Business Email Compromise

Business Email Compromise

Fake emails are a common tool used in scams

When payments are due, criminals send an email designed to look and read like a genuine message from a supplier. They tell you that the bank details for your payment have changed, provide new details and send a payment request.

These emails can be hard to spot:

- The attackers often use the supplier's authentic email address, or a spoofed email address which looks just like the legitimate address.
- They will make invoices look authentic.
- There may be no perceptible difference in the supplier employee's email signature.
- The message might have a sense of urgency. A common example is that the request is linked to a sensitive deal which requires a timely transfer.
- The attacker will have access to the email chain and will be able to reply using similar language and tone.
- Perhaps most importantly – often the payment they are requesting is actually due.
- Often the only difference is that the business's bank details have changed.

How does email compromise happen?

Email account takeover

- The attacker uses hacking, or stolen account credentials, to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user’s contacts, email style and personal data to make their messages more convincing.

Email impersonation

- The criminal sets up an account with a very similar address to the real one.
- Or they may use a spoof email envelope and header, hoping the recipient will not notice and engage with it as with a legitimate message.

CEO fraud

Criminals impersonate a senior manager in the company.

- The attacker uses hacking, or stolen account credentials, to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user’s contacts, email style and personal data to make their messages more convincing.
- Ensure that, wherever possible, you only take payment instructions from approved company communication channels. Fraudsters will often contact victims via open communication channels like messaging apps.