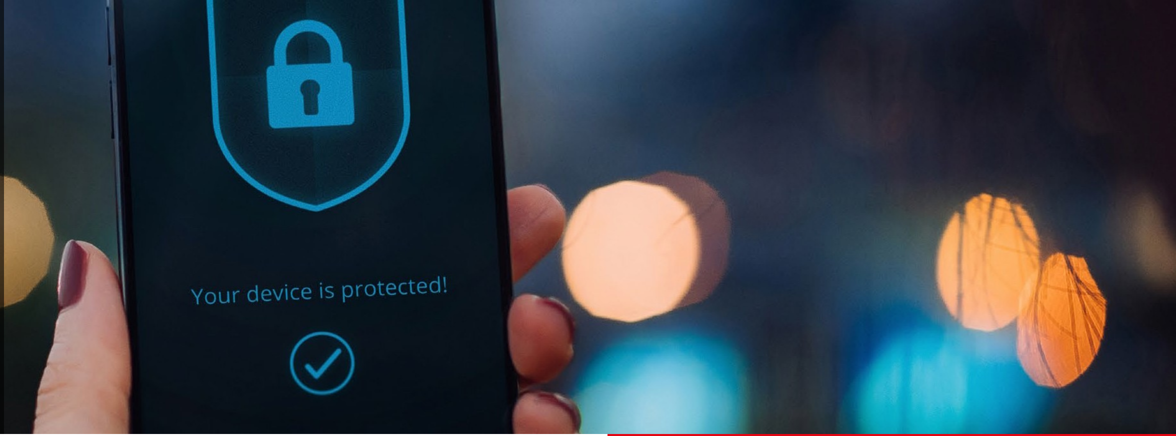
Protecting against Business Email Compromise



Use this guide to help you spot and minimise the impact of Business Email Compromise (BEC)

How do criminals use email to facilitate fraud?

BEC attacks can take different forms but a few common examples include:

- **Email account takeover:** accessing corporate email accounts through stolen credentials and gathering personal information to make their messages convincing.
- **Email impersonation:** setting up an account with a similar address to the real one or using a spoofed email envelope and header.
- **CEO fraud:** impersonating a senior manager in an email, requesting a large and urgent payment from the victim.

$10.2bn

Global cost of reported business email compromise attacks in 2022.

Source: FBI Internet Crime Complaint Centre

How do BEC attacks happen?

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 make a payment request.

These can be hard to spot:

- The attackers often use the vendor'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 vendor employee's email signature.
- The attacker will have access to the email chain and will be able to reply using similar language & 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.**

For more information on types of scams that could affect your business, click here.

Five key takeaways:

1. **Urgency is a red flag**, especially when relating to payments.
2. **Validate new and amended payment instructions** using known independent sources – this may be the single most important action in fraud prevention. DO NOT call a number from the email and always try to speak with the individual accountable for the change in details.
3. **Don't click on links or attachments** from unknown senders.
4. **Don't reply to a suspicious email** or use the contact details it contains. If it appears to be from someone you know, phone that individual to check and alert them.
5. **Treat external emails with caution**, especially if they're unexpected and contain links or attachments.

HSBC

PUBLIC