Social Engineering

Introduction and Techniques

Definitions

- “the art and science of getting people to comply to your wishes” (Bernz 2)
- “an outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system” (Palumbo)
- “getting needed information (for example, a password) from a person rather than breaking into a system” (Berg)

Definitions (contd)

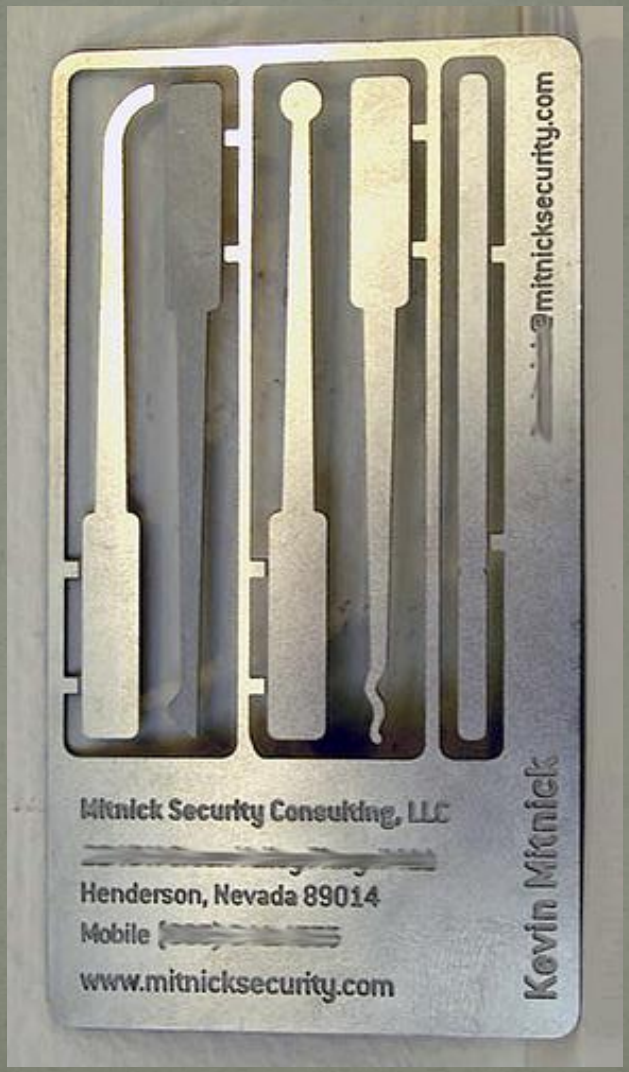
- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information.

Kevin Mitnick

- At age 12 started with petty crimes
- Used the Los Angeles bus transfer system to get free rides by abusing the punchcard system
- Later on the crimes escalated in terms of how much damage they did.

Kevin Mitnick

- Became well known as a phone phreaker
- Arrested again in February 1995 on federal offences related to a 2½-year computer hacking spree
- Law enforcement convinced: “start a nuclear war by whistling into a pay phone”



Social Engineering Techniques

- Pretexting
- Phishing
- Phone phishing
- Baiting
- Quid pro quo

Pretexting

- The art of creating and using an invented scenario to persuade a targeted victim to release information or perform an action
- These type of attacks are mostly done over the phone
- In order to perform these attacks you need to do prior research to create a realistic invented scenario
- This technique is often used in order to gain sensitive information from companies without their knowledge that you have gained it

Phishing

- A technique of fraudulently obtaining private information
- Phishing is mostly done by the use of e-mails
- Has other forms as well like telemarketers who manipulate people into buying fraudulent items
- 409 scams are prime examples of phishing

Phone phishing

- This technique is often used in conjunction with phishing
- It involves using an Interactive voice response (IVR) system.
- An (IVR) is a system which can be dialled into and provides automated response
- Examples of legitimate versions of these systems can be found in most call centres
- This technique is used in order to create a more realistic scenario to fool targets to fall for phishing scams

Baiting

- Baiting is leaving physical media in visible view of victim and then relies on the curiosity or greed of the victim
- Malware could be left on USB flash drives in the hopes that an unsuspecting victim would try to see what is on the flash drive
- This is very effective, cause it is in the nature of people to be curious

Quid pro quo

- The something for something technique
- An attacker would call random numbers inside a company in the hopes that someone has a problem with their system
- The attacker would offer assistance with a problem and if the problem exists the victim would greatly appreciate this help
- The attacker provide help to the victim, but also install some form of malware during the helping process

Social Compliance

Figure 8.10

Compliance: Getting Others to Say Yes

We all use—and are exposed to—many different techniques for gaining compliance—for getting others to do what we would like them to do. The one shown here is unusual, but suggests just how varied approaches for gaining compliance can be.

(*Source:* United Feature Syndicate, 12/15/98.)

Social Compliance Principles

- *Friendship or liking:* In general we are more willing to comply with requests from friends or from people we like than with requests from strangers or people we don't like
- *Commitment or consistency:* Once we have committed ourselves to a position or action, we are more willing to comply with requests for behaviours that are consistent with this position or action than with requests that are inconsistent with it

Social Compliance Principles (contd)

- *Scarcity:* In general, we value and try to secure outcomes or objects that are scarce or decreasing in availability. As a result, we are more likely to comply with requests that focus on scarcity than ones that make no reference to this issue
- *Reciprocity:* We are generally more willing to comply with a request from someone who has previously provided a favour or concession to us than to someone who has not. In other words, we feel obliged to pay people back in some way for what they have done for us

Social Compliance Principles (contd)

- *Social validation:* We are generally more willing to comply with a request for some action if this action is consistent with what we believe people similar to ourselves are doing (or thinking). We want to be correct, and one way to do this is to act and think like others.
- *Authority:* In general, we are more willing to comply with requests from someone who holds a legitimate authority—or simply appears to do so

Tactics Based on Friendship or Liking

- *Incidental similarity:* Calling attention to small and slightly surprising similarities between them and us
- The more similar you are, or at least seem to be, the more compliant they will be towards your requests

Tactics Based on Commitment or Consistency

- *Foot-in-the-door technique:* A procedure for gaining compliance in which requesters begin with a small request and then, when this is granted, escalate to a larger one (the one they actually desired all along)
- *Lowball procedure:* A technique for gaining compliance in which an offer or deal is changed to make it less attractive to the target person after this person has accepted it

Tactics Based on Reciprocity

- *Door-in-the-face technique:* A procedure for gaining compliance in which requesters begin with a large request and then, when this is refused, retreat to a smaller one (the one they actually desired all along)
- *That's-not-all technique:* A technique for gaining compliance in which requesters offer additional benefits to target people before they have decided whether to comply with or reject specific request

Tactics Based on Scarcity

- *Playing hard to get:* A technique that can be used for increasing compliance by suggesting that a person or object is scarce and hard to obtain
- *Deadline technique:* A technique for increasing compliance in which target people are told that they have only a limited time to take advantage of some offer or to obtain some item

Symbolic Social Influence

- People can influence you without them meaning it or even being present in the scenario
- If we are thinking of a friend whom we would help it is much easier for us to decide to help a stranger than it would be if we were thinking of someone that we would not help
- We are often influenced by others even when they are not attempting to exert such effects

References

- Berg, Al: “Al Berg Cracking a Social Engineer,” by, LAN Times Nov. 6, 1995. http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html
- Bernz 2: “The complete Social Engineering FAQ!” http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt
- Palumbo, John “Social Engineering: What is it, why is so little said about it and what can be done?”, SANS Institute, July 26, 2000 http://www.sans.org/infosecFAQ/social/social.htm
- R. A. Baron, N. R. Branscombe, D. Byrne. *Social Psychology 12th Edition,* Pearson Internal Edition