

# What you need to know about BEC scams

## One Crime - Many Attack Methods

Attackers Use Many Methods to Successfully Compromise a Business Email Account



### Business Email Compromise (BEC):

When a corporate email account is taken over and used for malicious activities originating from a legitimate trusted email address.

BEC is a growing crime—with a staggering price tag. Between 2013 and 2019, the Internet Crime Complaint Center (IC3) received complaints of more than \$10 billion in losses from BEC activities.

### What are some of the motives of BEC attacks?

- Distributing malware
- Spear phishing accounts with elevated privileges
- Executive business email compromise (BEC)
- Targeting customers and partners
- Access to VPNs or other cloud services to further infiltrate the corporation

### What makes BEC scams different than other phishing attempts?

In the typical phishing scam, the attacker uses an email address that looks similar to the real one.

In a BEC the attacker has gained access to the legitimate email account. Therefore, the receiver cannot tell if it is a scam based on the email address.

### Precautions and Best Practices

- Verify sender really sent email
- Pick up the phone and call to verify
- Check phone number. Do not call the number in the email
- Never wire money based solely on email instructions
- Be wary of unexpected emails from company owners and executives

### Example of a BEC Email

The image shows a screenshot of an email client interface. On the left, there are four callout boxes with arrows pointing to specific parts of the email:

- Real Address Was Accessed For Use:** CEO Fraudsters literally commandeer an official email through phishing, social engineering or other methods. (Points to the sender's name 'The Boss' in the header)
- An Urgent E-mail Subject Requesting Immediate Fund Transfers:** BEC scams typically use subject lines that imply urgency regarding payment inquiries or fund transfers. (Points to the subject line 'Quick Request')
- Body of the E-mail:** Scammers make it appear as if the fund transfer is urgently needed and should be executed as soon as possible. (Points to the body text)
- Position of the E-mail Sender:** Cybercriminals employing CEO fraud typically pose as someone influential in an organization. (Points to the signature 'Chief Executive Officer')

The email header shows:

To: Matilda <Matilda@company.com>  
From: TheBoss  
<TheBoss@company.com>  
Re: Quick Request  
Date: Tuesday, January 26, '21, 4:45pm

The subject line is: **An Urgent Message From The CEO:**

The body text reads: "Hi! Are you available? I need you to take care of an urgent transfer for me today. Sorry the request is last minute... but it is critical it be handled before 5:30pm. I'm leaving for an appointment but am sure you can manage this on your own... record any overtime needed to get this accomplished."

The signature is: "Thanks, The Boss, Chief Executive Officer"

**Need Help Securing Your Business?**

**Contact Anjolen Inc:**

**Michelle Tuttle: [mtuttle@anjolen.com](mailto:mtuttle@anjolen.com)**