MONEY

Stop the Scams

Business Edition

Spot the signs of fraud to stay safe

Contents

- Fraud vs scam: what's the difference?
- How do scams work?
- How to spot a scam call, text or email
- Quiz: can you spot a scam?
- Scam types: spotting & avoiding them
- Top tips to stay safe
- Reporting



Kicking things off



Fraud continues to evolve, and the tactics used to target businesses are becoming increasingly sophisticated.

While we're constantly strengthening our systems to protect your organisation, **your teams remain the first line of defence, and we're here to support you every step of the way**.

To help your business (and yourself!) stay ahead of emerging threats, we've created this short guide outlining the key red flags to watch out for. Taking a moment to **Stop, Think & Check** before sharing information or authorising payments can make a significant difference in preventing fraud.

Let's get started.

Fraud vs scam

What's the difference?



A scam is where you make or approve a payment believing it is genuine.

What does this look like?

Someone calls pretending to be from Virgin Money. They might ask you to 're-authorise' or 'reverse' a payment.



Fraud is when criminals take money from your account without you knowing.

What does this look like?

Someone gets your credit or debit card details and uses them without your knowledge.

How do scams work?

Fraudsters can seem to know a lot about you. Here's how.

They prepare

The fraudsters get as much info about their potential victims as possible before they get in contact.

This makes them sound more legit.

This could be:

- A Google search or scanning business websites.
- Buying leaked data on the dark web.
- Scam call, text or email attempts where you might have unknowingly entered personal or banking information.

They get in touch

The fraudster usually calls and uses the info they've learned to trick you into doing something urgently.

This could be:

- Handing over one-time passcodes or activation codes.
- Transferring money to another account they claim is safe.
- Downloading remote access software, such as Any Desk.

Did you know?

Victims enter what we call a 'Hot State'. This is when a fraudster creates a sense of urgency to get you to do something without taking time to **Stop & Think.**

They've got enough to get into your bank account.

They use the info you share to contact you again. This time, they ask you to do something.

They convince you to approve payments.

A fraudster calls...

Fraudsters pretend to be from a trusted company, like your bank, HMRC or the police.

They pressure you into clicking on malicious links, moving money or sharing things like your PIN or password.

We will NEVER direct you to a website or live chat to resolve an issue with a payment.



What does it sound like?

"Hi, it's the fraud team from Virgin Money. We've noticed some strange activity on your account. **Your account is blocked but we can help resolve it!"**

"Hi, it's HMRC. You have an outstanding tax bill, which needs to be paid now. If you don't pay in time, there will be a **warrant out for your arrest.**"

What to do

- It's ok to hang up if something sounds dodgy.
- Call us back using the number on our secure website or call 159.
- Stay in control – don't be pressured into sending money, clicking on unknown links or sharing business details like your PIN or one - time passcode.
- Trust your instinct.

Did you know?

Fraudsters can 'spoof' phone numbers, so they look genuine.

Always be suspicious.

A fraudster emails...

Scam emails look real, so they can be hard to spot.

They either:

- ask you to click on links or download attachments.
- Impersonate a senior member of staff or supplier, asking for bank details to be changed or urgent payments to be sent.



They'll usually pressure you to act straightaway. Don't.

What does it look like?

BestBank

Dear valued customer of BestBank.

We have received notice that you have recently attempted to withdraw the following amount from your current account: £135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

`http://www.Bestbank.com/general/custverifyinfo.asp`

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
BestBank

What to do

- Be suspicious of emails even if they are from a company or person you know.
- Don't click on any links or download attachments.
- Double check payment changes/requests on a trusted number.
- Don't reply to the email and report it to your bank or **report.phishing@virginmoney.com**, then delete it.

Top tip

Check the sender address very carefully **and hover over links to check the real destination.**

A fraudster texts...

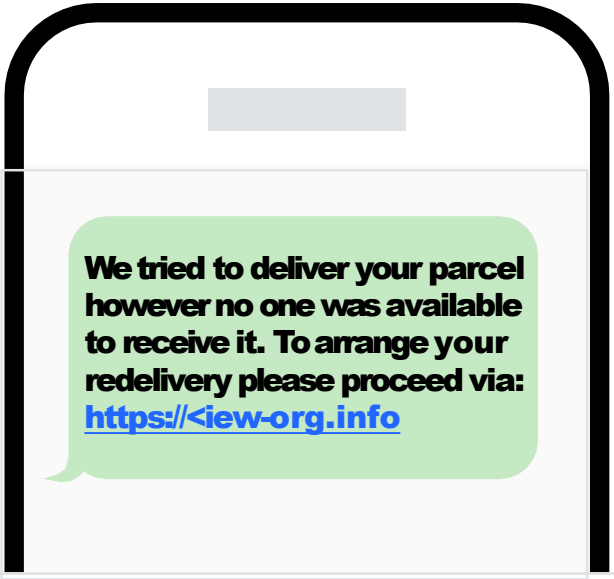
You get a text or WhatsApp message from a number you don't recognise. The text asks you to click on a link or call the number. **Don't do it.**

Fraudsters can 'spoof' phone numbers, so it looks real and might even appear in the same thread as a genuine message.

Always be cautious.



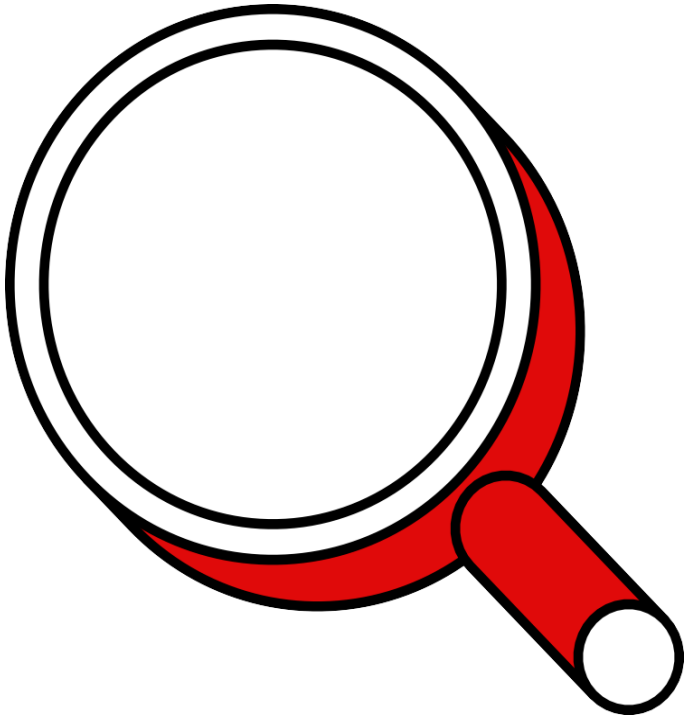
What does it look like?





What to do

- Be suspicious of texts from a number you don't recognise.
- Don't click on any links or attachments.
- Don't reply to the message or call the number. Call the organisation or person using a number you know is definitely theirs.



Quiz time

Let's head over to our industry partner, Take Five, to test your knowledge.

Are you scam savvy?

TAKE FIVE TO STOP FRAUD℠

STOP CHALLENGE PROTECT

Scam types

- Bank impersonation
- Invoice redirection
- Business email compromise
- Investment
- Purchase



Scam type: Bank Impersonation

What is it?

You get a call from someone pretending to be from Virgin Money, claiming there's some form of suspicious activity on your account and it's been blocked.

They say they can help resolve it and often direct you to a fake website, which contains malicious links. Clicking on the link can download remote access software, such as Any Desk, giving fraudsters access to your device and potentially your bank account.

Things to watch out for

Being asked to:

- Visit a website or live chat to resolve a payment or account issue.
- 'Authorise', 're-authorise' or 'reverse' a payment.
- Add a code, followed by a phone number to your landline or mobile number, which will divert your calls to a fraudster's phone.



Let's see what it looks like:

THE DEVIL'S IN YOUR DETAILS | Phone Fraud

What should you do

Stop, Think & Check.

- If at all suspicious, hang up and call us back using a number from our website or by calling 159.
- Never let anyone access your device remotely.
- Don't share activation codes, one-time passcodes or Token 3 response.
- Always check payee details are correct.

Scam type: Invoice Redirection

What is it?

You receive an email from a known supplier, telling you their bank details have changed. They ask for an immediate payment and for all future payments to be sent using the new details.

Things to watch out for

- Any supplier email advising of changes to their usual bank details.
- An unexpected, urgent demand for payment.
- A supplier claiming you have not paid an invoice when you are certain you already have.



What should you do

Stop, Think & Check.

- Be suspicious of any request to change bank details or contact information, especially if the request is urgent.
- Verify new supplier bank account details with them in person, or over the phone using a number you know to be genuine.
- Put business processes in place for everyone to follow, including checking payment details with the supplier directly, not via email.

Scam type: Business email Compromise

What is it?

This is a targeted scam where criminals impersonate a trusted person or gain access to a real email account to trick employees into sending money or sensitive information.

Things to watch out for

- An out-of-character request from a senior manager or supplier.
- An urgent request from a senior member of staff or supplier.
- Being asked to not follow the normal business processes.

What should you do

Stop, Think & Check.

- Protect business and personal email accounts with strong passwords and Multi Factor Authentication (MFA).
- Advise your customers to verify any change in payment details via a trusted phone number. Do the same for changes in payment instructions from your suppliers.
- Put business processes in place to verify financial instructions directly with the person (not via email).
- Create a culture where colleagues feel able to challenge a request from a senior member of staff.

Scam type: Investment

What is it?

Someone gets in touch out of the blue with investment tips. They persuade you to invest in a scheme, shares or 'valuable' goods, but they're either worthless or they don't exist.

This could be bonds, shares, crypto, gold or wine.

Things to watch out for

- Someone promises very high or guaranteed returns on an investment.
- Fake online adverts offering 'Get Rich Quick' schemes. They might look like they're backed by a celebrity.
- They ask you to set up a new account and transfer money to it.
- Or they might ask to open and manage a digital wallet for you.

What should you do

Stop, Think & Check.

- Speak to a reputable, independent financial advisor before investing.
- Do your research before parting with your money.
- Google 'FCA Register' and check the business you are dealing with is registered.

Scam type: Purchase

What is it?

This is when you pay for products or services that don't exist. It could be tools, IT kit or vehicles.

Things to watch out for

- Special Offers: with discounts that look too good to be true.
- Limited availability: they pressure you to act straightaway.
- Weird requests: like asking you to pay by bank transfer, instead of your debit or credit card.

Did you know?

Most purchase scams take place on social media sites and fake websites. Stay sharp when buying online.

What should you do

Stop.

- Take a moment before buying.
- Does it seem too good to be true?

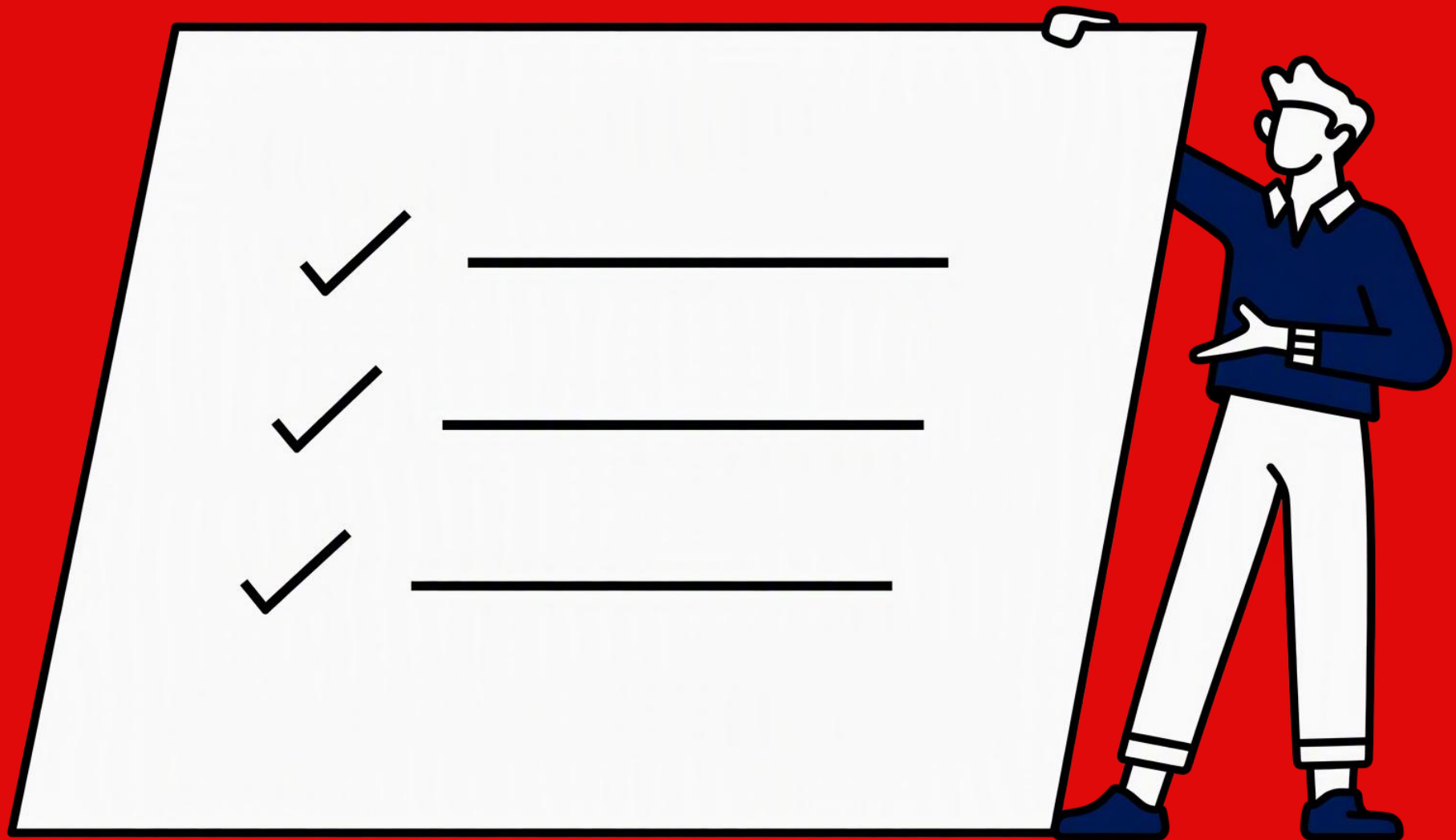
Think.

- Trust your gut instinct.
- Are they asking you to pay by bank transfer?

Check.

- Research the retailer and check reviews to make sure they're legit.
- Make sure the item exists, especially for big purchases.
- Double-check their returns & cancellation policies.

Top tips



Top tips

Stop. Think. Check.



Emails, texts, and even caller ID can be faked or spoofed.
They might look or sound genuine, but that doesn't mean they are.

It's ok to hang up or delete the message. Then give us a call using a number from our secure website or call 159.

Be suspicious & Be prepared

- Double check payment requests in person or on a trusted number
- Keep all devices and systems up to date
- Use strong, unique passwords
- Talk about fraud. Create a culture where colleagues feel confident and comfortable to challenge a request

Protect yourself.
Protect your business.
Protect your money.



If you think you've been scammed or have been a victim of fraud...

Report it - both successful & unsuccessful attempts

Call us on 0800 0121 353 – a direct line to our fraud team

Forward suspicious emails to Report.phishing@virginmoney.com

Forward suspicious texts to 7726 (free of charge)

Report it to 'Report Fraud'

Report Fraud is the national reporting centre for fraud and cybercrime. It collects reports about fraud on behalf of the police in England, Wales and Northern Ireland. Visit Report Fraud or call 0300 123 2040.

If you're living in Scotland, report it directly to Police Scotland by calling 101.


MONEY
Virgin