CHUBB

GUIDE TO PREVENTING SOCIAL ENGINEERING FRAUD

GUIDE TO PREVENTING SOCIAL ENGINEERING FRAUD

CONTENTS

SOCIAL ENGINEERING FRAUD FUNDAMENTALS AND FRAUD STRATEGIES

In the context of information security, human-based social engineering fraud, otherwise known as "human hacking," is defined as the art of influencing people to disclose information and getting them to act inappropriately.

Some criminals consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system: they have learned how to trick their targets into giving them information by exploiting certain qualities in human nature. They use various forms of communication, such as email, the Internet, the telephone, and even face-to-face interactions, to perpetrate their scheme of defrauding and infiltrating companies.

Social engineering attacks can take many forms and can be human- or computer-based. However, security experts recognize that most scams follow a four-stage method:

- Information gathering,
- Relationship development,
- Exploitation and
- Execution.

This methodology, along with the tendency for humans to be the weakest link in the security chain, creates a vulnerability that can have a serious operational impact.

According to Check Point Software Technologies, nearly half of global businesses surveyed in 2011 reported being the victim of one or more social engineering attacks that resulted in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Because social engineering is such a real threat in today's workplace, it is essential that employees across an entire organization be educated and trained on how to detect and prevent this type of fraud. Companies also need to develop and implement specific policies (for example, training for employees on what constitutes confidential and sensitive information and

on how to keep it safe) to prevent and respond to an attack. Companies are advised not to focus their efforts and security budgets entirely on defending against technical attacks from hackers and other electronic threats, and thereby underestimating, or even entirely overlooking, the system weaknesses posed by the human element.

A plan for mitigating the effect of social engineering attacks should be a part of any comprehensive security policy. It should include a component for raising awareness among employees and educating those who are most vulnerable: new hires, help desk personnel, contractors, executive assistants, human resource personnel, senior managers and executives, as well as information technology (IT) employees who handle technical and physical security.

Social Engineering Fraud Strategies

Human hackers use many different social engineering strategies to gather information from their targets, including the tactics listed below.

- **Impersonation/pretexting:** This common form of deception may involve an attacker using a believable reason to impersonate a person in authority, a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.

- **Phishing/spamming/spearphishing:** Phishing can take the form of a phone call or email from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.

- **IVR/Phone phishing (aka vishing):** This technical tactic involves using an interactive voice response (IVR) system to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to "verify" confidential information.

- **Trash cover/forensic recovery:** Attackers collect information from discarded materials such as old computer equipment (e.g., hard drives, thumb drives, DVDs, CDs) and company documents that were not disposed of securely.

- **Quid pro quo ("give and take"):** An attacker makes random calls and offers his or her targets a gift or benefit in exchange for a specific action or piece of information with the goal of rendering some form of assistance so that the target will feel obligated in some way.

- **Baiting:** A common method of baiting involves leaving an innocent-looking, malware-infected device—such as a USB drive, CD or DVD—at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into his or her computer.

- **Tailgating/direct access:** Attackers gain unauthorized access to company premises by following closely behind an employee entering a facility or by presenting themselves as someone who has business with the company. The attacker may state that he or she left security credentials inside the facility or at home if challenged by an employee while entering the facility.

- **Diversion theft:** The methodology in this attack involves misdirecting a courier or transport company and arranging for a package or delivery to be taken to another location.

In addition, social engineers will focus their attention on locating vital data such as account numbers, phone and client contact lists, organizational charts, and other information on key employees who have access privileges and computer system details (on servers, networks, intranets, etc.) during their information-gathering phase. They have also been known to go after tangible property such as keys, access cards, and identity badges—especially in cases where their method of operation is through direct access.

THE PSYCHOLOGY OF SOCIAL ENGINEERING (AND A CASE STUDY)

What is the motivation behind a social engineering attack, and why is it so often effective?

A social engineering scheme can have any number of goals; however, more often than not, the objective is simply financial gain. Attackers have learned to leverage the human qualities of trust, helpfulness and fear to manipulate their targets. Through pretexting, they play on the inherent desire of most people to trust another individual, and they rely on company policies that foster employees to be helpful, especially those in service-oriented positions.

Social engineers are adept at exploiting these traits as they go about gathering their information. In addressing the trust issue, former hacker turned security consultant Kevin Mitnik explains in his book *The Art of Deception – Controlling the Human Element of Security*:

> *"Why are social engineering attacks so successful? It isn't because people are stupid or lack common sense. But we, as human beings, are all vulnerable to being deceived because people can misplace their trust if manipulated in certain ways. The social engineer anticipates suspicion and resistance, and he's always prepared to turn distrust into trust. A good social engineer plans his attack like a chess game, anticipating the questions his target might ask so he can be ready with the proper answers. One of his common techniques involves building a sense of trust on the part of his victim."*

Social engineers also exploit a person's natural tendency to avoid doing something wrong or getting in trouble. If an attacker can make an employee feel that he or she caused a problem or performed a task incorrectly, then the employee may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols. An employee may also be made to feel that he or she must "cut corners" in order to avoid a situation where a superior becomes angry with the employee for possibly doing something wrong.

Case Study

Perhaps the easiest way to illustrate a social engineering fraud exposure is through an example.

> *The controller of a private distributor of component parts was responsible for making regular payments to overseas vendors from which the company purchased product for resale in the United States. After many months of working with the vendor and receiving regular shipments, the controller received an email that appeared to come from his contact, indicating that the vendor's bank was having issues with accepting payments, and asked if the next payment could be made to a new bank. The vendor was located overseas, making verification a challenge. After some pressure was applied by the supposed vendor, the invoice was paid by wire transfer.*
>
> *The following month, when the real vendor realized that its best customer was late on its payment, an investigation determined that the vendor's email was hacked and an imposter had been socially engineering the company into believing that the change in bank information was authentic.*
>
> *In the end, almost $250,000 was handed over to the fraudster.*

COUNTERMEASURES FOR COMBATING SOCIAL ENGINEERING FRAUD

The best defense for combating social engineering fraud is awareness through corporate culture, education and training. It is not enough for a workforce to simply follow a policy guideline; employees must be educated on how to recognize and respond to an attacker's methods and thus become a "human firewall."

A proper countermeasure training program should include the following measures:

- Conduct a **data classification assessment**, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social engineering scheme are likely to be. Remember, all employees are at risk.
- **Never release confidential or sensitive information to someone you don't know** or who doesn't have a valid reason for having it—even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email.
- Establish procedures to **verify incoming checks and ensure clearance prior to transferring any money by wire.**
- Reduce the reliance on email for all financial transactions. If email must be used, **establish call-back procedures to clients and vendors** for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.
- Establish procedures to **verify any changes to customer or vendor details,** independent of the requester of the change.
- **Avoid using or exploring "rogue devices"** such as unauthenticated thumb/flash drives or software on a computer or network.
- **Be suspicious of unsolicited emails** and only open ones from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.

- **Avoid responding to any offers made over the phone or via email.** If it sounds too good to be true, then it probably is. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter.

- **Be cautious in situations where a party refuses to provide basic contact information**, attempts to rush a conversation (act now, think later), uses intimidating language or requests confidential information.

- Physical documents and other tangible material such as computer hardware and software should **always be shredded and/or destroyed prior to disposal** in any on-site receptacles, such as dumpsters.

- **Proactively combat information security complacency** in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalog incidents of social engineering and implementing an incident-response strategy.

- **Train customer service staff to recognize psychological methods that social engineers use:** power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it's important enough to verify.

- Consider **conducting a recurring, third-party penetration test** to assess your organization's vulnerabilities, including unannounced random calls or emails to employees soliciting information that should not be shared.

- **Guard against unauthorized physical access** by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone "tailgating." Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.

- **Monitor use of social media outlets, open sources and online commercial information** to prevent sensitive information from being posted on the Internet.

CONCLUSION

Due to the increasing prevalence of social engineering fraud schemes, it is reasonable to suggest that it may be only a matter of time until a social engineer targets an employee at your organization. Given the potential for loss, and the comparatively low cost of loss control measures, instituting a countermeasure program makes good business sense.

Chubb Group of Insurance Companies | www.chubb.com

14-01-1157 (Ed. 10/14)