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?

Impersonation Email Scam Example

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.

ABA Insurance Services

Cyber Insurance Education

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