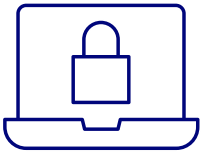
Cyber Security At Home

Stay safe online & on the phone

Bank of Ireland UK

Protect yourself from fraud online and on the phone

Fraudsters use different tactics to try and trick you into sharing your personal details so that they can steal your money.



What the fraudsters might do

They may pretend to be your bank, credit card company, another company you trust, or friends and family.

- **Send you a text message** pretending to be a friend or family member. They will tell you this is their new number, then after a short conversation ask you to transfer money for an urgently.
- **Send you an email or text message,** usually asking you to click on a fake link.
- **Phone you** asking for your password, full login PIN or bank account number.
- Ask you for a **'one-time password'** or code that you have received from Bank of Ireland by text.
- Ask you to **download an app** to allow necessary updates to your computer/service.
- Put you **under pressure** to provide your details, often being persistent and aggressive.
- Make **urgent threats**, for example, that you won't be able to use your bank account or your computer if you don't do what they say.
- Tell you the **first four digits** of your card number and ask you to confirm the rest.
- Ask if you made a **recent transaction** at a well-known store, such as a supermarket. The fraudster is only guessing this information to sound more believable.
- Try to convince you to **transfer money out** of your account, for example using a money transfer service.

What you can do

- **Don't give away personal or banking information.** No matter what story you are told, don't give away your passwords. If the query seems odd, don't share personal or banking details.
- We might send you a text with a one-time code in it so you can complete your online registration, verify an online card transaction, or add a new payee. **Never ever give that code to anyone**. **Only a fraudster will ever ask you over the phone for some or all of that code.**
- **Don't click on any suspicious links** in emails or texts. Bank of Ireland will never ask you for personal banking details in an email. Any suspicious emails relating to your Bank of Ireland accounts should be sent to **365security@boi.com**
- **Bear in mind that fraudsters can insert a fake text** into a thread of genuine Bank of Ireland messages. Use our Check your Text service: Forward the text message with the word **CHECK** inserted to the beginning to **50365**. We will reply telling you of the text is from us or not.
- **If you receive a suspicious call, hang up** and don't call back any number the caller has given you because it could be fake.
- **If you receive a text, email or social media message** claiming to be a friend or family, confirm your friend by contacting them on the number you already have. Or, ask them a question that they will only know the answer to. If the message is from a company, confirm them using a number you already have or using the official company's website.
- **Don't download apps you're not familiar with.** Only download apps from official app stores (such as the Apple App Store and Google Play Store) and not from links received in texts, emails, or on social media.
- **Log out** of your online banking session when you are finished.

Speak up

f you are concerned, speak to us at your local bank branch or, if you think you have already been a victim of fraud contact Action Fraud Report fraud, scams and cybercrime to **www.actionfraud.police.uk** or **0300 123 2040**.

Emergency Contact Numbers

Northern Ireland and Great Britain

Freephone: **0800 121 7790** (personal customers)

Freephone: **0800 032 1288** (Business On Line and Global Market Customers)

Republic of Ireland

Freephone: **1800 946 764** (personal and business)

Everywhere outside Republic of Ireland, Great Britain & Northern Ireland

Not Freephone: **00353 567 757 007**

NI call for service

Contact the PSNI if a call for service* is required.
Call **101**, or in an emergency **999**.

*A call for service can be requested when:

- a fraud is happening, or happened in the last 24 hours, and the suspect lives in Northern Ireland,
- the victim is vulnerable, or
- the report is necessary to ensure the police can secure evidence, or prevent loss.

bankofirelanduk.com/help-and-support/security-and-fraud/

UK37-1428N (09/24)