Understanding BEC

Short for **business email compromise**, BEC is one of the fastest growing scams that targets organizations. **It works like this: a cybercriminal gains access to the email address of a senior executive. They then spoof that email to send requests for money or information to employees who trust that senior executive.**

According to the FBI, BEC scams—also referred to as CEO Fraud—have cost organizations around the world $5.3 billion/€4.4 billion since 2013.[1]

In fact, according to a study conducted by Proofpoint, BEC attacks targeted nearly 85% of organizations in the first quarter of 2017 alone.[2]

What can you do about it? This is where we need everyone in our organization to play the role of Human Firewall! **Always treat requests for money or sensitive information with a high degree of skepticism. Stay alert for anything out of the ordinary, and remember there are no stupid questions. If you're not sure, please ask!**

Sources: 1. https://securityledger.com/2017/05/fbi-business-email-compromise-is-a-5-billion-industry/
2. https://www.proofpoint.com/sites/default/files/pfpt-us-ds-bec-quarterly-update.pdf

THE SOCIAL ENGINEER'S PLAYBOOK

IDENTIFY THE TARGET. Gather as much info about the target as possible (usually from data breaches that leak personal info, such as full names and email addresses).

DEVELOP A PRETEXT. A pretext is a made-up scenario used to trick victims.

ENGAGE with the target to gain trust, most often via phishing emails.

STEAL INFORMATION or finances from target.

Pretexting Definition
The practice of developing a fabricated scenario (the pretext) in order to elicit information from a target, often via phishing (emails) or vishing (phishing via phone calls/messages).

Going After Execs with CEO Fraud

Social engineers target executives and other high-ranking members of organizations via two basic phishing methods:

SPEAR PHISHING

By compromising their email addresses and sending requests for sensitive information or money transfers to lower-level employees.

WHALE PHISHING

By posing as government entities or business partners and emailing attachments of allegedly important documents which contain malware.

Good security comes from timely response. Report security incidents immediately!