Business E-Mail Compromise

Federal Bureau of Investigation, San Francisco Division

What to do if you are a victim

Report the matter to your bank

On international transactions, contact your financial institution to issue a **"SWIFT recall"**. For domestic transfers, also request your financial institution send a **"hold harmless letter"** to the beneficiary bank.

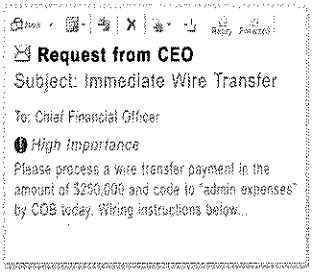
Report to law enforcement

After contacting your financial institution, immediately report the incident to the FBI San Francisco Division at 415-553-7400 or the Internet Crime Complaint Center at www.IC3.gov. Provide the following information:

- Date of incident
- Summary of the incident
- Victim Name
- Victim location (City, State)
- Victim bank name
- Victim bank account number
- Beneficiary name
- Beneficiary account number
- Beneficiary bank location
- Intermediary bank name
- SWIFT/IBAN number
- Date of transaction
- Amount of transaction
- Copies of e-mails to include header information

Notify your bank and/or local law enforcement of unauthorized wires as soon as possible. Days, hours, and minutes can make a difference in preventing monetary loss.

If there is no loss, still report the information above to www.ic3.gov



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 never sent the e-mail and knew nothing about the transaction. The company was the victim of a Business E-mail Compromise.

Business E-mail Compromise (BEC) is a sophisticated financial fraud targeting businesses of all types and sizes who work with foreign suppliers and/or regularly perform wire transfers. The scheme utilizes compromised and/or spoofed e-mail accounts to initiate wire transfers on the criminal's behalf. The actors target businesses of all sizes and often compromise the valid business e-mail accounts through social engineering or computer intrusion techniques. The Internet Crime Complaint Center (IC3) has seen a 270% increase in identified victims and exposed losses since January 2015 and combined losses exceeded $1.2 billion.

Common Techniques

- 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, buyers/ sellers, or attorneys in midst of real estate transactions
- Businesses who deal with overseas vendors/suppliers

Suggestions for Protection

1. 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.
2. Create intrusion detection system rules that flag e-mails with extensions similar to company e-mail or differentiate between internal and external e-mails.
3. Be careful when posting financial and personal information to social media and company websites including travel commitments and speeches by executives.
4. Regarding wire transfer payments, be suspicious of requests for secrecy or pressure to take action quickly. Scrutinize all e-mail requests for transfer of funds.
5. Be wary of free, web based e-mail accounts, which, are more susceptible to being hacked.
6. Register domains that are slightly different than your actual domain.
7. Employee awareness/education on how to identify the scam before sending payments to the fraudsters. Verify, via trusted channels, any change in customer personnel, processes, or payment amounts.

FBI – San Francisco Division | 450 Golden Gate Avenue, 13th Floor | San Francisco, CA 94102
415-553-7400 | Email: San.Francisco@ic.fbi.gov