Business Email Compromise

Tom Scarborough  
Senior Vice President, Director of Extended Security Programs

Darrin Steinmann  
Vice President, Director of Corporate Investigations
Business Email Compromise (BEC)

Compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds

The History of BEC:

• Became prominent in ~ 2012 - 2013
• Used to primarily target bank employees
• Saw a significant shift in 2015/2016 timeframe to target employees of the victim organization
• Many new “flavors” added in recent years
Business Email Compromise (BEC) – Social Engineering

Exploit our natural curiosity, desire to be helpful, love of a good bargain, and our time constraints

Business Email Compromise

• Used to obtain access to a business email account and imitate the owner's identity, in order to defraud the company and its employees, customers or partners.

• Focuses efforts on employees with access to company finances, payroll data and other personally identifiable information.

• Fraudulent request comes from a compromised executive's email account. Email address closely resembles a familiar one: johnasmith@gmail.com vs johnncsmith@gmail.com

• Tactics:
  – Sense of urgency
  – Use rules to forward emails to hidden folders
  – Wait until executives are on vacation
  – Use fake chains using subject lines with “Re:” or “Fwd:”. This technique grew more than 50% year over year.¹

The number of attackers using legal language increased 1,850% year over year.¹
The subject “lawyers call” was the most popular.

¹Proofpoint.(2018).The Human Factor Report 2018
Business Email Compromise: How it Happens

**Step 1: Identify a Target**
Organized crime groups target US and European businesses, exploiting information available online to develop a profile on the company and its executives.

**Step 2: Grooming**
Spear phishing emails and/or telephone calls target victim company officials (typically an individual identified in the finance department.)
Perpetrators use persuasion and pressure to manipulate and exploit human nature.
Grooming may occur over a few days or weeks.

**Step 3: Exchange of Information**
The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

**Step 4: Wire Transfer**
Upon transfer, the funds are steered to a bank account controlled by the OC group.
BEC Techniques

There are three different types of identity deception that criminals use to execute a BEC attack: spoofing, look-alike domains and display name deception.

BEC - Email Fraud

From: CEO
To: CFO
Subject: Payment

Distribution of most common email subjects in BEC attacks

Percentage of BEC attack attempts that spoof specific positions, 1H2017

Percentage of BEC attack attempts that target specific positions, 1H2017

1Proofpoint (2018). The Human Factor Report 2018
BEC – The Impacts…

Since May 2013… over $26 Billion in losses have been reported!

- The FBI reports that between May 2018 and July 2019, there was a 100% increase in identified global exposed losses. The scam has been reported in all 50 states and in 177 countries.

- Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to at least 140 countries.

Business Email Compromise (BEC)
By the Numbers

$1.7B
Reported losses to BEC in 2019

23,775
Complaints received by the Internet Crime Complaint Center in 2019

$75,000
Average loss per BEC scam per complaint

17%
Increase in number of BEC victims from 2018


Business Email Compromise Variations

Given the success the fraudsters have had to date, they have introduced new “flavors” of BEC fraud in recent years.

Common BEC Types:

1. W2
2. Invoice/Supply Chain
3. Direct Payroll
4. Real Estate
5. Attorney Impersonation
COVID19 Response

Many Employees are now working from home
Companies must remain diligent and maintain controls that have been embedded into money movement processes & procedures

Internal & External Threats
Organizations must consider insider threats as well as external. This includes process changes

Education
IT Professionals have reported a significant increase in email attacks and fraud schemes. Ensure everyone in the organization is aware of and knows how to handle such threats.
Best Practices to Combat BEC:

1. Leverage Dual Approval capabilities whenever possible

2. Know your customer and never accept requests for payments through email or other similar channels
   - Verify legitimacy of payment requests leveraging known good contact information
   - Never trust information received via email

3. Monitor your accounts regularly

4. Educate your employees

5. Use Multifactor Authentication capabilities provided by email providers when possible

6. Limit information shared on social media about your employer and your role

7. Ensure policies and procedures are being followed

8. Leverage appropriate security tools to protect your environment (anti-malware, web proxy, etc.)
If You Fall Victim to a BEC Scam

TIME IS OF THE ESSENCE

• Contact your financial institution immediately

• Request your FC contact the financial institution where the transfer was sent

• File a complaint with the FBI’s Internet Crime Complaint Center

• Contact Your Fifth Third Account Manager Immediately

• <<INSERT PHONE NUMBER FOR AFTER HOURS/ WEEKENDS IF NOT ABLE TO REACH ACCOUNT OFFICER>>
Fifth Third Response to BEC

FIFTH THIRD RESPONSE

• Case and Investigation opened

• Investigators work with clients to attempt recoveries

• Engagement of Law Enforcement
Just A Few Reminders. . .

• Employ continuous education on the importance of cyber security
• Create an environment where employees feel they can speak up about concerns
• Utilize the partnership of Fraud Prevention and Fifth Third Bank

"If you see something, say something."
Cyber security is a shared responsibility

We’re all in this together
Cyber Insurance

Cyber insurance is available and can provide services that include:

- Incident response services: Breach coach, legal fees, forensics, notification costs, credit monitoring, public relations

Cyber insurance can provide protection for exposures that include:

- Ransom/extortion
- Business interruption/loss of profits
- Social engineering
- Network liability: Failure to prevent transmission of viruses, etc.
- Privacy liability: Failure to protect private information
- Regulatory proceedings
- Media liability

*Fifth Third is the trade name used by Fifth Third Insurance Agency, Inc. Insurance products and services are offered through Fifth Third Insurance Agency, Inc., which is a wholly-owned, non-bank subsidiary of Fifth Third Bank, National Association. Banking and insurance decisions are made independently and do not influence each other. Insurance products are not FDIC insured, not guaranteed by a bank and are underwritten by unaffiliated, third party insurance carriers. Insurance products are not offered in all states. Please consult with a Fifth Third Insurance Professional.

The Fifth Third Insurance Agency can provide further information and advice on this topic.*
Questions?

Thank you
Important notice

This document has been prepared by Fifth Third Bank, National Association ("Fifth Third") or one of its subsidiaries for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Fifth Third to supply the proposed services. It is not intended to provide specific investment advice or investment recommendations and does not constitute either a commitment to enter into a specific transaction or an offer or solicitation, with respect to the purchase or sale of any security.

The information contained in this document has been compiled by Fifth Third and includes material which may have been obtained from information provided by various sources and discussions with management but has not been verified or audited. This document also contains confidential material proprietary to Fifth Third. Except in the general context of evaluating our capabilities, no reliance may be placed for any purposes whatsoever on the contents of this document or on its completeness. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Fifth Third or by any of its subsidiaries, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document or any other oral information made available and any such liability is expressly disclaimed.

This document and its contents are confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person in whole or in part without our prior written consent.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

Securities offered through Fifth Third Securities, Inc., a registered broker/dealer and member of FINRA and SIPC.