Information on the 2024 Campaign is available now. Click here to find out more.

Understanding Business Email Compromise

Business Email Compromise (BEC) or Email Account Compromise (EAC) is a common type of sophisticated fraud scheme that results in over **$2 billion** in loss every year. The bad actors gain unauthorized access to email accounts and use that access to coordinate payments or transfers of funds. This is the most prevalent cybercrime affecting businesses and individuals in the United States, and it's not a matter of IF you are targeted, but **WHEN**.

Who should be concerned?

- Any entity that uses email to conduct business activities.
- Individuals who may be making large purchases.
- Anyone who receives unsolicited emails from someone they know requesting an urgent or otherwise unexpected payment.

How it starts

- Potential victim has their email account login compromised through some form of social engineering such as a **phishing** attack or a network intrusion attack.
- Scammers use the stolen login credentials to access the email account and conduct "surveillance" of the target.
- Once the scammer identifies key individuals in a company or a specific transaction, the scammer will inject themself into the communication.
- The company or individual making the payment will receive fraudulent instructions to send funds to the scammer's account.

Common tactics

- Email/domain spoofing: Scammers create email addresses that closely resemble the legitimate email addresses of the victims and their business partners.
- Email inbox rules: Scammers access a compromised account and set up rules that automatically forward emails to a central email account controlled by the scammer.
- Sense of urgency: Scammers may introduce a sense of urgency to a payment or state they will be "unreachable," and the transaction must take place as soon as possible.
- Issue with bank account: Scammers may say their account is undergoing an audit or has received bad checks and cannot receive payments.

Prevention

- Multi-factor authentication to help prevent unauthorized logins to email accounts.
- External email "flagging" that makes it obvious a message was not sent from an internal email account.
- Robust verification policies before any payments are made (e.g. making a phone call to a **KNOWN** phone number to verify payment instructions).
- Employee education on BEC and how to identify these schemes.
- Purchasing similar domain names for your own entity to prevent spoofing.

Response

- Establish contacts with law enforcement prior to a security incident.
- Conduct tabletop exercises with IT security and administrative personnel who will be responsible for responding to an incident. Include law enforcement, if possible.
- Immediately report incidents to law enforcement **AND** your financial institution. Any delays will decrease the likelihood of financial recovery.
- Immediately change all login credentials.
- Conduct sensitive communication via alternative means (e.g. phone or alternate email).
- Engage with internal IT or external IT incident response to identify the source of the compromise and maintain records of all potential evidence.

Return to top of page