**The 5 types of Business Email Compromise (BEC)**

Business Email Compromise is a scam where cyber criminals hack into an official email account and impersonate the real email owner to deceive the company, customer, employees and/or partners, by tricking them to send sensitive data or money to the hacker’s account. The hackers usually target companies that have international suppliers and conduct wire transfers. Corporate email accounts of high-tier employees or executives related to finance or payments are spoofed or compromised through social engineering and phishing. Later, they are used to conduct fraudulent money transfers that result in losses worth thousands of dollars.

BEC attacks are also known as “Man-in-the-Email” scams. The name is derived from man-in-the-middle attacks where two parties that are communicating with each other are intercepted by an attacker who is listening and altering the communication from both ends.

**How Business Email Compromise Works**

BEC scams start with an attacker researching through publicly available data to find relevant targets. They will go through the information from your website, social media or press releases. They sift through the organization’s hierarchy, official names and job titles of higher company executives, and sometimes travel plans with the help of auto-replies to emails. They then try to access the target email account by using malware, phishing or other social engineering techniques. In order to stay undetected, they may also alter the “reply-to” address so that the email owner does not get notified when the scam is carried out.

Another way is to create a spoofed email, which looks almost same as the original email address with a slight difference. For instance, instead of [adam.smith@abc.com](mailto:adam.smith@abc.com), the attacker may use [adam.smith@abcinc.com](mailto:adam.smith@abcinc.com). If the receiver does not pay close attention, they might think that the extra “inc” attached to the domain is official address. Another real-world example is that of a spoofed domain “Paypa1.com”, which was a scam website imitating money transferring website paypal.com.

After spying on official communications for some time, the attackers then get a good idea of how to conduct a scam that works. They find out who has the responsibility of wire transfers and then create a scenario that is convincing enough to initiate quick transfer of funds.

**Types of Business Email Compromise**

There are five types of cyber-attacks in the form of scams that can result in a business email compromise.

1. **Fake Invoice Schemes**

In this type of scam, the targeted companies are often those that have foreign suppliers. The attacker pretends to be the supplier and requests fund transfer to an account that is owned by the attacker.

1. **CEO Fraud**

The hackers impersonate as the CEO or a higher management official of the company. They send an email to employees in the finance department, asking them to transfer money to an account, which is actually owned and controlled by them.

1. **Account Compromise**

In this type of Business Email Compromise, an attacker hacks an employee’s account and requests invoice payment to vendors that are listed in their contacts. These payments are sent to the attacker’s bank account.

1. **Attorney Impersonation**

In this type of scam, the attacker pretends to be an attorney or lawyer who is supposedly in charge of confidential matters of the company and asks for immediate payment of money to keep everything confidential. Such kind of requests are normally done through phone or email, and at the end of a business day for least suspicion.

1. **Data Theft**

Business email compromise cyber attacks don’t only have monetary motive, rather they also seek trade secrets or Personally Identifiable Information (PII) of executives and staff. This data is obtained usually by targeting accounts and HR employees. Cyber criminals can also keep this data to use for attacks in future.

**How to Protect Against BEC Attacks**

Before we look into how we can protect our business against BEC attacks, it’s important to know the reasons why these attacks turn out successful. There are mainly three reasons for this i.e. successful social engineering, insufficient security protocols and lack of employee awareness. If we target these three areas as a part of our cyber security policy, we can protect our business against these attacks.

Firstly, implement multi-factor authentication as a mandatory part of IT your security policy. Authentication helps stop unauthorized email access, particularly if the attacker is attempting to login from any new location. Also train your employees regularly about cyber security best practices and how they can spot and save themselves from falling for such scams. They should know how to identify fake emails and be skeptical about urgent money transfer requests coming especially from executives. Never fulfill a payment request unless verified via phone or in person.

**Current State of BEC Attacks**

According to a latest [Targeting Scams](https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009) report by Australian Competition and Consumer Commission (ACCC), Australian businesses lost around $132 million as a result of BEC attacks in 2019, which accounted to the highest financial loss incurred among all types of scams that year. The same year, a man in Lithuania was [found guilty](https://www.scmagazine.com/home/security-news/cybercrime/google-facebook-fraudster-pleads-guilty-to-stealing-123-million-in-bec-scams/) of single handedly stealing $123 million by conducting BEC scams targeted at Facebook and Google. He registered a fake business impersonating as a legitimate supplier of the tech giants, forged invoices, letters and contracts to make his requests look legitimate to the recipients.

The fact that even two of the biggest giants of tech industry fell prey to BEC attacks is a practical example of why focusing on cyber security is important for every business. These companies invest heavily on trainings and have security professionals tasked with protecting against every kind of cyber attack – if it can still happen to them, it can happy to any other business and result in dire consequences. Business Email Compromise scams are an existential cyber threat and we need to improve our cyber security measures proactively.

**KMTech’s Cyber Security Assessment**

KMTech provides a complete cyber assessment solution to businesses to help them discover vulnerabilities in the system and deal with potential threats that could emerge as a result of a Business Email Compromise scam. With our cyber assessment, your security professionals and CIOs can be confident that their most important cyber risks are addressed and their organization is well-prepared to proactively deal with any future threats. To find out more about how our solution works, book a free cybersecurity assessment with us [here](https://kmtech.com.au/book-a-cyber-assessment/).