TRAVELERS

Social Engineering Fraud Endorsement

COVERAGE HIGHLIGHTS FOR FINANCIAL INSTITUTION BONDS

What is social engineering fraud?

Social Engineering is when an employee is intentionally misled 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 institution... think again. This surprisingly successful fraud happens every day to organizations of all types and sizes. An unsuspecting employee can receive a message appearing to be from a legitimate vendor, client or fellow employee that contains a variety of requests and information. In many cases, the fraudster has infiltrated an email conversation and has been able to obtain the vendor, client or fellow employee's signature section to make it appear even more legitimate. Some fraudulent 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 more than doubled from 2012-2014[1]. And it has been reported that there are over 100,000 people affected by social engineering attacks each day [2].

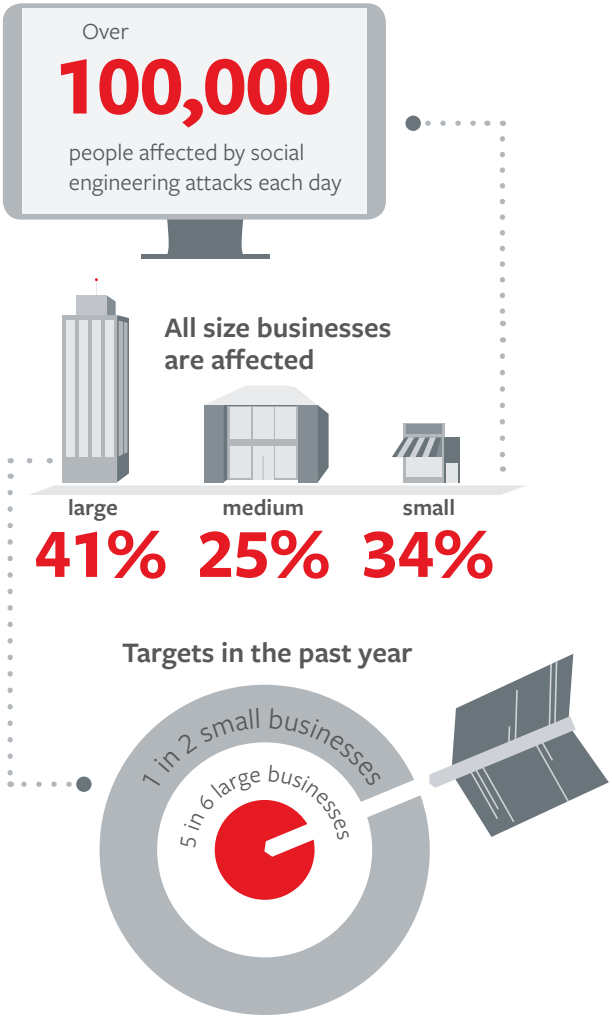
Who can be a target?

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

- 41% of large businesses
- 25% of medium businesses
- 34% of small businesses

And many companies have been targeted at least once within the past year[4]:

- 1 in 2 small businesses
- 5 in 6 large businesses



[1] Symantec Internet Security Threat Report 20

[2] Hillard Heintze The Front Line Report

[3] Symantec Internet Security Threat Report 20

[4] Symantec Internet Security Threat Report 20

Why your business needs protection

Even well managed financial institutions with proven best practices of employee training, business partner background screenings and financial checks and balances can be infiltrated. Fraudsters can gain the confidence of employees by posing as a vendor, supplier or client and instruct them to divert money. Most financial institutions don't even realize a deception has occurred until they are notified by the real vendor, or client who never received a legitimate payment. And once discovered it's often too late to recover a wrongfully made payment. Therefore it is important to understand the threat and be prepared to protect your institution from financial loss.

That is why Travelers is offering a Social Engineering Fraud Endorsement for the Select One Financial Institution Bond for community banks, credit unions and insurance companies. Traditional bond coverages often limit third party fraud losses to circumstances a financial institution is unaware of and require that the employees are not active participants in the scheme. This new endorsement extends coverage to include instances of Social Engineering Fraud from perceived vendors, clients or fellow employees.

Claim scenarios:

- The fraudsters intercept a legitimate invoice from a legitimate vendor's email correspondence. They create a new email with an email address very similar to the vendor's real email address. They send the invoice to the financial institution from the fake email address and tell the financial institution that their (the vendor's) bank account was hacked so they had to open a new one and to please remit the payment for the invoice to the new bank account number provided. The money is then quickly withdrawn by the fraudsters.
- The fraudster sends an email to an employee in the financial institution who routinely wires money. This employee may be in accounts payable, accounting, the CFO's office, etc. The fraudster pretends to be a high ranking employee of the financial institution and instructs the real employee to send money somewhere. There is always a back story, such as "we owe a debt on this and have to pay it very quickly or we will be sued" or "we are buying another company and we need this wire to initiate the deal." The instructions are usually cloaked in secrecy and always urgent. In some cases, the "purported" CEO or high ranking employee will tell the employee that they will be contacted via email by an attorney who will provide them the details of the wire.

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 Financial Institution Bonds coverage.

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

TRAVELERS

Available through the *Select One+*® suite of products

travelersbond.com