Businesses Unknowingly Sending Money To Fraudsters

There has been a significant increase in fraud cases due to businesses taking direction from unauthenticated email communications.

TAKE ACTION

AND CONSIDER IMPLEMENTING THESE CONTROLS:

DO NOT automatically trust or act solely on an email communication asking you to make changes to payment instructions from vendors, business partners, or internal management, even if it looks legitimate. To protect your company, procedures should be reviewed to ensure they include a validation step outside of email utilizing already known contact information, such as a verification phone call. For internal management email requests, you may want to require an actual signature as an added security measure. Think about all the things you do simply based on trusting an email. What risk are you taking if the email is not legitimate?

Utilize Dual Control options for authorizing ACH and wire payments within online banking, and make sure the staff reviewing those are trained properly to look for potential fraud or unusual activity. Another set of trained eyes can be an effective, if not foolproof, way to safeguard against fraud.

Contact The Bank Immediately if you believe you are a victim of fraud or have sent funds based on fraudulent instructions. We can best assist you if you call us first. (1-800-453-8700 option 2)

Utilize Multi-Factor Authentication
If you access your office remotely, use Office 365, Outlook Web Access, or some other cloud based email, ensure you utilize multi-factor authentication. If your credentials are compromised, the fraudsters can access your email account from anywhere. They monitor who you speak with and learn how you do business. Then they plan their attack and start communicating as you. They delete every sent and received communication to help hide their tracks. Please use multi-factor authentication whenever possible. It is as easy as receiving a 6 digit temporary access code that you key in every time you login with your username and password.

Train Your Staff about the risks of automatically trusting email as legitimate. Phishing emails can compromise your systems with malware or ransomware. Spear phishing emails hope to get your staff to take action and usually turns into money lost.

Secure Your Environment by ensuring your computer systems and network are routinely patched to help avoid vulnerabilities, and seek outside review or support regularly to make sure your internal controls are up to industry standards to avoid intrusion or takeover attempts.

If you have questions or concerns please contact us at (1-800-453-8700 option 2).

Mercantile® Bank of Michigan

Member FDIC