Heritage BANK

6 Ways to Protect Your Business from Email Compromise Scams

Companies of all sizes are being targeted by criminals through Business Email Compromise scams. In these scams, cybercriminals gain access to an employee's legitimate business email through social engineering or computer intrusion. The criminal then impersonates the employee, often a senior executive or someone who can authorize payments, and instructs others to transfer funds on their behalf.

Heritage Bank recommends the following tips to help businesses and employees avoid business email compromise attacks:

1) EDUCATE YOUR EMPLOYEES

You and your employees are the first line of defense against business email compromise. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

2) PROTECT YOUR ONLINE ENVIRONMENT

Shred receipts, bank statements and unused credit card offers before throwing them away.

3) USE ALTERNATIVE COMMUNICATION CHANNELS TO VERIFY SIGNIFICANT REQUESTS

Have multiple methods outside of email – such as phone numbers, alternate email addresses – established in advance through which you can contact the person making the request to ensure it is valid.

4) BE WARY OF SUDDEN CHANGES IN BUSINESS PRACTICES OR CONTACTS

If an employee, customer or vendor suddenly asks to be contacted via their personal e-mail address, verify the request through known, official and previously used correspondence as the request could be fraudulent.

5) BE WARY OF REQUESTS MARKED "URGENT" OR "CONFIDENTIAL

Fraudsters will often instill a sense of urgency, fear or secrecy to compel the employee to facilitate the request without consulting others. Use an alternative communication channel outside of email to confirm the request.

6) PARTNER WITH YOUR BANK TO PREVENT UNAUTHORIZED TRANSACTIONS

Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call backs, device authentication, multi-person approval processes and batch limits help protect you from fraud.

If you fall victim to a business email compromise scam:

Contact your **financial institution immediately** to notify them about the fraudulent transfer and request that they contact the institution where the fraudulent transfer was sent.

Contact your local **Federal Bureau of Investigation office** as they might be able to freeze or return the funds, if notified quickly.

File a complaint, regardless of dollar loss, at **www.IC3.gov**.

FOR MORE TIPS, SEE THE FEDERAL BUREAU OF INVESTIGATION'S INTERNET CRIME COMPLAINT CENTER'S PUBLIC SERVICE ANNOUNCEMENT.