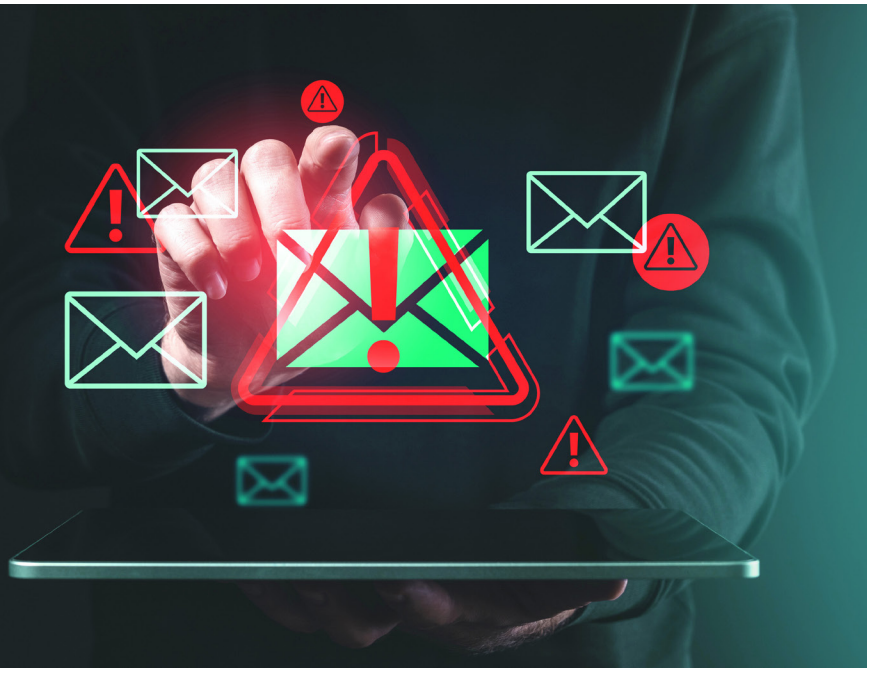
BUSINESS EMAIL COMPROMISE CHECKLIST

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Below are some tips for immediate and preventative actions.



IMMEDIATE ACTIONS

Internal Actions

01 Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) — looking for unusual activity.

02 Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?

03 Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as "auto forward" or "auto delete."

04 Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage.

05 Review all requests that asked for a change in payment type or location. ***Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend.***

Reporting the Incident

CONTACT YOUR BANK

01 Determine the appropriate contact at your bank, who has the authority to recall a wire transfer Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?

02 Notify your bank if you have been the victim of a Business Email Compromise.

AND

03 Request a wire recall or SWIFT Recall Message.

AND

04 Request they fully cooperate with law enforcement.

REPORT THE INCIDENT (OR ATTEMPT) TO THE FBI AT IC3.GOV

01 Provide all details for the beneficiary: Account numbers, contact information, and names.

02 Contact your local FBI Field Office.

PREVENTION & RECOGNITION ACTIONS

- Does the Routing Number provided to you, resolve to the expected bank used by the other party? *(Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S?)*

  Possible websites to verify a Routing Number:
  a. The Federal Reserve: **FRBServices.org**
  b. American Bankers Association: **RoutingNumber.ABA.com**

- Call a known/trusted phone number or meet in person to confirm the wire transfer information provided to you, matches the other party's information.

- Hover your cursor over suspicious email addresses — looking for indications of Display Name Deception or Spoofing.

- DO NOT hover on links within emails, as simply hovering may execute commands.

- Regularly check your email account log-in activity for possible signs of email compromise.

- Regularly check your email account for new "rules", such as email forwarding and/or auto delete.

- Be cautious of *"new"* customers, suppliers, clients and/or others you don't know who ask you to:
  a. …Open or download any documents they send
  OR
  b. …Sign into a separate window or click on a link to view an invoice or document
  OR
  c. …Provide sensitive Personal or Corporate information

- Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.
  a. Where did you get the account data?
  b. Is this the correct account number?

Source: Department of Justice, Federal Bureau of Investigation