Business Email Compromise (BEC) Playbook

What is Business Email Compromise (BEC)?

A Business Email Compromise (BEC) is an email-based fraud technique that is designed to allow an attacker to gain unauthorised access to confidential information or extract money through fraudulent requests for payment or wire transfer.

How does BEC work?

BEC attacks typically rely on the ability of the attacker to impersonate a well-known individual in an organisation (e.g. the CEO) or a trusted external contact/partner/entity. This can be achieved in various ways but the most common methods include (i) Email Domain Spoofing; (ii) Lookalike Email Domain; and (iii) Email Account Compromise. These terms will be elaborated later under the section of How to Respond to an Incident. Do note that the three scenarios provided in this playbook are not exhaustive.

As more organisations shift their operations online, the attack surface for cybercriminals have correspondingly increased. Cybercriminals now have more opportunities to launch BEC attacks, with such attacks sometimes also leveraging on current events or themes to enhance their plausibility and subsequently, increase the probability of success.

As organisations are the primary target of such attacks, there is a need to be vigilant and take steps in preventing BEC incidents and if such an incident occurs, be prepared to respond to it.

The purpose of this playbook is to provide guidance to organisations on the preventive steps to take and if an incident occurs, the possible steps which can be taken to remediate the incident. This playbook comprises three main sections (excluding the Annex):

- How to Prevent BEC
- How to Respond to an Incident
    - Email Domain Spoofing

How to Prevent BEC

Organisations should review their processes and implement appropriate measures to secure their corporate email accounts against BEC. Such measures include:

Promote a Culture of (Cyber) Vigilance Among Employees

- Regularly share cyber hygiene tips and news on current scam/phishing cases
- Conduct regular phishing drills and remind employees to verify the authenticity of emails, especially those that are suspicious or unsolicited

Enforce the Use of Strong Passwords and Enable 2FA

- Institute a password policy to ensure that all users use strong passwords (i.e., at least 12 characters with upper- and lower-case letters, numbers, and special characters)
- Enable two-factor authentication (2FA), where possible, as an additional layer of security to prevent unauthorised access to an email account in the event that the password has been compromised

Inspect Suspicious / Urgent Emails Closely

- Phishing campaign emails are usually crafted using urgent language and may detail dire consequences if the recipient does not take actions promptly BEC-type emails may also ask the recipient to change the designated account for receiving wire payments. Below are some examples of tell-tale signs of a possible phishing email:
    - C-suite executives asking for unusual information or non-standard type of questions
    - When attempting to reply to that email, the “To” email address does not match sender’s email address shown on the original email
    - Requests for the conversation thread to be private

  - Requests to skip the usual channels to perform the task
- Seek confirmation using a different medium (i.e. phone call or text message) before proceeding with any out-of-ordinary instructions sent via email
- Report any suspicious phishing email to the relevant IT department/vendor and do not click on any links or open any attachments found in the email

Maintain System Hygiene

- Ensure that automatic updates are enabled for the anti-virus software and perform a full scan of the machine(s) in your network regularly
- Conduct regular audits on user passwords against common password lists by using available resources and tools online
- Verify and remove any unauthorised/suspicious/dormant user accounts in the system as these could be leveraged to gain access into the system
- Monitor access logs and investigate multiple unsuccessful login attempts
- Ensure your email infrastructure can store audit and access logs for a minimum of six months (log retention policies may differ depending on organisational and legal requirements) to allow for proper forensics investigation on a suspected or confirmed incident

Implement Additional Verification Process for Finance-related Requests

- Implement a secondary confirmation* process to verify the authenticity of finance-related requests, including funds transfer, change of supplier or vendor bank account, and invoice payment

**This secondary confirmation should be conducted via a different medium (i.e. phone call or text message) to prevent direct communications with the cybercriminal, in the event the email account has been compromised.*

Prohibit Automatic Email Forwarding to External Addresses

- Attackers may create email rules to automatically forward emails received by the compromised account to an external email address. Organisations can consider prohibiting such rules by default and review any exceptions on a case-by-case basis

Install a Secure Email Gateway (SEG)

- SEG is a device or software used for email monitoring. It is designed to stop spam, malware, and viruses from being delivered to users via email. It can also detect a spoofed domain coming from an attacker (or impersonator) and will usually block them from delivery
- Administrators can use SEG to check for keywords commonly used in BEC incidents such as “payment”, “urgent”, etc. and flag such emails for further review

Use Email Authentication Techniques such as SPF, DKIM and DMARC

- Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) are anti-spoofing and email authentication techniques using DNS records to validate the sender of the email
- DMARC uses SPF and DKIM authentication protocols to verify emails sent from the organisation’s domain. Organisations can use DMARC to prevent malicious (e.g. spoofed, phishing) emails from reaching their users’ main inbox
- Use a digital signature to verify that the email is sent by the intended user

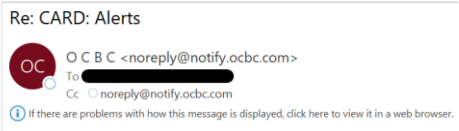
Review Organisation-wide Email Accounts Policy

- Assess and review if corporate email accounts should be made publicly available. Not releasing it publicly will reduce the attack surface.

How to Respond to an Incident

[Scenario 1] Email Domain Spoofing

In email domain spoofing, attackers try to trick users into thinking that an email came from an individual or an entity they are familiar with. To do so, attackers modify a malicious email's envelope and header such that the victim's email client displays seemingly legitimate information.


Re: CARD: Alerts

OC

O C B C <noreply@notify.ocbc.com>
To [redacted]
Cc noreply@notify.ocbc.com

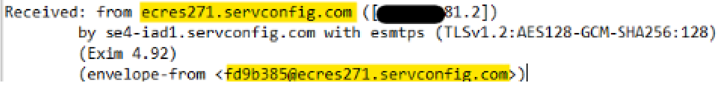
ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Figure 1: Email Domain Spoofing Sample

Step 1: Investigate & Analyse Evidence(s)

Identify and analyse the phishing/suspicious email(s) received from the spoofed email

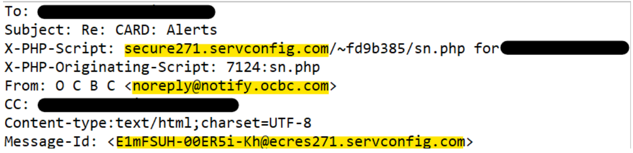
- Extract the email header to identify the originating sender's email address and the IP address of the mail server to confirm if the email came from a legitimate source. *[Instructions on how to extract email headers can be found in the Annex]*



```
Received: from ecres271.servconfig.com ([[redacted]81.2])
        by se4-iad1.servconfig.com with esmtps (TLSv1.2:AES128-GCM-SHA256:128)
        (Exim 4.92)
        (envelope-from <fd9b385@ecres271.servconfig.com>)
```

Figure 2: Extract of Sample Email Header

- Analyse the actual content of the email to determine the TTP of the attack (e.g. impersonating as the company's CEO, business partner or a known contact; phishing content; malicious attachment; how the attacker spoofed the email).



```
To: [redacted]
Subject: Re: CARD: Alerts
X-PHP-Script: secure271.servconfig.com/~fd9b385/sn.php for[redacted]
X-PHP-Originating-Script: 7124:sn.php
From: O C B C <noreply@notify.ocbc.com>
CC: [redacted]
Content-type:text/html;charset=UTF-8
Message-Id: <E1mFSUH-00ER5i-Kh@ecres271.servconfig.com>
```

Figure 3: Extract of Sample Email Header

- Look up any links contained in the email for further investigation
- Examine any attachment contained in the email (a malicious file attachment opened by the victim could potentially infect other parts of the company's network).

Step 2: Recovery/Restoration

- Report the identified originating sender's email address and the IP address of the mail server to the network hosting provider and domain registrar for takedown. This information can be retrieved from open-source whois websites such as https://centralops.net/co/. The email header can also be provided to the abuse teams as evidence of malicious intent.

- Implement Email Authentication Techniques such as SPF, DKIM and DMARC as recommended in the previous section to prevent spoofed emails from reaching the inboxes of users.

[Scenario 2] Lookalike Email Domain

Cybercriminals may spoof a legitimate email account with slight variations. For example, if the legitimate email account is john@kellymanufacturing.com, john@kellymanufacturinng.com may be used to trick victims into thinking that the lookalike email account is authentic. If cybercriminals have access to legitimate existing email threads, they may undertake conversation hijacking by inserting themselves into the conversation to enhance their credibleness to unsuspecting victims. If the victim falls for the scam, they will typically be instructed to divert an upcoming monetary transfer to a fraudulent bank account.

Step 1: Investigate & Analyse Evidence(s)

Identify and analyse the phishing/suspicious email(s) received from the spoofed email

- Extract the email header to identify the IP address(es) of the mail server for the lookalike email domain. *[Instructions on how to extract email headers can be found in the Annex]*
- Analyse the original email thread and determine its legitimacy based on prior email conversations, if available. If the previous email thread is legitimate, identify the original legitimate email address(es) contained within that thread. These accounts should be checked for any compromise. This can be done by reviewing email audit logs for anomalies (i.e. multiple failed login attempts, logins from unfamiliar IP address(es), logins at unusual hours, etc.).
- Depending on the organisation's network infrastructure, server(s) storing the organisation's emails should also be checked for any unauthorised access/activity.

If any email account(s) compromises are discovered, the organisation should identify the types of data which may plausibly be exfiltrated. If the data consist of Personally Identifiable Information (PII), refer to the following section for regulatory compliance. This should be done concurrently with the ongoing recovery/investigation.

Step 2: Recovery/Restoration

- If any compromises were found, attempt to identify the initial access vector. This can take the form of poor password management, software vulnerabilities, etc.. Upon identifying the cause of compromise, steps should be taken to remediate the incident (e.g. implementing a strong password policy, patching vulnerabilities, etc.).
- Regardless of whether email account(s) were determined to be compromised, if prior legitimate email conversations were present in the spoofed email, the passwords of previously identified email account(s) should be changed to secure the account(s). Two-factor authentication (2FA) should also be enabled if possible.
- As a precaution, run a full system scan using an updated Anti-Virus application to remove any known malware that may be installed in the organisation's network.
- Report the lookalike email address(es) and the IP address(es) of the mail server to the network hosting provider and domain registrar for takedown. This information can be retrieved from open-source whois websites such as https://centralops.net/co/. The email header can also be provided to the abuse teams as evidence of malicious intent.

[Scenario 3] Email Account Compromise

An organisation's email account(s) can also be compromised through a variety of ways such as phishing attacks, malware, the utilisation of data from past data breaches and credential dumps to perform credential stuffing attacks, as well as the harvesting of possible account information of victims from social media platforms. Cyber criminals may use the compromised email account(s) to impersonate unsuspecting legitimate individuals for monetary gains and/or to exfiltrate sensitive data.

✉ Step 1: Identify the Affected Email Account(s) and Determine the Extent of the Compromise

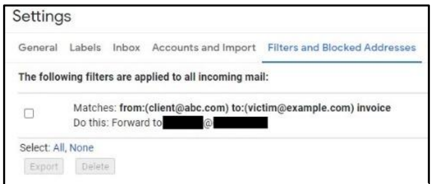
Identify the email account(s) that was used to conduct malicious activities, and the possible cause(s) that might have resulted in this compromise.

- Did the victim receive any phishing email(s) and subsequently provide their account credentials?
- Did the victim receive any suspicious email(s) and open any malicious attachment(s) that could have infected the victim's system and other devices in the same network?
- Was there any confidential information leaked to the attackers that could possibly compromise a part of or the entire organisation's network infrastructure?

The organisation should also identify the types of data affected by the compromised email account. If the data consist of PII, refer to the following section for regulatory compliance. This should be done concurrently with the ongoing recovery/investigation.

Step 2: Acquire Evidence(s) for Investigation and Analysis

- Extract the compromised email account(s)'s entire mailbox, including sent and deleted items for forensics investigation and analysis.
    - Look for suspicious email(s) that may have been used to conduct the fraudulent requests. Take note of the date and time stamp of the emails to help in the forensics investigation.
- Extract all email forwarding rules and check for any unauthorised rules created, such as auto forwarding rule(s).
    - The attacker may have created an auto forwarding rule to an external email to monitor any incoming emails from clients



The following filters are applied to all incoming mail:

□ Matches: **from:(client@abc.com) to:(victim@example.com) invoice**
Do this: Forward to [redacted]@[redacted]

Figure 4. Sample Email Forwarding Rule

and colleagues. This step could be taken in preparation to launch a BEC attack.

- Extract all relevant logs such as network, smtp and audit logs for further forensics investigation and analysis.

Step 3: Investigate & Analyse Evidence(s)

- Identify and analyse any phishing/suspicious email(s) sent from the compromised account
    - Analyse the actual content of the phishing/suspicious email(s) to determine the tactics, techniques and procedures (TTPs) of the attack (e.g. impersonating as the company's CEO, business partner or a known contact, phishing content, malicious attachment, etc.).
    - Lookup any links contained in the email for further investigations.
    - Examine attachment(s) contained in the email (a malicious file attachment opened by the victim could potentially infect other parts of the company's network). Any attachments can be uploaded onto VirusTotal (https://www.virustotal.com) to detect any known malicious content.

- Analyse the access logs to check for any anomalies such as multiple failed attempts, login from an unfamiliar IP address, or logins at unusual hours.
- Analyse the proxy logs to rule out any possible case of victim accessing malicious URL(s).

Step 4: Recovery/Restoration

- Change the password of the compromised account(s) immediately to a strong password of at least 12 characters which includes upper case, lower case, numbers and/or special characters (this may vary depending on your organisation's password policy)
- Implement the usage of multi-factor authentication (MFA) for all corporate email accounts, if possible.
- Delete any unauthorised forwarding rules created in the victim's email account.

- Check other email accounts that are within your domain for similar rules (if any) and remove them.
- Perform a full anti-virus scan with an updated anti-virus definition on the affected machine(s).
- Ensure that all systems and software are patched to the latest version.

Notify and Report the Incident

If your organisation handles sensitive information such as PII, you may be required to report the data breach/leak incident to the Personal Data Protection Commission (PDPC).

- Contact your legal team/provider to assist in the notification process. You may need to inform your customers, clients, and suppliers, as well as staff and employees.
- If required, report the incident to the PDPC at https://www.pdpc.gov.sg. The website also provides guides and other resources on handling sensitive data.
- If you believe that financial information has been compromised, also contact your financial institution to check for any unauthorised transactions.

Other Incident Reporting Channels

- Report the incident to SingCERT via our incident reporting form.
- If monetary loss(es), or criminal activity is involved, you may lodge a police report at any neighbourhood police post or online here.

Note: Several steps in incident response may be highly technical. If necessary, organisations should consider engaging a cybersecurity services vendor to assist with the investigation and/or remediation. Please refer to this list of Cybersecurity Advisory and Consultancy service providers (if required): https://sgtech-prod-api.sgtech.org.sg/api/Common/GetPDF?type=artical&&fileName=f509e67b-1734-4f68-b03e-743fdd659e95.pdf

Disclaimer: This playbook provides guidelines and recommendations on how to prevent and respond to possible BEC incidents. It is intended purely as a guide and is not comprehensive. Always consult a trained cybersecurity professional for advice before making any business-critical decisions within your organisation.

Annex: How to Extract Email Headers

This section serves as a guide on how to extract the email headers found in popular email platforms.

Apple Mail:

1. Open Apple Mail
2. Click on the email messages that you wish to download
3. Click on "File", then click on "Save As…" from the drop-down menu
4. Ensure the "Format" is set to "Plain Text". Then click "Save"

Gmail:

1. Login to your Gmail account
2. Open the email you wish to save
3. Click on the "3 vertical dots" icon beside "Reply"
4. Click on "Show original"
5. Right-click on "Download Original"
6. Manually change the extension from ".eml" to ".txt"

Outlook (Windows):

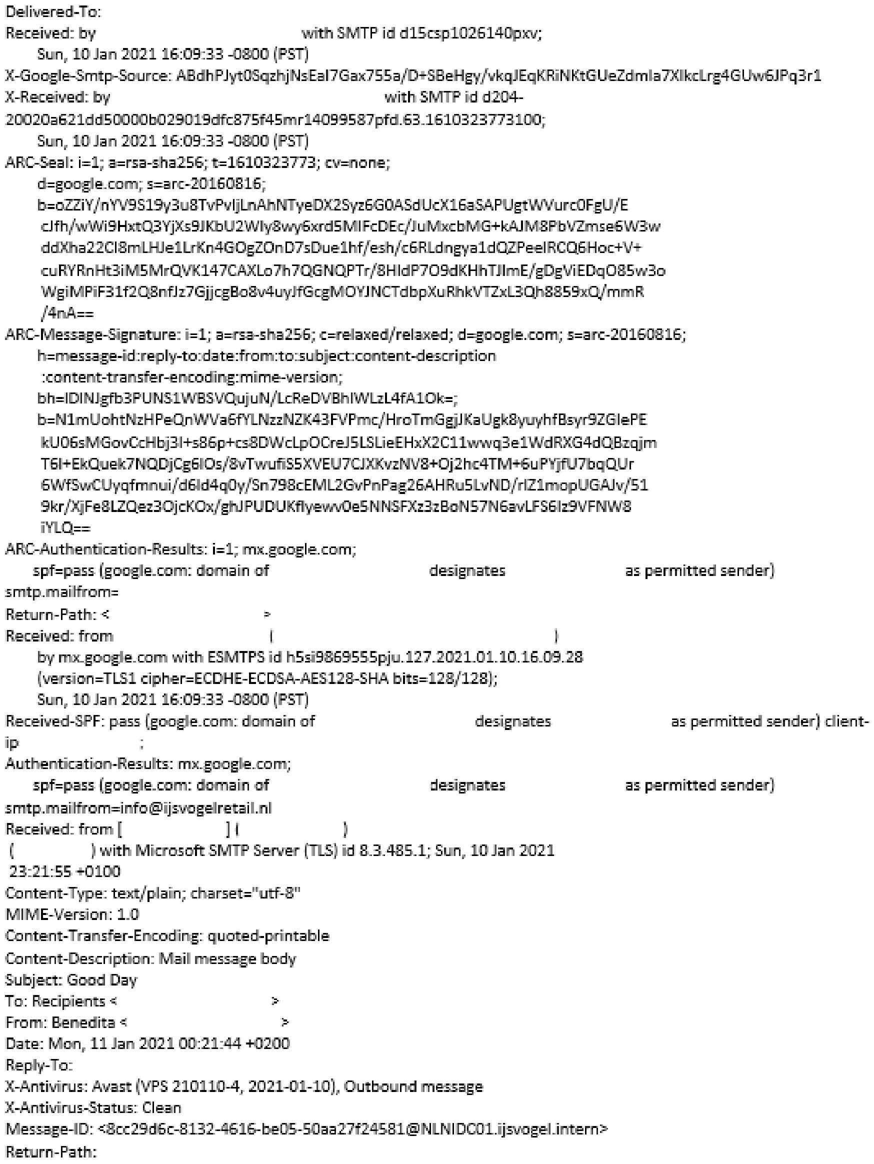
1. Open Outlook
2. Click on the email message you wish to download
3. Click on "File", then click on "Save As…" from the drop-down menu
4. Ensure the "Format" is set to "Outlook Message Format (.msg)"
5. Click "Save"

Outlook (MacOS):

1. Open Outlook
2. Click on the email message you wish to download
3. Click on "File", then click on "Save As…" from the drop-down menu
4. Ensure the "Format" is set to "Email Message (.eml)"
5. Click "Save"
6. Manually change the file format from ".eml" to ".txt"

Yahoo Mail:

1. Login to your Yahoo Mail account
2. Right-click on the email you wish to save
3. Click on “View Raw Message”
4. Copy and paste the content into a text editor (e.g. Notepad)
5. Save the file in “.txt” format



```
Delivered-To:
Received: by                                    with SMTP id d15csp1026140pxv;
        Sun, 10 Jan 2021 16:09:33 -0800 (PST)
X-Google-Smtp-Source: ABdhPJyt0SqzhjNsEal7Gax755a/D+SBeHgy/vkqJEqKRiNKtGUeZdmIa7XlkcLrg4GUw6JPq3r1
X-Received: by                                          with SMTP id d204-
20020a621dd50000b029019dfc875f45mr14099587pfd.63.1610323773100;
        Sun, 10 Jan 2021 16:09:33 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1610323773; cv=none;
        d=google.com; s=arc-20160816;
        b=oZZiY/nYV9S19y3u8TvPvIjLnAhNTyeDX2Syz6G0ASdUcX16aSAPUgtWVurc0FgU/E
         cJfh/wWi9HxtQ3YjXs9JKbU2WIy8wy6xrd5MIFcDEc/JuMxcbMG+kAJM8PbVZmse6W3w
         ddXha22Cl8mLHJe1LrKn4GOgZOnD7sDue1hf/esh/c6RLdngya1dQZPeelRCQ6Hoc+V+
         cuRYRnHt3iM5MrQVK147CAXLo7h7QGNQPTr/8HIdP7O9dKHhTJlmE/gDgViEDqO85w3o
         WgiMPiF31f2Q8nfJz7GjjcgBo8v4uyJfGcgMOYJNCTdbpXuRhkVTZxL3Qh8859xQ/mmR
         /4nA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=message-id:reply-to:date:from:to:subject:content-description
         :content-transfer-encoding:mime-version;
        bh=lDINJgfb3PUNS1WBSVQujuN/LcReDVBhIWLzL4fA1Ok=;
        b=N1mUohtNzHPeQnWVa6fYLNzzNZK43FVPmc/HroTmGgjJKaUgk8yuyhfBsyr9ZGlePE
         kU06sMGovCcHbj3l+s86p+cs8DWcLpOCreJ5LSLieEHxX2C11wwq3e1WdRXG4dQBzqjm
         T6l+EkQuek7NQDjCg6lOs/8vTwufiS5XVEU7CJXKvzNV8+Oj2hc4TM+6uPYjfU7bqQUr
         6WfSwCUyqfmnui/d6Id4q0y/Sn798cEML2GvPnPag26AHRu5LvND/rlZ1mopUGAJv/51
         9kr/XjFe8LZQez3OjcKOx/ghJPUDUKflyewv0e5NNSFXz3zBoN57N6avLFS6lz9VFNW8
         iYLQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of                    designates                  as permitted sender)
smtp.mailfrom=
Return-Path: <                    >
Received: from                    (                                        )
        by mx.google.com with ESMTPS id h5si9869555pju.127.2021.01.10.16.09.28
        (version=TLS1 cipher=ECDHE-ECDSA-AES128-SHA bits=128/128);
        Sun, 10 Jan 2021 16:09:33 -0800 (PST)
Received-SPF: pass (google.com: domain of                    designates                  as permitted sender) client-
ip                    ;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of                    designates                  as permitted sender)
smtp.mailfrom=info@ijsvogelretail.nl
Received: from [              ] (              )
 (          ) with Microsoft SMTP Server (TLS) id 8.3.485.1; Sun, 10 Jan 2021
 23:21:55 +0100
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Description: Mail message body
Subject: Good Day
To: Recipients <                    >
From: Benedita <                    >
Date: Mon, 11 Jan 2021 00:21:44 +0200
Reply-To:
X-Antivirus: Avast (VPS 210110-4, 2021-01-10), Outbound message
X-Antivirus-Status: Clean
Message-ID: <8cc29d6c-8132-4616-be05-50aa27f24581@NLNIDC01.ijsvogel.intern>
Return-Path:
```

Figure 5: Sample of Email Header