TRAVELERS

Social Engineering Fraud

COVERAGE HIGHLIGHTS AND BEST PRACTICES

What is social engineering fraud?

Social engineering fraud occurs when a bad actor intentionally misleads an employee into sending money or diverting a payment based on fraudulent information. This information is provided to the employee through a written or verbal communication such as an email, text, letter, fax or even a phone call.

How does this happen?

If you think this won't happen to your organization... think again. This surprisingly successful fraud happens every day to unsuspecting employees via a communication that appears to be from a legitimate vendor, client, employee or other authorized person. The communication typically contains a variety of misleading requests and information, and often includes a request to change certain banking information or payment instructions. In many cases, the fraudster has infiltrated an email conversation between a payor and payee, gaining significant information about financial transactions and electronic signatures. Fraudsters will even amend phone numbers in the signature block of an email, so a call back to the phone number listed in the email goes directly to the fraudster.

Business email compromise accounts for 50% of social engineering fraud incidents* and involves a hacker gaining access to an email account to trick others into fraudulent financial transactions.

According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3),

between

and

there were 137,601 U.S. victims of business email compromise schemes

amounting to an exposed U.S. dollar loss of $17,328,435,141**

Best Practices to Help Prevent a Loss

- Provide on-going anti-fraud training to all employees.
- Authenticate all change requests with a telephone call (or even video conference) using pre-determined contact information established early in the relationship, not from the change request. During call back, verify both the new payment details and the old payment details.
- Examine emails closely for changes in domain names (ex.: Hover over emails to determine true email addresses).
- Create a culture where it is acceptable and expected to question payment instructions, even those purporting to come from supervisors.
  - Look for red flags (i.e., is there an element of time pressure to make changes? Is there something unusual about the request?).
  - Allow employees to call a timeout if something feels out of place.
  - Encourage employees to slow down when it comes to changes.
  - Assume every change is fraudulent, and ask questions, such as, whether the new bank location makes sense.

Claim Scenarios

- An employee at a manufacturing company received an email that appeared to be from the company's CFO. Unbeknownst to that employee, a fraudster had gained access to the CFO's email account. As part of the scheme, the fraudster reconfigured the settings of the CFO's email account such that certain emails were immediately directed away from the CFO's inbox and into the fraudster's email account. Using the actual email address of the CFO, the fraudster requested a wire transfer to a bank account in China to complete the purchase of a small competitor. The email stressed urgency and the need for secrecy regarding the transaction until the acquisition could be formally announced. The payment was made per the instructions contained in the email message. When the employee placed a call to the CFO the next day to find out how the payment should be coded for reconciliation purposes, it was discovered that the CFO's email had been hacked and the request was fraudulent.
- An attorney at a law firm was engaged by a pre-existing client, in part, to manage the client's funds through the law firm's trust account. As part of their responsibilities, the attorney routinely wired funds from the trust account to fund the client's acquisitions of property and equipment. The attorney received an email communication from a fraudster directing them to wire transfer funds to close a purported transaction involving the client's purchase of industrial equipment. Although the client's name on the header of the email appeared legitimate, the underlying email address had been modified by the fraudster. Following receipt of the email, the attorney wired the funds from the trust account and sent a separate email to the client to confirm the transfer. When the client received the confirmation, they immediately notified the attorney that the wire transfer request was fraudulent.

- A retailer purchased 1,000 laptops from its supplier. Payment for the order was due to the supplier within 45 days. A few weeks after receiving the shipment of laptops, the retailer received a fraudulent email purportedly from the supplier providing revised bank account information for payment of the invoice. The retailer updated its accounts receivable and issued payment using the new banking instructions. A review of the email from the fraudster posing as a supplier revealed that the email address contained a "1" in the place where an 'l" belonged, as the fraudster had created a new email address intended to appear to be the supplier's with this one small change. This nuance, difficult to spot with the naked eye, was not identified by the retailer's employees. Subsequently, the retailer received an inquiry from the actual supplier regarding the status of the payment.

What Travelers can offer?

Travelers is offering a Social Engineering Fraud insuring agreement via an endorsement for Wrap+® and Executive Choice+® Crime Coverages. This endorsement specifically extends coverage to include instances of social engineering fraud perpetrated by a purported vendor, client, employee or other authorized person.

*Verizon 2023 Data Breach Investigations Report

**https://www.ic3.gov/Media/Y2023/PSA230609

TRAVELERS

travelers.com