Business Email Compromise Scams

> Cyber thieves stole nearly
> **$12.5 billion**
> from businesses in the last 4 1/2 years through business email compromise.
> *FBI PSA, July 2018*

The scam has been reported in ***all 50 States*** *and in* ***150 Countries.***

Need to know

Wire fraud initiated via business email compromise, is an increasingly common and sophisticated financial scam, targeting businesses that frequently perform wire transfer payments and/or those who work with foreign suppliers. Victims have ranked from large corporations to technology companies to non-profit organizations. Industry data also identifies manufacturing and construction companies as common targets. Victims in real estate transactions have also been heavily targeted in recent years, including title companies, law firms, real estate agents, buyers and sellers. According to the FBI's most recent PSA on email compromise, the scam has evolved to include the compromising of legitimate business email accounts to request employee information or W-2 forms for employees and may not always be associated with a request for money.

What can it look like?

- **Request for Funds:** The fraudster spoofs or hacks company email to assume the identity of a business executive or trusted vendor. They research the employees who manage money, then request a wire transfer in an email to an employee within the company known for processing such requests. Alternatively, employees trust an email received from a vendor to wire funds for an invoice payment to an alternate, fraudulent account. In a real estate transaction, the fraudster spoofs an email account and directs the victim to change the real estate payment type and/or payment location to a fraudulent account.
- **Data Theft:** The fraudster may also compromise legitimate email accounts through social engineering or computer intrusion techniques, and target human resources or bookkeeping for a fraudulent request for W-2's or employee data.

How can they do it?

While it is unclear how victims are selected, cyber criminals are known to monitor and study their victims prior to attempting the fraud. This "grooming" may occur over a few days or even weeks. Fraudsters may go to a company website to determine the names of the C-level officers and try to first forge the executive's email address to trick the employees if the email service is not properly secured. They could also register a phony domain email account with a similar domain name to make it harder to recognize as fraudulent in the subsequent email "from the executive" requesting the wire. Alternatively, they may create a new address using the executive's name with a different email provider (i.e. Hotmail vs. Gmail), and then send the wire request directly to the bank hoping that the banker doesn't recognize the discrepancy. Victims primarily report requests to send funds to accounts in Asian Banks located in China and Hong Kong. However, United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations. Some victims report using checks or gift cards as a common method of payment.

Supplier/Vendor Scam Example

> Cyber thieves stole nearly
> **$12.5 billion**
> from businesses in the last 4 1/2 years through business email compromise.
>
> *FBI PSA, July 2018*

I need you to process an urgent bank transfer for me today, Let me know if you are available so i can send you the bank details to process the transfer.

Kind Regards

How can you mitigate your risk?

Be alert to the red flags and carefully scrutinize all e-mail requests for wire transfers.

- The email will likely convey a sense of urgency in completing the wire or requesting the information.
- The fraudster will typically follow up shortly after as to the "status" of the request.
- There may be typos or grammatical errors in the text, such as "i" that isn't capitalized or other red flags.
- Requests may coincide with the "requester" being out of office or otherwise "unavailable".

Consider a mandatory policy that wire transfers must be authorized in person, or verified with the "sender" of the email, via phone using a pre-established identification procedure. Ensure the verification information does not include publicly available information.

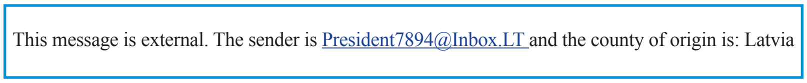
- Know that Montecito Bank & Trust will not initiate any wires on your behalf that have originated via email without prior authorization unless an account signer with sufficient authority can authorize the transaction in person.
- Question any variations to prior vendor payment instructions.

Education is key! Hold regular employee education sessions and train employees to be your eyes.

- Train employees not to open unsolicited emails or click on suspicious links.
- Communicate risks of posting to social media and company websites, especially job duties, hierarchy, and out-of-office details.

Scrutinize email requests for accuracy and beware of small characters that mimic legitimate addresses, such as:

- "username@abc.com" vs "userrname@abc.com"
- "username@abc.com" vs "username@abc.net"



This message is external. The sender is President7894@Inbox.LT and the county of origin is: Latvia

Consider adding a notification to external incoming email that includes the true sender's email address (pictured).

Reconcile banking transactions on a daily basis.

Immediately report suspicious activity to Montecito Bank & Trust at (805) 963-7511 or Fraud@Montecito.bank.

Make sure your email provider implements the Sender Policy Framework (SPF), and DMARC for protection against spoofed or forged emails.

- More info on SPF - wikipedia.org/wiki/Sender_Policy_Framework
- More info on DMARC - wikipedia.org/wiki/DMARC

The FBI Internet Crime Complaint Center (IC3) can be used to report scams that may have originated via the internet.

Research more about fraud or phishing emails, as well as how to set up multi-factor (or 2-step) authentication for email: montecito.bank/fraud. Montecito Bank & Trust offers digital banking services that are multi-factor by default.