

RECOGNIZING AND AVOIDING

BUSINESS EMAIL COMPROMISE ATTACKS

Stop Wire Transfer Fraud in Its Tracks

BEC Q&A

What Is Business Email Compromise?

A business email compromise attack — also known as a BEC attack — is a type of phishing attack in which a cybercriminal impersonates a high-level executive or other trusted contact and uses social engineering techniques to trick an email recipient into transferring funds into a fraudulent account.

Who Is Targeted in a BEC Attack?

Cybercriminals seek out situations in which fund transfers happen on a regular basis, and they have been known to attack organizations of all sizes across all sectors, as well as individuals. Anyone who is authorized to complete financial transactions as part of a normal course of business could be a target. Frequent victims include administrative assistants, controllers, accountants, and other individuals in finance-related roles.

How Does a BEC Attack Happen?

BEC attacks are often highly sophisticated and carefully planned, making it difficult for a target to identify the scam. Cybercriminals generally follow a pattern like the following:

DO THE RESEARCH

The attacker will identify an organization and/or the targeted individual(s). They will then gather information using social media channels, publicly available data, and phone calls, developing profiles they can draw on to create believable communications.



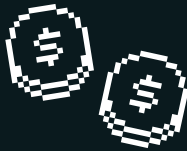
LAY THE GROUNDWORK

Attackers attempt to build relationships with individuals who have access to financial accounts. They often use a combination of phone calls and “spoofed” or hacked email messages, which appear as though they are coming from a trusted source (like a CEO, CFO, external supplier, or law firm). Multiple communications can take place over days, weeks, or even longer in order to create a sense of trust and familiarity.



STEAL THE FUNDS

The money is routed to an account controlled by the attacker. By the time the attack is discovered, it is often too late to track or recover the funds.



SET THE TRAP

Ultimately, the attacker asks the target to initiate a wire transfer for a seemingly legitimate business reason. Because the target believes the attacker is someone they trust, they often act on the request without reservation.



Are BEC Attacks Strictly About Wire Transfer Fraud?

BEC attacks are most commonly tied to fraudulent wire transfers, but similar techniques have been used to obtain sensitive information, like wage and tax statements and other confidential employee data. In these cases, the target is asked to send employees’ personally identifiable information (PII) to a seemingly legitimate requester, and that data is then used to commit tax fraud and other crimes.

BEC attacks are becoming more commonplace. Law enforcement agencies have seen these types of attacks affect all parties involved in real estate transactions (including buyers, sellers, and agents). These types of attacks are also used to make requests for gift card purchases, as well as to trick payroll personnel into rerouting employees’ direct deposits.

BEC Prevention and Protection

BEC attacks cannot succeed if you don’t take the bait! Use these tips to identify and avoid these types of attacks, and protect your organization’s funds, your coworkers’ data, and your own money and reputation.



Be careful about your social media posts and connections. Consider all information shared to be public and permanent.



Be on guard with all unsolicited emails and phone calls. Even seemingly small pieces of information — like vendor names and vacation schedules — are useful to cybercriminals.



Verify originating email addresses and phone numbers when sensitive requests are made. These details can be spoofed by attackers to make them look legitimate. In some cases, cybercriminals are able to steal email login credentials and send messages from a trusted account, making it extremely difficult to spot a fraudulent request.



Implement a form of two-factor authentication before initiating wire transfers or providing sensitive data. Call a known, verified phone number and have a voice-to-voice conversation to confirm the request is legitimate.

If you believe you have been a victim of a BEC attack, alert your supervisor, financial institution, IT department, and authorities as soon as possible. Quick action can help to minimize the damage.

