Social Engineering – Risks, Techniques and Safeguards

mimic TECHNOLOGIES

Proven RIA Technology Solutions

CONTAINED WITHIN

Social Engineering

Firms spend a great deal of time, money and effort to ensure that they have IT security in place and that it is sufficient to safeguard their systems. Security that protects company data, allows for firms to comply with state and federal laws, and protects the privacy of their client's information. That is all the good news. The bad news is that even the most robust security program can be bypassed through fraud-based attacks known as Social Engineering. This type of fraud is very effective, and its execution is a lot easier than you might believe. Social engineering is extremely low cost for attackers to use, and its low technology dependence makes it a perfect tool to overcome many standard information security measures.

Executive Summary

The basic goals of social engineering are the same as general computer hacking: with the most ominous being to gain unauthorized access to company systems and the information within in order to commit fraud. As for why an organization would be targeted through social engineering is pretty simple; because it is often a simpler way to gain access to information than through other forms of technical hacking. Even for computer hackers, sometimes it's just easier to pick up the phone and ask someone for their password. And, unfortunately, many times the information the hackers are targeting is readily given to them.

The basic goals of social engineering are to gain unauthorized access to company systems and the information within in order to commit fraud.

All too often IT staff and firm management believe that the computer security principles in place will safeguard them against information theft and that the "common sense" of their employees is enough to prevent fraud-based information loss. This is a dangerous and overreaching assumption. There must be a comprehensive IT security program that includes: training regarding information security and common social engineering techniques as well as prevention tactics.

In this paper we will discuss some common social engineering techniques employed by attackers. We will also analyze why employees fall for these cons and go over various tactics that can be utilized to mitigate your risk to social engineering.

What is Social Engineering?

Social engineering is the term used within the information security industry that refers to the psychological influencing of individuals with the goal of acquiring confidential and/or protected information. Attackers capitalize on the inherent trusting nature of people and their willingness to “help someone in need” in order to obtain information they are not supposed to have. If social engineering sounds like a fancy term for "lying", well, that’s because it is – and it can be ridiculously effective.

The Attacker Arsenal – Social Engineering Techniques

Pretexting is one of the most often used social engineering techniques. Pretexting occurs when someone attempts to gain access to personal nonpublic information (NPI) without the proper authority to do so. The most popular method of pretexting involves requesting private information while impersonating the account holder via phone or correspondence (i.e., letters, fax or e-mail) or by ‘phishing’ (i.e., using a bogus website or email to collect data – more on this later).

Pretexting to gain access to financial data was specifically banned by the Gramm-Leach-Bliley Act (GLB) in 1999. The pretexting restrictions defined by GLB apply to all organizations that handle financial data, including banks, Broker Dealers, and Investment Advisers. The Act's restrictions only apply to nonpublic personal information (NPI) and not to information that enters the public domain as a matter of public record (e.g., real estate transactions, property taxes or police records).

The Pretexting Protection section of GLB encourages organizations to implement safeguards against pretexting. These include having a well-written plan designed to develop, monitor, and test a program to secure all NPI. Such a plan would also feature sections on training employees to recognize and deflect inquiries made under pretext.

Dumpster Diving is a social engineering attack that involves searching through trash cans and dumpsters for useful information. While this technique may sound both silly and unappealing to most of us, this activity can provide volumes of valuable information. Burn bags and shredders are common throughout the securities industry for the disposal of information containing client specific data and NPI, but those only work when used properly for all pertinent company documents. Information that does not contain client-specific data and, therefore, might not make it into a shredded or burn bag include sticky notes with credentials, company directories, organizational charts, policy manuals and calendars. Rest assured, any of the information gleamed from within these documents could be used by a social engineer as a means to gain further access into a private network.

Shoulder surfing is another technique that requires little or no actual interaction with an employee. Shoulder surfing occurs wherever an attacker is able to eavesdrop on someone entering a password, discussing sensitive information, or working with sensitive files. This can be especially prevalent when sensitive information is discussed during meetings or phone conversations which occur in public places such as restaurants, coffee shops, or even by the office water cooler. Without a doubt, a careless slip of the tongue at the wrong moment is all it takes for someone else to take advantage.

Phishing is a technique of fraudulently obtaining private information via a deceptively created e-mail message or web site. Typically, the "phisher" sends an e-mail that appears to come from a legitimate business (e.g., a bank, payroll processer, prime brokerage) requesting "verification" of information. Commonly, this message will contain a warning of some dire consequence if the information is not provided (e.g., a disgruntled client will cancel their account, or the supervisor of the employee handling the inquiry will be upset for their failing to comply). The e-mail usually contains a link to a fraudulent web page that looks legitimate complete with company logos and content—and has a form requesting everything from a logon credentials to client's personal information such as home address to social security number and even information as private as ATM card number and PIN. Once the misled employee fulfills the request they are often redirected back to the actual decoy company web site, thus giving the impression that the transaction was legitimate.

Tailgating happens when a social engineer accesses a restricted area, secured by unattended electronic access controls, by simply walking in behind a person who has legitimate access. Following common courtesy and not without a little bit of irony, the person with the legitimate access will oftentimes hold the door open for the attacker. The legitimate person may fail to ask for ID because they don't want to come across as nosy, or rude - or they may simply accept the attacker's explanation that they had forgotten their ID card at home that day, or had accidentally left it on their desk.

REAL WORLD CASE STUDY

FINRA sanction 6/17/13

A registered representative in West Bloomfield, Michigan submitted a Letter of Acceptance, Waiver and Consent in which she was fined $5,000 and suspended from association with any FINRA member in any capacity for 30 days.

Without admitting or denying the findings, the representative consented to the described sanctions and to the entry of findings that she affected wire transfers totaling $13,400 from a firm customer's account to an unrelated third-party account after receiving fraudulent emails from someone purporting to be the customer. She received emails from an attackerpurporting to be the customer who requested the customer's account balance and then sent fully executed letters of authorization (LOAs) that fraudulently authorized wire transfers to an account at a third party bank. The findings stated that the representative did not authenticate the customer's signature contrary to firm policies and procedures, which required registered representatives and associated persons to speak to the customer prior to affecting a transfer of funds to an outside account. She processed the transfers and falsely indicated on the firm's internal system that she spoke with the customer and verified the customer's identity. The findings also stated that after the customer discovered the improper wire transfers on her account, she contacted the representative. While the representative and the customer were discussing the fraudulent wire transfers, the representative received another request from the hacker, requesting a third transfer of $7,350. The hacker attached an executed fraudulent LOA to the request. The representative did not respond to the request and contacted her firm's office management team and advised them of the previous transfers. The firm credited the customer's account for the full amount of the transfers. The findings also included that the representative caused her firm to maintain false books and records related to the wire transfers.

Baiting is a real-life Trojan horse attack that uses some sort of physical media and relies on the curiosity, helpful nature or greed of the victim.

In this type of attack, the attacker leaves a malware infected DVD or USB flash drive in a location where it will easily be found by an employee of the targeted firm. Common drop spots would consist of bathrooms, near elevators, or in firm's the parking lot. The malicious device could be labeled with a legitimate looking and curiosity-piquing label. After planting the bait, the attacker simply waits for a victim to plug in or attempt to view the contents of the device. The hope is that an unknowing employee might find it and subsequently inserts the disk or flash drive into a work computer to satisfy their curiosity, or that a Good Samaritan will view the contents with hope to identify the owner. Either way, as a consequence of merely inserting the device into a computer or opening files stored on the device the victim would unknowingly install malware. Malware that is secretly "phoning home" and likely providing an attacker access to the system or multiple systems within the targeted company's network.

Why Do We Fall for It?

Employees freely give out information for a number of reasons. In most cases, people just want to be helpful. It may be that it is their job to work with and provide such information to others and it becomes the norm. Or perhaps the individual is just talkative and enjoys keeping a conversation going regardless of what information they are sharing. In any case, it may not seem so out of the ordinary to them to be asked to divulge what might be considered sensitive information. Especially if they think that they are dealing with a colleague, client or an official representative of their client. People can also be coerced into believing that someone in a position of authority needs the information, and that they may be reprimanded for not assisting with the request of a superior. Or it could just be to make the annoying and persistent individual on the phone (or even at their desk!) to go away. Social engineers understand how to manipulate the natural desire to be helpful - a much-lauded trait in financial services - and use it to their advantage.

Social engineers understand how to manipulate the natural desire to be helpful - a much-lauded trait in financial services - and use it to their advantage.

What Can You Do about Social Engineering?

Efforts to protect against social engineering can be greatly improved with the implementation of well-defined policies and procedures. Furthermore, the training of employees (end-user) with respect to these policies and procedures is paramount to being able to identify and disarm social engineering attacks from the onset of the event. When these measures fail, it would be irresponsible to think that they never would, it is important to have security measures in place to protect the most often targeted assets your corporate network and the data it houses. The security measures to which we are referring would be your network security policies and procedures. While the network security which you need to have in place to protect your systems and the NPI they contain is a very important topic, it is a topic that is outside the scope of this primer on social engineering.

Nearly every month regulators report fining individuals and firms due to divulging client NPI

Employee security training is critical for firms to be able to protect themselves from social engineering attacks. Remember that employees (end users) are the weakest link in any firm's security program. Because of this, training them on relevant policies and procedures and then testing them on these topics is important to stopping these attacks.

Developing an Effective Social Engineering Training Program

- Make the information in training programs as relevant and engaging as possible. This will keep training programs - and, more importantly, the information covered by the training - fresh in the minds of the attendees.
- Teach employees basic social engineering techniques. When employees understand how social engineering schemes work, they will be in a better position to recognize these types of attacks and protect against them.
- Teach employees that almost any data could be valuable to a social engineer – not just what might normally be considered "sensitive" or protected as NPI. The social engineer's goal is to get at your firm's sensitive data and they are willing to take many less conspicuous steps to attain their end game
- Teach employees that it is okay to say "No". A very effective and often used tactic of social engineers is veiled threats that if the employee doesn't assist them, their boss/manager will hear about it and be angry. As a matter of procedure, employees should not be penalized for being reluctant to share sensitive information over the phone or through email.
- Evaluate the effectiveness of your training programs and threat awareness through "social" and "physical" penetration testing. Penetration tests are mock social engineering attacks orchestrated by professionals trained in imitating realistic attackers. Such exercises will demonstrate to employees how easily one can be duped. Being the target of a successful social engineering exercise defines the reality of the threat for your staff as well as allows the firm to understand how vulnerable they are to these risks.

In addition to the items mentioned above, here are some other techniques to follow:

- Establish security protocols, policies, and procedures for handling sensitive information. Make sure ALL employees are made aware of them. Regularly reiterate their importance.
- Train employees in security protocols relevant to their position.

- Identify information that is considered sensitive and evaluate its overall exposure to social engineering risk. Specify to trained personnel when, where and how this information should be securely handled and stored.
- Identify information categories that may not be considered sensitive but could still be targeted by social engineers for the purpose of advancing their attacks.
- Implement effective physical security controls such as visitor logs, escort requirements, and background checks for new employees or temporary workers.
- Establish a system where sensitive documents and media are securely disposed of and not simply thrown out with the regular office trash. If not already in place, insist on the use of dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff.
- Consider banning the use of non-corporate storage media such as flash drives.
- Institute the use of a web content filtering system that allows you to block employee access to questionable and potentially malicious web sites that can lead to system compromise.

The items listed are not intended to be all-inclusive nor specific to the state (or states) in which your firm conducts business. Rather, they are intended to serve as a starting point for a detailed discussion on safeguards that should be implemented in order to protect your firm from social engineering and data security breaches.

Conclusion

Social engineering poses a significant threat to firms of all sizes. Nearly every month regulators report that individuals and firms are fined due to divulging client NPI or, worse yet, wiring their client funds to unrelated third parties after receiving fraudulent phone calls or e-mails. Organizations must address these threats as part of an overall risk-management strategy.

Firms need to be mindful that social engineering techniques change, and there are always new and different schemes to be employed. Employees may not realize the information they deal with every day is a valuable commodity to a social engineer and that they need to protect it. A strong defense strategy against these threats is to generating overall awareness through training and testing.

Ongoing training will provide employees with the information and skills they need to recognize and respond to new or evolving social engineering threats. Having these proper tools at your disposal can improve the safety of your data and help protect against abuse. Testing will actively keep your employees' awareness piqued while giving management a “health check” on how well their staff is equipped to stop these threats.

Contact us:

888-99-MIMIC (64642)

Fax: 847-919-3862

info@mimictechnologies.com