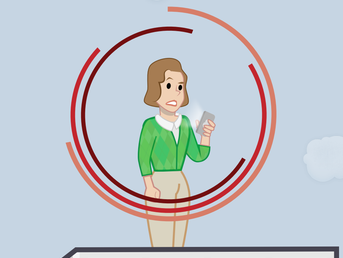
Business Email Compromise



You don't need to click a link or download an attachment to fall for a malicious email. A scam called the Business Email Compromise (BEC) has stolen at least $2.3 billion US[1] from organizations around the globe, simply by asking for it.

Total amount of funds stolen by BEC scammers as of early 2016.

Average USD amount stolen in an average BEC scam.

In which a BEC scam has been reported.

A BEC attack is as simple as it is effective, but it is always carefully planned. Attackers exploit public email listings, social media, or even compromised accounts to learn more about our company's structure and procedures.

Attacks are sent when the impersonated person is most vulnerable—when they are traveling, out of the office, or otherwise unavailable to discredit the request.

There are three types of BEC emails

1. CEO Fraud: A simple wire request from a compromised executive's email account. Often, an attacker will forward replies to another email address so that the executive remains unaware. *(Figure 1)*
2. Bogus Invoice Scheme[2]: Imitates a supplier invoice email, but with new payment instructions/procedures.
3. Payment Request Emails: An employee's email account is compromised, and payment requests are sent to suppliers or colleagues in the employee's address book. *(Figure 2)*

Figure 1

From: **Your CEO** <ceo.name@example.com>
Subject: Request

Are you busy? i need you to process a wire transfer for me today. let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my Phone

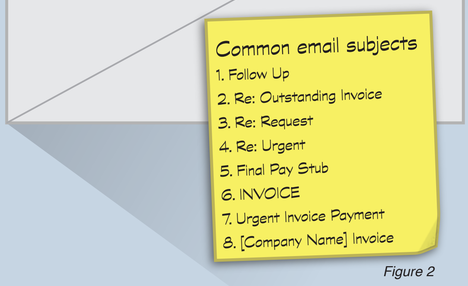


Figure 2

Why doesn't my spam filter catch this?

BEC emails are well researched and highly personalized. They are sent to only one or a few recipients at a time. Lacking the signature traits of a spam email, they often find their way into the target's inbox.

Who is Targeted?

Companies most at risk are those that frequently work with foreign suppliers and regularly perform wire transfers. Individuals most at risk are controllers, financial officers, or others who typically execute wire transfers.

Fortunately, you can avoid falling victim to these attacks.

Take your time.

The email may urge you to act quickly or outside of procedure. Even if the email looks like it is from your supervisor, don't fall for it.

Scrutinize emails carefully.

Analyze the email for spelling and grammatical errors, and look for clues that the sender isn't who they say they are.

Always verify.

Do not respond to the sender. Instead, verify the request with your supervisor or with the sender via a telephone call.

If something seems suspicious, do not respond to the email or initiate a transfer. Instead, report it immediately to help keep our organization safe from a potential attack.

1. https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
2. https://www.ic3.gov/media/2015/150122.aspx

PHISHME