Bloomberg BNA

Accounting Policy & Practice Report®

Fraud

Email Impersonation Scams Costing Billions, AICPA Warns

By Laura Tieger Salisbury

Accountants who work with foreign suppliers and perform wire transfers to foreign banks should be wary of e-mails that appear to come from a high-ranking executive asking for a wire transfer.

The American Institute of CPAs on Sept. 21 issued a guide for the accounting profession on red flags that could indicate an attempted scam.

Business e-mail compromise (BEC) has been reported in all 50 states and in 100 countries. It has caused actual or attempted theft of $3.1 billion globally, according to Federal Bureau of Investigation statistics.

Subtle Differences. The AICPA report by David Zweighaft, managing Managing Director of DSZ Forensic Accounting & Consulting Services, and AICPA's Fraud Task Force member, highlights some tell-tale signs of this scam.

The e-mails usually come from a senior executive or key vendor or supplier. The impersonator's e-mail address is very similar to the real—noncriminal— person's email address.

There are some minor, very subtle differences in the e-mail address that can be detected by hovering the cursor over the e-mail address until a slightly different underlying address reveals itself. As an example, the report cited a hypothetical case that varied the false address from the real one by only one letter—CEO@victimco.com versus CEP@vicitimco.com.

The e-mail may include other employees whose e-mail addresses have been modified in the same, hard-to-detect fashion.

Sense of Urgency. The e-mail request conveys an element of urgency and secrecy and will be sent when the executive is traveling and cannot be contacted to confirm or deny the origin of the e-mail. The amount of money requested is often within the range of normal transactions to avoid suspicion. The requestor will ask for payments to be sent to a foreign bank, according to the AICPA report.

Simon Platt, managing partner of Stone Turn Group, LLP, that provides forensic and expert witness services to attorneys, corporations and government officials on high-stakes legal and compliance issues, previous U.S. audit partner for Deloitte, spoke with Bloomberg BNA Sept. 22 about this type of ''spear phishing'' or spoof e-mail.

Platt said that while he had not encountered this type of email scam, he compared it to another type of impersonation, such as a telephone call asking for bank passwords. All these frauds must sound reasonable, and allow the person to feel that this is a sufficiently unusual situation that makes it alright to override the company protocol or controls in place, he said.

Platt told Bloomberg BNA that regulators have taught companies a ''salutary lesson'' in the last five years, and companies have been putting in place company-wide policies, training, and awareness of controls (10 APPR 1117, 12/5/14).

Audit IT Procedures. The Public Company Accounting Oversight Board inspections staff said in a staff inspection brief July 14 that audit procedures involving information technology—particularly auditors' use of software tools—and procedures to assess and address risks of material misstatement posed by cybersecurity will be new focus areas for the staff in 2016 ((12 APPR 19, 9/23/16).

Companies should take the following preventative measures to stay one step ahead of the cyber criminal, according to the report:

- increase training for employees responsible for wire transfers, educate them about BEC scams and data security;
- hire cyber-risk security consultants to identify, monitor these threats, take down fraudulent accounts, continuously monitor important employee and company accounts for signs of being compromised;
- email requests should be verified by phone calls to company-registered phones;
- require two employees to approve wire requests and authenticate recipient's identity before releasing the wire;
- conduct risk assessments of the wire transfer process to identify potential weaknesses in the system; and
- register ''lookalike domains in the company's name before the hackers make the attempt.

''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,'' Zweighaft said.'' 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.''

 ISSN 1558-6642

To contact the reporter on this story: Laura Tieger Salisbury in Washington at lsalisbury@bna.com

To contact the editor responsible for this story: S. Ali Sartipzadeh at asartipzadeh@bna.com

☐ *The AICPA's Forensic and Valuation Services Semi -Annual Report on Fraud Trends and Topics is available at http://src.bna.com/iML*

  APPR ISSN 1558-6642