Don't Bite the Bait: Protect Organizations From Phishing Attacks

One Friday afternoon, the treasurer of Platte County, Mo., received an email from the presiding commissioner, requesting the immediate transfer of funds to an out-of-state consultant. The treasurer tried to verify the request, but the commissioner was away on vacation and not easily reachable. Driven by the urgency of the email, the treasurer arranged the transfer without waiting for an appropriate response, overriding county procedures designed to prevent illegitimate movement of funds.

Then he got a call from the commissioner, who was totally unaware of the request.

And just like that, the county lost $48,000 to a cyber criminal in a single afternoon.

The "Kansas City Star" reported this incident just days after the loss.

"Deception fraud or social engineering fraud is the 21st century version of an ancient con game, only now it's played out much faster using electronic communications," said Mike Kosednar, assistant vice president and product manager for management and professional liability insurance, The Hartford.

"Email inherently carries an element of urgency, and the fraudsters prey on our desire to respond quickly, especially to emails from the boss."

Losses from social engineering, specifically phishing scams, have skyrocketed as cyber thieves grow adept at mimicking internal emails.

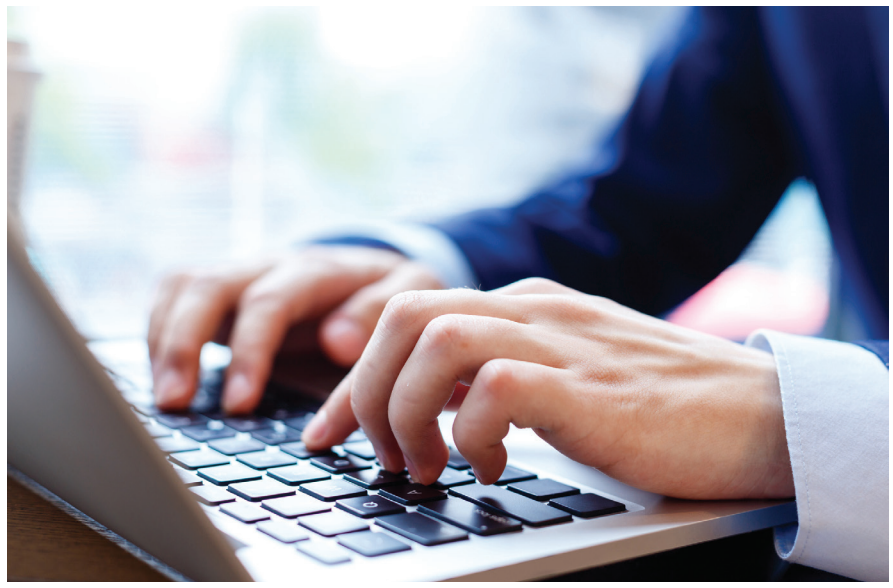
According to statistics gathered by the FBI, law enforcement agencies across the globe received reports from 17,642 victims from October 2013 through February 2016, resulting in more than $2.3 billion in losses.

Since January 2015, the FBI has seen a 270 percent increase in identified victims and exposed loss, according to the FBI's Cleveland division.

And the phishers aren't just targeting organizations with deep pockets. Social engineering fraud can hit companies of all sizes.

"While a large public company may have a loss exceeding eight figures, for a smaller business, getting tricked into sending $6,000 or $7,000 can be significant," Kosednar said.

It's relatively easy for cyber thieves to identify the CEO or CFO at their target company and then emulate their email style, mimicking their tone and signature, and making it appear as though the message is coming from the company's server.



Phishing scams have skyrocketed as cyber thieves grow adept at mimicking internal emails.

PEOPLE MORE THAN TECHNOLOGY ARE THE CRITICAL RISK

While there are several technology solutions that companies can implement to enhance their system security, such as continually updated firewalls; the use of closed, private Wi-Fi networks; requiring a two-factor authentication for log-in; or third-party testing of firewalls, these safeguards are expected — any business operating in today's digitized world knows it needs to pay attention to its IT security.

Human error is often a bigger risk.

"In social engineering fraud, the weakest link in the security chain is the employee who accepts a scenario at face value and doesn't check its legitimacy," said Kosednar, "A willingness to please can undermine common sense."

"Social engineering losses are almost 100 percent preventable. Agents and brokers play a critical role in educating their clients about these risks."

— Mike Kosednar, assistant vice president and product manager for management and professional liability insurance, The Hartford

The best defense against these insidious attacks, therefore, is employee education and training.

According to Kosednar, training requires — at a minimum — a three-pronged approach:

• Establish a process.

Companies can identify fraudulent requests by developing a formal procedure around the transfer of funds that limits transfer ability to a small number of employees and requires a next-level supervisor to sign off on the request. It should also involve independent verification of the email's sender.

"Verification needs to be made to predetermined email addresses and phone numbers and not by hitting 'reply' or calling a phone number provided as part of the request."

• Regular reinforcement.

Constant reminders emphasize the importance of following proper procedures in every situation. Some companies choose to do this by randomly testing their employees with bogus emails. The company might send a message that appears to be from a senior manager, imploring staff to click on a suspicious looking link, for example.

"Seeing the percentage of employees that failed helps determine additional training needs," Kosednar said. "This should include a heart-to-heart conversation with the employees who failed, which should be constructive and encourage them to speak up and ask questions when they suspect they've received a fraudulent email."

• Change your culture.

Since social engineering fraud is often most successful at companies where questioning one's superiors is frowned upon, companies can create an environment where it is acceptable and even encouraged for employees to double-check a wire transfer request from anyone regardless of their rank.

INSURANCE PROTECTION

Even well-managed organizations with proper security controls in place can fall victim to a phishing attack, so it is important that a company's crime insurance also includes coverage specifically for deception fraud.

"Traditional crime coverage is designed to respond to cases of employee theft or robbery and burglary," Kosednar said. "However, sending money to someone voluntarily doesn't fit into any of those categories, so the deception fraud coverage was created to specifically address this new risk."

The Hartford offers deception fraud coverage as an option to its CrimeSHIELD® Advanced for public companies and Private Choice Ovation® for private entities.

Insurance can help mitigate losses resulting from deception fraud, but it is not a substitute for proactive risk management practices.

"Social engineering losses are almost 100 percent preventable," said Kosednar. "Agents and brokers play a critical role in educating their clients about these risks and the importance of having appropriate training and procedures in place, as well as insurance coverage options to protect their business in the event of a loss."

Reach Mike Kosednar at Michael.Kosednar@thehartford.com. For more information regarding The Hartford's crime coverages, visit www.thehartford.com/crime.