Social Engineering

What is Social Engineering?

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim. Social engineering is the seemingly insidious practice of obtaining confidential information by manipulating legitimate users. A talented social engineer will often use the telephone or Internet to trick people into revealing sensitive information - such as a password or credit card number - or get them to do something that's normally against policy. And just like that, a savvy hacker can punch right through sophisticated, technical defenses.

Social engineering techniques and terms

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases (A cognitive bias is a pattern of deviation in judgment that occurs in particular situations). These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create attack techniques, some of which are listed here:

Pretexting

Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is typically done over the telephone. It's more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target.

This technique is often used to trick a business into disclosing customer information, and is used by private investigators to obtain telephone records, utility records, banking records and other information directly from junior 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).

As most U.S. companies still authenticate a client by asking only for a Social Security Number, date of birth, or mother's maiden name, the method is effective in many situations and will likely continue to be a security problem in the future.

Pretexting can also be used to impersonate co-workers, police, bank, tax authorities or insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the target. The pretexter must simply prepare answers to questions that might be asked by the target. In some cases all that is needed is a voice of the right gender, an earnest tone and an ability to think on one's feet.

Voice over IP programs are starting to become a standard in pretexting, as it is harder to track an IP address than a phone number, making the pretexter less vulnerable to capture.

Phishing

Phishing is a technique of fraudulently obtaining private information. Typically, the Phisher sends an email 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 done. The letter usually contains a link to a fraudulent web page that looks 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 he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently 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 actually had listed credit card numbers with eBay legitimately.

As another example, you might receive an e-mail message that appears to come from your bank or other financial institution that asks you to update your account information. Internally, at a company or a governmental agency, the email message may appear as if it came from the Help Desk or another individual within your organization who typically handles questions. The e-mail message may ask for logins and passwords or other personal information and provide a link that appears to go to a legitimate Web site, but really takes you to a spoofed or fake Web site. If you enter your login, password, or other sensitive information, a criminal could use it to gain access to company or personal information. This is one way that identity theft occurs. Phishing e-mail messages often include misspellings, poor use of grammar, threats, and exaggerations.

Spear Phishing

Spear Phishing is any highly-targeted e-mail or telephone scam; but they usually are employed in a business environment. Spear Phishers send e-mail messages or make calls that appears genuine to all the employees or members within a certain company, government agency, organization, or group. The message might look like it comes from your company, agency or from a colleague who might send an e-mail message to everyone in the company, such as the head of a department. It might include requests for user names or passwords or might contain malicious software, like a Trojan or a Virus.

IVR/phone Phishing

This technique 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 email) to call in to the "bank" via a provided (ideally toll free) number and verify information. A typical system will continually reject logins ensuring the victim enters PINs or passwords multiple times, often revealing several different passwords. More advanced systems will even transfer the victim to the attacker posing as a customer service agent for further questioning.

Someone could even record the typical commands ("Press one to change your password, press two to speak to customer services" ...) and play them back manually in real time, giving the appearance of being an IVR without the expense.

Trojan Horse

The Trojan Horse takes advantage of the victims' curiosity or greed to deliver Malware. An example of a Trojan Horse might be the "email Virus" which arrives as an email attachment promising anything from a "cool" or "sexy" screen saver, an important anti-Virus or system upgrade, or even the latest gossip about an employee. Victims succumb by opening the attachment which would then activate. Since naive users might unthinkingly click on an attachment without considering legitimacy, the technique can be quite effective and a number (for example the "I love you Virus") even made international news as a result.

Similarly, a program which grants the attacker access by hiding inside other software (spyware being an example) or by pretending to be something it is not (for example a download pretending to be a "free" copy of a new software title) behaves much like the famous Horse of Troy and allows an "insider attack".

Road apple

A road apple is a real-world variation of a Trojan Horse that uses physical media and relies on the curiosity of the victim. The name is taken from a euphemism for Horse manure.

In a road apple attack, the attacker leaves a Malware infected floppy disc, 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 example, an attacker might create a disk featuring a corporate logo, readily available off the target's web site, and write "Executive Salary Summary Q1 2008" on the front. The attacker would then leave the disk on the floor of an elevator or somewhere in the lobby of the target 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 to see the contents, the user would unknowingly install Malware on their computer, likely giving an attacker unfettered access to the victim's PC and perhaps the target company's internal computer network.

Unless other controls block the infection, PCs set to "autorun" inserted media may be compromised as soon as a rogue disk is inserted.

Quid pro quo - Something for something

An attacker calls random numbers at a company claiming to be calling back from technical support. Eventually they 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 and/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. Some respondents likely made up false passwords on the spot just to claim the prize, thereby socially-engineering the surveyors.

Other types

Even if they lack cracking skills, common confidence tricksters or fraudsters could also 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. The latest type of Social Engineering techniques includes spoofing or hacking ids of people having popular email IDs like Yahoo, Gmail, hotmail, etc. Here the reason for the hacks may be multifold, some of them are:

1. Phishing the credit card accounts numbers and their passwords and laundering money to the tunes of millions.
2. Hacking private emails, Chat histories and manipulating them by using common editing techniques and using them to extort money and creating distrust among individuals.
3. Hacking Websites of organizations and destroying their reputation.
4. Creating disharmony in the Society. Organizations spend a great fortune of their money in securing their websites by using state of the firewalls and upgrading the infrastructure but hackers still find a way to break through their defenses. Hence one should be cautious while transacting over the net, it could be either carrying out monetary transactions, sending mails or downloading freebies everything could be spoofed and hacked and you will end up having no clue of the person behind it.

The information above was taken from Wikipedia's Open Information Database.

Protecting yourself from Social Engineering

Do not reveal any personal information in e-mail, online or on the telephone unless you know who you are dealing with and why. Additionally, make sure you are in a secure environment: that's the key to help you avoid any type of attack.

We can fight Social Engineering by following some common-sense guidelines:

1. Don't ever give your passwords away to anyone.
2. Don't reuse your passwords when going online for business or personal matters. Use different passwords and rotate your personal passwords so they are not the same as your business passwords.
3. Don't have confidential conversations in public settings.
4. Shred sensitive information before throwing it in the recycle bin. **Shredded material is recycled.**
5. If you find CD's or Thumb Drives, do not place them into your computer to see what is on them - Turn them into your security group.
6. Show caution when opening email attachments.
7. Don't respond to or forward unsolicited email advertisements, chain letters, and hoaxes.
8. Password-protect your personal email account.
9. Log out of sensitive programs when you walk away from your computer.
10. You can also be Phished in real-time by strangers visiting a company, standing by a side entrance of a building, hanging out in a public space like coffee shop. Avoid talking about confidential business in public.
11. If you receive telephone calls looking for someone or asking for company or personal information about you or other employees, be very cautious. Unless you can confirm their identity, be safe and don't share the information.