BUSINESS EMAIL COMPROMISE

What is Business Email Compromise?

Business Email Compromise (BEC) is a form of targeted phishing attack (spear-phishing) that attempts to extract sensitive information and, typically, request that bank details are altered to an account under their control by way of impersonation.

The Warning Signs

- You receive an email from an executive, influential staff member of an organisation or customer you are dealing with requesting to update banking details or send an invoice with details that aren't on record.
- The sender requests that the transaction is expedited as soon as possible or the request comes in at the end of the work day/week.
- The message may press the recipient to bypass normal polices and procedures.
- The sender says that they are travelling, or is otherwise unavailable to take a call.

Report it to us using our Cyber Concerns Online Reporting Form

The Do's & Dont's

- Don't act on a request to send money or sensitive information, or change details on record without first confirming it is authentic.
- Don't reply to suspicious emails. Speak directly to the person the sender claims to be. on a known contact detail or in person.
- Immediately contact your designated finance officer or financial institute if you discover a fraudulent transfer.
- All emails or any other evidence should be preserved to provide to investigators and authorities if required.
- Follow your organisation's reporting procedure for fraudulent activity.

Recommendations

1. Always check any email adresses to identify if it matches you known and trusted records.

2. Mandate fraud is more likely to be perpetuated against an organisation. Be alert to any requests to alter their bank details.

3. Validate all requests for bank account changes using established contact details, never use any of the contact details contained on letters or emails asking you to update your details.

4. Undertake a check on the internet for any new bank account sort codes and account details to identify the location of the bank as well as any information indicating this communication to be a scam.

5. Adopt dual control procedures for authorising payments and ensure that a senior member of your finance team formally authorises the change of bank account details.

6. Regularly reconcile your bank statement and report anything suspicious to your bank immediately.

7. Business managers should regularly review and update security policies ensuring that all staff are fully trained to spot potential fraud.