**Understanding Business Email Compromise**

Email is a critical part of communication for businesses of all sizes, and when it's compromised, the effects can be devastating. A business email compromise (BEC) attack occurs when an email is sent to a company with the intention of fooling someone into performing an action, such as clicking on a link or opening an attachment. This type of attack can be very costly for businesses, both financially and in terms of damage to reputation.

**What is a business email compromise?**

Business email compromise or BEC is an attack targeting organisations that conduct wire transfers and export goods and supplies. It can be carried out in a number of ways, but typically involves compromising an email account and then using that account to send fraudulent messages to other employees in the company. The goal of the attack is to get the victim to perform an action, such as clicking on a link or opening an attachment, that will allow the attacker to gain access to sensitive information or money. These attacks can be incredibly costly for businesses, with the average attack costing companies more than $140,000, according to the FBI. BEC attacks can be very costly for businesses, both financially and in terms of damage to reputation.

**What are its effects?**

The effects of a BEC attack can be devastating for organisations. In addition to the financial losses that can be incurred, they also suffer damage to their reputation. Employees may also lose trust in the company's email system, which can impact communication and business operations.

Employees who are unaware of the risks of BEC attacks may be more likely to fall for these scams. In some cases, employees have transferred large sums of money to scammers or provided them with sensitive information that has allowed the hackers to steal the company's money or identity.

**How can this be prevented?**

There are a number of steps organisations take to help prevent BEC attacks. Employee training is essential, and businesses should ensure that employees are aware of the signs of a BEC attack. Email security solutions can also help to protect businesses from these attacks.

**1. Implement two-factor authentication**

Two-factor authentication is a security measure that requires two forms of identification, such as a password and a code sent to the phone, in order to access your account. This measure can help protect your account from being compromised by a BEC attack.

**2. Create strong passwords**

Creating strong passwords is another important way to protect your account from being compromised. Your passwords should be long and include a mix of numbers, letters, and symbols.

**3. Be cautious of unusual emails**

Be cautious of any emails that appear to be from a trusted source but are asking you to take action that seems out of the ordinary. Hover your mouse over any links in the email to see where they are actually going, and don't open any attachments that you aren't expecting.

**Conclusion**

With the number of business email compromise (BEC) attacks on the rise, organisations need to be acutely aware of the risks posed by these schemes and take steps to protect themselves. BEC attacks are waged by fraudsters who send phishing emails to employees with the goal of obtaining sensitive information or installing malware. In order to protect themselves from these attacks, organisations should train their employees to be aware of the common tricks used in phishing emails and to identify suspicious emails. They should also deploy an email security solution that can detect and block phishing emails.

**References**

1)<https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)>

2)<https://www.proofpoint.com/us/threat-reference/business-email-compromise>

3)<https://www.barracuda.com/glossary/business-email-compromise>

4)<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/>

5)<https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf>

6)<https://www.armorblox.com/learn/business-email-compromise/>

7)<https://terranovasecurity.com/examples-business-email-compromise/>