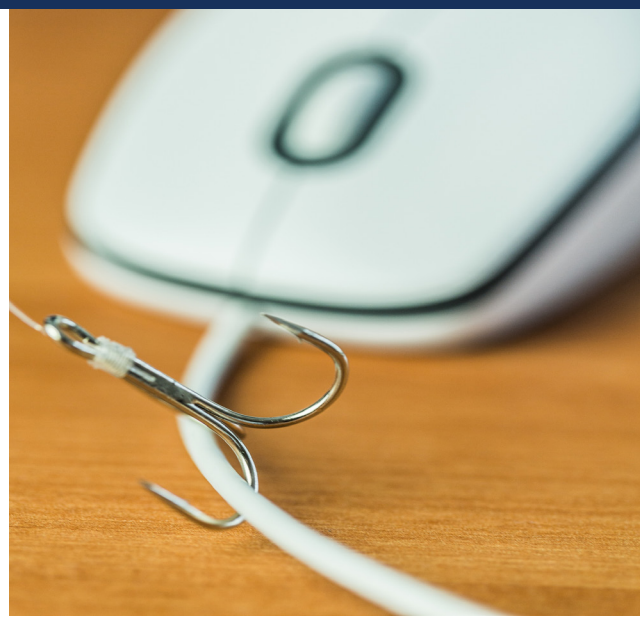
Social Engineering & Funds Transfer Fraud



There is an increasingly common and sophisticated type of crime known as " Social Engineering". An attacker poses as a trusted vendor, prospect, client, or employee to deceptively gain the confidence of an employee and induce them to part with money. This is a highly targeted operation in which the hacker has at least some information that he / she can use to make himself / herself seem familiar to the intended victim. For example, an employee can be intentionally misled into spending money or diverting a payment or diverting a payment based on fraudulent information that is provided t them in written or verbal communication such as an email, fax, letter or a phone call. Social engineering is the art of deception. While it can be amazingly complex, it is also very simple.

COVERAGE

Social Engineering coverage extensions can be obtained through the following type of policies depending on the carrier:

- Crime Policies
- Cyber Policy

LIMITS OFFERED

Coverage is available from $100,000 - $1M limits

TARGET COMPANIES

- Private, publicly-held, and not-for-profit entities are all targets.
- Companies, large and small, can be victimized.
- Small companies are often the most vulnerable to fraud because they may lack the financial or wire transfer controls that larger companies routinely employ.

SOCIAL ENGINEERING CLAIM EXAMPLES: (1)

Illegitimate Client

Public company with under 50 employees.

A business manager handling bill payment and bookkeeping services for a client received an email, purportedly from a client, inquiring about her balance and availability of funds for a wire transfer. The email included details regarding the scope of services that were provided, as well information about other transactions that had recently been performed. The wire, for $100,000, was to go to an offshore account, purportedly for the purchase of a new piece of real estate. After the purported client won the business manager's trust, the business manager authorized wiring the funds to the fraudster's account.

Fake CEO scam

Public company with over 250 employees.

The regional CFO of a subsidiary of a large, publicly traded company received an email purporting to be from the assistant to the CEO in the United states. The email requested that the CFO transfer a large sum of money immediately to facilitate covering a tax payment in China. When the CFO questioned the request, a follow up phone call was made to the CFO, assuring him that the proper authority was granted and that it had come "from the highest levels" within the organization. With intimate knowledge of company policies, and an official looking letter on company letterhead "authorization" the transfer, the CFO transferred the money by wire. The scam was detected after another attempt at transferring funds was stopped by the subsidiary bank.

Vendor Email Hacked

Private company with under 250 employees.

The controller for a distributor of components parts was responsible for making regular payments to overseas vendors from which the distributor purchased products for resale in the United States. After many months f working with one particular vendor and receiving regular shipments, the controller received an email that appeared to come from his vendor contact, indication that the vendor's bank was having issues with accepting payments, and asking if the next payment could be made to a new bank. Due to the vendor's overseas location, verification was a challenge. After the supposed vendor applied some pressure, the controller paid the invoice via wire transfer.

Worldwide Facilities, LLC
Experience a World of Difference

BROKERAGE

wwfi.com