

COMMERCIAL BANKING

---



## FRAUD GUIDANCE

---

Helping you protect your business



**LLOYDS BANK**

---

This guide gives you the information you need to help protect your business against this growing threat. We show you how and where fraud can take place throughout your organisation and highlight the telltale things to look out for. We've also included key actions you should take to safeguard yourself and your business. Taking some very basic steps can make a real difference to fraudsters' success rates.

---

# Contents

---

Cheque fraud	3
Card fraud	4
Online fraud	6
How to protect your business	9
Employee fraud	10
Virtual currencies	11
Scams	12

---

The background of the entire page is a photograph of two large satellite dishes. The dishes are silhouetted against a bright, colorful sky at sunset or sunrise, with hues of orange, yellow, and blue. The dishes are positioned on the left and right sides of the frame, with their intricate metal structures clearly visible. The sky is filled with soft, wispy clouds, and the overall atmosphere is serene and technological.

Over 40%

The number of businesses in the UK that have experienced fraud in the last year.

---

# Cheque fraud

---

## Using cheques illegally to acquire funds

---

### 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 cheque books, 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.

### How to protect your business

Follow these steps to issuing your cheques safely:

- Cross through spaces on cheques you issue, after the payee name and amounts.
- Always use a black or blue ballpoint or a pen with indelible ink and apply more pressure than normal, to make the writing difficult to remove.
- Write payee names in full e.g. "British Broadcasting Corporation" rather than "BBC".
- If you use boxed cheques, enter ZERO rather than NIL, which can be changed to NINE.
- If you issue cheques using a laser printer, use one recommended for cheques.

---

### Is a cheque the best way to pay?

Online payments, BACS, CHAPS can be faster.

---

### Cheque Best Practice

**Reconcile cheque payments** to statements and report inaccuracies immediately.

---

**Keep cheque books secure.**

---

**If you are expecting a new cheque book**, contact us as soon as possible if it does not arrive.

---

Look out for cheques that have been **removed from the middle or back** of your cheque book.

---

Make sure cheques can't easily be **recognised in the post.**

---

Another common scam for fraudsters is to overpay using a cheque and then request a refund before the cheque has been cleared.

The cheque issued to you is then returned unpaid.

- Confirm the cheque has definitely been "paid" and that the funds are cleared in your account before releasing goods or returning any funds.
- Don't accept cheques made payable for a higher value than you were expecting.

For further guidance on cheque fraud, visit **[www.actionfraud.police.uk](http://www.actionfraud.police.uk)**

---

# Card fraud

---

## Misusing personal information from credit, debit or store cards

---

### How can you protect your business?

- Ensure you are the only person that knows your PIN – banks or the police will never ask for it.
- You can arrange to collect valuable items such as new plastic cards or cheque books from a local branch if other people have access to your mail.
- 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 you deal with straightaway. Ask the Royal Mail to redirect your post for at least a year.
- If you suspect your mail is being stolen or interfered with contact the Royal Mail Customer Enquiry Line on **08457 740 740**.

### Travelling overseas

Take your card company's 24-hour contact number with you.

### On the Internet

- Protect your PC with the latest firewall browser and Anti-virus software.
- Look for the padlock symbol when buying online – it shows the information you input will be encrypted.
- Always log out properly after shopping.

### Prevent ID Theft

Keep important personal documents, plastic cards and cheque books in a safe place. Don't share personal information unless you are confident you know who you are dealing with.

### Cash Machines

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.

### Mail and Phone

- Never leave your card or card details lying around or keep your card and PIN together.
- Never let anyone else use your card and never send a supplier a copy of the front or back of your card.
- Only make telephone transactions if you have instigated the call and are familiar with the company.

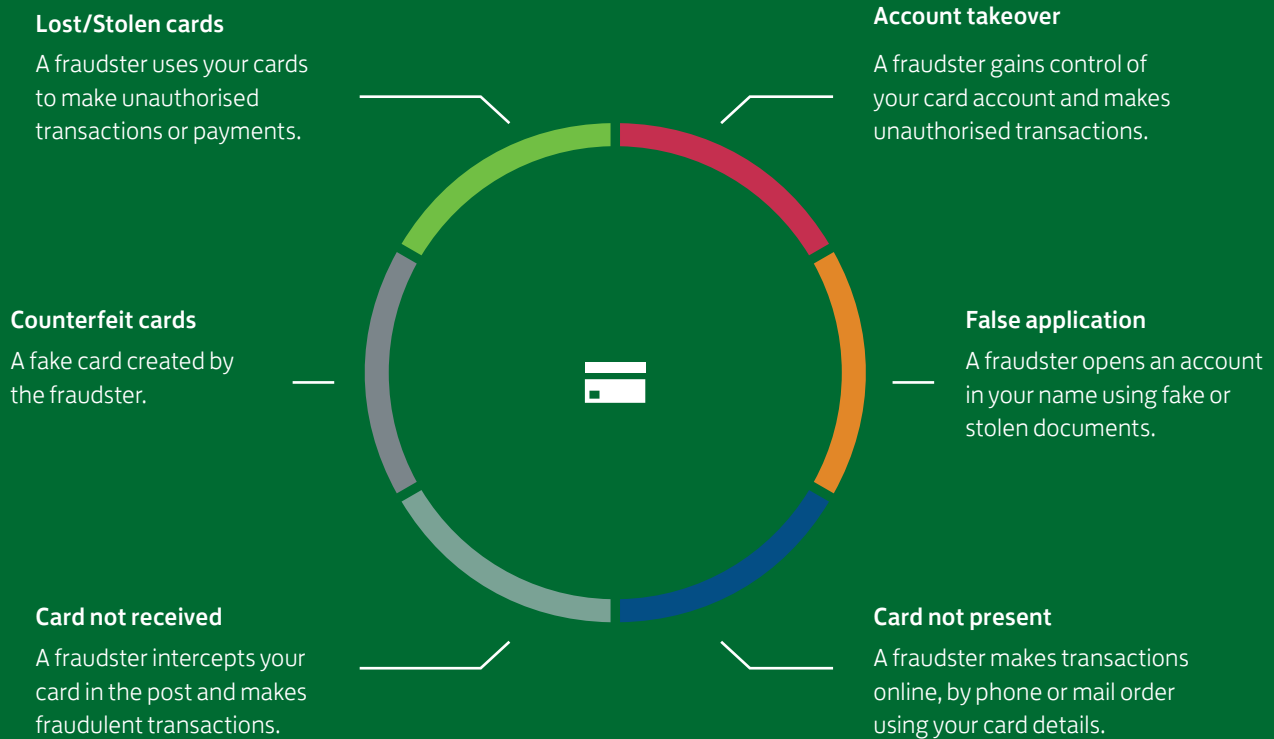
---

For more guidance on credit and debit card fraud visit the Action Fraud website at [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

---

---

## Common types of fraud



---

# Online fraud

---

## Crimes on the Internet

---

### What does it look like?

#### Vishing

Telephone scams, usually to obtain online banking passwords confidential details or persuade you to move money. Fraudsters will call you to report a problem with your account, and ask you to call back on an official number, say from your bank statement. By holding the line open until you call back, they convince you that you've reached the bank. They'll usually ask you to transfer funds to a 'safe' account under their control.

#### Spoofing

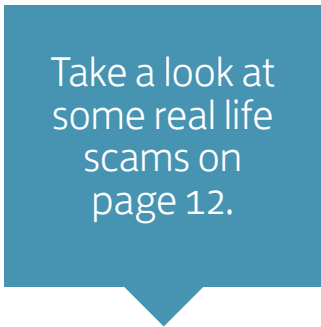
Spoofing is used to describe a fraudsters use of technology to imitate genuine telephone numbers and email addresses of financial institutions or other trusted people or organisations. This can allow them to alter the incoming number which appears on your phone's caller display, to one which you know 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.

#### Malware

Malicious software such as viruses and Trojans. Malware is often hidden in attachments and free downloads. It can 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. This information can be used by fraudsters to access your online accounts and make fraudulent payments.

#### Phishing

Email scams when fraudsters masquerade as your bank or other trusted organisation to obtain confidential information such as personal information, bank details or passwords. The email will usually link through to a fake website, which looks almost identical to the legitimate one. A message usually suggests that you need to act urgently, for example to prevent your online access from being blocked.



Take a look at  
some real life  
scams on  
page 12.



## Malware

10 warning signs that your computer might be infected and you should check for malware.

### 1 Slow running

Malware often slows down your operating system, your Internet speed or the speed of applications.

### 2 Pop ups

If unexpected pop ups appear on your computer screen, this could indicate a spyware infection.

### 3 Crashes

If your programmes crash regularly or you often experience what is known as “the blue screen of death” this could be a sign that your system is infected.

### 4 No available hard drive space

Many types of malicious software will use up the available storage space on your hard drive.

### 5 Unusual activity

Unusual messages appear or programmes start automatically.

### 6 New home page or browser

A new home page opens or different toolbars appear on your browser which opens unwanted websites or tabs.

### 7 Strange emails

Your friends and/or colleagues say that they have received strange messages or emails from you.

### 8 Your Antivirus solution becomes disabled

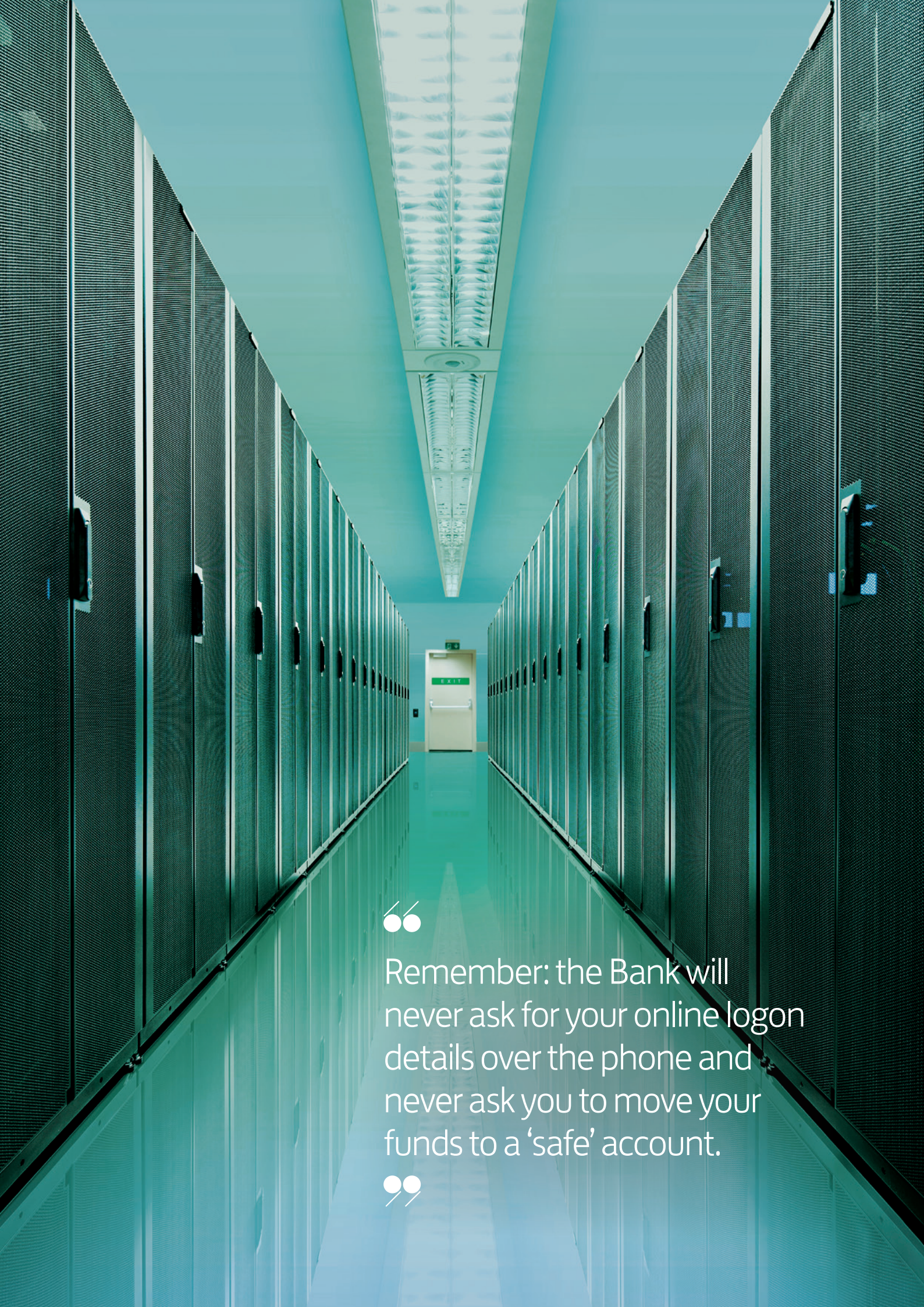
Your antivirus software doesn't appear to work anymore or the update module becomes disabled.

### 9 Higher than normal network activity

If a user is not connected to the Internet and no programmes are connected to online servers but a high network activity is found, check your computer for malware.

### 10 Suspicious hard drive activity

If you notice that your hard drive is more active than normal, even if it is not used any more, or there is no programme or download running at that moment, you should check your systems for malware.



“

Remember: the Bank will never ask for your online logon details over the phone and never ask you to move your funds to a 'safe' account.

”

---

# How to protect your business

---

## Be safe online

---

### Against vishing

If you're not certain it's the Bank calling, even if the number appearing in the caller display appears to be correct:

- Call back on a number that you know is correct from a different phone.
- If this is not possible ensure the phone line is clear first by waiting at least 5 minutes before calling back.
- Test the line by calling a friend or family member first.

**Never tell your online banking passwords to anyone.**

### Against malware

- Ensure all PCs are protected by high quality anti-virus and anti-spy software. Update it regularly and run frequent scans.
- Only download programmes to your PC from sources you trust.
- Make sure key staff are trained in fraud awareness.
- If possible provide a few designated workstations for use solely for processing bank transactions which are not allowed to be used for web browsing, email and all other activities that could bring malware onto the system.

### Against phishing

- Watch out for emails that are poorly worded, spelt badly or that begin with 'Dear valued customer' or similar. A genuine bank email will always contain your name.
- Hover over links within emails to see the true web address.
- Use a SPAM filter to remove unwanted emails and opt out of marketing emails on websites.
- Keep personal and business information stored online and on networking sites to a minimum.

### Key steps for safe online banking

- If you use a card and card reader, remove the card as soon as you've logged on and only re-insert to carry out a signing action.
- Check the detail for every payment you make thoroughly, in particular the beneficiary account number and if possible set up your system to require more than one individual to set up, amend and send each payment. Remove beneficiary details from your payment library, if you do not intend to make further payments to their account.
- Always log out correctly when you've finished online banking.
- Log out and call the bank immediately if you see unexpected screens or pop-ups, or if your PC runs unusually slowly.



---

**If you think you have been the victim of online fraud please contact us immediately.**

---

---

# Employee fraud

---

A growing risk to business

---

## How it works

Employee fraud has escalated recently across the UK. The most common example is when corrupt employees present cheques drawn on your business account for personal gain, usually forging signatures.

## How to protect your business

The costs of dealing with employee fraud are high and the chance of retrieving lost money is slim. So your priority should be a robust recruitment policy, aligned to your business type and risks, and a culture that minimises fraud opportunities.

### Steps to consider:

- Implement a robust recruitment process, including criminal record and character checks for applicants.
- Regularly review access to business bank accounts, telephony/Internet password security and check your bank statements thoroughly.
- 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.

## Help when you need it

If you fall victim to employee fraud please tell us. Your account manager can provide practical support including:

- Help to contain the extent of losses and recover stolen funds.
- Help to secure and protect the bank account and records.
- Support for internal and Police investigations.
- Financial support, advice and guidance.



WHERE TO FIND  
OUT MORE

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)  
[www.cyberstreetwise.com](http://www.cyberstreetwise.com)  
[www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)  
[www.getsafeonline.org](http://www.getsafeonline.org)

---

# Virtual currencies

---

## The risks of unregulated, digital money

---

### How do they work?

Virtual currencies, such as Bitcoins, are not legal tender; they are not recognised by a legal system as a valid way to meet a financial obligation. But they are often traded in online marketplaces or gaming communities and can be used to purchase real world products or exchanged for traditional currencies.

They have no central repository or single administrator but depend on a distributed system of trust. Individuals can obtain the currency through their own computing or manufacturing effort.

### What risks do they pose?

- As the use of virtual currencies is still a relatively recent concept in terms of wider usage, the precise nature of some of the threats resulting from crime are only just becoming known.
- Due to their decentralised nature and lack of regulation, virtual currencies are particularly attractive to fraudsters wanting to launder criminal funds.
- Organised fraudsters have manipulated virtual currency markets in order to lower the value, enabling them to purchase in bulk, before driving the value up, so they can sell them on for profit.



---

# Scams

---

## Take a look at real life fraud scenarios

---

### The fraudulent invoice scam

XYZ Building Plc\* regularly purchases materials from ABC Merchants.

A fraudster sent a letter to XYZ on what appeared to be ABC Merchant headed paper. It advised that ABC had changed their bank account, quoting a new sort code and account number for all future payments to be sent to.

XYZ amended ABC account details in their payment records held with their bank. When ABC sent the next monthly invoice of £60,000 for materials supplied, XYZ instructed their bank to send the payment.

The £60,000 was sent to the new account controlled by the fraudster. ABC contacted XYZ chasing non-payment, at which time the fraud was discovered and the funds long gone.

### The cheque overpayment scam

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 £62,000. They contact the client who says the overpayment is a processing error.

The new client asks for Alpha to return the extra £60,000 to a specific bank account. Alpha returns the £60,000 using online banking and dispatches the goods for the original £2K order.

A few days later Alpha realise that the £62,000 payment was actually a cheque paid in at a branch counter and has been returned unpaid. They've lost £60,000 in cash and £2,000 in goods. They contact the bank immediately for help. Luckily the stolen funds are still in the fraudsters account at another bank and a full recovery is made.

---

#### How to protect your business:

- Carry out a thorough review of existing processes for sending and receiving payments and ensure that there are strong authentication measures in place.
- Establish a single point of contact (SPOC) with each regular supplier.
- Confirm any requests to change payment details with your SPOC, calling them via their verified company switchboard number.

---

#### How to protect 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.
- Check with the bank if you need to know whether a cheque has been “paid” – one that has purely “cleared” can still be returned.

\* The business names used in these case studies have been changed, to protect the identity of genuine clients.

---

## The phishing scam

999 Doctors Surgery\*, receives an email from the Bank advising them of upcoming improvements to their online banking service, and asking 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 their details including confidential information that the screen asks for.

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

## The vishing scam

Farming Limited\* receive a phone call 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 advised to contact their Bank immediately using the telephone number from the back of their card, to secure their funds.

Farming Ltd call the number printed on their card. They are advised to move all funds (£350,000) to a ‘secure’ account, which they do following instructions.

The next day they contact the Bank and realise the call was not genuine. When Farming Ltd had phoned the number from their card, they had unknowingly continued the same call with the fraudster as the fraudster had kept the phone line open.

They had been tricked into sending £350k to an account at another bank under the fraudster’s control.

---

### How to protect your business:

- Genuine Bank emails will contain your name – be wary of anything that begins with ‘Dear valued customer’ or similar.
- We’ll never send an email asking you to enter log-on, account or personal details, or an email with a link to a page that requires this information.
- Hover over any links within emails, to see what the true web address is.

---

### How to protect your business:

- If you are not certain that it is the Bank calling, call the Bank back using a number known to be correct, preferably using a different phone line. Or wait at least 5 minutes before calling back, or call a friend or family member first to test the line.
- The Bank will never ask for your online log-in details on the phone and will never ask you to move money to a “safe” or “secure” account.
- Be wary of calls received seemingly from the Bank, at night or at weekends. Fraudsters know that businesses may not report their suspicions to the bank at these times.

---

## 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 [lloydsbank.com/business/contactus](https://lloydsbank.com/business/contactus)

---

## Find out more

---

 Go to [lloydsbank.com/business](https://lloydsbank.com/business)

 Or call us on 0800 056 0056  
Lines are open 7am–8pm Monday to Friday  
and 9am–2pm Saturday

 Visit your local branch

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 Text Relay (previously Typetalk) or if you would prefer to use a Textphone, please feel free to call us on 0845 601 6909 (lines open 7am–8pm Monday to Friday and 9am–2pm Saturdays).

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

---

### Important information

Lloyds Bank plc Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Telephone: **020 7626 1500**. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.



**LLOYDS BANK**

M60416 (12/14)