The Psychology of Social Engineering

Contributor: Edna Wong, Marsh Canada

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 such as housing.

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:

"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."

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.

Countermeasure 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."

Here are some handy tips on what a proper countermeasure training program should include:

- Conduct a data classification assessment, identifying which employees have access to what types and levels of sensitive company information.
- 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.
- 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.
- 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.
- 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.
- Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.
- Monitor the use of social media outlets, open sources and online commercial information to prevent sensitive information from being posted on the Internet.

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 for your organization.

This information was provided by Chubb Group of Insurance Companies (www.chubb.com). BCNPHA Crime policy does not currently include Social Engineering coverage and does not contain Social Engineering Endorsement CE 14-02-21666. There is an additional premium for this extension and Chubb will consider the addition of this coverage at the next renewal.