United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO BUSINESS EMAIL COMPROMISES

Business Email Compromise (BEC) is a sophisticated fraud scheme targeting businesses that use wire transfers as form of payment. The BEC scheme affects large global corporations, governments, and individuals, with current global daily losses estimated at approximately $8 million. Specific vulnerable sectors are real estate, finance, education, healthcare, and information technology.

Criminals compromise legitimate business email accounts through various hacking schemes, to include social engineering and the use of malware. Once a business email account is compromised, a fraudulent email is sent directing the recipient of the email to unwittingly transfer funds to an illicit account. Criminals obtain and use privileged information to convince BEC email recipients that the transfer instructions are legitimate.

PREVENT

Register all similar domain names that can be used for spoofing attacks.

Create rules that flag and delineate emails received from unknown domains.

Monitor and/or restrict the creation of new email rules within the email server environment.

Enable multi-factor authentication.

Conduct BEC drills, similar to anti-phishing exercises.

Educate employees, clients, and vendors to:

Authenticate all financial transactions through dual-factor authentication.

Confirm all payment method changes using trusted and authenticated information.

Learn the habits of those with whom they conduct financial transactions.

MAIL AUTO FORWARDING

A criminal logs in to a compromised email account just once to set up an auto forward inbox rule to forward emails to their own email address.

This rule will remain in effect even if a password is changed.

WARNING SIGNS

Urgency of Request: A request to transfer funds is sent with a pronounced sense of urgency.

Different Domains: Email communication originates from unknown or spoofed domain.

Out of Contact: Requestor is unreachable, but insists on the urgency of the transfer.

Language and Grammar: Syntax is different or erroneous.

Multiple Emails: Multiple recipients receive emails requesting transfer of funds.

Incorrect Context: Emails are not in the standard context normally encountered or for alternate business purposes while requesting a transfer of funds.

Secrecy: Email sender requests that information about transfer be kept secret.

RESPOND

Time is money! An immediate response is crucial, funds are moved within minutes of a BEC incident.

Contact your bank to reverse the wire, for hold harmless and indemnification.

Contact local law enforcement to request a report, which is needed to reverse a wire.

Contact a Secret Service field office Cyber Fraud Task Force.

Law enforcement can work with FinCEN to initiate Financial Fraud Kill Chain.

File a complaint with the Internet Crime Complaint Center (IC3).

Review email systems for unauthorized access or rule creation.

Conduct a cyber security analysis on your systems.

Change all login credentials.