old phish called Executive Impersonation and its costing companies billions of dollars.

Sep. 21, 2016

That next cyber attack apparently could come from your boss. It's a new twist on an old phish called Executive Impersonation and its costing companies billions of dollars.

Executive Impersonation is a growing cyberattack trend that is part of what law enforcement refers to as Business Email Compromise (BEC). According to the Federal Bureau of Investigation, BEC is a cyber scam targeting companies that work with foreign suppliers and businesses and that regularly perform wire transfers to foreign banks. The FBI says BEC attacks have been reported in all 50 states and in 100 countries, and have resulted in actual or attempted theft of $3.1 billion globally.

It starts with a simple email. Based on extensive research, a cybercriminal creates a

Executive Impersonation has become pervasive enough that the American Institute of CPAs has issued practical guidance on how to prevent it in a new fraud report. The report offers case studies of companies who have experienced this type of cyberattack, and practical steps to recognize and avoid it.

"This sophisticated type of cyberattack is stealing millions of dollars from companies in a manner that should be particularly concerning to company stakeholders because it persuades employees to ignore internal controls," said Annette Stalker, CPA, CFF, owner of Stalker Forensics and chair of the AICPA's Forensic and Litigation Services Committee. "Executive Impersonation bypasses the security systems that company IT departments have put in place to neutralize cyberattacks by going where companies and their employees are most vulnerable, their email systems. We felt it was time to raise awareness within the accounting profession about this type of cyberattack."

The AICPA report cites several characteristics of Executive Impersonation fraud:

- Email requests come from a senior (C-suite) executive or a key vendor or supplier.
- The email address is substantially similar to the purported sender's address, with very minor, subtle differences. The email display name may appear correct, but when the cursor hovers over the email address, a different underlying address is displayed. For example, if the actual address is CEO@victimco.com, the impersonator address might be CEO@vicitmco.com.
- Requests occur when the executive is traveling and cannot be contacted.
- There is an element of urgency or secrecy regarding the disbursement.
- The amount is within the normal range of transactions so as not to arouse suspicion.
- Other employees are referred to or copied in the email, however, their email addresses are also modified.

- Requested payments are payable to a foreign bank.

- Engaging cyber-risk security consultants to identify, monitor and mediate spear-phishing threats, including identifying employee-targeted attacks on social networks, finding and taking down fraudulent and impersonating accounts, and continuously monitoring important employee and company accounts for signs of being compromised.
- Reviewing policies and procedures for requesting, initiating and approving wire transfers. Email requests should be verified by phone calls to company-registered phones. Require two employees to approve wire requests and authenticate the recipient's identity before the wire is released.
- Conducting a risk assessment of the wire transfer process to identify weaknesses that could be exploited. Identify "look-alike" domains and register them in the name of the company to prevent hackers from attempting BEC attacks.

"Awareness, training and repetition are the best steps you can take to prevent Executive Impersonation fraud, but when this type of cyberattack is suspected, early mobilization and assessment of the impact are crucial," said David Zweighaft, CPA, CFF, Managing Director of DSZ Forensic Accounting & Consulting Services, and the member of the AICPA's Fraud Task Force who wrote the report. "Companies should be ready to quickly assemble a response team, including in-house counsel, the CIO and staff responsible for IT security, and outside consultants. It is critical that they undertake an internal investigation to gather all the relevant facts for management and the board of directors to support their decision-making. It also will provide a foundation for responding to law enforcement and government investigators, and for purposes of insurance recovery."

The AICPA's Forensics and Valuation Services specialty subject area, which supports the Certified in Financial Forensics (CFF) credential for CPAs, offers a wealth of information to assist companies in dealing with fraud and cyberattacks. The new fraud report and more information on combatting fraud can be found at aicpa.org.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us