E-COMP NOW!

Business Insurance Simplified

Social Engineering Insurance Coverage

Why pay attention to social engineering attacks?

Why now?

MITIGATING FINANCIAL LOSS AND EXPENSES TRIGGERED BY SOCIAL ENGINEERING INCIDENTS

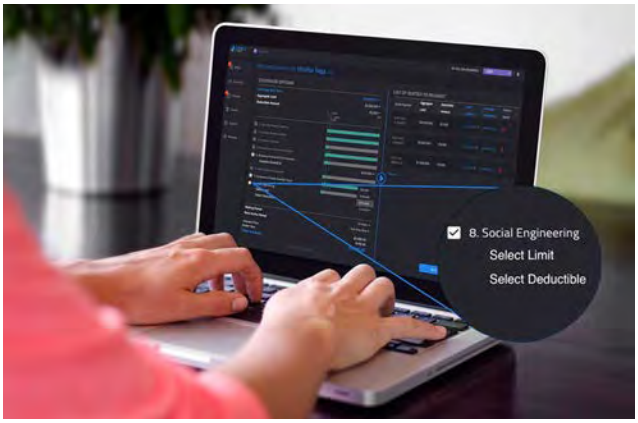
Social engineering can be broadly defined. In the context of cyber security, social engineering is the psychological manipulation of people into:

1. Performing specific actions that benefit the perpetrator such as transferring funds to the bank account of a cyber criminal. The cyber criminal might not gain access to any business system or data but intentionally leads an employee, often an executive with privileged access, to perform an act that leads to a loss for the business.

2. Divulging confidential information, such as credentials to unintentionally give access to sensitive data, intellectual property or access to company or third party valuable information.

Both cases can happen under the umbrella of a social engineering attack such as phishing, email spam or other.

Up to 98% of cyberattacks deploy social engineering methods showing how cyber criminals excel at exploiting human weakness. The global pandemic has been very unsettling for everybody: job disruption, the fear of getting sick, or the need to work from home. In a March 2020 communication, the World Economic Forum warns that cybercriminals are taking advantage of the situation and exploit fear and uncertainty. In a crisis situation, people tend to make mistakes they would not have made otherwise and fall victim of phishing, the most common type of social engineering.



GETTING ADEQUATE PROTECTION FOR SOCIAL ENGINEERING

Businesses of all sizes should consider cyber insurance programs that take an expansive approach to social engineering, including cases where the cyber criminal does not gain unauthorized access to company assets per say. Once a Social Engineering coverage is triggered for loss coverage then other traditional coverages could be triggered as well, depending on the specific incident and the coverage requirement, to cover other expenses.

TWO CLAIM EXAMPLES

Phishing email - scenario 1:

Employee (accountant) receives an email from the CEO that looks legitimate but is a fake, asking to transfer funds from the company bank account to an illicit bank account. The email is malicious, but the fund transfer is performed by the employee with legitimate access. In this case the employee is initiating the transfers of funds and the transaction by itself is authorized. The only fraudulent part of this social engineering event is the party that receives the money.Under Cowbell Prime 100, the incident would trigger the Social Engineering coverage all things considered. Financial loss and expenses are covered up to the specific sublimit.

Phishing email - scenario 2:

The company accountant receives an email from the CEO that looks legitimate but is fake, and includes a link to a login page where the hacker simply harvests company credentials. The cyber criminal then uses the credentials to log in and transfer funds from the company bank account to an illegitimate bank account. In this scenario, because the cyber criminal gets credentials and gains unauthorized and persistent access to company assets until discovered and stopped, financial loss and expenses could trigger the Computer and Funds Transfer Fraud coverage (FTF), if all other conditions for FTF are met.

Note that FTF covers other scenarios such as an attacker switching out account numbers on invoices, sending out actual instructions to a financial institution to release funds to a 3rd party or instructions sent to a distributor instructing them to release goods to a 3rd party.

COMMON TERMINOLOGY RELATED TO SOCIAL ENGINEERING:

Vishing:
is phishing applied to phone calls. We have all received calls pretending to be our bank. Scam calls represented 30% of all phone calls made in 2018.

Smishing:
is phishing applied to SMS

Whale Phishing:
is a phishing attack that is specifically aimed at powerful individuals with privileged access to numerous systems or data.

Deepfake phishing attacks:
can be terrifying. Deepfake employs machine learning and artificial intelligence to fabricate synthetic human images or voice content to impersonate real people, making these phishing attacks more difficult to detect.

Download our special report on cyber resilience in times of covid-19 for recommendations to keep your business protected.

Finally, stay informed, don't hesitate to ask questions: if you need clarification on Social Engineering versus other coverages, what is covered or not, feel free to contact us. Call: 888-493-2667 or email us: service@goecomp.com.