TOP

Financial Cyber-Security Tips From Montgomery Bank

MARCH 23RD 2016 BY DEE LOFLIN

Financial Cyber-Security Tips From Montgomery Bank

Dexter, Missouri - The potential of your business experiencing an electronic theft attempt is ever-growing. Would-be crooks are becoming smarter, and their schemes more sophisticated, as security practices of companies heighten. According to the Federal Bureau of Investigation (FBI), one such scheme, Business E-mail Compromise (BEC), is a growing financial fraud that is more sophisticated than any similar scam it has seen before. BECs, in their various forms, have resulted in actual and attempted losses of more than one billion dollars to businesses worldwide.

Typically using wire or electronic fund transfers as their method for theft, criminals use a well-crafted email sent to a member of the company's financial office staff that appears to be sent from an executive officer of the company. The email directs the staff member to initiate an electronic transfer or wire transaction of funds to an account to which the criminal has access. The phony email address is nearly identical to the executive’s actual address, and therefore the fraudulent email is nearly impossible to detect. Without secondary identification and authorization processes in place, an unsuspecting staff member will complete the transaction, and the money is often never recovered.

The information below regarding BECs is from the FBI. At Montgomery Bank, we use these steps to help prevent successful fraud attempts, and thought this might

be valuable information for you to incorporate into your wire transfer security protocol as well.

Call to verify wire transfers. Before authorizing a wire transfer, call the person requesting to verify they really asked for it. Don’t call any number in the email or reply to the email; call the requestor directly.

Train employees to look out for these scams. The FBI provides a list of tips and other helpful information to avoid becoming a BEC scam victim.

Confirm any changes to wire transfer processes or locations. If a vendor suddenly asks for money to be sent to a new location, verify the new location over the phone or separately from the email thread.

Use social media cautiously. Make executives and managers aware and encourage them to limit how much they share on social media. Many of these scams use knowledge gleaned from social media about executives’ and managers’ whereabouts and activities.

Register domains similar to your corporate domain. Fraudsters may use similar domains that are one letter off of the victim’s domain to receive email responses or set up spoofed websites.

Conduct regular social engineering assessments. In addition to network penetration tests, organizations should also conduct social engineering assessments, including phone and email, to gauge the effectiveness of security policies and training. Use the results to update policies and educate employees. BEC scams are difficult to spot, so don’t rely on any single method to avoid your business becoming a victim. The fraudsters will change their tactics to increase their chances of success. As these tactics change, the defenses must change as well. As with so many attacks of this type, security awareness and good processes are vital keys to crime prevention.

If your company has been victimized by a BEC scam, it is important to act quickly. Contact your financial institution immediately and request that they contact the financial institution where the fraudulent transfer was sent. Next, call the FBI, and also file a complaint—regardless of dollar loss—with the Internet Crime Complaint Center (IC3) at **https://www.ic3.gov/complaint.**

If you have questions regarding this or other security issues regarding your Montgomery Bank accounts, please do not hesitate to contact your Relationship Manager or contact our Customer Service Department at 800-455-2275.

LAST UPDATED ON MARCH 23RD 2016 BY DEE LOFLIN

https://showmetimes.com/Blogpost/v3sn/Financial-CyberSecurity-Tips-From-Montgomery-Bank

Go to post

More from ShowMe Times:

SUBSCRIBE TO "LOCAL NEWS"

ShowMe Gold Sponsors