Understanding of Business Email Compromise (BEC) Attacks

Introduction: Explanation of Business Email Compromise (BEC) and its significance

BEC attacks are sophisticated scams involving email fraud where attackers masquerade as trusted entities to manipulate employees into transferring money or sharing sensitive information. These attacks exploit the trust and routine procedures within organizations, making them particularly insidious and effective.

Unlike typical phishing scams that may target anyone, BEC schemes are carefully tailored and researched, often involving reconnaissance on the targeted company and its employees. This level of personalization makes BEC attacks not just challenging to detect but also more likely to succeed. Their significance lies in the direct financial losses and potential data breaches they can cause, along with the long-lasting damage to the reputation and trust within and outside the organization. As BEC attacks continue to rise, both in frequency and sophistication, understanding their nature and the importance of vigilance and reporting becomes paramount for businesses of all sizes.

Identification: Techniques for recognizing BEC attempts

Business Email Compromise (BEC) attacks can be subtle and sophisticated, making them challenging to detect. Here are key techniques to help recognize BEC attempts:

Unusual Email Requests

- Be wary of emails requesting urgent wire transfers, especially if the request deviates from normal procedures.
- Look out for requests for sensitive information or access to confidential data that seem unusual or unexpected.

Changes in Banking Details

- Pay attention to emails instructing changes in bank account details for invoice payments.
- Verify any such changes through direct, independent communication channels.

Email Sender's Identity

- Examine the sender's email address closely for slight changes that mimic legitimate addresses (e.g., .co instead of .com).
- Be cautious of emails that come from high-level executives, particularly those sent with a sense of urgency or secrecy.

Language and Tone Anomalies

- Look for unusual language or a different tone from what you would normally expect from the sender.
- Grammatical errors, spelling mistakes, or uncharacteristic language can be red flags.

Pressure to Act Quickly

- BEC attackers often create a sense of urgency to bypass normal checks and balances.
- Be skeptical of emails pressuring immediate action, especially involving financial transactions.

Attachment and Link Scrutiny

- Be cautious of unexpected attachments or links, even from known senders.
- Avoid clicking on links or downloading attachments from suspicious emails.

Contextual Clues

- Consider the context of the email. Does it make sense for this person to be making this request?
- Cross-reference the request with known events or schedules (e.g., the CEO is out of office but sends an urgent email).

Double-Checking Email Threads

- Look for inconsistencies or anomalies in ongoing email conversations.
- Be aware of hijacked email threads where attackers insert themselves into legitimate conversations.

Unusual Payment Methods

- Requests for payments via unconventional methods, such as gift cards or wire transfers to foreign accounts, should raise suspicions.
- Always confirm payment methods through established, secure communication channels.

Reporting Suspected BEC

- Report any suspected BEC attempts to your organization's IT or cybersecurity team.
- If financial information was shared, also report to your financial institution and consider contacting law enforcement.

Recognizing BEC attempts requires a combination of vigilance, skepticism, and adherence to internal protocols. Training staff to identify and appropriately respond to these indicators is essential in protecting against BEC attacks.

Immediate Actions: Procedures for responding to and reporting BEC incidents

When a Business Email Compromise (BEC) incident is suspected or identified, immediate and decisive action is required to mitigate potential damages. Here are the critical steps to follow:

Verify the Request

- Independently confirm the legitimacy of the email request using established communication channels. Do not reply directly to the suspicious email.
- Contact the supposed sender via phone or in person, using contact information you know to be accurate.

Alert IT and Security Teams

- Immediately report the incident to your organization’s IT or cybersecurity department.
- Provide them with all relevant information, including the email itself and any actions taken so far.

Preserve Evidence

- Retain the original email, including its headers, without altering any content.
- Document all communications related to the BEC attempt, as they might be required for investigation.

Notify Financial Institutions

- If the incident involves financial transactions, contact your bank immediately to stop payments or flag the transaction.
- The bank can also provide advice on further steps to secure financial accounts.

Change Credentials

- If the BEC attempt involved account or credential compromise, change all relevant passwords immediately.
- Ensure that the new passwords are strong and unique.

Internal Communication

- Inform relevant departments (like finance or HR) about the incident, especially if it involves their processes or personnel.
- Encourage vigilance and reinforce the importance of following verification procedures.

Legal and Compliance Reporting

- Report the incident to appropriate legal authorities, especially if financial fraud is involved.
- Check for any regulatory requirements in your industry for reporting such incidents.

Review and Strengthen Policies

- After handling the immediate threat, review your organization’s email and financial policies to identify any weaknesses that the BEC exploit exploited.
- Strengthen policies and procedures to prevent future incidents, focusing on email verification and financial transaction protocols.

Train and Educate Staff

- Conduct training sessions for staff to recognize and appropriately respond to BEC attacks.
- Regularly update training materials to reflect the latest BEC tactics and trends.

External Communication

- If clients or external stakeholders are affected, prepare a communication strategy to inform them, taking care to manage potential reputational impacts.

Quick and informed action can greatly reduce the damage caused by BEC incidents. Regularly reviewing and updating security policies and employee training are key to maintaining a strong defense against these sophisticated email attacks.

This project was funded by the European Union’s Internal Security Fund - Police Programme under Grant Agreement No 101038738