TRAVELERS

Social Engineering Fraud Endorsement

COVERAGE HIGHLIGHTS

What is social engineering fraud?

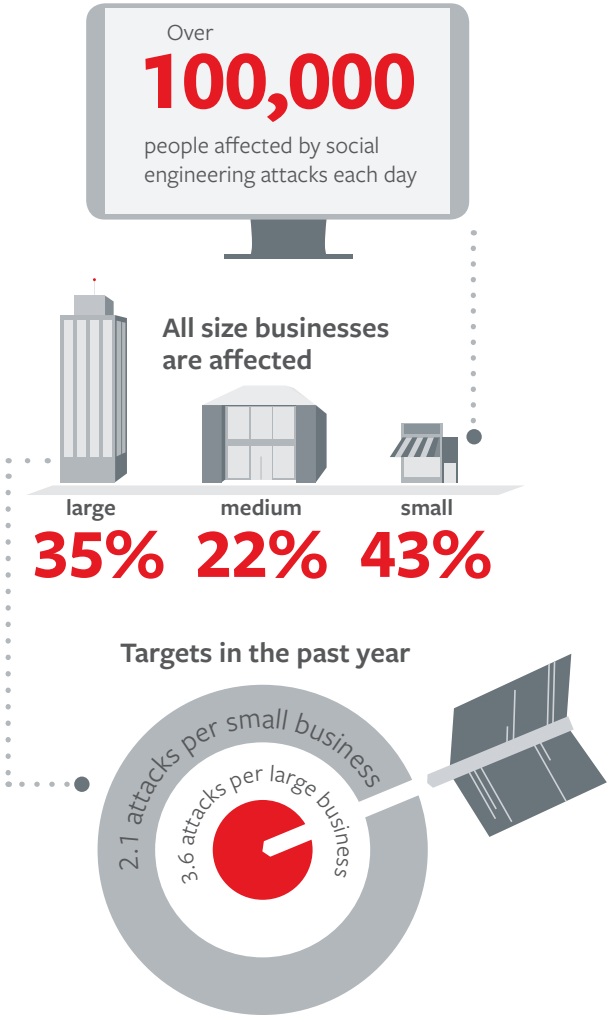
It is a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information that is provided to the employee in a written or verbal communication such as an email, fax, letter or even a phone call.

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 with the receipt of a message that appears to be from a legitimate vendor, client, internal employee or authorized person that contains a variety of misleading requests and information. In many cases, the fraudster has infiltrated an email conversation and has been able to obtain a copy of a signature section to make the fraudulent message appear even more legitimate. Some messages even amend phone numbers in the email panel, so a call back to a phone number is directed to the fraudster, who will of course verify the information.

How often does this happen?

Targeted attacks on businesses have increased 55% in 2015.[1] And it has been reported that there are over 100,000 people affected by social engineering attacks each day.[2]



Who can be a target?

Businesses of all sizes are affected by targeted attacks[3]:

- 35% of large businesses
- 22% of medium businesses
- 43% of small businesses

And many companies that are targeted receive multiple attacks[4]:

- 2.1 attacks per small business
- 3.6 attacks per large business

[1] Symantec™ Internet Security Threat Report 2016

[2] Hillard Heintze The Front Line Report

[3] Symantec™ Internet Security Threat Report 2016

[4] Symantec™ Internet Security Threat Report 2016

Why your business needs protection

Even well-managed businesses with proven best practices of employee training, partner background screenings and financial checks and balances can be infiltrated. Fraudsters can gain the confidence of an employee by posing as a vendor, client, employee or authorized person, and instruct him or her to transfer or divert money. Most companies do not even realize a deception has occurred until they are notified by the real recipient who never received a legitimate payment. And once discovered it can be too late to stop the fraudster's theft. Therefore it is important to understand the threat and be prepared to protect your business from serious financial loss.

That is why Travelers is offering an endorsement with a social engineering fraud insuring agreement for ***Wrap+***® and ***Executive Choice+***® Fidelity and Crime coverages. Traditional Fidelity and Crime insurance policies often limit losses to fraud schemes that a business is unaware of and is not an active participant in the scheme. This endorsement specifically extends coverage to include instances of social engineering fraud perpetrated by a purported vendor, client, employee or authorized person.

Claim scenarios:

- An employee at a manufacturer received an email that appeared to be from its CFO, requesting a wire transfer to a bank account in China in order to complete the purchase of a small competitor. The email stressed the urgency and also 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 in order 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 his 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 directing the attorney to wire transfer funds to close a purported transaction involving the client's purchase of industrial equipment. 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 he immediately notified the attorney that the request was fraudulent and the purchase did not exist.
- 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 an 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. Subsequently, the retailer received an inquiry from the actual supplier regarding the status of the payment. The supplier's email system was hacked, and the change to the supplier's banking instructions was fraudulent.

Why Travelers?

- We've provided effective insurance solutions for more than 150 years and address the needs of a wide range of industries.
- We consistently receive high marks from independent ratings agencies for our financial strength and claims-paying ability.
- With offices nationwide, we possess national strength and local presence.
- Our dedicated underwriters and claim professionals offer extensive industry and product knowledge.

Travelers knows Fidelity and Crime coverage.

To learn more, talk to your independent agent or broker, or visit travelersbond.com.

TRAVELERS

Available through the ***Wrap+***® and ***Executive Choice+***® product suites.

travelersbond.com