Somerbys IT

Email Security Guide

Business email compromise

Business Email Compromise (BEC) is a way for cybercriminals to send emails under false pretences, making them seem like they're coming from a trustworthy source.

Phishing attempts or social engineering tactics can lead to someone's email being compromised- after which point the attacker may request anything from fraudulent wire transfers to sensitive information about their company or employees.

The main difference between BEC and other types of phishing attacks is that there isn't any malware found within the messages; so most spam filters won't catch these unless they are set up explicitly to do so.

More than 6,000 UK businesses are targets of a Business Email Compromise (BEC) attack every month.

5 Examples of Business Email Compromise

Most attackers use some variation of 5 examples of business email compromise. These include:

1. False Invoice Schemes

In these scams, a cybercriminal will take over the employee email account used to process invoice payments and fund transfers. The attacker will then use the account to ask another employee to transfer the funds or pay an invoice to the fraudster's account.

2. CEO fraud

A cybercriminal steals the email account of a CEO or business owner and uses this to trick other users into giving up sensitive information or money. The hacker will send the victim an email with a subject line requesting a money transfer.

Phishing attempts or social engineering tactics can lead to someone's email being compromised

3. Account Compromise

One of the most common BEC attacks is where the hacker obtains access before mining the employee's contact list for company vendors, partners, and suppliers. The attacker will then message these contacts requesting payments be sent to a fake account controlled by the cybercriminal.

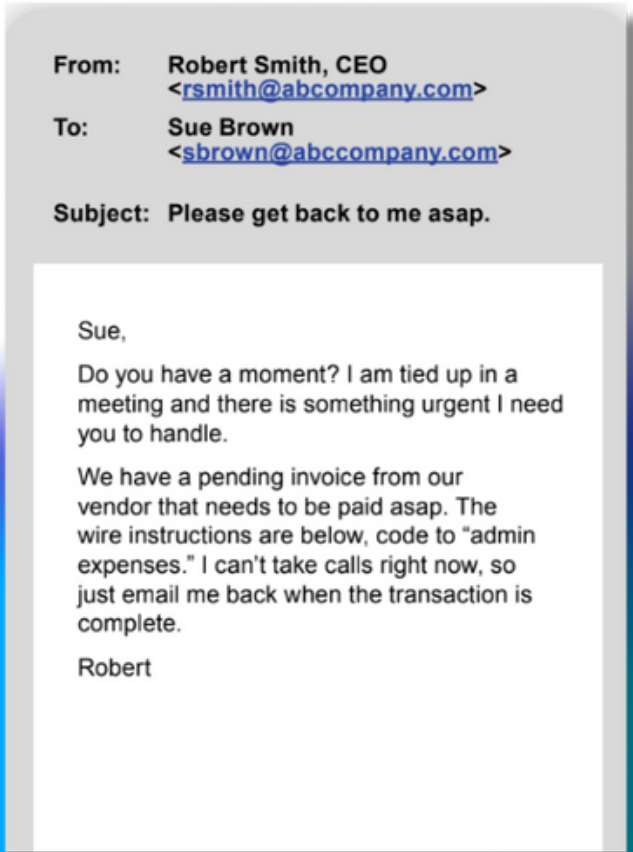
4. Legal Impersonation

This is when an attacker impersonates a lawyer or legal representative. Lower-level employees are commonly targeted through these types of attacks where one wouldn't have the knowledge to question the validity of the request.

5. Data Theft

These types of attacks typically target HR employees to obtain personal or sensitive information about individuals within the company such as CEOs and executives. This data can then be leveraged for future attacks such as CEO Fraud.

Here's an example of what a fraudulent email could look like. Note the slight variation in the email address.



How to Prevent BEC Attacks

Businesses can take some simple steps to prevent BEC from taking place. These include:

1. Raise awareness

Knowledge is power: educate your employees about the five types of BEC attacks. Teach employees how to identify BEC and phishing attempts. Deliver regular security awareness training and send ongoing communications about threats, keeping email security at the forefront of employee's minds.

2. Social engineering

Be mindful of shared information: Attackers will sometimes use social media to gather information on their target. Limit the information you share both professionally and publicly.

3. Security procedures

Ensure that processes and procedures are in place. Any suspicious requests made over email should be verified in person with the user and escalated to higher management.

Be mindful of shared information: Attackers will sometimes use social media to gather information on their target.

4. Protect your password

Ensure employees keep password information private and systems are set up to change passwords on a regular basis. This practice will decrease the risk of your accounts being compromised via password spray.

5. Enable two-factor or multi-factor authentication

Adding this feature to all of your organisation's email accounts will add an extra layer of security.

6. Invest in a multi-layered security solution

Email security depends on multiple defence features. No single security feature alone is enough to defend email against advanced attacks. An effective business email security solution should include multiple features and technologies designed to work harmoniously to detect and block threats in real-time, building on each other to provide stronger, more robust protection than any of these features would on their own.

7. Update all infrastructure

Ensure all applications, operating systems, network tools, and internal software are up-to-date and secure. Install malware and anti-spam software.

Like all cyber threats that rely on manipulation, it only takes a single employee to make a misguided decision to click on a malicious link or hand over personal information before dealing with a data breach that impacts your entire business.

By arming employees with the knowledge and common examples of business email compromise attacks, you provide them with the tools they need to spot manipulative phishing emails. You also reduce the chance of an attacker being able to trick your users into giving up sensitive information.

In September 2022, Uber suffered a catastrophic security breach. The breach was down to a social engineering-based approach towards an employee. The hacker, identified as an 18yr old lone worker, acquired access by impersonating a coworker and duping an Uber employee into handing over their credentials. You'd think that Uber's data would be impenetrable, but it wasn't due to human error.

Key stats

- 43% of organisations have experienced a security incident in the last 12 months, with 35% stating that BEC/phishing attacks account for >50% of the incidents.
- 1 out of 4 organisations say 76-100% of malware they detect is delivered via email.
- In the current work from home environment, 39% of organisations say they experience spear phishing on a weekly basis.
- 65% of IT security pros say their organisation has experienced spear phishing in 2021, while 51% say it has increased in the last 12 months.
- The good news – 69% say that their organisation is prepared to handle a cyberattack, and 71% believe their employees are prepared to identify a malicious email.

*Source: Helpnet security

Can your business afford not to be one step ahead?

The good news is, the team at Somerbys IT are cyber security experts. Get in touch today to find out how we can help your business not to be a victim to the fraudsters.

Get in touch with the team at Somerbys IT:

0333 456 4431 | info@somerbysit.co.uk

The Dock
75 Exploration Drive
Leicester, LE4 5NU

Somerbys IT