National Cyber Security Centre

# Business email compromise

## Dealing with targeted phishing emails

This advice, produced in association with the National Crime Agency (NCA), helps you to spot the most obvious signs of targeted phishing emails. These attacks, also known as business email compromise, are typically sent to executives or budget holders within larger organisations in order to trick staff into transferring funds, or revealing sensitive information.


## What is business email compromise?

Business email compromise (also known as BEC or Payment Diversion Fraud) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain viruses disguised as harmless attachments, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

**If you've been a victim of BEC (Payment Diversion Fraud), report now to your bank or contact Action Fraud on 0300 1234 2040 (www.actionfraud.police.uk).**



## Make yourself a harder target

**Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.**

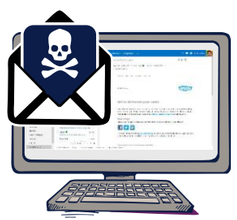
**Review your privacy settings, and think about what you post across your social and professional accounts.**

**Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.**

**If you spot a suspicious email, flag it as spam/ junk in your email inbox. Tell your IT department that you've identified it as potentially unsafe.**

**Will the emails you send get mistaken for phishing emails? Consider telling customers what they should look out for (such as *'we will never ask for your password*').**

## What to do if you've already clicked ?



**The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.**

**If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell then, the more likely they'll be able to help.**

## Tell tale signs of phishing

**Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.**

**Think about your usual working practices around financial transactions. 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 high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it 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, logging into an account, or confirmation by post or in-person).**

**Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like *'send these details within 24 hours*' or *'you have been a victim of crime, click here immediately*'.**

**Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?**