine, screen prompting you to enter passwords and codes which can be captured. Fraudsters will use this information to access your online accounts and make fraudulent payments.

How does malware download to your systems and devices?

Malware code is often hidden in attachments, links and free downloads. Criminals are always looking for different ways of downloading malware and malvertising is one of the methods that is used. Malvertising uses unprotected online advertising to spread malware and involves injecting malicious or malware-laden code into advertisements on legitimate online internet site advertising networks and web pages.

Protecting your business

- Protect all PCs and devices with anti-virus software
- Install software updates as soon as they are available
- Ensure unique, strong and secure passwords are used. Change often
- Only download software from verified and trusted sites
- Train all staff in online fraud awareness.

Phishing is a key tool for malware to be downloaded onto your system.

See more about this on the next few pages.

84% of fraud reported nationally in April–September 2018 was estimated to be cyber-enabled.

2019 National Strategic Assessment of Serious and Organised Crime (SOC).

https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file

Phishing emails

A seemingly genuine email designed to trick you into following its instructions.

What is phishing?

Phishing is an email scam designed by fraudsters who masquerade as your bank or another trusted organisation to obtain confidential information such as personal information, bank details and passwords. Often the email will link through to a fake website and it may appear almost identical to the legitimate website. Additionally, the email communication will usually suggest that you must act urgently, maybe to prevent your online access from being blocked.

Remember, phishing emails can look extremely convincing by copying branding and spoofing email addresses to seem genuine.

Protecting your business

- Protect all PCs and devices with anti-virus software and install updates as soon as they are available
- Set up effective and on-going staff awareness training and testing
- Implement a supportive process so that phishing emails can be reported – early reporting means that quick action can be taken to reduce that risk exposure.

A case study: How does phishing work?

999 Doctors Surgery* receives an email from the bank advising them of upcoming improvements to their online banking service. It asks them to log-on, re-validate their security details and register new security questions. The email 'helpfully' provides a link for 999 Doctors Surgery to use.

A staff member follows the link which appears to take them to their online banking homepage. They enter the confidential security information that the screen asks for.

Unfortunately, although the sender's email address had Bank of Scotland within the name, the full email address was not genuine and was from a fraudster. By following the link to a fake site, 999 Doctors Surgery has now given the fraudster information that they may be able to use to access their online banking.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

How to avoid a phishing scam

Best practice.

1. **Think before you click**

   Beware of clicking on links or opening attachments contained in emails.

   Hover the mouse over the link and the URL details should come up and show if it is genuine.

   Ensure that the email address fully matches the trusted organisation's email address.

2. **Be wary of emails asking for confidential information**

   The bank will never email you asking you to disclose passwords or any other sensitive information.

3. **Open up a new web page in your browser and go to the website independently rather than clicking on an email link**

   A link within a phishing email could result in a virus or malicious software (malware) being downloaded onto your machine which the fraudsters will use to steal things such as your account details and data.

4. **If suspicious – contact the sender directly**

   Do not use the contact details or links provided in the email or reply to the email.

5. **Use a SPAM FILTER on all your email accounts**

   If you spot a suspicious email mark it as spam and delete it immediately without clicking on any links or attachments.

6. **Other key signs**

   Things such as the spelling and grammar are of poor quality, including graphic designs and images.

   Email is addressed to 'Dear Customer' for example where you hold a standing relationship with this organisation and previous communication has been addressed to you directly.

Ransomware

Malware extortion attack.

What is ransomware?

Ransomware is a growing threat to businesses of all sizes and across all sectors. This is a type of malware that operates by blocking access to key files typically by encryption, which requires a private key to decrypt files and restore your access.

An attack is followed with a ransom demand to restore your access to the files and documents. The ransom payment is usually requested by digital currency e.g. Bitcoin which is almost impossible for the authorities to trace.

Businesses of all sizes and across all sectors are targeted.

A case study: How does ransomware work?

Jayne's PC at ABC School* displayed a message which stated that all of the data on the computer had been encrypted and it demanded a ransom of £500, payable in Bitcoin, for an encryption key.

The message stated that the encryption key will be destroyed at a set time within a short period, therefore Jayne and the organisation had a short timescale to act. The school decided not to pay the ransom, but because the data had not been backed up for two weeks the school lost that data and had to spend time reconstructing it.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Protecting your business

- Ensure all PCs are protected by high-quality antivirus software, keep your firewalls switched on and run frequent scans
- Always ensure updates are actioned promptly. These updates will often contain important security upgrades which will help protect your devices from viruses and hackers
- Make sure staff are trained in online fraud awareness and understand the importance of not opening any files attached to an email from an unknown, suspicious or untrustworthy source
- Backup all of your important data to an independent source such as an external hard drive or an online backup service.

Visit 'No More Ransom' website for information on how to prevent this type of Fraud:

www.nomoreransom.org

Depending on your level of preparation, ransomware infection can cause minor irritation or wide-scale disruption.

Source: National Cyber Security Centre – Protecting your organisation from ransomware.

*Source: **http://www.dailymail.co.uk/sciencetech/article-5063313/Fast-growing-cyber-crime-threatens-financial-sector-Europol.html#ixzz55gAC3mS8**

Telephone Frauds

Social engineering methods using the phone.

What is telephone fraud?

Telephone fraud, which is often referred to as "vishing", is a scam which is intended to trick you into providing online banking passwords, confidential details or to persuade you to transfer money from your account.

Fraudsters, often purporting to be from your bank's fraud department, may call you to report a problem with your account and ask you to confirm that payments are genuine or ask you to move money into a "safe account".

Often, through the research carried out, the fraudsters will have your name, address, colleague names and bank details – essentially the kind of information that you would expect a genuine caller to have. Additionally, the fraudster will create a state of urgency and inform you that your money is at risk and that you have to act quickly, creating fear that no action will lead to a financial loss.

What is a text fraud?

A fraud which targets the users of mobile phones using text messages is sometimes referred to as a "SMiShing" scam. The fraudsters aim to obtain private and confidential information from individuals or encourage them to ring a number or click on a link for more information.

The message will typically alert you to a problem with your account. Fraudsters may spoof (see p4) the message onto a genuine message thread.

Protecting your business

- Take care if divulging confidential or personal information over the phone, text or email even if it seems genuine
- Verify the identity of the person/entity contacting you. Contact the company on a public number that is TRUSTED and VERIFIED
- Remember, the Bank will never ask for your online login details on the phone and will never ask you to move money to a "safe" or "secure" account.

A case study: How does a typical telephone scam work?

Builders Limited* receive a phone call purporting to come from the bank stating that their account has been targeted by fraudsters and they need to take immediate action. The phone number displaying on the incoming call shows a number known to match that of the bank.

They are given information that leads the building firm to believe that the call is genuine. They are advised to move all funds (£250,000) to a 'secure' account, which they do following instructions. The next day they contact the bank and realise the call was not genuine. They had been tricked into sending £250,000 to an account at another bank under the fraudster's control. When contact was made with the bank who received the funds they advised that all monies had been transferred into accounts at multiple banks. Only £27,000 was recovered for the building firm.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Email Frauds

Business Email Compromise is where a fraudster impersonates a supplier or senior member of your business.

What is Business Email Compromise?

Business Email Compromise (BEC) is the most common type of fraud we've seen targeting businesses. Fraudsters will usually prepare for this type of attack by monitoring existing genuine email traffic between a business and their suppliers, contractors and employees. Then by hacking into an email chain at an opportune moment, fraudsters can launch a very convincing attack.

The fraudulent email when it's received will be made to look like it's been sent by a genuine supplier (invoice fraud) or a senior employee (CEO fraud). It may even come from their email account if they've been hacked and the content of the email will look genuine, containing previous email exchanges and attachments. It will often be timed so that it falls in line with expected payment dates. Everything could look genuine apart from the account number which will be altered to a fraudulent one.

Common frauds using Business Email Compromise

- **CEO Fraud** – called CEO because this is a fraud which impersonates a senior person within an organisation. The request will often state that the payment needs to be made urgently and be labelled as strictly confidential and therefore not to be shared with any other staff due to the sensitivity of the transaction. If the fraudster has done some research on the individual they are impersonating, they will likely send the request when the genuine person is not available due to holiday or meetings. Of course this is all intended to deter the member of staff from questioning the payment or to rush things.
- **Invoice Fraud** – refers to a fraudulent payment which a victim makes in the belief that it's a payment being made to a usual or genuine beneficiary – one which the business intended to pay. However in reality the fraudsters have tricked a member of staff into making the payment to a fraudulent account number. A common way in which this happens is where fraudsters impersonate a supplier or contractor and provide fraudulent account details on an invoice or email communication. If the accounts details are not checked before the invoice is paid, the funds will be lost.

How to avoid Email Fraud

Best Practice.

- Don't rely on the email address appearing to be legitimate or the wording to be familiar when it comes to making payments. Email is not a secure method of communication.
- Don't assume that because you've confirmed aspects of an email to be genuine previously, the recent bank account number, or contact phone number supplied in that same email thread is also genuine.
- Independently verify all requests to change bank account details or changes to contact details by calling on a number known to be correct for the genuine payment recipient.
- Remember that emails can be intercepted between staff within your own business. Checking new payment instructions or changes to account details received in internal emails can be just as important.
- Have a clearly documented procedure so that all staff know how to handle payment requests and changes to payment details.
- Raise staff awareness of the current scams on a regular basis.

A case study – How does a typical email fraud work?

XYZ Building PLC* purchases materials from ABC Merchants*.

There are many emails exchanged between the two businesses to confirm precise details of the order and phone calls are also made about the delivery arrangements.

However, fraudsters have infected ABC's IT system with malware and have access to their email accounts. They find the latest email thread regarding the order and respond to XYZ, attaching a PDF invoice using ABC's exact format, but quoting a fraudulent account number for payment.

XYZ receive the email and see that it is from ABC's genuine email address, it contains all of their previous email conversations including reference to the delivery phone call. They send a payment of £38,000 to the account number specified within the invoice. When ABC send the genuine invoice a week later, the fraudulent email is uncovered and XYZ lose the full amount of the payment.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

"Email is not a secure method of communication for payment related details."

Senior manager
Fraud and Financial Crime
Lloyds Banking Group

Cheque overpayment

Advance payment scam.

What is cheque overpayment?

This is a common scam that is targeting businesses of all sizes.

This is where a fraudster purporting to be a new customer contacts you to order goods or services. Whilst the fraudster will lead you to believe that the payment will be transferred into your account electronically and ready for immediate use, it will actually be a counterfeit or stolen cheque that will be credited. The cheque will be made out for much more than the value of goods or services purchased. Following the payment, the fraudster will dupe you into urgently processing the refund for the overpayment.

The fraud is only discovered when the stolen/ counterfeit cheque is returned unpaid but by that time you have paid the fraudster 'the overpaid' amount and are now left out of pocket.

Protecting your business

- Be suspicious of any new clients who send a larger amount of funds than you were expecting
- Ask the Bank to check the origin of any such overpayments before returning the money
- Check with the Bank to know whether a cheque has definitely been 'paid'.

A case study: How does cheque overpayment work?

Alpha Limited* receives an order for £2,000 worth of goods from a new client. The client promises to send an online payment so the goods can be dispatched. When Alpha check their bank account they find a payment for £20,000. They contact the client who says the overpayment is a processing error.

The new client asks for Alpha to return the extra £18,000 to a specific bank account. Alpha returns the £18,000 using online banking and dispatches the parts for the original £2,000 order.

A few days later Alpha realise that the £20,000 payment was actually a cheque paid in at a branch counter and has been returned unpaid. They have lost £18,000 in cash and £2,000 worth of goods. They contact the bank immediately for help, but unfortunately £12,000 had been moved out and was unrecoverable.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Employee Fraud

Fraud committed by an employee or book-keeper.

What is employee fraud?

Internal or employee fraud is when fraud is committed against the company or organisation a person is working for.

There are a number of ways in which employees or contractors can commit fraud against their employers and include falsifying expenses claims, misappropriating assets and making financial payments drawn on the business for personal gain.

Employee fraud has escalated recently across the UK and the risks that are involved can have serious consequences for businesses across all sectors and sizes. The costs of dealing with this type of fraud are high and the chance of retrieving lost money is slim.

Where to find out more:

www.actionfraud.police.uk

www.getsafeonline.org/business

Protecting your business

- Implement a robust recruitment process, including criminal record and character checks for applicants
- Regularly review employee access to business bank accounts, telephony and Internet passwords and to your computer systems and files. Restrict access to only those who need it
- Treat cheque books and cards with the same level of security as cash
- Ensure employees dealing with business finances are adequately supervised by senior colleagues. Have open conversations with employees and publicise the steps taken against fraudsters to show that fraud is not tolerated
- Have a strong whistleblowing reporting facility to allow employees to report suspicious activity anonymously.

Card and Cheque Fraud

Cheque fraud.

What are the risks?

Criminals can target your business by printing counterfeit cheques to take money from your account. They can steal genuine unused cheques or chequebooks, then forge your signature. Or they can fraudulently alter cheques you have written by changing the payee name or, if they are the payee, by increasing the amount that's payable to them.

Protecting your business

- Complete cheques fully before signing and cross through spaces on your cheques after the payee name and amounts
- Write payee names in full e.g. "Lloyds Banking Group" rather than "LBG or Lloyds"
- If you issue cheques using a laser printer, use one recommended for cheques
- Keep cheque books secure and reconcile cheque payments to statements reporting inaccuracies immediately
- If you are expecting a new cheque book, contact us as soon as possible if it does not arrive.

Card fraud from the user's perspective.

Protecting your business

- Ensure you are the only person that knows your PIN – banks or the police will never ask for it
- Watch out for card expiry dates. If your replacement card doesn't arrive, call the bank
- If you move your business correspondence address, tell your bank, card issuer and other organisations that you deal with straightaway. Ask the Royal Mail to redirect your post
- Always shield the keypad to prevent anyone seeing you enter your PIN. If you spot anything unusual about the cash machine don't use it – report it to the bank concerned immediately.

On the Internet

- Protect your PC with the latest firewall browser and antivirus software
- Look for the padlock symbol when buying online – it shows the information you input will be encrypted.

Card fraud from a merchant's perspective

Protecting your business if you need to accept payments made by card:

- Consider 3D secure for processing card payments – it offers greater protection from fraudulent payments
- Ensure your business has sufficient staff who know how to review high risk transactions referred by your merchant services supplier
- Chip & PIN terminals must be held securely at all times to avoid unauthorised tampering
- Any cardholder information must be held securely and in accordance with the card payment industry requirements. Access to this information should be restricted only to those staff needing it
- Comprehensive security information will be available from your merchant services provider. Ensure that all key staff are aware of the security guidance.

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at **bankofscotland.co.uk/business/contactus**

Lloyds Banking Group is committed to protecting our customers. If you have any concerns or need some support with understanding the information in the brochure you have just read, due to your personal circumstances, please contact your relationship management team. We will do all we can to help you understand the content of this brochure.

Get in touch

bankofscotland.co.uk/fraud

Contact your relationship management team

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use Relay UK. More information on the Relay UK Service can be found at: relayuk.bt.com/

Calls may be monitored or recorded in case we need to check we've carried out your instructions correctly and to help improve our quality of service.

1/4520996-6 (02/20)

BANK OF SCOTLAND