Business email compromise: defending your organisation

How to disrupt email phishing attacks that target senior executives or budget holders.

This guidance helps small to medium sized organisations deal with business email compromise (BEC). It provides actions to help businesses reduce the likelihood of being affected by BEC, and includes steps to take if you think your organisation has already been compromised.

> **Note:**
> Larger organisations may wish to refer to the NCSC's detailed guidance on defending organisations from email phishing attacks, which includes technical mitigations that will help counter BEC.

What is BEC?

Business email compromise (BEC) occurs when a criminal accesses a work email account in order to trick someone into transferring money, or to steal valuable (or sensitive) data.

In a typical BEC attack, the victim (who believes they are responding to a legitimate request) is coerced into transferring money into an account controlled by the criminal. For this reason, BEC attacks are often directed at senior staff, or those that can authorise financial transactions.

BEC is usually conducted by a **targeted** phishing mail. Unlike standard phishing emails (which are sent indiscriminately to millions of users), BEC emails are tailored to individuals within organisations. The email might impersonate someone the victim already corresponds with regularly, or even include the text from an existing email thread, so the victim believes they're dealing with a legitimate correspondence. Since these phishing emails often target a 'big fish' (often a board member or an employee with access to valuable assets), this type of cyber attack is also known as 'whaling'.

Since BEC emails are normally sent in low volume, standard email filters (designed to identify 'scam emails') may struggle to detect them, especially if they come from a legitimate email account that has already been hacked. Alternatively, a BEC email may have been sent from a 'spoofed' domain, designed to trick users that they are dealing with a legitimate organisation. Some BEC emails may contain viruses disguised as invoices, which are activated when opened.

For all these reasons, BEC is a threat to organisations of all sizes and across all sectors, as the NCSC's recent reports on the Cyber threat to the UK legal sector and the charity sector both illustrate. These reports also point out that following the pandemic, there's been a rise in BEC attacks. This is because more staff are now working at home, often using their own equipment, which makes it harder for organisations to manage devices and protect them from these kinds of attack.

If you think you've lost money to BEC

The most important thing is not to panic.

If you think you've been tricked into making a fraudulent payment, contact your bank directly using their official website or phone number. You should also report it as a crime to Action Fraud on 0300 1234 2040 (http://www.actionfraud.police.uk). If you're in Scotland, contact the police by dialing 101.

Most BEC fraud is a result of clicking on phishing emails, so you should also contact your IT department (if you have one) as soon as you can. The earlier you tell someone, the more likely they'll be able to help.

You may find that your account has been compromised (that is, somebody else has gained control of it). This may be easy to detect, such as emails being sent from your account that you didn't write, but the signs could be more subtle such as changes to security settings, password reset messages, or activity from your account that you don't recognise. In such cases, please contact your IT team if you have one. If not, you can refer to the NCSC's guidance on recovering a hacked account, which is a step-by-step guide to recovering online accounts.

Reducing the likelihood of BEC

There are several steps you can take that make it harder for criminals to attack your organisation. This reduces the likelihood of you falling victim to BEC.

Reduce your digital footprint

If there is information about senior staff on work and private websites, including social media accounts and networking sites, criminals can use this to make their phishing emails appear more convincing. This information, freely available on the internet, is known as a 'digital footprint'. Without this information, the phishing emails used to conduct BEC should be easier to spot as fraudulent.

All staff, but especially senior executives who have access to valuable assets or information, should review their privacy settings on their social media accounts, and think about what they post in order to reduce their digital footprint.

Help staff to detect phishing emails

Spotting a phishing email is difficult and many messages will trick even the most careful users. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap. If you have any doubts about a message, contact the organisation directly. Don't use the links, phone numbers or addresses in the message – use the details from their official website.

If staff spot a suspicious email, they should flag it as spam/junk in their email inbox, and tell the IT department (or someone in your organisation who is responsible for IT) that they've identified it as potentially unsafe.

Many cyber security providers often place too much emphasis on 'phishing simulations', designed to help your staff to spot all phishing emails. This approach risks wasting both time and money without improving security. Instead you should:

1. Help your users to recognise fraudulent requests.
2. Create an environment that encourages your staff to report phishing attempts.

Both of the above are covered in detail in the NCSC's guidance on defending your organisation from phishing attacks, but the key points are summarised below.

- 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 senior 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?
- Does the email contain a veiled threat that asks 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'.
- Some emails will try and create official looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

It's particularly important that your staff know that they can report BEC incidents (or potential incidents) without fear of reprisal. Staff who fear reprisals will not report mistakes promptly, if at all. This is crucial for BEC, as emails are unlikely to be identified unless a customer/ client informs the company of the potential discrepancy in their email correspondence, at which point significant funds may have already been extracted.

Set up 2-step verification

One of the most important steps an organisation can take to reduce the risk of compromise is the implementation of 2-step verification (often shortened to 2SV). Accounts that have been set up to use 2SV will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts. The extra step could be a code that's sent to you by text message, or that's created by an app on your phone.

It only takes a couple of minutes to set up 2SV, which is also known as multi-factor authentication (or MFA). Once you've done it, your accounts are instantly safer. You can learn what method is right for your organisation by reading the NCSC's guide to setting up 2-step verification.

Apply the principle of 'least privilege'

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

Only provide this 'privileged' access to people who need it for their roles. Regularly review these and revoke privileges if no longer needed. Remove or suspend accounts that are no longer being used, such as when a member of your organisation leaves, or moves to a new role.

Ensure that all 'important' email requests are verified using another method (such as text message, a phone call, logging into an account, or confirmation by post or in-person). For example, you should establish a robust process for verifying any **changes** to payment instructions, payments to a new supplier, or unusually high transactions. Never rely solely on contact details provided in an email.

Where the losses involved could be significant (for example, when setting up payments to a new provider), consider designing processes so that two or more individuals need to work together to perform them.

Register with the NCSC's free 'Check your email security' tool

We'd encourage organisations of all sizes to register with the NCSC's free Check your email security online tool, which can prevent criminals exploiting your email domain in phishing attacks. If your organisation is targeted, your business could be disrupted, your reputation damaged, and your customers could suffer real-world harm. Using the 'Check your email security' tool will make life harder for online criminals, and protect other organisations (as well as your own) from becoming victims of cyber attacks.

Plan for compromises

Simply making your employees aware of social engineering techniques doesn't make them invulnerable. Some BEC techniques are too well crafted and no amount of user awareness and training can guarantee their detection.

For this reason, you should ensure you’ve rehearsed your response (or at least considered what you should do) in the case of different types of incidents. For example, how will you reset a user’s password if it’s stolen? Who is responsible for removing viruses or other types of malware from a device, and how will they do it? For more information, refer to the NCSC's Incident Management guidance.

Incident response plans should be practised **before** an incident occurs. The best way to do this is through ‘exercising’, which is when you rehearse your response to an incident (as you would do for a fire drill) so you your organisation is better prepared should it happen for real. If you're new to this, the NCSC has created Exercise in a Box, a free online resource which helps you to find out how resilient you are to cyber attacks, and lets you practise in a safe environment.

PUBLISHED

30 April 2024

REVIEWED

30 April 2024

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations