

# What to do if you think you're being targeted by a scam

At Unity Trust Bank, we take fraud prevention and safeguarding our customers seriously. To help our customers stay protected from the ever-evolving threat of criminal attacks, we've put together some handy information to help your organisation stay protected.

## If you suspect you are being targeted by a scam



### Remember:

Unity Trust Bank will never ask you to log in to your account or share sensitive security information over the phone. If you receive a call or email from someone claiming to be from Unity asking for sensitive information about your account, hang up and call us from a trusted number.

### Stop. Take a Moment.

Scammers often try to create a sense of urgency. They may tell you that your account is at risk, a payment must be made immediately, or that you need to act now.

**Pause before doing anything.** A few moments of thought can help prevent fraud.

### Look out for the warning signs - be cautious if someone:

- Contacts you unexpectedly by phone, email, text or social media
- Claims to be from Unity and asks for passwords, security details or login information
- Tells you to move money to a "safe account"
- Pressures you to act quickly
- Asks you to approve a payment you weren't expecting
- Tells you that bank details have changed, or asks you to send money elsewhere

### Challenge anything that doesn't feel right

It's always OK to say, "I want to check this first." Genuine organisations will understand.

# If you think you've been scammed

## 1 Contact us immediately

Report the issue as soon as possible so that we can investigate what has happened and quickly move to protect your accounts.

## 2 Save any evidence

Keep copies of emails, text messages, phone numbers, payment details and any screenshots you have of the activity. All of this can help with our investigation and help stop future scam attempts.

## 3 Report it

- If you're in **England, Wales or Northern Ireland**, report it to **Action Fraud**.
- If you're in **Scotland**, contact **Police Scotland on 101**.



## Remember these three steps

### 1 STOP

Take a moment before sending money or sharing information.

### 2 CHALLENGE

Question unexpected requests. Verify them independently.

### 3 PROTECT

If something doesn't feel right, contact us straight away and report it.

## Simple ways to stay safe

- Use strong, unique passwords
- Turn on multi-factor authentication wherever possible and keep device software updated
- Never share security information with anyone or give them remote access to your device
- Be cautious of unexpected emails, texts, links and attachments
- Always double-check changes to bank details before making payments

## What makes a strong password?

- Use a mixture of upper case and lower case letters, numbers and symbols
- Don't use anything easily related to yourself or your organisation
- Don't re-use passwords for multiple sites, keep them unique

**When it comes to fraud, it's always better to check than to take risks.** If you're unsure, stop and check with us directly before making any decisions.

You can find much more information on how to protect your organisation, here: **[www.unity.co.uk/how-to-report-fraud-or-a-scam](http://www.unity.co.uk/how-to-report-fraud-or-a-scam)**