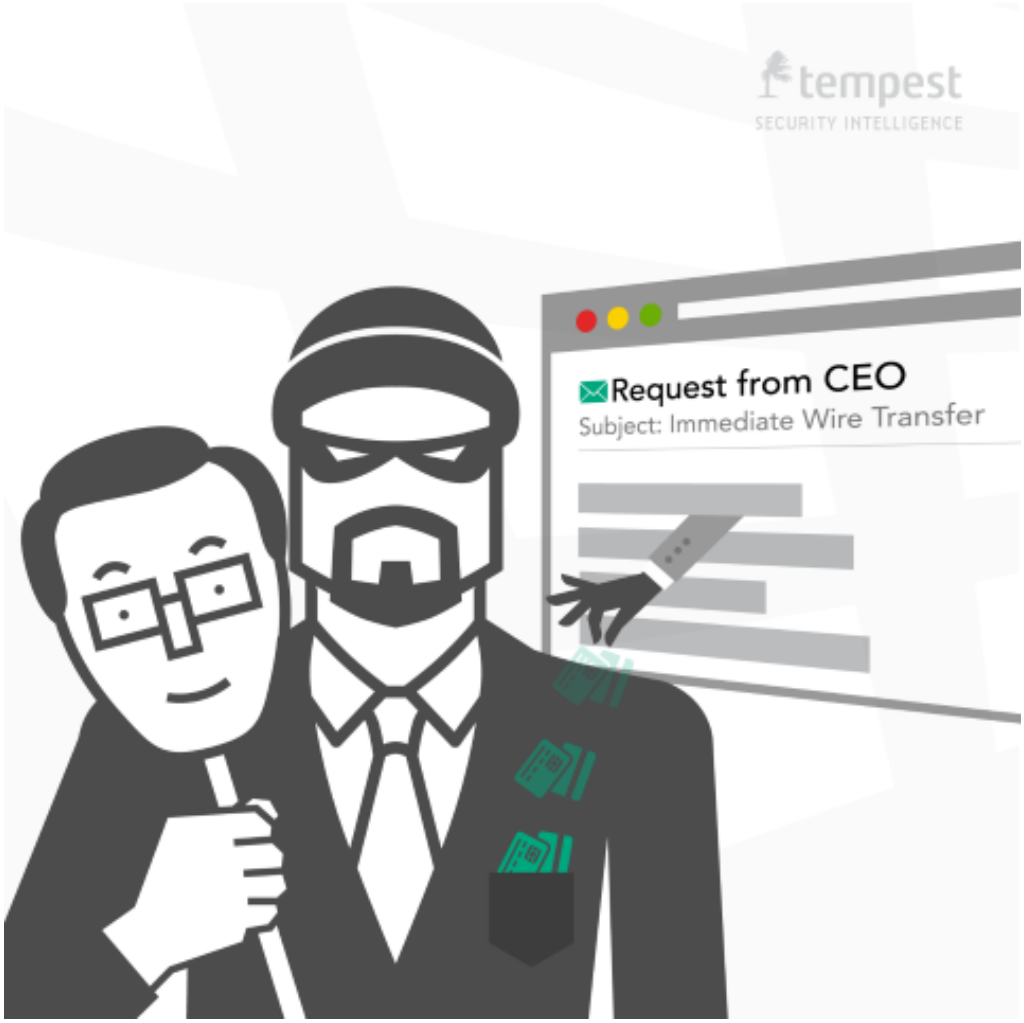
Special Bulletin - Fraud Alert!



Email scams known as "CEO Fraud" are very common right now. They are a type of "Business Email Compromise" (BEC). There have been numerous recent cases reported in the media, and we too, are seeing many reports by our customers. One customer described these attacks as 'rampant'.

How to prevent business email compromise attacks?

Some business email compromise (BEC) attacks involve the use of malware, others rely on social engineering techniques for which antivirus, spam filters, or email whitelisting are useless. However, one of the most rewarding things you can do is educate employees and implement internal prevention techniques, especially for those employees who are most likely to be the recipients of initial phishing attempts.

Here are some self-defense strategies that can help you mitigate attacks and protect your organization:

1. Enable multi-factor authentication for business email accounts. This type of authentication requires several types of login information such as password and dynamic pin, mail or biometric data. The implementation of multi-factor authentication makes it difficult for a cybercriminal to access employee emails, making it difficult to launch a BEC attack.
2. Do not open any emails from unknown persons. If you do, do not click on links or open attachments, as they often contain malware that gains access to your computer system.
3. Protect your domain. Domain spoofing uses subtle changes to legitimate email addresses to trick BEC victims. Registering domain names similar to yours will go a long way in protecting against email spoofing, which is the basis of successful attacks.
4. Double-check the sender's email address. A fake email address often has an extension similar to a legitimate email address. For example, the scam example@abc_company.com

or example@abc-company.biz instead of legitimate example@abc-company.com.

5. Always check where you are sending money or data. Make it a standard operating procedure for employees confirming bank transfer email requests or confidential information. Confirm this in person or by phone call using previously known numbers, not the phone numbers provided in the email.
6. Pay attention to changes in customer and supplier behavior. If there is a sudden change in business practices, be careful. For example, if a business partner suddenly asks you to use their personal email address when all previous correspondence has gone through the company's email, the request could be fraudulent. Check the request through another source.
7. Implement and enforce DMARC (DMARC stands for "Domain-based Message Authentication, Reporting & Conformance", an email authentication, policy, and reporting protocol) on your organizational (active & inactive) domain levels (including subdomains that you used).

--