MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

IVAN FRANKO NATIONAL UNIVERSITY OF LVIV

Department

of Foreign Languages

for Sciences

SUMMARY

“Social Engineering: The Art of Human Hacking 1st edition”

Christopher Hadnagy

2010

By Nazar Yuras

2nd Year Student of

Applied Mathematics and Informatics

Lviv-2021

This semester I have read the next three chapters of the book “Social Engineering: The Art of Human Hacking 1st edition” by Christopher Hadnagy to improve my knowledge about social engineering.

In short, Social Engineering is a way to gain influence over others without them knowing. Social engineering is a set of psychological tricks that exploit human vulnerabilities to influence a target’s actions. These tricks can manifest themselves as spoken language, body language and hidden suggestions.

Social engineers combine rapports, neurolinguistics programming, physical and mental tools, etc to manipulate their targets without them ever being the wiser. The best way to protect ourselves is to know their methods and how they work.

These are sophisticated psychological methods that require training and practice.

Remember, any and all information can be valuable to an attacker. So be careful what you share with strangers.

If you don’t want to get duped, it’s important to educate yourself about social engineering tactics. The more you know about elicitation, body language and so on, the better equipped you will be to recognize when someone is trying to use these tactics on you.

What about reciprocation? Reciprocity is the inherent expectation that when others treat you well you respond in kind. The rule of reciprocity is important because often the returned favor is done unconsciously. Knowing this means that you now have a step up on how you can use it as a social engineer.

**A few words about scarcity: scarcity is often used in social engineering contexts to create a feeling of urgency in a decision-making context. This urgency can often lead to manipulation of the decision-making process, allowing the social engineer to control the information provided to the victim. This is done commonly by using a mixture of authority and scarcity principles.**

**No less important is the awareness of the value of information. Before giving out information to someone, determine whether the person who is calling or interacting with you deserves it.**

**A social engineer often uses charm to start a conversation about the weather, work, the product, anything at all, and uses it to reveal the information sought. This is where a good security awareness policy comes into play— your educating about what tactics might be used against them can save them from acting out of fear.**

**The last read by me chapter was about prevention and mitigation. Prevention is the action taken to decrease the likelihood that an event will occur. Author of this book said, that the first stage in social engineering prevention and mitigation is to learn about the attacks.**

**To sum up, I want to say, that like a computer, the human mind can be hacked. Criminals use psychological tactics, contrived cover stories and careful wording to manipulate and scam their targets. The best protection is to be aware of their methods.**

**Undoubtedly, this book should be read by anyone who does not want to fall victim to social engineers. Everything is in your hands!**