



Business Email Compromise (BEC):

Preventative and Remedial Measures

Business Email Compromise.

What is Business Email Compromise?

Business Email Compromise (BEC) usually occurs when a cybercriminal gains unauthorised access to an email account or email server belonging to an organisation. To carry out a BEC attack, an attacker only requires two pieces of information; username and password. The first is the easiest to acquire and can often be found by researching the target organisation and its employees online.

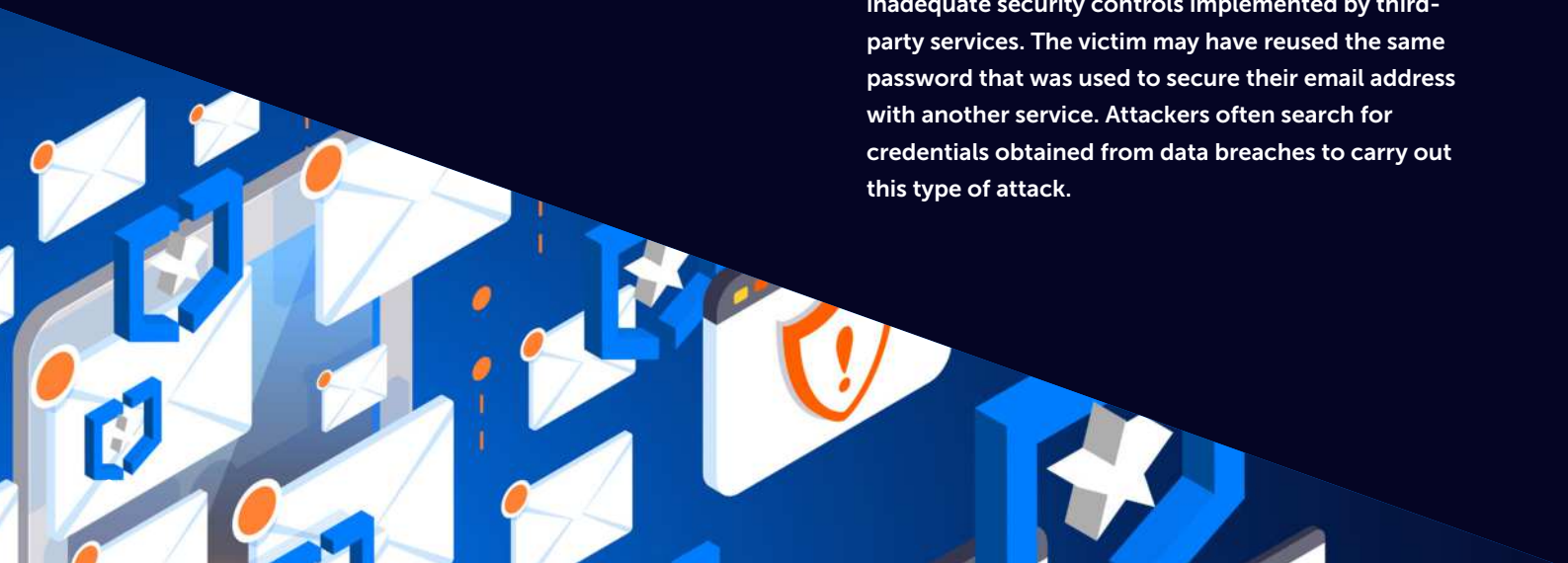
To identify the password used to secure an account, a criminal may use the following techniques:

🛡️ **Brute-Force:** An attacker attempts to exhaust a list of common passwords against an account.

🛡️ **Password Guessing:** An attacker invests time and effort into researching individuals to uncover passwords they may use, based on their interests or other publicly available attributes, such as personal information on social media.

🛡️ **Password Spraying:** An attacker attempts to log into an account using a statistically probable password which conforms to the bare minimum complexity requirements of a password policy (such as 'Winter2023!' or "CompanyName1!").

🛡️ **Credential Stuffing:** An attacker exploits inadequate security controls implemented by third-party services. The victim may have reused the same password that was used to secure their email address with another service. Attackers often search for credentials obtained from data breaches to carry out this type of attack.



At the Cyber and Fraud Centre, we provide an Incident Response Helpline to support organisations that have fallen victim to cyber attacks or financial fraud. One of the most reported incidents is Business Email Compromise (BEC) attacks.

✪ **Credential Theft:** An attacker sends an email to the victim posing as a legitimate service provider with whom the victim regularly interacts. The attacker then collects the credentials entered by the victim into a resource under their control. Alternatively, the attacker may try to trick the user into running malware that is designed to steal their login credentials.

The most common form of attack used to gain credentials for BEC are [phishing attacks](#), as they are easy to set up and carry out. It's essential that an organisation has robust protections against phishing, such as using strong spam filters, email security settings in place and training staff to identify the [signs of a phishing attack](#).

What are the motivations behind BEC attacks?

BEC attacks, like any other cyber attack, are not motivated by a single factor. The reason behind these attacks is determined by what the cybercriminals believe they can gain from hacking into the targeted organisation.

There are some typical motivators we see for Business Email Compromise attacks:

✪ **Financial Motivation:** Attackers can easily take advantage of the trust between an organisation and its customers to send out fraudulent invoices and financial transaction requests to prompt customers to send money to the attacker's bank account. Often, cybercriminals will send out a phishing email stating that the compromised organisation has changed their bank details and for all payments to be made to a new bank account belonging to the hacker.

✪ **Data Leaks and Information Gathering:** Given the significant volume of information shared via email, malicious actors can locate and disclose sensitive information about an organisation by accessing emails that are visible to a compromised account.

✪ **Supply Chain Attacks:** This involves targeting third-party service providers to participate in a larger-scale attack. Attackers compromise a trusted third party, allowing them to send phishing emails that appear legitimate to another organisation.

What impact can a BEC attack have on an organisation?

The damage caused by a Business Email Compromise attack can vary depending on the attack's motivation, the compromised account type, and the information typically sent over email in the compromised organisation.

The following points are common impacts that BEC attacks can have:

✳ **Data Loss/Exfiltration:** The illicit extraction of sensitive information, including personal information, financial details, intellectual property, or supply chain information, may lead to its sale on the internet and possible further attacks against your organisation. Additionally, such data exfiltration may result in a data breach and require the affected organisation to report the incident to the ICO.

✳ **Financial Loss:** Cybercriminals employ various tactics, such as hacking into email systems or using social engineering, to obtain information about corporate payment systems. They then deceive company employees into transferring money into their bank accounts.

✳ **Onward Access (Lateral Movement):** Compromise of additional services by authenticating as the controlled account for broader access or leveraging current access as a stepping-stone to target internal or external contacts.

✳ **Reputational Damage:** An organisation can suffer severe consequences beyond financial losses due to a data breach or fraud attack. The resulting reputational damage can be devastating and may even cause some organisations to never fully recover.

It is worth noting that numerous organisations only become aware of an account compromise when informed by an external party. Business Email Compromise attacks may remain undetected for extended periods, and the perpetrator can easily conceal emails sent to and from the compromised account, it's often the case that the criminals will add forwarding rules to email accounts and often private emails are being read by the hackers long before the business is aware of any criminal activity.

What should you do if you suffer a Business Email Compromise attack?

If an account compromise is detected, the following measures can be implemented to minimise harm and eliminate the criminal's access to the compromised email account:

✳ **Temporarily Disable the Account and Invalidate Existing Sessions:** The email administrator should deactivate the account until communication with the victim is established. Additionally, if necessary, all existing session tokens should be forcibly expired to invalidate active login sessions. This step is crucial in preventing the attacker from retaining temporary access until the session cookie's expiration after a password change.

✳ **Debrief with the Victim:** Discuss whether the victim has observed anything suspicious recently, such as a potential phishing attack or abnormal behaviour on their email account. This could help uncover other affected accounts or provide a basis for investigating a possible endpoint compromise or a credential harvesting phishing attack that may have targeted other users within the organisation. It is essential to conduct this discussion without assigning blame or causing embarrassment to the victim to ensure that other staff members are encouraged to report any suspicious activity or potential phishing attacks.

✳ **Password Changes:** Promptly change the compromised account's password to a new one. To ensure password strength, the National Cyber Security Centre recommends using a combination of [three random words](#), which should not match any other passwords (whether personal or work-related). The victim should also be advised to change their password for any other accounts where they may have used the same password.

✳ **Check for Forwarding Email Rules:** Check your email forwarding rules and delete any rules that were added without your knowledge or consent. If you come across any suspicious URLs, IP addresses, or email addresses in the forwarding rules, it may be useful to record them in case an incident needs to be reported to the police.

How can you prevent Business Email Compromise attacks?

To prevent Business Email Compromise (BEC) attacks, several measures can be taken that will also enhance overall cyber security for an organisation. These measures include:

- ✪ **Robust Password Policy:** Implementing a password policy with a minimum length of 8 characters and requiring password changes every three months can result in weaker passwords being chosen. Instead, a 14-character password changed annually is better. Additionally, consider allowing users to see their passwords while typing them to avoid easy-to-guess passwords. For more information, refer to the [NCSC's guidance on password management](#).
- ✪ **Two-Factor Authentication (2FA):** 2FA is an effective way to prevent account compromises. It provides an extra layer of security that is difficult for hackers to bypass.
- ✪ **Password Managers:** Password managers generate and store passwords securely, removing the burden of remembering multiple passwords from the individual. They can also enable easy and safe sharing of credentials for accounts used by multiple people within an organisation. Password managers can be online-based or store credentials locally.
- ✪ **Strong Spam Filters:** Phishing attacks are the most common way BEC attacks occur. Having strong spam filters can prevent phishing emails from reaching employees and reduce the likelihood of a BEC attack.
- ✪ **Training:** Educating employees regularly on how to identify and respond to phishing attacks can reduce the chances of an employee falling victim to one. A system for alerting employees when a phishing attack has bypassed spam filters can also help raise awareness.

- ✪ **Review Public Information:** Reviewing information shared on an organisation's website, such as email addresses, interests, roles, and responsibilities, can help identify information that attackers may use to their advantage.

- ✪ **Robust Financial Processes:** Implementing [anti-fraud measures](#) for verifying financial transactions, such as two-factor authentication and verifying transaction details against previous records, can prevent financial gain as a motive for BEC attacks.

- ✪ **Detection and Analysis Methods:** Proactive detection mechanisms can be implemented to identify account compromises as they occur. Most email service providers record details such as login attempts and emails sent, allowing organisations to identify unusual or malicious activity.

- ✪ **Business Continuity Plan:** A BEC attack mitigation plan should be added to an organisation's business continuity plan. This plan should be easily accessible to all employees and clearly outline the steps to take in the event of a BEC attack.

In case you suspect that you have fallen victim to a Business Email Compromise incident, reporting the crime to Police Scotland is recommended, and this can be done by **calling 101**.

It is also a good idea to review your business insurance policy, as you may have cyber insurance coverage included as part of your regular business policy.

Alternatively, if you require additional guidance or support regarding a Business Email Compromise incident, you can contact the Cyber and Fraud Centre's [Incident Response Helpline](#) on:

0800 1670 623



📍 Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

☎ 01786 447 441

✉ enquiries@cyberfraudcentre.com

🏠 www.cyberfraudcentre.com

🐦 [@cyberfraudcen](https://twitter.com/cyberfraudcen)

🌐 [cyber-and-fraud-centre](https://www.linkedin.com/company/cyber-and-fraud-centre)