

WHAT IS SOCIAL ENGINEERING?

Social Engineering is the practice of tricking an employee into revealing sensitive information or sending money to an unauthorized recipient. One popular form of **Social Engineering** fraud occurs when criminals trick an employee into sending them money by impersonating a business vendor, customer or senior/C-level executive.

4 Steps of Social Engineering Fraud



Gather Info

Using online sources, the scammers gain details to effectively impersonate an employee, vendor or customer



Hook Target

The imposter then contacts a target employee (usually with financial authority)



Provide Instructions

The imposter requests a fraud payment with transfer instructions



Receive Money

Using a sense of urgency, criminals induce the target employee to transfer funds into their account



REAL PAM OR REAL SCAM EMAIL?

Chuck in accounts payable receives the following email instruction "allegedly" from Pam, the CFO, who, coincidentally, is out of the office at a CFO conference in Florida:

"Chuck, I just landed a great deal with a widget supplier out of Tulsa. Please wire \$20,000 to the following account on my authority so I can lock in this great rate. I'll fill you in when I'm back in the office. Thanks, Pam"

PROTECT YOUR BUSINESS

- ✗ **Never provide confidential information** via email, phone or text.
- ✗ Be wary if someone is requesting payment through an email or phone call. **Verify the source using another channel** such as a confirmation phone call to another number or contact person.
- ✗ **Never let urgency** in the sender's message **cloud your judgment**.
- ✗ **Review your website and social media usage** to ensure travel and related plans are not inadvertently divulged.
- ✗ **Maintain a security aware culture**. Educate employees at all levels of the organization and **don't ditch the controls**, even for the CEO.

INSURANCE TIPS

- ✗ Policies typically cover direct loss only and not indirect or consequential damages (e.g. late fees owed to a vendor who did not receive payment).
- ✗ Take note: a policy may require a verification procedure such as a call back.

Cyber Insurance Education

- Fraudulent Funds Transfers
- Extortion / Ransomware
- Social Engineering**
- Business Interruption
- Data Breach/Privacy
- Network Security
- Website Media Liability

ABA
Insurance
Services

The loss prevention information presented is intended to provide guidance and is not intended as a legal interpretation of any federal, state or local laws, rules or regulations applicable to your business; it is intended only to assist policyholders in the management of potential loss producing conditions involving their operations based on generally accepted safe practices. The liability of Great American Insurance Company and its affiliated insurers is limited to the terms, limits and conditions of the insurance policies underwritten by any of them. The claims examples are provided for informational purposes only. No representation is made as to the truthfulness or accuracy of any fact, circumstance, allegation, or legal conclusion contained in or inferred from the examples presented above, nor is any representation made as to whether any claims example would constitute a "claim" or satisfy any other requirements for coverage under the applicable policy. Coverage for any claim is determined upon the specific facts presented, the terms and conditions of the policy and applicable law. ABA Insurance Services Inc. is an OH domiciled agency with its principal place of business at 3401 Tuttle Rd., Suite 300, Shaker Heights, OH 44122. © 2021 ABA Insurance Services Inc., dba Cabins Insurance Services in CA (License No. OG63200), ABA Insurance Services of Kentucky Inc. in KY, and ABA Insurance Agency Inc. in MI. 082021.SBM31