Prepare Your Employees:
Review, Train and Test to Help Prevent Business Email Compromise (BEC) Attacks

Try these six best practices to help safeguard your organization against BEC:

1 Review your email security practices

Talk to your senior technology leaders about:

- Multifactor authentication to provide additional security beyond usernames and passwords.
- Parameters to quickly detect email inbox forwarding rules that send all or selected emails to an external email address.
- 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.

$1.7B

in losses to BEC in 2019 alone[1]

2 Train employees on BEC prevention

Teach employees how to identify and report suspicious emails relating to payment transactions. Stress the importance of performing callbacks to the person making the request, using a phone number from a system of record, for all payment requests, new accounts and account or contact information changes.

3 Test your employees regularly

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

CHASE J.P.Morgan

4 Standardize validation for payments and account changes

Establish with your customers and business partners how changes in account information will be communicated and validated. Also confirm how you expect them to validate changes to your banking information.

5 Create a social media policy

Construct, implement and enforce a social media policy that prohibits sharing details about company roles and responsibilities, so cybercriminals cannot develop a picture of your corporate structure, including addresses to target your employees.

6 Protect your web domain

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

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.

For more resources on how to protect your organization, visit
jpmorgan.com/cb/cyberfraud-protection

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