PREVENTING BUSINESS EMAIL FRAUD

Author – Andrew Smith

June 2024

Preventing Business Email Fraud

Recently, there has been a notable increase in instances where employees tasked with issuing payments on behalf of their companies are duped into transferring money into accounts controlled by malicious actors. How do these frauds occur, and what measures can your organization implement to avoid falling victim to email fraud?

Mechanisms of Email Fraud:

Fraudsters often gain unauthorized access to email chains through several methods, including:

- *Hacking the company's network or that of a vendor*
- *Unauthorized access by a malicious insider*
- *Social engineering or phishing emails*
- *Using compromised email login details, potentially through malware or unsecured Wi-Fi networks without VPN protection*

Identifying the exact method of compromise can be challenging. Once access is gained, fraudsters create email addresses that closely mimic legitimate ones within the email chain. They then send emails from these fake addresses, often claiming something like "Our bank account is under audit; please transfer the payment to this alternative account." Subsequent emails push for quick payment, with victims frequently failing to notice slight differences in email addresses. As a result, all further communications are diverted to the fraudster, making it extremely difficult to recover the funds once transferred.

Preventive Measures Against Email Fraud:

To safeguard your company from such frauds, consider the following steps:

- *Conduct cybersecurity awareness training for all staff*

Instruct payment-authorizing employees to:

- *Inform management of any requests to change payment details*
- *Scrutinize the sender's email address for authenticity*
- *Directly contact the company via phone to confirm such requests*
- *Include clauses in service agreements with new vendors that specify bank account details for payments and steps to verify requests for account changes*

These proactive measures can significantly reduce the risk of becoming a victim of email fraud.

Actions to Take if You Fall Victim:

If your company becomes a victim of email fraud, it is crucial to:

- *Retain electronic copies of all original emails in the chain, especially those requesting payment changes and follow-ups from the fraudster*
- *Ensure these copies are not forwarded internally to preserve the embedded email header information*

Email headers contain critical data, such as the originating IP address and timestamps, which can help identify the Internet Service Provider (ISP) and the location of the sender. Law enforcement can then request information from the ISP to track down the fraudster. Preserving original emails in an electronic format is vital for this investigative process.