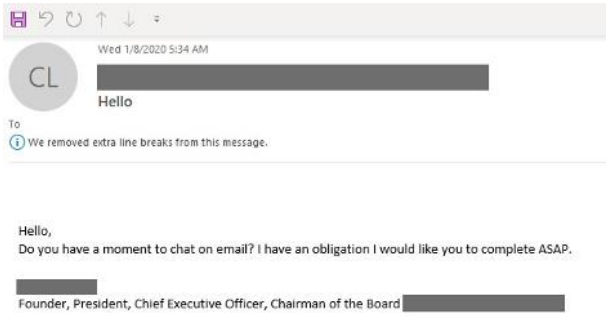
Three warning signs of a Business Email Compromise (BEC) attack

Business Email Compromise (BEC) has become a major concern for organizations of all sizes, in all industries, all around the world. In 2019, the FBI's Internet Crime Complaint Center (IC3) recorded 23,775 complaints about BEC, which resulted in more than $1.7 billion in losses.

BEC is perpetrated when attackers spoof a trusted identity to lure their targets into providing sensitive information and rerouting funds. Since these attacks rely on publicly available research and social engineering rather than malicious links or attachments, they can be especially hard to detect using traditional tools and methods. While these attacks have become more refined and targeted in recent years, there are a few tell-tale signs that can help these deceptive messages stand out. To successfully identify and protect against BEC attacks, keep these three common warning signs in mind:

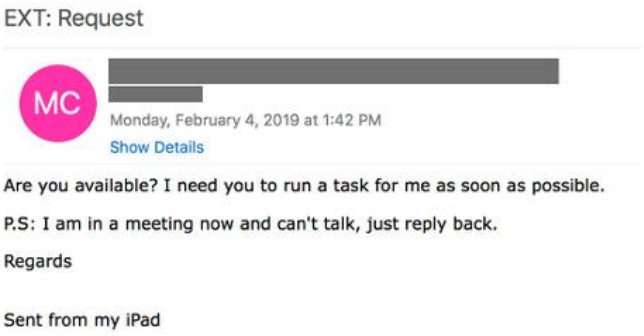
1. Time sensitive and covert requests

When executing BEC attacks, attackers often try to elicit an emotional response from their targets. Commonly spoofing the identity of an executive or high-level manager within their target's department, these messages will request 'last minute changes' or 'personal favors', relying on the targeted employee's desire to help their boss or a company executive. As these types of attacks are becoming more and more refined, these requests will also come at the end of the workday and week, putting pressure on targeted employees to finish requests before the end of business hours.



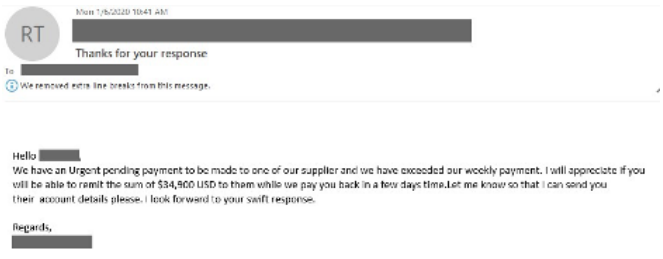
2. Messages from personal mailboxes and mobile

Another common tactic that threat actors may exploit to get around existing defenses is spoofing an executive, employee or supply chain partner's personal mail address, such as a Gmail or Yahoo account. To give off the impression of a last-minute request, these messages can say something to the tune of "Hi <employee>, I had to leave the office on my way to the airport, but we just received a message from <critical supply chain partner> and we need to change their routing information by EOD. Can you assist while I'm traveling?" with a stock signature giving the impression it was sent from their mobile phone.



3. Direct messages from supply chain partners

An increasingly frequent tactic in BEC and Email Account Compromise (EAC) attacks is the use of supplier identities, whether spoofed or through compromised user accounts. Taking on the identities of supply chain partners is very effective for threat actors, circumventing any internal processes, and taking on an identity that the receiver is not as familiar with as a fellow employee. Messages that use these tactics can be identified by their direct nature - an employee may receive a request directly from the supplier to suddenly change payment routing or shipping information without going through the typical process and the proper paperwork.



Learn more

Looking out for these common warning signs can help your organization prevent these attacks from going any further than the inbox. However, to truly combat BEC effectively, organizations need multi-layered defenses that combine end-user training, email gateway, and email authentication for full protection. To learn more about how you can fully protect your organization and its employees, find out more about Proofpoint Email Security and Proofpoint End-User Security Awareness Training

bsi.

proofpoint.