



CORPORATE ACCOUNT TAKEOVER

According to government officials, an increasing number of fraudulent electronic funds transfers are committed by computer hackers, usually located outside the U.S. One common method is known as a “corporate account takeover” by law enforcement; this type of crime is also called a business email compromise (BEC) or invoice scam. In a typical scenario, an employee at a company—such as an accounts payable staff member—receives an email that appears to come from a legitimate sender, such as a vendor or the company’s bank. The email contains an attachment, which appears to be important, so the employee opens the email and clicks on the attachment.

However, this is really a [phishing email](#) sent by a hacker, and the attachment now downloads a malicious program—known as financial malware—onto the company’s computer system. By tracking employees’ keystrokes, malware may collect sensitive financial information about the company such as online banking accounts, usernames, and passwords. In another scenario, financial malware is used to trick an employee into revealing the company’s wire transfer or ACH authorization token. Using this information, the hackers can illegally transfer funds out of the victim company’s accounts, often in a matter of minutes or less.

Man-in-the-Middle Attacks

Another sophisticated electronic funds transfer fraud is a “man in the middle” (MITM) attack. Hackers use malware to gain access to a corporate email account, and then monitor the victim company’s payment requests and related communications. Posing as a trusted vendor, the cyber-criminals send a request for payment, instructing the company to wire the money to a bank account that appears to be legitimate but is really under the criminals’ control. By the time the fraud has been detected, the money has often been collected and the thieves have disappeared.

If you have questions, please contact:

Heather Steele
SVP, Treasury Management Sales Officer

(O) 615-956-0273
hsteele@fnbmt.com

Ryan Crouch
Banking Officer
Treasury Management Implementation Specialist
(O) 931-474-4989
rcrouch@fnbmt.com