# The FAQ on BEC

## What is BEC?

Business Email Compromise is one of the latest trends in digital scamming to hit the business world. This sophisticated scam specifically targets companies that work with foreign suppliers or that regularly perform wire transfer payments. The fraudulent parties compromise legitimate business e-mail accounts to conduct unauthorized transfers of funds or information. This is accomplished through social engineering or computer intrusion techniques.

## How prevalent is BEC?

BEC is the fastest-growing type of spear phishing attack. Since January 2015, BEC has increased 270 percent. From 2013 to 2015, it cost global businesses more than $1.2 billion. This scam has been reported in all 50 states and 79 countries. If no attempts have been made to hit your company with this scam, it will likely happen soon.

## What can fraudsters gain from BEC?

Many e-mail users don't realize the value of their accounts. Proper precautions are not taken because of the assumption that no one would value their e-mail enough to compromise it. This is a poor assumption. Consider the extremely valuable information someone could obtain if they had full access to your business e-mail account.

- Email addresses of your contacts (who will then receive spam and phishing attacks)
- License keys to software you have purchased
- Access to cloud storage accounts
- Information on other email accounts you have set up using this one
- Financial institution/account information

The list could go on to include any other important accounts you access that have ever used your e-mail address or sent information to that address.

The main focus of BEC is impersonation. Using your legitimate address, the fraudulent party can send out seemingly authorized requests for information or fund transfers. From that point on, millions of dollars are at risk.

## What does BEC look like?

Typically, victims receive an e-mail from a seemingly legitimate source. This message contains a malicious link. If clicked on, this link downloads malware, which gives the fraudulent party access to the victim's data.

Fraudulent parties use compromised e-mails to then make seemingly legitimate requests from CEOs or trusted business partners. Imagine getting a message from the CEO asking for a transfer of funds to a domestic bank account. It references a familiar business deal and raises no red

flags. The transfer is completed, and the fraudulent party walks away with the $100,000 the unsuspecting employee just sent them.

Another method is for fraudsters to contact victims via phone or e-mail pretending to be representatives of law firms who are handling confidential matters. With this framework, they pressure the victim into acting quickly and discreetly with a funds transfer.

Other times, the actual e-mail has not been compromised, but the fraudulent party uses a look-alike address that goes undetected as different from the legitimate account.

Often, these scams occur at the end of the business day or work week. It is also common for these attempts to be made while the CEO is away from the office.

The average loss resulting from each BEC is $130,000.

### Why are BEC attempts difficult to detect?

For several reasons:

- Many common methods used to detect scams fail to pick up on attempts at BEC. Spear phishing e-mails are individually targeted, and spam filters search for large volumes of similar messages. This allows the e-mail to slip past the filter.
- Fraudsters create return e-mail addresses for each scam, so the e-mail doesn't show up on blacklists.
- Typical keywords that raise red flags, such as Nigeria or Viagra, do not appear in these communications.
- The request appears to be from someone the victim trusts, and involves everyday business matters.

### How can my business prevent BEC?

A company can put policies in place to help prevent the success of BEC attempts. Healthy policies include:

- Never wire money unless you see the face of the person requesting it. They must also be part of your office.
- Use a filter to verify if an e-mail address is similar to but not identical to a known contact. For example, the system would flag jsmith@My-Company.com if the legitimate address is jsmith@MyCompany.com.
- Register company domains that are similar to the actual domain.
- Scrutinize all e-mail requests for fund transfers to establish if they are out of the ordinary.
- Confirm requests via a different channel, such as SMS or an alternate e-mail.

### What should I do if we fall victim to BEC?

- If you discover a fraudulent transfer, immediately contact your financial institution. Ask them to also contact the financial institution where the transfer was sent.

- Contact the FBI. They may be able to freeze or return the funds.
- File a complaint with www.IC3.gov

### What if my question is not covered here?

For more information on BEC, contact McCann Investigations. Expert investigators are available to assist you.