Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Protecting against business email compromise

First published: October 2020
Last updated: October 2021

Introduction

Business email compromise is when malicious actors use email to abuse trust in business processes to scam organisations out of money or goods. Malicious actors can impersonate business representatives using similar names, domains and/or fraudulent logos as a legitimate organisation or by using compromised email accounts and pretending to be a trusted co-worker.

Common scams associated with business email compromise include:

- **Invoice fraud:** Malicious actors compromise a vendor's email account and through it have access to legitimate invoices. The malicious actors then edit contact and bank details on those invoices and send them to customers with the compromised email account. The customer pays the invoice, thinking they are paying the vendor, but instead send that money to malicious actors' bank accounts.

- **Employee impersonation:** Malicious actors compromise a work email account and impersonate a co-worker via email. Malicious actors can use this identity to commit fraud in a number of ways. One common method is to impersonate a person in power (such as a chief executive officer or chief financial officer) and have a false invoice raised. Another method is to request a change to a worker's banking details. The funds from the false invoice or the worker's salary is then sent to malicious actors' bank accounts.

- **Company impersonation:** Malicious actors register a domain with a name very similar to a large, known and trusted organisation. Malicious actors then impersonate the organisation in an email to a vendor and request a quote for a quantity of expensive goods, like laptops. Malicious actors negotiate for the goods to be delivered to them prior to payment. The goods are delivered to a specified location, however, the invoice is sent to the legitimate organisation, who never ordered or received the goods.

How do I prevent my email accounts being compromised?

Be vigilant against phishing

Phishing (pronounced 'fishing') are scams that are made to appear as if they were sent from individuals or organisations you think you know, or you think you should trust. Malicious actors can steal credentials using phishing techniques and then do further harm, using those compromised credentials to login and send out malicious or fraudulent content to your contacts.

Phishing is not just limited to email. These scams are delivered via SMS, instant messaging and social media, and pretend to be trusted organisations like:

- State and Territory police or law enforcement
- utilities such as telecommunications, postal services, power and gas companies
- banks, and other financial institutions
- Government departments, such as the Australian Taxation Office, Centrelink and Medicare, or government services such as myGov.

Reputable organisations will not call, SMS or email to verify or update your information. This includes companies such as Amazon, PayPal, Google, Apple and Facebook. When you receive unsolicited contact from organisations, there are a number of simple things you can do to keep yourself safe.

- Check details such as the spelling of a sender's domain name. Double-check by comparing it to previous correspondence.
- Use spam and message scanning services offered by your email, SMS or social media providers to filter potentially harmful content.
- Exercise critical thinking and vigilance when receiving phone calls, messages and emails.
- Exercise caution opening messages or attachments, and clicking on links from unknown senders.
- Do not provide personal information (such as usernames, PINs, passwords, passphrases or secret/security questions and answers) to unverified sources.

Many organisations have security pages that identify active scams using their branding. If a message seems suspicious, contact the person or organisation separately, using contact details you have verified separately (for example, obtaining the phone number from the organisation's official website) to check if they are likely to have sent the message.

Use multi-factor authentication and strong passphrases

Use multi-factor authentication so that workers can authenticate their credentials when accessing business email and systems. Multi-factor authentication is one of the most effective controls you can implement to prevent unauthorised access to computers, applications and online services. Using multiple forms of authentication makes it much harder to access your systems. Malicious actors might manage to steal one type of credential but it is very difficult to steal the correct combination of several credentials for any given account.

Multi-factor authentication can use a combination of:

- something the user knows (a passphrase, PIN or an answer to a secret question)
- something the user physically possesses (such as a smartcard, physical token or security key)
- something the user inherently possesses (such as a fingerprint or retina pattern).

Finally, encourage workers to use a biometric or strong passphrase to lock their devices – especially the portable ones.

Have protective business processes in place

Establish a clear and consistent business process for workers to verify and validate requests for payment and sensitive information. Protect worker contact details from the public, particularly departments that are likely to be targeted by scams, such as accounts, finances or human resources teams.

Ensure workers are aware of following warning signs:

- an unexpected change of bank details
- an urgent payment request or threats of serious consequences if payment isn't made
- unexpected payment requests from someone in a position of authority, particularly if payment requests are unusual from this person
- an email address that doesn't look quite right, such as the domain name not exactly matching the supplier's company name.

Ensure workers have clear guidance to verify account details, to think critically before actioning unusual requests, and have a reporting process to report threatening demands for immediate action, pressure for secrecy or requests to circumvent protective business processes.

Help combat your business reputation from being used in scams

Develop and maintain good cybersecurity. Malicious actors can gain access to a legitimate email account by compromising your systems. Follow the Australian Signals Directorates (ASD)'s Essential Eight and implement the controls detailed in the *Essential Eight maturity model*, particularly on computers used by your finance, human resources and senior executive teams.

Consider registering domains that look similar to your organisation's (for example, replace letters such as 'l' and 'o' in your organisation's name with digits such as '1' and '0'). This will help prevent malicious actors from scamming others by using a domain that looks similar to yours. You can check for domains masquerading as your business by monitoring certificate transparency logs. There are also commercial entities that will provide this service.

If you manage your own email server and domain, implement email verification. Sender Policy Framework (SPF) and Domain Message Authentication Reporting and Conformance (DMARC) are controls designed to detect fake emails by specifying which mail servers are authorised to send emails on behalf of an organisation's domain.

How do I recover from business email compromise?

If you have been the victim of business email compromise, follow the following steps as soon as possible:

- if you've sent money or banking details to a scammer, contact your bank immediately
- report the cybercrime incident to ASD

- if any of your email accounts were compromised, change your password for your email account(s), notify anyone affected, and protect your stakeholders with a warning notice on your website informing them of the scam.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information on phishing is available in the *Detecting socially engineered messages* publication.

Further information on multi-factor authentication is available in the *Implementing multi-factor authentication* publication.

Further information on how to implement SPF and DMARC is available in the *How to combat fake emails* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

AUSTRALIA

Australian Government

Australian Signals Directorate