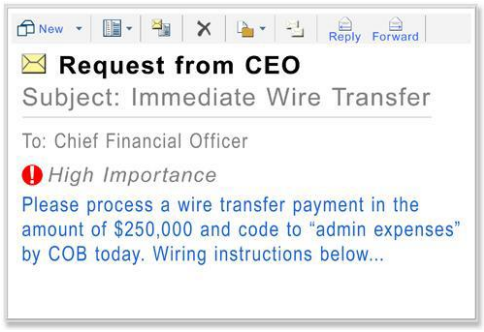
Business E-mail COMPROMISE

How and When to Report the Matter to the Federal Bureau of Investigation

The CFO of a U.S. company received an e-mail from her CEO while the CEO was on vacation out of the country. The CEO requested a transfer of funds for a time-sensitive payment that required discretion. The CFO followed the instructions and wired $250,000 to a bank in Hong Kong. The next day, the CEO called about another matter. The CFO mentioned she had completed the wire the day before, but the CEO said he never sent the e-mail and knew nothing about the transaction. The company was the victim of a BEC.

A BEC is a type of sophisticated financial fraud targeting businesses of all types and sizes. BECs are carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusions to conduct unauthorized transfers of funds.



Common Variations

- Hacked accounts via spear phishing
- Spoofed accounts made to look similar to authentic accounts (john.kelly@abc.com vs. john.kelley@abc.com)
- Spoofed accounts with slight variations in domains (abc@lawfirm.com vs. abc@lawflrm.com)
- Spoofed accounts mimicking the real account until one reviews the extended header or hovers a curser over the e-mail address

Common Targets

- Free web based e-mail users
- Bookkeepers, accountants, controllers
- Title companies and attorneys representing buyers or sellers in any transaction

Statistics

The Internet Crime Complaint Center (IC3), has seen a 270% increase in identified victims and exposed loss since January 2015. The scam was reported in all 50 states and in 79 countries. Fraudulent transfers were sent to 72 countries; however, the majority went to banks in China and Hong Kong. More than 8,000 victim complaints totaling almost $800 million were reported to the IC3 from October 2013 to August 2015.

Suggestions for Protection

- Employee awareness/education on how to identify the scam before sending payments to the fraudsters.
- Verify wire transfer requests and changes to vendor bank accounts with two-factor authentication such as a secondary sign-off and/or using voice verification over known phone numbers.
- Create intrusion detection system rules that flag e-mails with extensions similar to company e-mail or differentiate between internal and external emails.
- Be wary of free, web-based e-mail accounts, which are more susceptible to being hacked.
- Be careful when posting financial and personnel information to social media and company websites
- Regarding wire transfer payments, be suspicious of requests for secrecy or pressure to take action quickly.
- Register domains that are slightly different than your actual domain.
- Know the habits of your customers, including the details of, reasons behind, and typical payment amounts.
- Scrutinize all e-mail requests for transfers of funds.

Minneapolis Field Office
January 2016

What to do if you are a victim

Request your financial institution issue a "SWIFT recall" and file a Suspicious Activity Report or "SAR." For domestic transfers, also request your financial institution send a "hold harmless" letter to the beneficiary bank.

Experience has shown that after three days, funds have likely been transferred out of the beneficiary account. This is not always the case and the FBI may still be able to pursue a criminal prosecution.

Funds wired within last 3 days?

If the amount was approximately $50,000 or more: Immediately report the incident to the FBI's Minneapolis office at 763-569-8000. Provide the following information:

- Summary of the incident
- Victim name
- Victim location (city and state)
- Victim bank name
- Victim account number
- Beneficiary name
- Beneficiary account number
- Beneficiary bank location
- Intermediary bank name
- SWIFT/IBAN number
- Date of transaction
- Amount of transaction

Request the duty agent contact the supervisor of the Economic Crimes Squad immediately.

If the amount was significantly less than $50,000: Report the matter to the FBI via the Internet Crimes Complaint Center (IC3) at www.ic3.gov. You may also want to consider notifying local law enforcement.

Funds wired more than 3 days ago?

If the amount was approximately $50,000 or more: Immediately report the incident to the FBI's Minneapolis office at 763-569-8000 and the IC3 at www.ic3.gov.

If the amount was significantly less than $50,000: Report the matter to the FBI via the IC3 at www.ic3.gov. You may also want to consider notifying local law enforcement.

For additional information on Business Email Compromises, go to www.ic3.gov. Specific public service announcements on this scam include:

- Alert Number I-082715a-PSA dated 8/272015 (http://www.ic3.gov/media/2015/150827-1.aspx)
- Alert Number I-082715b-PSA dated 8/272015 (http://www.ic3.gov/media/2015/150827-2.aspx)
- Alert Number I-012215-PSA dated 1/22/2015 (http://www.ic3.gov/media/2015/150122.aspx)