iBusiness Banking
Security Factsheet

iBusiness Banking has been developed to offer you an efficient way of carrying out a diverse range of banking functions from a single application.

Whilst we have made the security of your information on iBB a priority, it's important that your employees who are using iBB appreciate that cyber enabled crime is constantly evolving. Good security behaviour by those using iBB will help minimise the risk to your information systems and reduce fraud.

There are a number of things that you can do to create a culture that has security as a cornerstone. If your employees naturally think about security it will go a long way to protecting your information and your business.

- Adopt an Internet and email usage policy that is easy to understand and is supported and used by senior management
- Ensure that all your networked computers have up-to-date anti-malware and anti-spam software
- Manage User access so that staff only access what they need. Review this regularly and make sure anyone who leaves is removed promptly
- Apply software patches regularly and in good time to address known vulnerabilities in the software you use
- Introduce regular cyber security awareness activity into your staff briefings
- Assess your risk. Which information means the most to you and how much might it cost you if it was lost, compromised or unreliable
- Work out and test how you will react to a problem and minimise any impact
- Monitor your network for unusual activity that might indicate an attack
- Apply the same standards of security to anyone working away from the office
- Manage the use of portable devices that can store data such as CD-RW, USB drives etc to reduce the risk of data being removed inappropriately

Best practice for your iBB Users

- Never let anyone else use your Digipass PIN or Passphrase.
- Never tell anyone what your Digipass PIN or Passphrase is.
- If you use a Password Manager ensure that no one else can gain access to this.
- Choose a Passphrase that is hard to guess and easy to remember, for more advice on how to manage your Passphrase please visit our Help Centre at www.aibgb.co.uk/help-centre
- Login using the URL www.aibgb.co.uk/ibusinessbanking and never click on URL links in emails
- Always logout correctly, ensuring you close all open browser windows
- Check for a secure session by ensuring the URL, once logged in, starts with https://
- Be aware of fraudulent emails or SMS Texts. Remember we will never send you emails or SMS texts asking for login or account details or personal information.

Report Suspicious Activity

If you suspect any of your details have been compromised or notice suspicious activity on your iBusiness Banking system email alert@aib.ie or telephone 0370 243 0331† between 8:30am and 5:30pm or you can contact our 24 hour Helpline on 0800 0391 140 or 028 9023 6644 where a customer service adviser is available 24 hours a day.

For more information on threats and tips to protect yourself visit our Security Centre which can be found within our Help Centre at www.aibgb.co.uk/security-centre or takefive-stopfraud.org.uk

Protect your business against Cyber threats, for more information and guidance visit The National Cyber Security Centre on www.ncsc.gov.uk/guidance/10-steps-cyber-security

†Call charges may vary, please refer to your service provider.

recycle
When you have finished with this please recycle it.

Business Advice – Online Scams

Why should business be concerned?

Fraudsters are turning to more sophisticated methods of scamming people and businesses out of money, with businesses increasingly a target. A common tactic they may use are sending spoof emails impersonating a senior member of staff and trying to deceive employees into transferring money. The email usually requests an urgent payment is made outside of normal procedures, often giving a pressing reason such as the need to secure an important contract.

Criminals can also pose as regular suppliers to the company or organisation and make a formal request for bank account details to be changed. This is known as invoice fraud and fraudsters may trick a company into changing their bank account payee details for a sizeable payment.

Criminals who specialise in invoice fraud are often aware of the full details of the relationship between companies and suppliers – they know when regular payments are due and, equipped with sophisticated information, they make contact with finance teams within companies and pose convincingly as suppliers.

Similarly, through mandate fraud criminals convince firms to change a direct debit, standing order or bank transfer mandate by pretending to be an organisation the business makes regular payments to, for example a subscription or membership organisation or supplier.

CEO Spoofing

If you receive an email from your CEO or some other senior member of staff asking you make an urgent payment outside of normal procedures, don't automatically follow their lead. It's become very easy for fraudsters to manipulate the characteristics of an email, including the sender address, so that it looks genuine, but when you transfer the money, it goes straight to an account controlled by a criminal. Keep an eye out for any emails that might be written in a different style to usual, and always check any unusual payment requests directly, ideally in person or by telephone, to confirm the instruction is genuine.

Invoice Fraud

It's not hard for criminals to investigate business invoice details (even down to payment dates) and then pose as regular suppliers. If a supplier contacts you to make a formal request for bank account details to be changed, always verify with that supplier using their on-file details. It's important that everyone inside a business is warned of the dangers of invoice fraud, and that everyone knows to always check invoices to identify potentially fraudulent transactions as soon as possible.

Information correct as at January 2018