



Republic of Namibia
Financial Intelligence Centre

FINANCIAL INTELLIGENCE CENTRE (FIC)

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

FOREWARNING REPORT: BUSINESS EMAIL COMPROMISE

ISSUED: OCTOBER 2022

1. Background

The Financial Intelligence Centre (FIC) has observed an increase in fraudulent conduct, commonly known as the “Business Email Compromise” (BEC).

BEC, also known as the man-in-the-email scam, is a form of phishing attack where a criminal attempts to trick unsuspecting persons into making payments or revealing sensitive data. The attacker hacks into a corporate e-mail account and impersonates the real owner to defraud the company, its customers, partners and employees into sending money or sensitive data to the attacker’s account. The attacker sends convincing-looking emails that might request unusual payments or contain links to bogus websites. Some emails may contain viruses disguised as malicious attachments, which are activated when opened.


2. How does it operate?

BEC attack is one of the most financially damaging online crimes. It exploits the fact that so many people rely on emails to conduct business. The attack relies significantly on spear phishing¹ and social engineering². It often targets individuals that handle finances or sensitive company information.

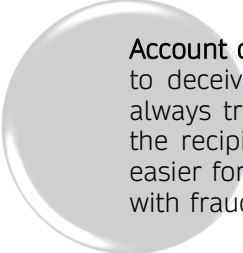
Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals and can be harder to detect. To carry out these crimes, the criminals make use of some of the following methods:

¹ Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or businesses.

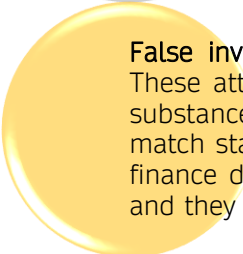
² Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.




Chief Executive Officer (CEO) fraud: An attacker poses as a CEO and sends an urgent request for funds or sensitive information transfer. Employees are inclined to trust the CEO at the company and they sometimes obey the request for money or data transfers without questioning the legitimacy of the message. Individuals in the finance department are especially likely to encounter these types of schemes.



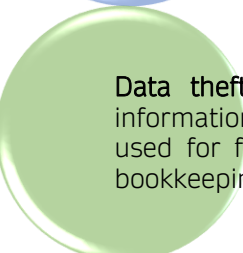
Account compromise attacks: The criminal manages to take over an employee's email account and uses such to deceive unsuspecting persons. Given that it comes from a legitimate email address, the email will not always trigger any suspicions, nor security notifications when received. Additionally, if it is an email address the recipient is familiar with, they might let their guard down. Having a legitimate email account makes it easier for hackers to internally request sensitive data and request their victims to update the payment details with fraudulent bank details.



False invoice schemes: A criminal impersonates a supplier and asks for payments from an organization. These attacks are often very sophisticated. Criminals usually go to great lengths to duplicate the style and substance of a typical invoice. The criminals usually do their research, and fraudulent requests are likely to match standard payment related documents and communications. The perpetrators can also send this to the finance department, impersonating a legitimate supplier, stating that they have changed their bank account and they provide new fraudulent bank details.



Attorney impersonation scams: Criminals pretend to be a lawyer who is working with an organization. The supposed lawyer may ask for money or data. Convinced by the apparent authority of the sender, recipients sometimes fulfil the request before double-checking the message's authenticity.



Data theft: An attacker infiltrates an organization's system (often data storage platforms) to steal key information. Instead of money, attackers in a data theft aim for personal or sensitive information that can be used for future attacks or to sell on the dark web. The main target for these attacks is often the HR and bookkeeping department, which collects and stores the most sensitive personal data from employees.

3. How can we protect ourselves

While some BEC attacks involve the use of malware, many rely on social engineering techniques, to which antivirus, spam filters, or email whitelisting are ineffective. However, one of the most useful things you can do is to educate people in key positions and deploy internal prevention techniques, especially for frontline staff who are most likely to be recipients of initial phishing attempts. Below are some measures we can employ to protect ourselves:

Avoid free web-based e-mail accounts: Establish a company domain name and use it to create company e-mail accounts in place of free, web-based accounts.

Enable multi-factor authentication for email accounts: This type of authentication requires multiple pieces of information to log in, such as a password and a dynamic pin, code, or biometric. Implementing multi-factor authentication makes it difficult for a cybercriminal to gain access to employees' emails, making it harder to launch a BEC attack.

Do not open any email from unknown parties: Do not click on links or open attachments as these often contain malware that accesses your computer system.

Double-check the sender's email address: A spoofed email address often has an extension similar to the legitimate email address. For example, a fraudulent one could look like this: tjoe@abc_company.com, in an attempt to imitate this real one: tjoe@abc-company.com.

"Forward," do not "reply" to business emails: By forwarding the email, the correct email address has to be manually typed in or selected from the address book. Forwarding ensures you use the intended recipient's correct e-mail address.

Do not overshare online: Be careful what you post on social media and company websites, especially job duties and descriptions, hierarchical information, and out-of-office details.

Always verify before sending money or sensitive information: Make it standard operating procedure for employees to confirm email requests for a wire transfer or confidential information. Confirm face-to-face, or through a phone call using previously known phone numbers, not phone numbers provided in the emails.

Know your customers and clients' habits: If there is a sudden change in business practices, beware. For example, if a business contact suddenly asks you to use their personal email address when all previous correspondence has been through company email, the request could be fraudulent. Verify the request through a different source.

REMEMBER

Business Email Compromise (BEC) is a cyber-attack involving the hacking, spoofing or impersonation of a business email address. The victim of a BEC attack receives an email that appears to come from a trusted business. The email looks and feels genuine. But it typically contains a phishing link, a malicious attachment, or a request to transfer money or sensitive information to the attacker.

If you become a victim of a BEC attack, immediately file a report with the FIC at the Bank of Namibia or contact the nearest police station to initiate a criminal investigation. This can enable intervention that reduces risks of future illicit activities. Minimizing the occurrence of these attacks reduces the chances of laundering proceeds from such activities in the financial system.