Social Engineering & Funds Transfer Fraud

Your accounting department receives new wiring instructions from a trusted vendor. No problem, right?

It could be fine, but what if they are mistaken and the email is from someone posing as your vendor. There is an increasingly common type of crime known as “Social Engineering” funds fraud, and 59% of attacks are directed at small and medium sized businesses. In today’s digital and connected world, attackers of this type hide in the anonymity of cyber space; and they pose as a trusted vendor, prospect, client, or employee to deceptively gain the confidence of an employee and induce them to part with money.

Social Engineering Fraud Defined.

When an employee is intentionally misled into spending money or diverting a payment based on fraudulent information that is provided to them in written or verbal communication such as an email, fax, letter or even a phone call.

No Company is Too Big or Small.

Any company, regardless of size and industry (and individuals as well), is a target for social engineering fraud. 83% of large, 63% of medium, and 45% of small businesses were targets of attacks in 2014. Attackers know smaller companies typically lack the financial and accounting controls that larger companies have in place. In many cases, it takes months to discover you have been a victim, and recovering the funds is close to impossible.

An Accelerating Reality. This Could Happen at Your Company.

In the first eight months of 2015, there was a 270% increase in victims of compromised business emails. Examples like these are all too common:

- **Vender Impersonation.** Someone posing as one of a company’s primary vendors sends an email saying the mailing address or wire instructions for payments has changed. Your office updates the records and sends payment. **The funds never make it to the actual vendor.**
- **“Fake President” Crimes.** Your accounting office receives an email which appears to be from a person of authority within the organization, instructing them to transfer funds by wire to another bank. Not recognizing that the email has been subtly altered, the well-intentioned employee sends the money. **The money is gone and the fake account is closed by the time the fraud is discovered.**

What You Can Do.

- **Gain Awareness.** It starts with awareness and understanding of the many types of Social Engineering threats businesses face today. *(See Appendix Section II, pg 2)*
- **Train Your Employees.** Often times the weakest link in your security chain is a well-intentioned employee who falls victim to a scam. *(See Appendix Section III, pg 2)*
- **Improve Controls.** Evaluate your internal controls and take action. Update and implement smart loss control measures. *(See Appendix Section IV, pg 3)*
- **Consider Increased Insurance Protection.** Not every crime can be prevented. Contact Gowrie Group about possible insurance solutions through Crime or Cyber policies/endorsements that may work for you. Know what is and isn’t covered by your insurance policy. *(See Appendix Section I, pg 2)*

Gowrie Group. Always on Watch. As one of the nation's Top-50 independent insurance agencies, Gowrie Group provides total risk management services to individuals and businesses with complex insurance needs. Gowrie Group offers comprehensive insurance solutions matched with trusted advice and a commitment to service excellence. Gowrie Group's portfolio of offerings includes commercial, home/auto, equine, and yacht insurance, as well as employee benefits solutions. The company's 150+ professionals service clients across the US from offices in Westbrook CT, Darien CT, Marshfield MA, North Kingstown RI, and Newport RI. For more information, www.gowrie.com, 800.262.8911, or info@gowrie.com.
APPENDIX: SOCIAL ENGINEERING FRAUD.

SECTION I: INSURANCE COVERAGE

Social Engineering Fraud is an emerging issue and insurance contracts have not necessarily been modified to address it. In many cases, neither a Cyber Policy nor a standard Crime Policy covers losses and claims resulting from Social Engineering Fraud, leaving the company with no recourse to recover the funds. However, companies can work with their insurance agent to explore the possibility of adding an endorsement that addresses Social Engineering Funds Fraud specifically, which may include coverages for:

- Vendor/supplier impersonation
- Executive impersonation
- Client impersonation

SECTION II: SOCIAL ENGINEERING TACTICS

Social Engineering Tactics\(\textit{v}\): The first line of defense against social engineering fraud is being aware of the common and changing tactics, such as:

- **Impersonation, pretexting**: An attacker using a believable reason to impersonate a person in authority, a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.

- **Phishing, spamming, spear-phishing**: Phishing can take the form of a phone call or email from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.

- **IVR/Phone phishing (aka vishing)**: This technical tactic involves using an interactive voice response (IVR) system to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to “verify” confidential information.

- **Trash cover, forensic recovery**: Attackers collect information from discarded materials such as old computer equipment (e.g., hard drives, thumb drives, DVDs, CDs) and company documents that were not disposed of securely.

- **Quid pro quo (“give and take”)**: An attacker makes random calls and offers his or her targets a gift or benefit in exchange for a specific action or piece of information, so that the target will feel obligated in some way.

- **Baiting**: Leaving an innocent looking, malware-infected device (such as a USB drive, CD or DVD) at a location where an employee will come across it, and then out of curiosity plug/load the infected device into his or her computer.

- **Tailgating, direct access**: Attackers gain unauthorized access to company premises by following closely behind an employee entering a facility or by presenting themselves as someone who has business with the company.

- **Diversion theft**: The methodology in this attack involves misdirecting a courier or transport company and arranging for a package or delivery to be taken to another location.

SECTION III: EDUCATION AND TRAINING

Employee Education and Fraud Training\(\textit{vii viii}\): Empower employees to recognize and defend against attacks; foster a security-aware culture. 

- Keep employees informed on the type of scams being perpetrated.
- Provide anti-fraud training on how to recognize an attack and report suspicious behaviors that violate company policies and procedures.
- Train employees on what information is confidential and what should never be released unless approved by management.
- Train employees to slow down if the message conveys a sense of urgency, intimidation, or high pressure sales tactics.
- Train employees not to forward, respond to, or access attachments or links within unsolicited emails.
• Educate employees to avoid using or exploring “rogue devices” such as unauthenticated thumb/flash drives or software on a computer or network.
• Train employees on strong password tactics and good password hygiene.
• Hold employees accountable, but also create a culture where they are rewarded for verifying suspicious activity.

SECTION IV: CONTROLS

Internal Controls\textsuperscript{ix x}: Defend against social engineering fraud with improved and new internal controls, such as:
• Authenticate changes to vendor or customer contact information and internal bank information. Use previously known phone numbers and email addresses when verifying.
• Require supervisor sign-off on any changes to vendor and client information.
• Validate requests from vendors and clients.
• Validate all internal requests to transfer funds.
• Limit wire-transfer authority to specific employees. Consider two-factor authentication and verification.
• Guard against unauthorized physical access (theft of keys, access cards, ID badges etc.).
• Keep physical documents locked and secured and shred documents no longer in use.
• Monitor the use of social media.
• Develop reporting and tracking programs that document incidences of deception fraud or attempts of deception fraud.
• Keep cyber security software up to date.
• Implement mobile device security procedures.
• Use two factor authentications on your organizations computer platform(s).

SOURCES & NOTES.

\textsuperscript{i} Symantec ISTR20, Internet Security Threat Report 2015
\textsuperscript{ii} Travelers Insurance
\textsuperscript{iii} Symantec ISTR20, Internet Security Threat Report 2015
\textsuperscript{iv} FBI Public Service Announcement, I-082715a-PSA, August 27, 2015
\textsuperscript{v} Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. \textit{As defined by the Internet Crime complaint Center of the FBI.}
\textsuperscript{vi} Guide to Preventing Social Engineering Fraud, CHUBB, October 2014
\textsuperscript{vii} Guide to Preventing Social Engineering Fraud, CHUBB, October 2014
\textsuperscript{viii} Advisen Insurance Intelligence, The Hartford, Spear-Phishing Attacks: Reeling in Corporate America, August 2015
\textsuperscript{ix} Guide to Preventing Social Engineering Fraud, CHUBB, October 2014
\textsuperscript{x} Advisen Insurance Intelligence, The Hartford, Spear-Phishing Attacks: Reeling in Corporate America, August 2015