


PROTECT YOUR BUSINESS FROM FRAUD

Businesses and organisations are increasingly becoming targets of fraud and cybercrime. We want to help all our customers to protect themselves against these attacks, by providing some practical advice when using Bank of Ireland's digital channels.

We have created a helpful checklist of Bank of Ireland Business On Line's tools available to help protect customers with the security of their online banking.

Checklist			✓
1	Put a payment policy in place	<p>Ensure a payment policy is in place to standardise the procedures and governance across your business and staff and how they manage access to online systems and payment risk. The policy should be prescriptive and maximise the use of the tools available within the chosen channels.</p> <p>It is important to review this policy on a regular basis to account for internal and external changes, and to reflect current and emerging risks. All staff with access to digital channels should be required to familiarise themselves with the policy and attest to their compliance with it regularly.</p>	
2	Set daily control limits	<p>Set a daily control limit on the profile which is commensurate with your payment requirements. Always apply the lowest tolerable figure and review this regularly to ensure it remains relevant to your requirements. Where this figure needs to be raised, you may also consider availing of a temporary increase to cover a specific time period.</p>	
3	Ensure users have unique usernames	<p>Always ensure every user has their own unique username for logging on to Business On Line. This allows actions completed within the channel to be traced and makes who executed each action transparent.</p>	
4	Give users the minimum access necessary	<p>Always apply the minimum access necessary for each user to undertake their duties. Each user can be assigned to a unique user group and you can create multiple user groups with different 'tiers' of access. Be particularly selective about which employees are granted access to authorise payments, for example, only those employees of a supervisor or manager level.</p>	

Checklist 		
5	Split responsibilities	Split the responsibility to initiate a transaction from the responsibility to authorise it, so that no one person can do both. This helps ensure that the information being entered and acted on is correct.
6	Add a '4-eye' checkpoint	Require that two different people are needed to authorise payees and payments. This adds a '4-eye' checkpoint to confirm the accuracy and authenticity of each request, at each step in the payment journey.
7	Use authorisation limits	Use the authorisation limits on Business On Line (also known as payment panels) to require that higher value payments are authorised by specific authorisers, or multiple authorisers.
8	Train your staff on threats	Conduct regular training with your staff on the threats to your business, ensuring they are aware of the new and persistent risks and how they can occur outside of the workplace and work environment.
9	Protect Your Business Technology	<ul style="list-style-type: none"> • Ensure you have up to date anti-virus software in place on your devices and schedule regular checks on your computer systems. • Always run your computer or network on the most up to date version of the operating system. • Apply security patches as soon as possible after they become available. • Back up your data. • Ensure you have a firewall enabled on your technology.
10	Use Security Zone as a guide	<p>Finally, we would encourage you to visit our dedicated fraud pages on our ROI & UK websites regularly for guidance on what to look out for and further tips on how to keep safe online. Please visit the following pages:</p> <p>Republic of Ireland customers Security Zone - Bank of Ireland Group Website https://www.bankofireland.com/security-zone</p> <p>Northern Ireland Great Britain customers Security and Fraud - Bank of Ireland UK https://www.bankofirelanduk.com/help-and-support/security-and-fraud/</p>

Did you Know...

You can check the legitimacy of any Bank of Ireland text you receive using our TextChecker service. Simply send the word 'Check' followed by the Bank of Ireland message you want to verify to 50365

REMEMBER: WE WILL NEVER ASK FOR ACCOUNT INFORMATION BY EMAIL

- ▶ If you get a request to make a payment or update bank account details for a customer or supplier, ALWAYS call them first to make sure that the request is genuine and that the account details you are using are right.
- ▶ We will never call you and ask you for a password from your Approve app, so never give these passwords to anyone, no matter who they say they are or why they say they need them.

When dealing with a new supplier, make sure to carry out due diligence and confirm the payment details. This should be verbal and with a contact you know or can verify – never rely solely on email.

How to report fraud

To report online fraud, suspicious activity, or if you have shared your banking details in response to a suspicious email, text or call, please notify us as soon as possible via the Freephone numbers listed below.

Emergency Contact Numbers

Republic of Ireland

Freephone: 1800 946 764 (personal and business)

Great Britain & Northern Ireland

Freephone: 0800 121 7790 (for 365 credit card customers)

Great Britain & Northern Ireland

Freephone: 08000 321 288 (for Business On Line & Global Market customers)

Everywhere outside Republic of Ireland, Great Britain & Northern Ireland

Not Freephone: + 353567757007