Inspiratron.org - Natural language processing, machine learning and cybersecurity

Introduction to Social engineering

by Nikola Miloševi? - Thursday, May 23, 2013

https://inspiratron.org/blog/2013/05/23/introduction-to-social-engineering/

Social engineering is one of the main security issues these days. Most of companies invest to infrastructure to be hardly hackable, but they don't educate people. Social engineering is quite common attack since the begining of 1980'. And many big corporate networks were infiltrated using these attacks. And the only way to prevent them is to educate your employees. Every one of them. If you have one person that cannot say no on phonecall asking to reset or give some password, IP addresses ranges or anything else, your entire organization is at risk.

What is Social Engineering?

Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

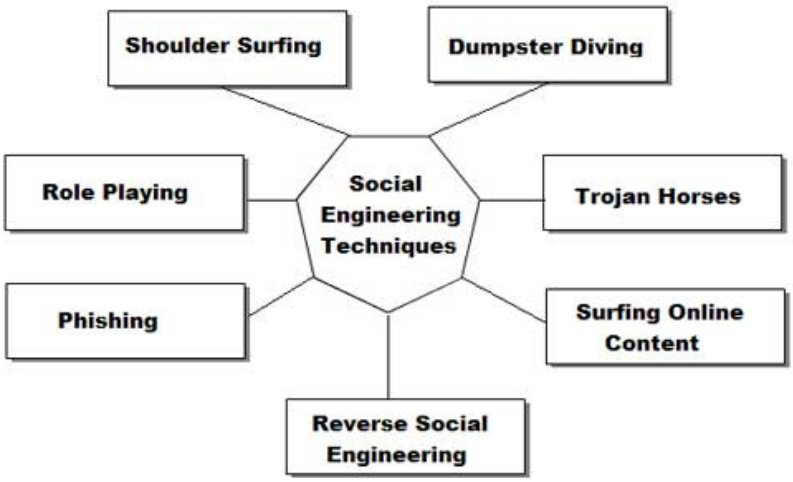
Social engineering, in the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or gaining computer system access. It differs from traditional cons in that often the attack is a mere step in a more complex fraud scheme.

"Social engineering" as an act of psychological manipulation had previously been associated with the social sciences, but its usage has caught on among computer and information security professionals.

[youtube=http://www.youtube.com/watch?v=yY-lMkeZVuY]

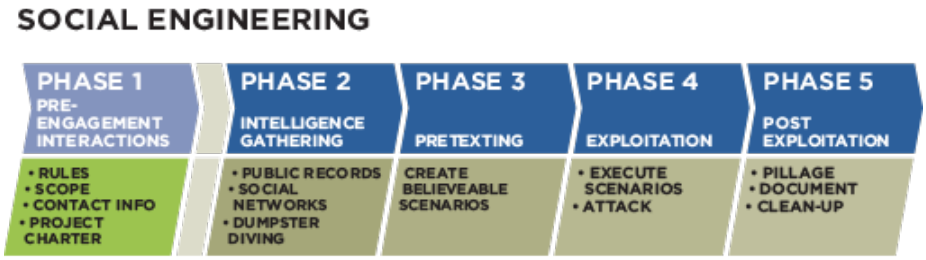
Well known attacks

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create attack techniques.

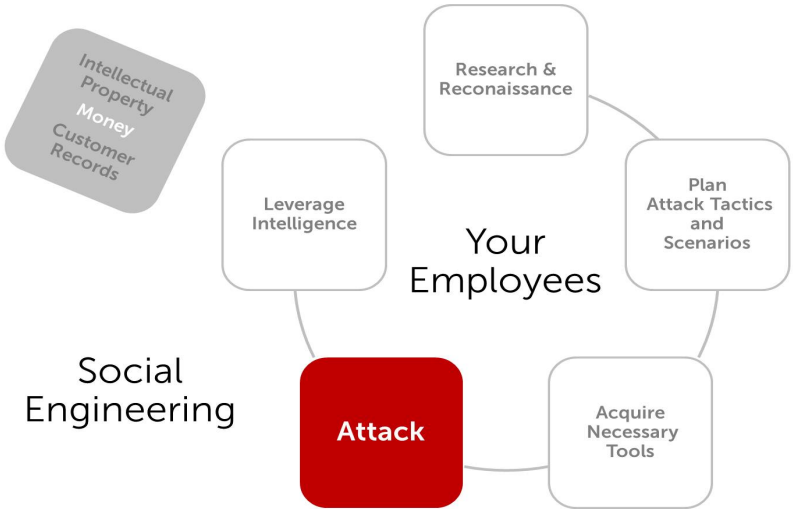


Pretexting

Pretexting (adj. **pretextual**), also known in the UK as *blagging* or *bohoing*, is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target.



This technique can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives. The information can then be used to establish even greater legitimacy under tougher questioning with a manager, *e.g.*, to make account changes, get specific balances, etc.



Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to

questions that might be asked by the victim. All that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario. There are also other techniques to get from people what attacker wants. One way is to be likable. People are used to do a favor for people they like, so all is needed is use charm, give a few compliments and ask to do what is needed. Other way is better described better in part called Quid pro quo.

Diversion theft

Diversion theft, also known as the "Corner Game" or "Round the Corner Game", originated in the East End of London.

In summary, diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for a legitimate delivery that the consignment is requested elsewhere — hence, "round the corner".

Phishing

Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN.

For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless a link provided was clicked to update a credit card (information that the genuine eBay already had). Because it is relatively simple to make a Web site resemble a legitimate organization's site by mimicking the HTML code, the scam counted on people being tricked into thinking they were being contacted by eBay and subsequently, were going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who already had listed credit card numbers with eBay legitimately, who might respond.

Smishing is term used for phishing in mobile communication. Actually this is phishing over the SMS messages.

IVR or phone phishing

Phone phishing (or "vishing") uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" information. A typical system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker posing as a customer service agent for further questioning.

Baiting

Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim.

In this attack, the attacker leaves a malware infected floppy disk, CD-ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate looking and curiosity-piquing label, and simply waits for the victim to use the device.

For example, an attacker might create a disk featuring a corporate logo, readily available from the target's web site, and write "Executive Salary Summary Q2 2012" on the front. The attacker would then leave the disk on the floor of an elevator or somewhere in the lobby of the targeted company. An unknowing employee might find it and subsequently insert the disk into a computer to satisfy their curiosity, or a good samaritan might find it and turn it in to the company.

In either case, as a consequence of merely inserting the disk into a computer to see the contents, the user would unknowingly install malware on it, likely giving an attacker unfettered access to the victim's PC and, perhaps, the targeted company's internal computer network.

Unless computer controls block the infection, PCs set to "auto-run" inserted media may be compromised as soon as a rogue disk is inserted.

Hostile devices, more attractive than simple memory, can also be used. For instance, a "lucky winner" is sent a free digital audio player that actually compromises any computer it is plugged to.

Dumpster diving

Dumpster diving is the practice of sifting through commercial or residential waste to find items that have been discarded by their owners, but that may prove useful to the dumpster diver. Dumpster diving is also viewed as an effective urban foraging technique Dumpster divers will forage dumpsters for items such as clothing, furniture, food, and similar items in good working condition. Companies usually dump staff that

can be used by attacker, like some documents that are expired or not used, lists of employees, with some personal information, lists of former employees. All this things can be then of great use for creating pretexting scenarios and information gathering.

Quid pro quo

Quid pro quo means *something for something*:

- An attacker calls random numbers at a company, claiming to be calling back from technical support. Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware.
- In a 2003 information security survey, 90% of office workers gave researchers what they claimed was their password in answer to a survey question in exchange for a cheap pen. Similar surveys in later years obtained similar results using chocolates and other cheap lures, although they made no attempt to validate the passwords.

Tailgating

An attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker. The legitimate person may fail to ask for identification for any of several reasons, or may accept an assertion that the attacker has forgotten or lost the appropriate identity token. The attacker may also fake the action of presenting an identity token.

Shoulder surfing

Shoulder surfing is technique when attacker gets close to victim. Then attacker askes victim to log in some secret area of interest and watchs victim over the shoulder. By watching attacker tries to figure out user names, passwords, credit card numbers and other sensitive information.

Other types

Common confidence tricksters or fraudsters also could be considered "social engineers" in the wider sense, in that they deliberately deceive and manipulate people, exploiting human weaknesses to obtain personal benefit. They may, for example, use social engineering techniques as part of an IT fraud.

A very recent type of social engineering technique includes spoofing or cracking IDs of people having popular e-mail IDs such as Yahoo!, GMail, Hotmail, etc. Among the many motivations for deception are:

- Phishing credit-card account numbers and their passwords.
- Cracking private e-mails and chat histories, and manipulating them by using common editing techniques before using them to extort money and creating distrust among individuals.
- Cracking websites of companies or organizations and destroying their reputation.
- Computer virus hoaxes

Protection

Social engineering attacks uses peoples' vulnerability and peoples' lack of information. Establishing security procedures and training employees can quite well reduce company risk of being victim of social engineering attack. Some of the best practeses are:

- Establishing frameworks of trust on an employee/personnel level (i.e., specify and train personnel when/where/why/how sensitive information should be handled)
- Identifying which information is sensitive and evaluating its exposure to social engineering and breakdowns in security systems (building, computer system, etc.)
- Establishing security protocols, policies, and procedures for handling sensitive information.
- Performing unannounced, periodic tests of the security framework
- Reviewing the above steps regularly: no solutions to information integrity are perfect
- Using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff.
