5 Tips for Defending Against BEC and EAC Attacks

Proactive steps you can take to engage end users and prevent successful attacks

There is no escaping the fact that people are the last line of defense against business email compromise (BEC) and email account compromise (EAC) attacks.[1] Cybercriminals are using imposter emails, emails from compromised accounts, vishing (voice phishing) phone calls, pretexting, and other social engineering techniques to craft highly believable attacks designed to trick your end users into making costly mistakes.

Technical safeguards can only do so much. These types of attacks more easily evade perimeter defenses because they generally exclude hallmarks associated with other kinds of phishing emails, like spammy language, embedded links, and infected attachments. That's why security awareness training about this particular topic is so critical.

To Defend Against BEC and EAC Attacks, You Must Engage Your Employees

When it comes to BEC prevention, the I's have it. Keep these five points in mind:

1. Identify individuals within your organization (like controllers, accountants, HR representatives, etc.) who would be likely targets of BEC and EAC attacks. Also identify individuals and partner organizations that may legitimately request wire transfers, invoice payments, gift card purchases, and transfers of sensitive data (like employees' W-2 information).
2. Inform users—particularly those in key roles—about BEC/EAC attacks and the ways cybercriminals will try to mislead them. (Our infographic can help, as can our Business Email Compromise training module.)
3. Instruct employees to be immediately suspicious of any requests like those outlined above—even if requests appear to come from someone they know and trust. Any requests that provide "updated" account or bank routing information—including those related to employee payroll—should immediately raise warning bells.
4. Insist that, prior to executing on a request like those outlined above, some form of "manual" two-factor authentication must happen. We suggest that the person who receives the request reach out and contact the requestor via a **known, trusted channel**—like a frequently used phone number—to receive voice-to-voice confirmation. No request of this nature should be fulfilled based on an inbound request (whether that comes via email, phone, text, or another form of communication).
5. Implement a code word or phrase as an additional layer of security for these types of transactions. The code word/phrase should be changed regularly and should never appear in email or text messages. Be sure to document all procedures for establishing and distributing code words/phrases, as well as processes for authenticating requests. You should also have an action plan in place for situations in which an employee suspects a fraudulent request has been made.

[1] BEC and EAC attacks are closely related; in fact, EAC attacks are often referred to as BEC attacks. At Proofpoint, we characterize the distinction this way: In the case of BEC, the attacker pretends to be a trusted contact; in the case of EAC, the attacker appears to BE the trusted contact. It's important for users to be aware that, in the case of EAC, a request could in fact originate from a known source and still be dangerous. You can read more about EAC on our blog.