Detect and Protect – Fraud and Cybercrime

Helping our customers protect their business

This document is for information purposes only. Following any guidance in this document may help reduce the risk of fraud but will not eliminate it or guarantee that the types of fraud described, or other fraud, will occur.

Royal Bank of Scotland

rbs.com

Your journey through this pack

Insight

Providing you with insight into facts and figures on how fraud has impacted the market

Types of Fraud

Understanding the different types of fraud will help you keep one step ahead
Fraud Methods include:

- Social engineering
- Insider fraud
- Invoice fraud
- Payment: Card, Cheque and UK Domestic
- Malware & Ransomware

Protecting your Business

How to protect your business when using our channels:

- Bankline
- Bankline Direct

We have also included links to relevant websites for mobile and online customers

Support

How Royal Bank of Scotland can provide tips on improving your cyber security

Insight

Providing you with insight into facts and figures on how fraud has impacted the market

Insight

How Fraud and Cybercrime affects you

One quarter of UK businesses admit they've fallen victim to a financial scam or have experienced attempted scams since 2014. Despite this trend, 49% believe it's unlikely to happen to their business

- Cybercrime costs the UK Economy £15 billion a year
- Cyber crime is forecast to grow from $3 trillion (globally) in 2015 to $6 trillion by 2021
- The volume of attacks seeking out Internet of Things devices increased by 310% in 2016

- There were 14,673 reported cases of phishing attacks in 2016
- One fraud or cyber crime is committed every 6 seconds in the UK
- 3.6 million cases of fraud and 2 million computer misuse offences were recorded in 2016
- There was 20,088 reported cases of online fraud in 2016, totalling £101.8 million in the UK

- Payment card fraud makes up 80% of 2016 financial fraud losses
- Fraud losses on UK-issued cards has risen by 29% from £479 million in 2014 to £618 million in 2016
- Cheque fraud valued at £13.7 million in 2016, down by 28%

- Banks have managed to stop £6.40 in every £10 targeted in 2016
- General Data Protection Regulation (GDPR) is being implemented in May 2018. Non compliance can result in fines of up to 4% turnover
- £1.9 billion investment by the government by 2021 to protect the UK against cyber attacks

Source: FinancialFraudAction:FraudFacts 2017, The paypapers, Ipsos Mori/UK Govt research 2017 , Aiginternattional.com/Cyber and Cybersecurity Ventures 2017

Types of Fraud

Understanding the different types of fraud will help you keep one step ahead

Social Engineering

Your staff are one of your best fraud defences. They are capable of spotting and stopping a whole variety of criminal attempts, but they also have potential to be one of the weakest links in your security. Criminals exploit our natural tendency to trust and use this to manipulate people into providing confidential information or complete an action. This approach of targeting people is known as social engineering. Frauds and scams are not always complex, sometimes a simple email or phone call is all it takes.

Phishing Emails

The sender usually impersonates well known businesses or government departments. They are designed to entice or scare you into clicking on a link or opening an attachment. Phishing emails usually contain malicious software, so being able to spot them is important to keeping your business safe.

Spot the fraud

- The email is unexpected and asks you to click on a link or open an attachment
- The offer is too good to be true or is time sensitive putting you under pressure to act quickly

Vishing (Telephone fraud)

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 utility companies).

Spot the fraud

- 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 Smart-Card codes. Or follow instructions for you to key a test payment, reverse or cancel a transaction

Smishing (Text Fraud)

This is where a fraudster sends a text message pretending to from your bank. The message may say that there is a problem with your account and usually has sense of urgency to it asking you to take some action, usually clicking on a link or calling a number provided.

Spot the Fraud

- Fraudsters are able to make fake messages appear in the same text chain as a genuine one which make these messages really tough to spot
- Forward any suspicious messages mentioning Royal Bank of Scotland to 88355
- Do not text back or reply STOP to the messages
- Do not call the number. Always contact the bank using a number you know and trust

Impersonation (Bogus Boss)

Anyone can be impersonated. The amount of information available online through social media and websites helps criminals be even more convincing when they send emails impersonating senior management, staff, customers and suppliers.

Spot the fraud

- Urgent or unusual emails asking you to make a payment
- The email address has characters added or removed. It can be tricky to spot multiples of lower case l and i, so check carefully
- Look out for the email address changing when you hover over it, or when you look at its properties
- It's not just requests for payments to be made. Data about your customers, staff and intellectual property is valuable to your business and criminals too

Reducing the threat

- Have regular fraud and cybercrime awareness training and refreshers for all staff so they know what to look for
- Slow down. Don't be put under pressure to make an urgent decision. Look at takefive-stopfraud.org.uk for further information
- Know what information is out there in the public domain about you and where you work. Criminals use information easily found on the internet to make their communication more convincing
- Be alert to unsolicited emails and avoid clicking on links or attachments from unknown sources
- Consider ethical phishing campaigns to see how good your staff are at spotting them
- Increase your cyber safety with Cyber Essentials and Cyber Essentials Plus https://cyberessentials.ncsc.gov.uk
- Share the Bogus Boss video and leaflet with your staff. It can be found here: https://www.youtube.com/watch?v=aJP-7SvA9WA
- Share the Vishing video and leaflet with your staff. It can be found here: https://www.youtube.com/watch?v=ZBBYkTRycy4 **Do not disclose confidential banking information over the phone**

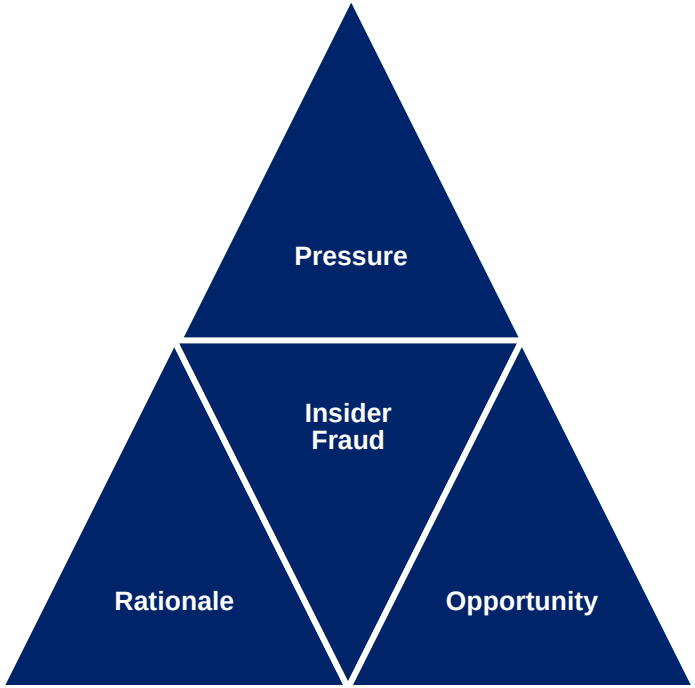
Insider Fraud

Insider fraud

This is also called employee or internal fraud and is when a person within your company commits a fraud against it. Insider fraud often starts with small amounts of money being taken. If these go undetected, the value taken may increase as the person gains in confidence. Because employees have the advantage of knowing how the business works to allow them to hide their tracks, it often takes several months or years before the fraud is discovered.

Insider fraud cases often feature the three elements below:

- **Pressure:** can be driven by financial difficulties, addictions, trying to maintain a certain standard of living or organised crime involvement. These can motivate or pressure the employee to commit fraud
- **Rationale:** employees convince themselves what they are doing is justified. For example staff thinking they aren't paid enough or that the company can afford it
- **Opportunity:** an employee sees an opportunity and takes it. The opportunity can often occur as a result of lack of internal controls and processes, access to financial systems provided when it's not needed and an abuse of authority



Spot the fraud

- Be alert to employees having financial difficulties, changes in their behaviour, lifestyle or performance
- Employees who are reluctant to take holidays
- People always staying late or being the first in
- New member of staff who resigns shortly after joining
- Customer complaints about missing documents
- Suppliers who insist on dealing with the same employee

Protect your business

- Ensure robust pre & post employment screening processes are followed. Validate the employees right to work, qualifications, references and criminal record
- Make sure there is clear segregation of duties, especially for staff dealing with payments (consider dual authorisation)
- Regularly reconcile bank statements & other accounts
- Restrict and monitor access to sensitive information
- Have a robust annual leave policy in place. Reluctance to take leave could be a fraud indicator
- Have a zero tolerance to fraud policy in place

Invoice Redirection and Change of Bank Details Requests

What is Invoice Redirection

- The fraudster makes contact via letter, email or telephone and asks for account details to be updated, with any payments going to the new account
- Fraudsters will spend time and effort identifying key relationships between businesses. They will use information in the public domain such as what is available on an internet search combined with social engineering techniques to get the information that they need to commit this fraud

How does the fraud happen

- Having changed the beneficiary details to those requested, your next payment will be unknowingly sent to a fraudulent account, rather than the intended beneficiary. Typically the delay in identifying non receipt of payment and the cause, significantly impacts the ability to recover funds, and can have severe impact on the buyer / seller relationship and financial position.

Changing Bank Details

- Changes that are being implemented in the UK Financial sector to separate everyday banking services from investment banking. This change is to protect the industry from the type of financial crisis seen in 2008 and as is known as “Ring-Fencing”
- Ring-fencing may result in some companies being provided with new account details by their bank. Fraudsters may use this as an opportunity to send in fraudulent change of bank detail requests hoping that they will go unnoticed amongst other genuine requests
- Always verify any change of bank details request prior to making any amendments to your records. Use a number you know and trust to contact the business, or source for a number independently

Protect your business

- Share the Invoice video with your staff. It can be found here: https://www.youtube/dNG8A-P23bY
- Always verify any changes to bank account details using contact information that you already hold on file, or that your have sourced independently. Don’t rely on any contact details with the request as the fraudster may have altered these too
- Make sure that you verify the change of details prior to updating your system and making a payment
- If a response is sent in the post, check the quality and clarity of the printing. Compare it with a previous invoice that you know is genuine. Written instructions, company logos and the signatures of key personnel to ‘authorise’ the instruction may be easily obtained from the internet
- Segregation of duties- requiring more than one person to approve and pay invoices reduces the risk of internal fraud

Payments - Cheque Fraud

Fighting Cheque Fraud

Overview

The number of cheques being used has declined in favour of electronic payment systems like CHAPS, BACS or Faster Payments. Such systems have the added benefit of inherent additional security and anti-fraud measures absent in cheque payment methods.

Cheques are valuable and lack of care or attention in how they are stored and written, either by hand or computer printed, can lead to misuse by fraudsters and potentially cause financial loss. Cheque fraud has become more 'organised: as advances in computer and printing technology, coupled with the relatively low cost of equipment, mean that the fraudster can now target almost any cheque written.

When writing cheques

- Begin writing/printing at the very left of the cheque
- Draw a line through unused space on the cheque so unauthorised people cannot add extra details
- Do not leave large spaces between words and rule out the space not used after the words in each line
- Do not leave space between the "£" sign and the amount inserted in the figures box and again rule out any space not used after the amounts

Remember to:

- Always keep cheques in a secure place
- Compare underlying paperwork with all cheques written
- Use cheques in serial number order
- Ensure all cheques remain in the book and none are removed from the middle or towards the back
- Always account for spoiled cheques and destroy if appropriate
- Reconcile bank statements upon receipt and report anything unusual

Non Standard Printed Cheques

There are stringent anti-fraud and other industry standards that must be incorporated in all cheque designs for which the bank can provide full guidelines.

It's a Scam

You receive a cheque for far too much money and are asked to send the balance back to the drawer by CHAPS or Faster Payments on online transfer. Be aware as the chances are you could end up with a bounced cheque and a debit to your account!

Payments - Plastic Card Fraud: Merchant Services

Customers are the front line against card fraud, which can result in a double theft: against the genuine card holder and against the company. Together, Royal Bank of Scotland and the payment industry are working to fight fraud and safeguard your money.

Plastic Card Fraud

Cardholder present Chip and PIN transactions

- Follow the prompts on your terminal
- Ask the cardholder to enter their pin
- If a Chip and PIN card is not processed correctly when the customer is present, for example swiping the magnetic stripe or manually keying the card, you may be held liable for the transactions in the event it is later confirmed to be fraudulent

Note: Not all cards in circulation have chip technology. If the card is not Chip & PIN enabled, you should take the opportunity to check security features such as holograms, logos and signature strip, as you have sight of the card.

Security Checks

- Be alert to customers seeming to make indiscriminate purchases, especially if the goods can be re-sold
- Be alert to customers buying low-value items using debit cards and asking for the maximum cash back
- Check that the title on the card matches the person presenting it
- Look for any tampering of the signature strip
- Be aware of cards that have been signed in felt tip pen, as this may be an attempt to cover genuine signature

Be wary of:

- A customer who provides several cards for payment after the initial and any subsequent authorisation requests have been declined

Remember

Make a ‘code 10’ authorisation call if you are suspicious about the card holder or presenter.

This will allow you to discreetly check on a suspicious card or cardholder when they are nearby and you’re not able to talk freely.

Cardholder not present transactions

- Present a higher risk to your business, because there is no opportunity to physically check the card or meet the cardholders

Protect your business:

- Ensure that your terminal has both address verification service and card security code checking function enabled
- Call back cardholders using independently obtained or verified land line numbers
- Goods should be delivered to the cardholder’s address and never released to third party
- If you accept card payments via the internet then consider using the MasterCard Securecode and Verified by Visa solutions which assist in making Cardholder Not Present transactions safer from the threat of fraud

Be wary of

- A new customer placing a large order and who appears disinterested in the price/detailed description of goods
- A customer who hesitates when asked technical questions about the goods they are purchasing
- A customer who offers more than one card as payment for order – this is against the scheme rules

Fees and charges apply. Please speak to your Relationship Manager for more details.

Payments - Plastic Card Fraud: Using your card

Plastic Card Fraud

Cardholder Not Present (CNP)

Where your card itself was not physically presented at the point of sale, however your card details (such as the 16 digit number and expiry date) were used. Typically, these will be internet or mail/telephone orders - 'remote' purchases. Your card details may have been compromised for example, after previous use or via phishing emails/scams.

Protecting yourself

- Ensure your device & internet connection is safe, secure and that you are using a trusted retailer
- When transacting over the phone, ensure that you cannot be overheard.
- Never share or allow your card/PIN details to be written down, emailed or faxed– including to friends, colleagues, the bank or police
- 'https' should be visible in the web address in addition to a locked padlock symbol when submitting card details online. If these are not visible, your card details may not be protected

Best Practice Guidelines

- Frequently review statements & reconcile transactions
- Ensure your contact details are up-to-date on bank records
- Do not let your card out of your sight when transacting & keep it stored safely when not in use
- Your PIN is your PIN, we would suggest not keying it into a phone, writing it down or sharing it – not even with the police, your friends, colleagues or bank staff
- If your card nears its expiry date, notify us if your new card does not arrive when expected
- Sign your card as soon as you receive it
- When using your Card & PIN, be wary of shoulder surfers and distraction

Contactless

- Contactless transactions have the same protection as chip & PIN payments, making them safer than cash. Contactless cards are also embedded with multiple layers of security to protect you against fraud
- Contactless only works when a card is within a few centimetres of the terminal, making it highly unlikely for any details to be intercepted while in use. Any data obtainable from a contactless card is visible on the front of the card and would be of limited use to a fraudster. The visible details could not be used to make a cloned card
- For added protection from fraud, you will also be asked to enter your PIN to verify a transaction from time to time

Contactless Terminals

Contactless payments can be operated seamlessly alongside your existing terminals and other ways of taking payments, whether by cash, cheque or card

Risk reduction

As with all card payments, the risks to the retailer are lower than other payment types for a number of reasons:

- Existence of an audit trail
- Assured payment
- Risk managed by the card/device – for the majority of transactions, the decision-making process will be between the card or device and the terminal

Fees and charges apply. Please speak to your Relationship Manager for more details.

UK Domestic Payment Products

Bacs Credit

Security and control over payment submission

- Customers who are direct submitters use smart cards to authorise payments
- Minimum of 2 party security contacts must be set up and it's they who control and set up additional contacts and their privileges
- Customers who are indirect submitters, this will vary depending on the set up they have chosen with their Bacs provider

Ability to recall once submitted

- Once a Bacs Credit file has been submitted it can be recalled up to 12:00 on Day 2 of the Bacs 3 day processing cycle

Recovery of misdirected funds

- Payments are submitted in files, firstly a Bacs trace must be performed to verify the beneficiary
- Once known, the Credit Payment Recovery (CPR) process is used to recover funds
- CPR is used for payments over GBP15 made in error within past 36 months
- Beneficiary must consent to the funds being taken back before action can be taken. When the bank has made an error, the funds are immediately returned once due diligence has been performed

CHAPS

Security and control over payment submission

- Customers who submit CHAPS payments on Bankline have a choice of sole or dual authorisation
- You can set different user access rights and privileges
- Bankline offers a comprehensive audit trail of user activity

Ability to recall once submitted

- Payments can not be recalled once submitted
- CHAPS submitted up to 180 days in advance on Bankline can be amended/cancelled up to 16:00 the day before the payment is due to be sent

Recovery of misdirected funds

The new CHAPS rules explain that:

- The beneficiary bank whose customer has received funds in error is only allowed to debit their customer's account with the customer's permission
- If the customer disputes that the payment was made in error, the beneficiary bank is able to provide the customer's contact details to the sender of the payment (and/or their sending bank)
- When the bank has made an error, the funds are immediately returned once due diligence has been performed

Faster Payments

Security and control over payment submission

- Customers submitting Faster Payments on Bankline have a choice of sole or dual authorisation
- You can set different user access rights and privileges
- Bankline offers a comprehensive audit trail of user activity

Ability to recall once submitted

- Immediate Faster Payments can not be recalled once submitted
- Faster Payments submitted up to 180 days in advance on Bankline can be amended/cancelled up to 16:00 the day before the payment is due to be sent

Recovery of misdirected funds

- The Credit Payment Recovery (CPR) process should be used to recover the misdirected funds
- CPR is used for values over GBP15 made in error within the last 36 months
- Beneficiary must consent to the funds being taken back before action can be taken. When the bank has made an error, the funds are immediately returned once due diligence has been performed

Fees and charges apply. Please speak to your Relationship Manager for more details.

Malware and Ransomware

Malicious Software (Malware)

Overview

- Malware is a name given to malicious software which is designed to do harm to computers and mobile devices. Malware is typically distributed through clicking on links or attachments in phishing emails, compromised websites and ad banners.

How to protect your business

- Ensure your browser, operating system, firewall and anti-virus/anti-malware software are up-to-date and you run regular scans of the system
- Avoid clicking on links or opening attachments from unknown sources
- Take care when connecting USB devices and CDs/DVDs as they are common carriers of malware
- Take care if using public WIFI - avoid logging on to your secure website i.e., internet banking

Ransomware

Overview

- Encrypts data or restricts access on compromised devices before demanding a ransom be paid
- Often disguised as an attachment in an email or delivered to the victim through an exposed software vulnerability, ransomware will infect files, drives and networks at great speed
- The infected computer receives a message (or even a phone call) offering to decrypt the now inaccessible files or information in return for payment – usually in the form of an untraceable bitcoin

How to protect your business

- Regularly back up your files to a different storage device
- Ensure your browser, operating system, firewall and anti-virus/malware software are up-to-date and you run regular scans of the system
- Avoid clicking on links or opening attachments from unknown sources

Keep your computer secure

- Install a firewall and employ up-to-date antivirus software
- Keep your computer's operating system and web browser up to date with the latest security patches and regularly update other key software that interacts with the internet such as media players, PDF readers and Java applications
- Use a web browser that has been obtained from a reputable website. Some web browsers offer added security to help protect you from phishing attacks and spyware

Protecting your business

How to protect your business when using our channels

Bankline

Bankline

Overview

- If you are a Bankline customer, use the dual authorisation feature which enhances security by ensuring that two individual Bankline users have to authorise payments

How to protect your business

- All Bankline users must keep their security credentials (for example, PINs, passwords, smartcard challenge & response codes) secret, and ensure they are not shared with any other persons, either within or outside the company.
- Firewalls and anti-virus software must be applied to all of the PCs which are used to access Bankline, and these controls must be kept fully up to date. Your browser, operating system and key software applications should also be updated regularly with the manufacturer's latest security patches.
- We would suggest that you have the PCs which are used to access Bankline checked on a regular basis by an IT professional, and where appropriate, arrange for them to be fully cleaned to remove any malware.
- You should never open email attachments or click on links within the email if you are unsure about the content or the legitimacy of the sender. Attachments in ZIP or EXE file formats are often used to spread virus and malware infections.
- When logging in, signs that a virus may be present include the slow loading of screens, and changes to the regular appearance or content of the log-in screens themselves.
- We would strongly advise that you regularly check the payments, including the payee bank account numbers and sort codes that have been keyed through your Bankline user profile, as quick identification of any fraudulent activity is essential.
- Always read Bankline Broadcast Messages for the latest news concerning fraud and security threats.

For further information, please visit the Bankline Security Centre at:
https://www.business.rbs.co.uk/business/bankline/bankline-security-centre.html

Bankline Security Action

- We will never ask for your full PIN and password online – only 3 random digits are required
- We will never ask for smartcard codes to login or change your PIN and passwords – these codes are used to authorise payments and should not be shared
- We will never ask you to make test payments
- We will never ask you to download software such as TeamViewer, which allows another person to take control of your PC remotely
- Genuine bank staff will never ask you to provide details of your Bankline PIN, password or smartcard challenge & response codes over the telephone in any circumstances. You should be suspicious of any telephone calls requesting such details. End such calls immediately and report the incident to us, but use a different telephone handset because the fraudster may try to keep the line open and intercept your call.
- Be aware of Fraudsters calling Bankline users claiming to be from your ISP, stating there is a technical problem with your router or equipment. They ask you to download software, log on to Bankline and pay a small fee for technical support
- If you're concerned about your Bankline security or concerned about fraudulent activity, please call the Bankline Security Centre on 0345 300 8483

Fees and charges apply. Please speak to your Relationship Manager for more details.

Protecting your business

Bankline Direct

Bankline Direct

Overview

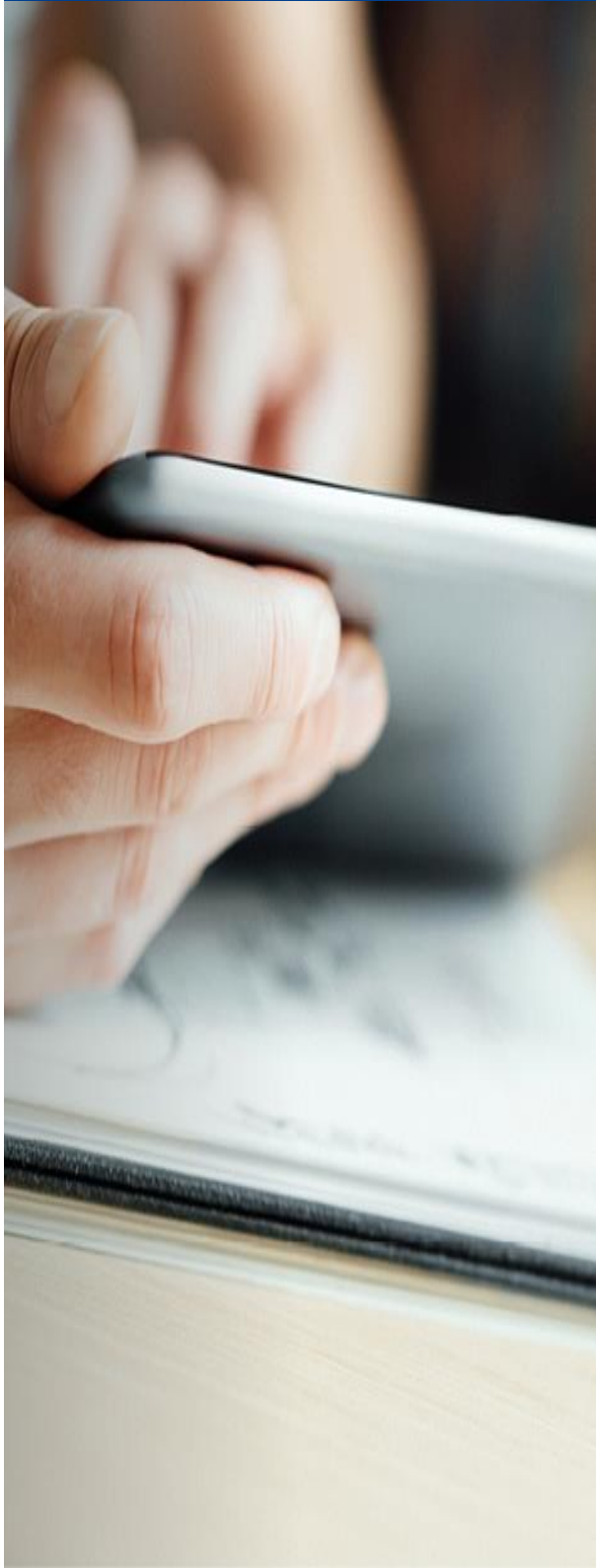
- Bankline Direct offers customers a secure, integrated channel for exchange of payment and reporting files
- Robust security is provided via secure network protocols and additional digital signing

How to protect your business

- **Secure connectivity**. We offer a range of file and message based connectivity solutions, which are designed to integrate with our customers systems. These include;
  - **Internet** connections for the transmission of files, such as Secure File Transfer Protocol (SFTP) and Connect:Direct Secure +
  - **SWIFTNet** connections for the transmission of files (SWIFTNet FileAct) and individual messages (SWIFTNet Fin)
- **Additional Security**. We offer additional security features to help keep you safe. The digital signing options include;
  - **Pretty Good Privacy (PGP)** uses public key cryptography, where 2 complementary keys, public and private, are used to secure files during communication
  - **XML X509** – The XML-signature syntax associates the content of resources listed in a manifest with a key via a strong one-way transformation
  - **Hardware Security Module (HSM)** a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto-processing

Bankline Security Action

- We will never ask for your full PIN and password online – only 3 random digits are required
- We will never ask for smartcard codes to login or change your PIN and passwords – these codes are used to authorise payments and should not be shared
- We will never ask for details of your PIN and password, or any smartcard codes over the telephone - Genuine bank staff will never ask you to provide details of your Bankline PIN, password or smartcard challenge & response codes over the telephone in any circumstances. You should be suspicious of any telephone calls requesting such details. End such calls immediately and report the incident to us, but use a different telephone handset because the fraudster may try to keep the line open and intercept your call.
- Be aware of Fraudsters calling Bankline users claiming to be from your ISP, stating there is a technical problem with your router or equipment. They ask you to download software, log on to Bankline and pay a small fee for technical support
- If you're concerned about your Bankline security or concerned about fraudulent activity, please call the Bankline Security Centre on 0345 300 8483



If you are an Online and Mobile Banking customer, you can visit the following websites for ways to protect your business when using these services

Mobile App: https://personal.rbs.co.uk/personal/ways-to-bank/mobile-app/security.html
App available to customers with Digital Banking and a UK or international mobile number in specific countries

Online Banking: https://www.business.rbs.co.uk/business/rbs-business-bankingsupportcentre/fraud-and-security-advice/online-security.html
Digital Banking available to customers aged 11+ with a Royal Bank of Scotland account

Royal Bank of Scotland

Fees and charges apply. Please speak to your Relationship Manager for more details.

Support

How we can provide tips on improving your cyber security

10 Steps to better Cyber Security

As the threat of cyber attack on your business increases, and as the type and nature of such attacks shifts, it may be tempting to add keeping your business safe to the “too difficult to do” pile. But creating a secure working environment, where the risk of an attack is minimised, is possible if you follow these key steps:

Identify a responsible individual

Select a team member who will be able to keep tabs on cyber security. They should be aware of any business functions that have a digital element (these days, there are few that don’t), know where the most important data is kept, and be able to identify the major risks that have the potential to wreak havoc on the business.

Where is data on customers kept, for example? Is this data regularly backed up offline? How many staff work remotely and how safe are those systems? The person in charge of cyber security can create a system of checks and balances and decide how frequently safety assessments are carried out.

Protect your network

While it’s essential to establish a secure perimeter, threats don’t always come from outside the business. A firewall – software that analyses communications entering your network – can stop staff accessing sites that might pose security risks.

Many internet service providers (ISPs) offer a built-in firewall, but it’s a good idea to shop around and see what other options are available.

Keep everything up to date

Software and operating systems often update automatically, fixing bugs in the system and improving security. Switching off automatic updates can compromise computers and smartphones. For example, the WannaCry ransomware attack that took place in May 2017 was reportedly caused in part by large organisations not updating their operating systems.

Use passwords for sensitive documents

Protecting individual documents can be a hassle, but it provides an additional level of security if your firewall should fail, and also offers some protection against human error. But remember to use a proper password protocol and not the same one for all your documents. Update passwords regularly and be disciplined about who details are shared with, although it’s important for a select number of staff to have access to everything, so holidays and sick leave don’t negatively impact the business.

Most operating systems have security options, or – if the documents are very important – it may be best to invest in specialist encryption software.

Protect against viruses

Malicious software, also known as malware, includes viruses, so-called Trojan horses and spyware. Anti-virus software can protect against these. As viruses are frequently adapted and altered by cyber criminals, it’s crucial to make sure that software updates are installed.

Source: http://rbs.contentlive.co.uk

Maintain security beyond the office

With remote working increasingly common, remember that anywhere staff might work becomes an extension of your workplace and security needs to be maintained at the same level. Your network is only as strong as its weakest point, so educate staff on the importance of following protocol on devices they use for work. This might be easier to do if the company owns all the devices used on its network. If you can’t afford to provide them, at least approve each device that’s used for work.

Any device must have appropriate anti-virus software, password protection and firewall software installed. The ability to wipe the device remotely if it’s lost or stolen is also possible (this is a feature on some email servers, for example), but the right software needs to be installed in the first place.

It’s especially important for mobile workers to be aware of the dangers of connecting to unencrypted, public wifi, because these hotspots are more vulnerable to hackers who can intercept data. Set out clear guidance for staff and make sure they understand the need to check that any hotspots are genuine before using them and make sure file-sharing is off and firewall is on.

Check all disks and drives

Mobile devices are a potential source of viruses, as are any disks and USB drives, which can transfer malware. If these items are used on shared, public computers or employees’ home computers, the risk of transferring a virus to the office increases further.

Keep a record of anyone using removable hardware, and use anti-malware software to scan disks and drives when they are returned to the office. Have a clear policy on bring your own device (BYOD) and make sure staff are aware of the rules.

Anticipate the worst

It’s useful to know all the areas of business activity that could be affected by an attack, from serving customers to processing payroll. Firewall software should be configured to indicate if something unusual is happening.

Have a specialist on call in case of emergency, and formulate a plan for contacting customers, clients and suppliers – anyone who needs to know that your network has been compromised.

It’s a good idea to rehearse this, so that staff members know how to respond and what they are responsible for. It will also help to reduce the stress of the situation.

Educate staff

People, as with many areas of business, are the frontline defence for your business. Systems only respond to how they are used by staff. Explain to your staff the threat that cyber security poses and how crucial it is to maintain best practices, such as creating secure passwords and not being too open on social media about how the company operates. Employees should be continually reminded of the risks of cybercrime, such as open Wi-Fi networks in cafes.

Keep records

Maintain good records offline as well as online (in case of a security breach) of all digital devices used to access the business’s server or with company files. Being able to refer to a document that lists all the tests that have been made and what software is in use will be useful if you need to communicate any problems to an IT expert.

How we can help

Protecting our customers

Royal Bank of Scotland takes its duty of care towards its customers very seriously, and has invested significant sums to help prevent cybercrime

- For example, we have built multiple layers of security into Bankline, our online banking platform for larger businesses, working with cutting edge technology and the most innovative vendors to protect our customer's financial assets and confidential banking data
- We regularly cascade fraud intelligence via the Bankline Broadcast Message facility and the bank's social media channels, so that our customers are informed of the latest threats and evolving risks
- The bank delivers seminars and webinars on how on preventing cybercrime – these sessions were attended by over 11,000 customers in 2017 and a broad range of collateral including videos and brochures are available to keep the topic front of mind. Indeed, informed businesses are much less likely to be victims of cybercrime

Useful references

National Cyber Security Centre
www.ncsc.gov.uk
Financial Fraud Action
www.financialfraudaction.org.uk
Get Safe Online
www.getsafeonline.org
Visit our Security Centre on
www.rbs.co.uk
IBM Trusteer Support
www.trusteer.com/ProtectYourMoney
Visit our Dedicated Bankline pages
https://www.business.rbs.co.uk/business/bankline/bankline-security-centre.html

What if I'm a victim of fraud?

If you think you're been a victim of fraud – report it to the bank immediately!
If you suspect fraudulent activity on Bankline call
0800 161 5157
Opening Times: Monday – Friday 7am-8pm
Royal Bank of Scotland Digital Banking customers call us on
0800 161 5154
Opening Times: Monday – Friday 8am-8pm, Saturday 8am-6pm, Sunday 9am-5pm
Credit Card Fraud (Commercial Customers) call us on
0845 300 4351
For all other fraud Royal Bank of Scotland customers can call us on
0800 161 5151
Report suspicious emails
phishing@rbs.co.uk
Reporting a suspicious text message, forward it to 88355
Action Fraud
www.actionfraud.police.uk
0300 123 2040

Video and paper awareness

Vishing
https://youtube/p0kP-jR0JYg
Bogus Boss
https://m.youtube.com/watch?v=yzLOvPPkT-k
Invoice Redirection
https://youtube/dNG8A-P23bY
CIFAS Data to GO
https://www.youtube.com/watch?v=sq-0tjv4_BA&t=2s
10 ways to stay safe
http://rbs.contentlive.co.uk/content/637d57d1-da7e-99ec-9246-3aa97d2ddf56
Seven biggest threats to your business
http://rbs.contentlive.co.uk/content/5822132a-271c-964c-bbeb-a027ffbce8b1
10 steps to better cyber security
http://rbs.contentlive.co.uk/content/aaba2ca6-a56b-9833-908a-8b4f478bfd4e

Disclaimer

Fees and charges apply. Please speak to your Relationship Manager for more details.

This document has been prepared by The Royal Bank of Scotland plc or an affiliated entity ("RBS") exclusively for internal consideration by the recipient (the "Recipient" or "you") for information purposes only. Following any guidance in this document may help reduce the risk of fraud but will not eliminate it or guarantee that the types of fraud described, or other fraud, will occur This document is incomplete without reference to, and should be viewed solely in conjunction with, any oral briefing provided by RBS. RBS and its affiliates, connected companies, employees or clients may have an interest in financial instruments of the type described in this document and/or in related financial instruments. Such interests may include dealing in, trading, holding or acting as market-maker in such instruments and may include providing banking, credit and other financial services to any company or issuer of securities or financial instruments referred to herein. RBS is not and shall not be obliged to update or correct any information contained in this document. This document is provided for discussion purposes only and its content should not be treated as advice of any kind. This document does not constitute an offer or invitation to enter into any engagement or transaction or an offer or invitation for the sale, purchase, exchange or transfer of any securities or a recommendation to enter into any transaction, and is not intended to form the basis of any investment decision. This material does not take into account the particular investment objectives, financial conditions, or needs of individual clients. RBS will not act and has not acted as your legal, tax, regulatory, accounting or investment adviser; nor does RBS owe any fiduciary duties to you in connection with this, and/or any related transaction and no reliance may be placed on RBS for investment advice or recommendations of any sort. Neither this document nor our analyses are, nor purport to be, appraisals or valuations of the assets, securities or business(es) of the Recipient or any transaction counterparty. RBS makes no representation, warranty, undertaking or assurance of any kind (express or implied) with respect to the adequacy, accuracy, completeness or reasonableness of this document, and disclaims all liability for any use you, your affiliates, connected companies, employees, or your advisers make of it. Any views expressed in this document (including statements or forecasts) constitute the judgment of RBS as of the date given and are subject to change without notice. RBS does not undertake to update this document or determine the accuracy or reasonableness of information or assumptions contained herein. RBS accepts no liability whatsoever for any direct, indirect or consequential losses (in contract, tort or otherwise) arising from the use of this material or reliance on the information contained herein. However, this shall not restrict, exclude or limit any duty or liability to any person under any applicable laws or regulations of any jurisdiction which may not be lawfully disclaimed. The information in this document is confidential and proprietary to RBS and is intended for use only by you and should not be reproduced, distributed or disclosed (in whole or in part) to any other person without our prior written consent.

The Royal Bank of Scotland plc. Registered in Scotland No. SC083026. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB. The Royal Bank of Scotland plc is authorised by the Prudential Regulation Authority, and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

National Westminster Bank Plc. Registered in England & Wales No. 929027. Registered Office: 250 Bishopsgate, London EC2M 4AA. National Westminster Bank Plc is authorised by the Prudential Regulation Authority, and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

The Royal Bank of Scotland plc and National Westminster Bank Plc are authorised to act as agent for each other.