Business Email Compromise

What is Business Email Compromise (BEC)?

BEC is when a cybercriminal hacks into a corporate email and impersonates the owner/ user of the email domain intending to entice the recipient to make a wire transfer or other electronic payment to a bank account controlled by the cybercriminal. In some cases the cybercriminal will request sensitive information to engineer attacks within the organization to obtain money illegally.

BEC has become an emerging financial cyber threat by organized cybercrime groups. These groups target small and large companies/ organizations including non-profits, churches, school systems, and well known corporations. These cybercrime groups operate in every state as well as more than 100 other countries from around the world.

The cybercriminals have sophisticated this global fraud system and countless professional businesspeople continue to be victimized, resulting in cybercrime losses. According to an FBI report, these losses have been totaled in the billions of dollars, which only continues to grow.

To read more on the FBI report https://www.ic3.gov/media/2017/170504.aspx

The most common employees targeted by cybercriminals are high level executive officers and people working in the financial department. Although anyone in a company can get targeted it is more common for the two listed groups due to the access that they have to the company's/ organization's financial records.

Examples of Tools/Schemes Used to Target and Exploit Victims of BEC Cybercriminals

PHISHING SCAM

This is when fraudulent emails, usually with links, are generated to trick the recipient into being directed to a false site where it asks the recipient to provide sensitive information such as banking & credit card details, passwords, or a person's date of birth/ address/ and social security number.

SPOOFING EMAILS & WEBSITES

This scheme/tool is when a cybercriminal creates an email address or website with a slight variation from a legitimate email or website. The criminals will direct any responses received to an account that they set up and control.

An example:
michelesmith@domain.com/
michellesmith@domain.com

MALWARE

Cybercriminals use programs designed to damage or disable the computer system without the user's knowledge. Various types exist which include, but are not limited to, viruses, Trojans, spyware, and worms. Malware is used to make sure that when fraudulent wire transfers are requested, suspicions are not raised. It can also be used to access the victim's data such as passwords and financial account information.

TIPS TO PREVENT BUSINESS EMAIL COMPROMISE (BEC)

- Do not open an attachment from emails that have any slight changes in the body from previously received emails.
- Be suspicious of any small changes in email addresses that are similar to legitimate email addresses in your address book.
- Do not click on web address links in emails. Enter all website addresses manually from outside organizations/companies.
- Report any suspicious emails immediately and delete the email.
- Limit the amount of employees that have access to submit or approve company/ organization financial funds. At the same time, do not permit a sole employee to have full authority over electronic funds.
- Implement a two factor authentication for initiating electronic fund transfers which includes signatures from both parties.
- When employees must access the email system remotely, institute a two factor authentication process.
- Be suspicious of any email with urgent requests for personal and business related financial information.
- Ensure that all employees participate in periodic trainings to recognize the signs of fraud and to detect suspicious activity in all correspondences.
- If an email seems suspicious do NOT hit reply. Create a new email with the email address that you have on file requesting confirmation of the authentication. If you have a known phone number of the email's sender, the best thing to do would be to call the person to ask them about the email. Do not use the phone number listed in the email, use only known contact information.
- Limit the amount of computers that are programed to access the company's/ organization's financial information.
- Continuously update the computer system's anti-virus software and firewalls to combat malware and deter intruders in the computer system.

What to do if the company/organization becomes a victim of BEC

1. Upon discovering that the fraudulent transfer took place immediately contact your financial institution.
2. Regardless of the loss amount, file a complaint with the Internet Crime Complaint Center at www.ic3.gov or contact your local FBI office. When making the report be as descriptive as possible and identify the complaint as Business Email Compromise or BEC.

   **Waiting even 24 hours to make a report greatly decreases the likelihood of the financial institute or law enforcement's capability to recover the funds.*
3. Conduct an internal review to discover how the attack occurred and if any changes are necessary to prevent future attacks.

Contact the ISA Risk Management Division today for more information on these and other risk management services and resources.
Call 800-622-8272 or email riskmanagement@siegelagency.com.

irwin siegel agency
INSURANCE PROGRAMS & RISK MANAGEMENT