Business E-mail Compromise (BEC)

A sophisticated scam targeting people and businesses everywhere

WHAT IS IT?

Business E-mail Compromise (BEC) is a sophisticated scam using e-mail and/or other electronic communication to impersonate a business executive, employee, or other person with authority to request payments or access to employee payroll and W2 information on behalf of a business.

HOW DOES IT WORK?

A BEC scam may begin when a legitimate user downloads malicious software (malware) by clicking on a malicious attachment or link in a spam or phishing e-mail; or acts upon a spoofed e-mail payment request crafted to look like it came from a company executive. An example of such a spoofed e-mail address from ceo@abc_company.com might appear as ceo@abc–company.com. In cases where malware or malicious links are used, the malware can provide criminals with full control of the user's computer, including access to passwords, documents, and e-mail. Alternatively, criminals can obtain a user's e-mail login information if it was stolen previously and sold online. In either case, the criminal's goal is to assume the identity of the legitimate user and request new payments, change the banking information of pending payments, or request copies of employee records for some alleged payroll purpose. Prior to executing the BEC scam, more sophisticated cyber criminals may even monitor business communications for extended periods of time in order to understand operating procedures and the communication style of the individuals they want to impersonate. While e-mail is most common, sophisticated BEC criminals have also used a fax or phone call to confirm or follow up on an e-mail request to send money.

WHO IS BEING TARGETED?

The BEC threat is highly adaptable and constantly evolving, but criminals have been particularly active in targeting small to large companies and individuals which may transfer high-dollar funds or sensitive records in the course of business. As such, the following industries are popular with criminals utilizing BEC scams:

- Third Party Payroll
- Real Estate (Buyers, Sellers, Realtors, Title Companies)
- Legal Services
- Import/Export
- Education, Government, and Healthcare Sectors

WHAT ARE THE WARNING SIGNS?

- An e-mail request to change established wire transfer, payment procedure, or bank deposit instructions
- A request that the payment be expedited
- A requestor who indicates he/she will be out of the office and/or will not be readily available for re-contact
- A requestor that is seeking sensitive employee payroll or W2 information by e-mail

WHAT CAN YOU DO?

- Require a secondary, independent verification of any payment requests or changes to existing beneficiary accounts.
- Use complicated passwords or long phrases for company and personal e-mail accounts, change passwords regularly, and do not use the same password for multiple accounts.
- Consider using commercial Antivirus and AntiSpyware products.
- Avoid doing formal business on free web-based e-mail accounts; establish a company domain name and limit formal communications to company e-mail accounts.
- Have your IT department create intrusion detection system filters that flag e-mails with extensions that are similar to company e-mail. For example, a detection system for legitimate e-mail of ceo@abc_company.com would flag fraudulent e-mail from ceo@abc-company.com.
- Educate employees and IT staff on the latest trends by attending training and conferences, and through other online resources. A company which outsources their payroll and IT should ask those providers to outline the steps they take to protect the integrity of company data and networks.

WHAT TO DO IF YOU ARE A VICTIM

- Immediately contact your bank and initiate a recall.
- Contact your local FBI Office.
- File a detailed complaint at www.IC3.gov and review additional resources under the "Press Room" link.
- Change e-mail passwords and check your e-mail account for any changes to your mailbox rules, such as Mail Forward, Delete, CC, or BCC.
- Change all e-banking and/or other pertinent passwords, pins, and security questions or answers.

For more information please visit:
www.ic3.gov/media

FBICYD 226 Rev9 10-2017