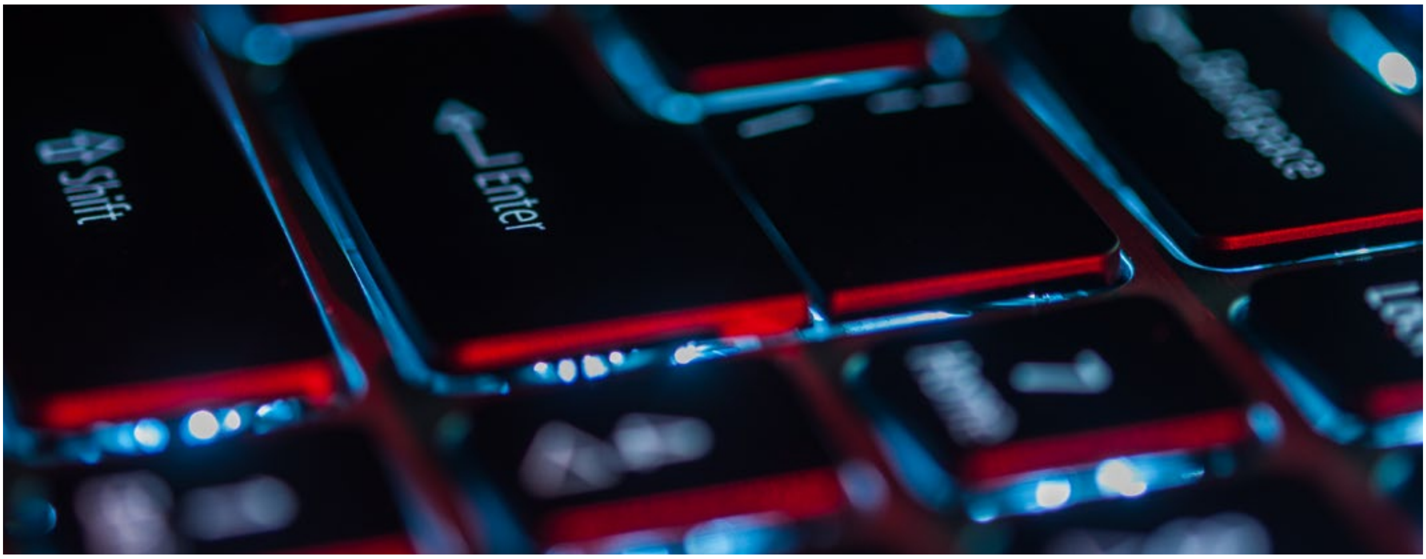
HSBCnet

Business email compromise

Risks to your business:

Significant financial loss

Reputational damage



Cyber-attacks have increased steadily in recent years. With criminals constantly devising new ways to steal information and money, one of the newest emerging threats is Business Email Compromise.

Also known as: CEO Fraud • Chairman Fraud • President Fraud • Imposter email • Payment redirection • Whaling

How Business Email Compromise works

A fraudster emails a company's payments team, impersonating a contractor, supplier, creditor or even someone in senior management. The email might appear to be from the CEO, asking that an urgent payment be made, or from a supplier, requesting that future payments go to a new account. Often it instructs the recipient not to discuss the matter with anyone else.

Since the sender's email closely matches a known address, this type of fraud often goes unnoticed until it's too late. Cybercriminals may even hack into a real email account - from which fraudulent communications are hard to identify.

Your information is valuable

The scam can appear even more convincing if thieves obtain information about a company's leaders and finance team, for example from the firm's website.

Social media posts may also tell them when senior staff are away from the office at meetings or conferences. Fraudsters see that as an opportunity to send their emails because it's difficult for the recipient to check whether the request is genuine.

In the US, the FBI reports **hundreds of millions of dollars** are lost each year. The average amount is around

USD140,000

Source: https://www.ic3.gov/media/2016/160614.aspx

HSBC

Business Email Compromise in the real world

Actual business case: $400,000 loss

A company's payment team received an email, claiming to be from the CEO, asking that payments be set up for new beneficiaries. A member of the team created and authorised the payments. By the time the team realised that the requester's email address did not exactly match the CEO's, it was two days later and the perpetrator had stolen nearly $400,000.

Since **January 2015,** there has been a

1,300%
increase

In identified exposed losses, now totaling

over $3 billion

Source: https://www.ic3.gov/media/2016/160614.aspx

How to keep your business safe:

- Make sure your employees are aware of this type of fraud.
- Implement an internal two-step payments verification process which includes a non-email check with the requester.
- **Phone the requester using a verified phone number** to follow up an email request.
  - DON'T reply directly to the initial email
  - DON'T use any phone numbers or other contact information included in the email.
- Check email addresses match your internal records exactly.
- Be on guard for payment requests that are unexpected or irregular, whatever the amount involved. If in doubt, don't make the payment.

If you suspect you have been the victim of fraud, contact your HSBC representative immediately.