Prepare Your Employees: Don't Fall Prey to Business Email Compromise Attacks

Business email compromise (BEC) is among the most serious fraud threats businesses face today. According to the FBI's Internet Crime Complaint Center, BEC attacks resulted in $1.7 billion in losses in 2019 alone[1]. Although it's a familiar scheme, companies continue to fall prey. However, you can help prevent your organization from becoming the next victim with the proper preparation, controls, training and testing.

Try these seven best practices to help safeguard your organization against BEC.

1 Review your email security practices with your senior technology leaders. Consider:

- Multifactor authentication to provide additional security beyond usernames and passwords.
- Software to prohibit or parameters to detect email inbox forwarding rules that send all emails or selected ones to an external email address. Fraudsters frequently establish rules that send payment-related emails to outside email accounts under their control.
- Automatic labeling of external emails to help prevent the impersonation of employees.
- Robust email logging that can be leveraged for investigation in case of a successful BEC attack.

Develop a BEC Response Plan

The sooner you report a BEC attack, the better your chances of recovering losses. Be sure to have a plan in place to immediately notify your bank of the fraud, make a report to IC3.gov and reach out to your local FBI field office. The plan should also include quickly engaging your IT and information security staff to determine if there has been a network or email compromise.

2 Deliver BEC training to all employees involved in payments. This training should emphasize how to identify suspicious emails relating to payment transactions and performing callbacks to payment recipients from a system of record for all payment transactions, new account establishment and account changes.

3 Establish an employee testing program that uses both phishing and BEC attempts that appear to come from your senior leaders and trusted business partners.

4 Confirm with your customers and business partners who will be remitting payments to you and who might be debiting your account. Also confirm how you expect them to validate changes to your banking information.

5 Construct, implement and enforce a social media policy that prohibits sharing too much information about company roles and responsibilities. Manage organizational information closely so cybercriminals cannot develop a picture of your corporate structure, including email addresses, to target your employees.

6 Consider hiring a firm that will notify you of web domains that have been registered to deceptively look like your own; cybercriminals can use look-alike domains in BEC attacks to trick your employees or business partners into diverting funds.

7 Make sure your payments staff has clear procedures to scrutinize and re-authenticate unusual transactions that are brought to your attention by your bank. Many BEC losses occur when clients release payments even after their banks warn them of suspicious payments.

CHASE

J.P.Morgan

For more information, please contact your Chase or J.P. Morgan representative or visit: chase.com/cb

[1] FBI's Internet Complaint Center (IC3) 2019 Internet Crime Report