What you need to know about BEC scams

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

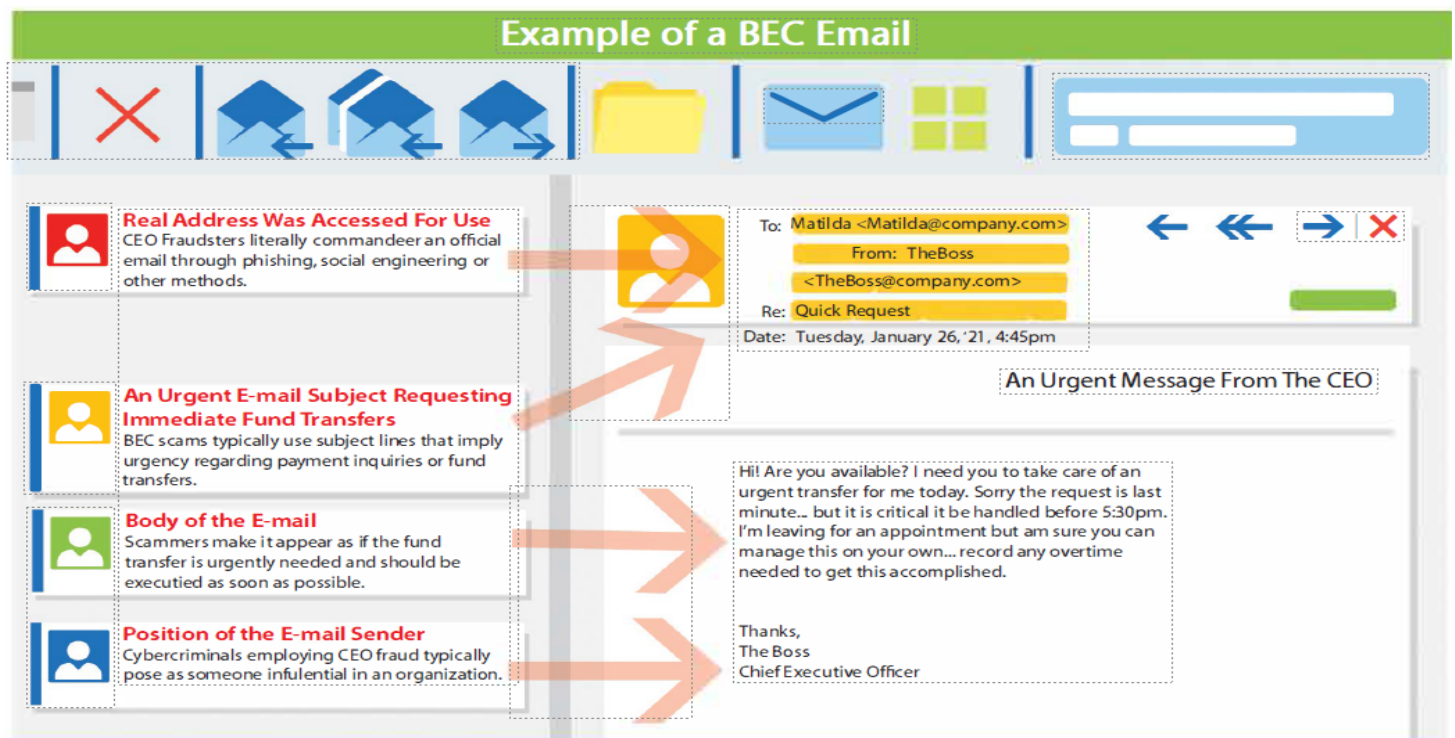
What makes BEC scams different that other phishing attempts?

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



Need Help Securing Your Business?

Contact Anjolen Inc:

Michelle Tuttle: mtuttle@anjolen.com

Anjolen, Inc. | E: info@anjolen.com | A: 287 Genesee St. Suite 103, Utica, NY 13501 | P: 315-332-9237 | www.anjolen.com