AIB iBB Security Brochure

How to stay safe online

AIB

As criminals are coming up with more inventive ways of defrauding you in order to steal your personal information and money, we've put together the information below to help you protect your accounts and stay safe online.

Email Scams

Be wary of emails requesting you to change bank account details or make a payment to someone you have not paid before. Scam emails may have the following characteristics:

- Emails pertaining to be from Suppliers advising they have changed their account details for payments for a variety of reasons
- The "from" field is designed to look like the emails are from a company manager, director or senior staff member's email account requesting that an urgent payment is made
- The email address may be slightly different to the genuine one e.g. there may be a slight misspelling
- The language/wording used may be unusual for your company / supplier; e.g. asking you to "sort" or complete a "financial obligation" or a "wire transfer"
- The email may have an unusual timestamp, this indicates that it's coming from a jurisdiction different to what you would expect

The sender may indicate they are uncontactable on the phone.

Malware

Be wary of malware on your PC that displays screens that purport to be iBB screens. Examples of fraudulent requests include:

- Verify your identity
- Terminal Digipass Synchronisation
- Security challenge
- User Authentication

This is a sample fraudulent screen that attempts to trick customers into providing information:

Be wary of opening documents from sources you are not familiar with.

- In particular be wary of opening documents containing macros or which state that the content will not be visible until the macro feature is enabled
- Ensure macros are automatically disabled as standard on your PC.

DO's

- If you have multiple iBB Users make it mandatory that at least two iBB Users are involved in the Creation and Authorising of payments
- Be wary of any emails or phone calls claiming to be from the bank or suppliers requesting you to update information or to make payments
- Install and regularly update firewall software
- Review your anti-virus software protection on every PC & Laptop used to access iBusiness Banking and be on your guard for suspicious activity on your PC eg slow response times, unusually high CPU/ Memory utilisation

and DON'Ts

- Never enter codes from an iBB screen into your Digipass. iBB never asks you to do this. Contact us immediately on 0818 720 000 if this happens.
- Never make payments on foot of an email request without contacting the Supplier, Manager or Director using the existing agreed phone number to verify the request – do not use any of the information in the email to make contact.
- If you choose to share your iBB logon details with a Third Party, please check that the Third Party is authorised by the Central Bank of Ireland or another European Regulator. Never share your iBB logon details with Third Parties who are not authorised with a relevant Regulator.
- For more information, visit our Security Centre on www.business.aib.ie/securitycentre

AIB iBBSL/DL 02/18