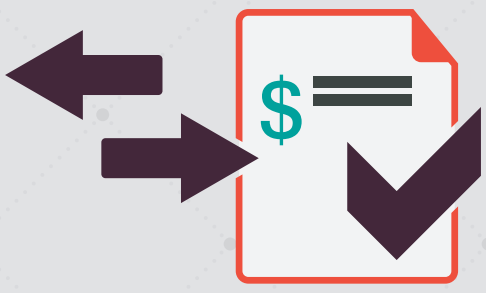


RECOGNIZING AND AVOIDING BUSINESS EMAIL COMPROMISE ATTACKS

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?

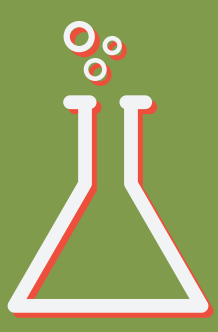
Cybercriminals seek out situations in which fund transfers happen on a regular basis, and they have been known to attack organizations of all sizes across all sectors, as well as individuals. Anyone who is authorized to complete financial transactions as part of a normal course of business could be a target. Frequent victims include company controllers, accountants, and parties involved with real estate transactions (including agents, buyers, and sellers).

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.

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.

Steal the Funds

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

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 by the Numbers

Between October 2013 and May 2018:

Source:
Federal Bureau of Investigation Public Service Announcement, July 12, 2018

More than

- **$12.5 billion** in exposed losses reported by financial institutions worldwide
- **78,000 global incidents** reported by financial institutions worldwide
- **43,000 victim complaints** worldwide with **$3.6 billion** in exposed losses

136% increase in identified exposed losses between December 2016 and May 2018

BEC scams reported in **150 countries and all 50 US states**

Fraudulent wire transfers sent to **115 countries**

Approximately 900 reported W-2 phishing attacks in 2017

Source: Internal Revenue Service News Release, January 17, 2018

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 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.

40 24th St., Pittsburgh, PA 15222
www.wombatsecurity.com
+1 (412) 621 1484 | +44 (0) 118 402 9163

wombat™ security
a division of proofpoint.