Business email compromise

certnz

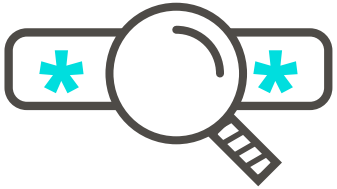
Here's what you need to know to help secure your business email.

What is business email compromise?

Business Email Compromise is when an attacker gains access to a business email account without the organisation's knowledge, and then uses that account to carry out a range of attacks or scams.

Why would anyone want to do that?

Business emails hold a lot of handy information, like details on billing cycles and bank accounts. If scammers gain access to your business email, they could cause a lot of damage by stealing personal and financial information, or redirecting payments to their bank account instead of yours. Attackers often target Accounts Payable and Accounts Receivable teams within organisations. They do this to intercept invoices and change the payment details to their own bank account. This can result in payments going to the attacker, rather than the intended recipient.



How do we stop this?

There are several ways you can secure your business email to minimise the risk of attackers gaining access:

- Add an extra layer of security to your accounts with two-factor authentication (2FA)
- Use strong, long and unique passwords on all your accounts. Encourage staff to use a password manager to help them remember all their passwords.
- Be careful what personal information you share online, especially on social media
- Always verify payments with a SMS or call the person who sent you the invoice

Ways to monitor your business emails

- Always monitor auto-forwarding/filtering rules on email accounts for any rules that you **did not** set up, especially those relating to accounts receivable.
  This can prevent an attacker from automatically forwarding accounts information to their own account and hiding responses from victims.
- Check your email access logs to look for any un-usual login behaviour like unusual login times and unexpected or foreign IP addresses. This can act as an alarm if anyone is trying to access your account.

What if this happens to me?

If you discover that an email account within your business has been compromised, there are some steps you can take to help reduce the impact:

- Change the passwords on all affected email accounts immediately to prevent the scammer from accessing the account and sending any further emails.
- Set up 2FA for future security.
- Tell your IT provider.
- Ask your IT provider to check your system for any installed malware.
- Report to CERT NZ
  https://www.cert.govt.nz/individuals/report-an-issue/

For more information on business email compromise see
www.cert.govt.nz/business/common-threats/

6102 CERT OCT20