MARCH 2016

SOCIAL ENGINEERING CRIMINALS MAY BE TARGETING YOUR ORGANIZATION: ARE YOU VULNERABLE?

Ryan Roberts | Vice President, Account Executive
Michael Reph | Account Executive

What is social engineering fraud?

Human-based social engineering fraud (sometimes referred to as human hacking) is defined as the art of influencing people to disclose information and getting them to act inappropriately. The consequences of social engineering fraud usually manifest when an employee is intentionally misled into sending money or diverting a payment based on fraudulent information. In 2014, over 100,000 new social engineering attacks were attempted every day against businesses of all sizes. This represented a 91% increase from the previous year, and has continued to rise[1]. Often, the attackers utilize cleverly disguised phone calls or emails based on well-researched personal and company information, available in the public domain. An attacker may even pose as a trusted vendor or spoof your internal email addresses to resemble an internal email from a co-worker.

How is this happening?

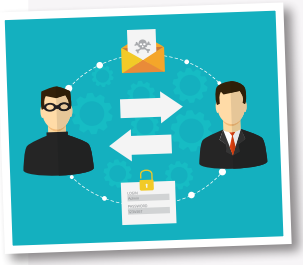
Human hackers use a number of effective strategies to infiltrate an organization such as impersonating a vendor, IT representative, or even an internal person of authority. This kind of fraud is surprisingly effective and is happening daily to many businesses. Additionally, human hackers are using a variety of sophisticated spamming, phishing, phone phishing, and even data recovery from discarded computer hardware and other devices that were not property destroyed. For example, a phishing attack may mirror an email from the company's financial institution, suggesting that there was a problem and requesting the employee to respond with confidential information, which is then used to gain access to bank accounts, etc. Often times, the communication in these emails will give corroborating instructions with dummy email and phone numbers controlled by the hacker to give an added sense of security. Another tactic gaining traction is targeting businesses on or around times when employees who work together may be out on vacation, the intent being that normal face-to-face communication will be supplanted with email correspondence.

Social engineering fraud may have a number of objectives, but most often, the goal is simply financial gain.

> Social engineers realize that often it's **easier to trick someone into revealing a password** than trying to hack the system.

[1]Symantec 2014 Internet Security Threat Report

continued >



REAL LIFE EXAMPLE

A company's controller received a request from one of the company's equipment vendors indicating the vendor had changed its banking arrangements. The email was from the normal individual at the vendor's accounts receivable department and provided information of the new banker and where to now wire funds for a recent large equipment purchase made by the company.

The company even called the phone number listed for the bank in the vendor's email, and it was confirmed by the person on the phone that they were indeed the new bank for the vendor.

Of course, all of the above was not true. The perpetrator had hacked into the vendor's system, used the vendor's email to send the fictitious banking information, with a fictitious phone number, which was answered by an accomplice.

The company only learned of the fraud when the vendor sent an overdue payment reminder to the company.

Preventative Measures

Make sure employees across the organization are educated and trained how to best detect these kinds of fraudulent schemes. Be wary of unsolicited emails, calls, and never give out confidential company information outside of set protocols. The common weak link that hackers depend on is the human link. Make sure your organization, financial institution, and partner vendors have specific policies and procedures to prevent and respond to attacks.

Additional helpful tips are available through the United States Computer Emergency Readiness Team at www.us-cert.gov.

What is the role of insurance coverage?

Traditional crime and/or cyber insurance policies are not necessarily intended to cover social engineering fraud losses. With the ever increasing activity in this space, many insurance companies have responded with social engineering fraud endorsements to explicitly cover these types of losses. Ensuring that this gap is covered in either your crime or cyber insurance policy is crucial.