Five tips to help safeguard your organization from BEC

Business Email Compromise (BEC) scams targeting domestic and foreign businesses that regularly perform wire transfers continue to be the number one threat to our customers' financial assets. Data from the FBI estimates that the total loss of this global threat to be in excess of $1.2 billion* Based on several recent high-profile incidents, that number is sure to increase, emphasizing the need for heightened awareness and vigilance in executing key internal controls.

To help shield your organization from fraud, there are various internal control enhancements and security practices to consider. While no single control or set of controls will offer absolute assurance, we suggest the following tips:

one: Confirm and verify email requests for fund transfers. Contact the requestor by phone using an independently obtained phone number or one that you already have on file. Special scrutiny should be paid to transfers requested to new or recently updated accounts. Nearly all BEC scams can be stopped in their tracks if organizations adopt this basic control.

two: Use dual control for money movement activities. This allows for two levels of scrutiny and authorization to help stem the risk of illegitimate funds transfers.

three: Use multi-factor authentication for web-based email accounts. Fraudsters are known to leverage actual accounts of executives with email credentials pilfered from spear phishing campaigns. Multi-factor authentication adds another layer of control to deter cybercrooks from accessing employee accounts.

four: Communicate quickly when fraud or security events occur. Notify your key banking partners and information security staff immediately. If appropriate, contact law enforcement and file a complaint with the FBI's Internet Crime Complaint Center.

five: Create awareness within your organization. Evaluate staff compliance with internal controls by using real-world security awareness testing.

*Source: 8/27/2015 FBI Public Service Announcement. Data compiled from Oct. 2013 through Aug. 2015

Links: http://www.ic3.gov/default.aspx
http://www.ic3.gov/media/2015/150827-1.aspx

usbpayment.com

Data Security Content