Business email compromise
Defending your organisation

National Cyber Security Centre
a part of GCHQ

What is business email compromise?

Business email compromise (BEC) is when a criminal accesses a work email account to trick someone into transferring money, or to send them valuable information. Some BEC emails contain viruses disguised as attached invoices, which are activated when opened. BEC emails often target senior staff with access to funds or valuable data.

If you think you've lost money to BEC

Contact your IT team (if you have one) as soon as you can. The earlier you tell someone, the more likely they'll be able to help.

Contact your bank directly using their official website or phone number. Report it as a crime to Action Fraud on 0300 1234 2040. If you're in Scotland, contact the police by dialling 101.

If your account has been compromised, you can refer to the NCSC's guidance on recovering a hacked account, which is a step-by-step guide to recovering online accounts.

Help staff to detect phishing emails

If you get an email from an organisation you don't do business with, treat it with suspicion.

Look out for emails that appear to come from a senior person within your organisation. Does the email sound legitimate, or is it trying to mimic someone you know?

Ensure that all important email requests are verified using another method (such as SMS message, a phone call, or confirmation by post or in-person).

Does the email ask you to act urgently? Be suspicious of phrases like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Reduce your digital footprint

Criminals use information about staff that's available on websites and social media platforms, to make their BEC emails appear more convincing. All staff, but **especially** senior members should review their privacy settings on their online accounts, and think about what they post online in order to reduce their 'digital footprint'.

Apply the principle of 'least privilege'

Check who in your organisation can authorise payments, or has access to valuable information. Not everyone should be able to make high-value payments.

Set up 2-step verification

Protect your email (and other valuable accounts) by setting up 2-step verification (also known as 2SV). Even if a criminal knows your password, they won't be able to access those accounts protected by 2SV.

Plan for incidents

Ensure you've rehearsed your response in the case of different types of incidents. For example, how will you reset a user's password if it's stolen?

- A good way to rehearse your response is through 'exercising', and the NCSC's Exercise In A Box, is a free tool that helps you do this in a safe environment.
- Register with the NCSC's free Check your email security online tool, which can prevent criminals exploiting your email domain in phishing attacks.