Protect your business from fraud

Bank of Ireland UK

Fraud and cybercrime are increasing. We want to help you protect your business. This includes giving you clear, practical advice on how to stay safe when using Bank of Ireland's digital channels.

Use this checklist to review how you protect your business when using Business On Line.

Checklist			✓
1	**Put a payment policy in place**	Have a payment policy for your business. It should set clear rules for: ▸ How staff access online systems ▸ How payments are approved ▸ How you manage payment risk. Make the policy simple and practical, so your staff know exactly what to do. Review it regularly, so it reflects changes in your business and new risks. Anyone who uses digital banking should read the policy. They should regularly confirm that they understand it and follow it.	
2	**Set daily control limits**	Set a daily control limit that suits your business needs. Use the lowest limit possible. Review it regularly, to make sure it is still right. If needed, you can apply a temporary increase for a short period.	
3	**Ensure users have unique usernames**	Every user should have their own unique username when they access Business On Line. This helps you track activity and see who carried out each action.	
4	**Give users the minimum access they need**	Only give users access to what they need to do their job. You can: ▸ Create user groups ▸ Set different access levels for each user group ▸ Assign users to a user group with the minimum access required to complete their role ▸ Control who can approve payments and payees. Limit payment and payee approval access to trusted staff, such as supervisors or managers.	
5	**Separate key tasks**	Do not let one person set up and approve the same payment. Split responsibilities so: ▸ One person sets up the payment ▸ Another person approves it. ▸ This reduces the risk of errors and fraud	
6	**Add a '4-eye' checkpoint**	Make sure at least two people approve: ▸ New payees ▸ Payments This extra check helps confirm that the request is genuine and correct	
7	**Use authorisation limits**	Use the authorisation limits on Business On Line (also known as payment panels). This lets you make sure that higher value payments are approved by specific users or by more than one person.	

8	**Train your staff**	Train your staff regularly on fraud risks. Make sure they understand common fraud types, how fraud can happen and what to do if something goes wrong. Start with common risks like investment scams, bank impersonation and invoice redirection.	
9	**Protect your business technology**	Keep your systems secure. Make sure you: ▸ Use up-to-date anti-virus software ▸ Keep your operating systems updated ▸ Apply security updates quickly ▸ Back up your data regularly ▸ Use a firewall ▸ Never share codes from your Approve app ▸ Never approve a push notification if you did not request it. Beware of fraudsters who ask you to download legitimate apps to gain remote access to your device. Never give control of your computer to someone who contacts you unexpectedly. No matter how genuine they seem.	
10	**Using our fraud web pages as a guide**	Visit our dedicated fraud pages regularly for updates and advice. UK customers Security and Fraud - Bank of Ireland UK Republic of Ireland customers Security Zone - Bank of Ireland Group Website	

Final reminders to keep your business safe

- We will never ask for account information by email.
- Do not reply to a text, click a link, or call a number in a text unless you are sure it is genuine.
- Never share codes from your Approve app with anyone. No matter who they say they are or why they say they need them.
- We will never call and ask you to approve a push notification from your Approve app. Never approve a push notification, if you did not request it.
- Always call a supplier on a known, trusted number, to confirm payment details if they change.
- Do not rely on email alone to confirm payment details.
- Make sure you and your staff are aware of common scams and how to stay safe.

Did you know?

Use our Text Checker service to check if a Bank of Ireland text is genuine. Text **Check** followed by the message to 50365.

How to report fraud

If you think you have been targeted or have shared your banking details, call us straight away on the numbers listed below. Available 24 hours, 7 days a week.

UK

Freephone: 0800 121 7790
(for Personal customers)
Freephone: 0800 032 1288
(for Business On Line & Global Market customers)

Republic of Ireland

Freephone: 1800 946 764
(personal and business)

Everywhere outside UK and Republic of Ireland

Not Freephone: + 353 56 775 7007

UK37-1646N.3 (09/26)