Business Email Compromise (BEC) Fraud

Business Email Compromise (BEC) is a sophisticated scam targeting businesses that regularly perform wire transfer payments. Fraudsters compromise legitimate business email accounts through social engineering or hacking to conduct unauthorized fund transfers.

What to do IF & WHEN a BEC Occurs

- Immediately contact your bank via telephone and email.

- Ensure all employees have banking contact information.

- Inform the bank of the fraudulent transaction and provide all relevant details.

- Request a wire recall from the beneficiary bank.

- Report the incident to the FBI via the IC3 website or your local field office.

- Engage IT/security staff to investigate potential email compromise.

- Prepare necessary regulatory and internal reports.

Developing a BEC Response Plan

A structured response plan is crucial in mitigating losses from BEC fraud. For international wire transfers exceeding $50,000, the FBI's Financial Fraud Kill Chain (FFKC) process can be utilized to recover stolen funds. Additionally, companies should establish robust internal controls and incident response policies.

How to Defend Against BEC

- Educate employees on fraud awareness and phishing tactics.

- Verify all payment instructions through an independent channel (e.g., phone verification).

- Implement dual-authorization for financial transactions.

- Monitor unusual changes in vendor payment details.

- Restrict business computer use for work purposes only.

- Enforce strong authentication methods, such as multi-factor authentication (MFA).

- Encourage cybersecurity best practices and regularly update security policies.

Recommendations and Mitigations

- Establish social engineering safety training for employees.
- Use out-of-band verification for large transactions.
- Standardize validation for vendor account changes.
- Beware of urgent requests for immediate fund transfers.
- Implement email security protocols (DMARC, DKIM, SPF) to prevent spoofing.
- Regularly audit and update security settings to prevent unauthorized access.

Common Red Flags of BEC

- Unusual or sudden changes in payment instructions.
- Emails requesting urgent wire transfers under secrecy.
- Requests from email addresses that slightly differ from known contacts.
- Poor grammar or unusual language in financial transaction emails.
- Emails sent outside normal business hours requesting payments.
- Unexpected links or attachments from supposed business partners.

Technical Mitigations

- Enable two-factor authentication (2FA) on email accounts.
- Block auto-forwarding of emails to external addresses.
- Enable security alerts for suspicious login attempts.
- Configure firewalls and email filters to block malicious attachments.
- Regularly audit access logs for unauthorized changes to email settings.
- Use endpoint security solutions to detect malware and phishing attempts.