



Social Engineering

Nathan O'Neal

UAH Information Security Club

March 21, 2013

Disclaimer

This presentation is not intended
to be used to learn how to
manipulate individuals with the
intentions of seeking personal
gain



Social Engineering: Overview

- What is Social Engineering
- Types of Social Engineering Attacks
- Social Engineering Framework
- Tools of the Trade
- Prevention and Mitigation



Social Engineering

What is Social Engineering

Nathan O'Neal



What is Social Engineering

- Social Engineering is nothing new
- Definitions
 - Social
 - Engineering
 - Social Engineering
- Used in every day life



Social Engineering

Types of Social Engineering Attacks



Types of Social Engineering Attacks

- Computer Based
 - Phishing / Spear Phishing
 - Email Attachments
 - Fake Websites / Pop-up Windows
- Human Based
 - Shoulder Surfing
 - Impersonation / Third Party Attacks
 - Insider Attacks



Social Engineering

Social Engineering Framework

Nathan O'Neal



Social Engineering Framework Overview

- Information Gathering
- Elicitation
- The Pretext
- Target Manipulation



Social Engineering

Information Gathering

Nathan O'Neal



Information Gathering

- Profiling the Target
 - Who or what are we targeting
- Understand the Organization
 - What does the organization do
- Know Who the Key Individuals Are
 - Management
 - Human Resources
 - IT / Technical Employees



Information Gathering

- Common Sources
 - Google; LinkedIn; Facebook; Twitter
 - Personal websites, blogs and videos
- Traditional Sources
 - Corporate websites; Publicly accessible servers
 - Public data / reports from third party sources
- Non-traditional Sources
 - Outside interactions with employees
 - Third party experts



Social Engineering

Elicitation

Nathan O'Neal



Elicitation

- Definition
 - Elicit
- Why Elicitation Works So Well
 - Play off the desire to be polite
 - Most respond politely to a show of concern
 - Maintain their ego
- The Goal of Elicitation



Elicitation

- Master the Art of Communication
 - Educate yourself on the subject
 - Be natural
 - Don't be greedy
- Preloading
 - Influence a target on how to react to certain information



Social Engineering

The Pretext

Nathan O'Neal



The Pretext

- Definition
 - Pretext
- Importance of Pretexting
- Basic Principles
- You WILL Be Confronted
- Know When to Walk Away



Social Engineering

Target Manipulation

Nathan O'Neal



Target Manipulation

- Modes of Thinking
 - The senses
 - Dominate sense
 - Importance of understanding the mode
- Eye Cues
 - Easiest to see, hardest to identify
 - While you are watching them, they are watching you



Target Manipulation

- Facial Expressions
 - Universal expressions
 - Involuntary muscle movements
 - Linked to an emotion
- Create an Emotional Response
- Identify Contradictions
- Change in Behavior



Target Manipulation

- Human Buffer Overflow
 - The mind runs “software”
 - Similar to a buffer overflow in a program
 - Inject commands to manipulate the process of thought in a certain direction



Target Manipulation

Green Yellow Black Blue

Purple Red Orange Green

Black Orange Yellow Purple



Target Manipulation

- Human Buffer Overflow
 - Why was the exercise difficult
 - What does this show
 - Most decisions are made with more than just what you hear



Target Manipulation

- Building an Instant Rapport
 - Starts with listening
- Develop a Relationship with the Target
 - Develop a common ground
 - Mirror speech and behavior
- Rapport Can be Destroyed Instantly
- Closing the Target



Target Manipulation

- Influencing the Target
 - Reciprocation
 - Obligation
 - Concession
 - Scarcity
 - Social Proof



Social Engineering

Tools of the Trade

Nathan O'Neal



Tools of the Trade

- Physical Tools
 - Lock picks
 - Cameras and recording devices
 - GPS
- Computer Based Tools
 - Maltego
 - Social Engineer Toolkit
 - Common User Passwords Profiler



Social Engineering

Prevention and Mitigation

Nathan O'Neal



Prevention and Mitigation

- Learn to Identify Social Engineering Attacks
- Outline the importance of the Type of Information Sought by Social Engineers
 - Enforcement of existing policies
 - Clean desk policies
- Keep Software Updated
- Security Through Education



Social Engineering

Summary and Conclusions

Nathan O'Neal



Summary and Conclusions

- Social Engineering is not Always Negative
- Information Is Key
- Your Pretext Makes You Believable
- Influence and Manipulation
- Made Aware of Malicious Tactics



Social Engineering

Questions and Comments

Nathan O'Neal



Social Engineering

References

Nathan O'Neal



References

- C. Hadnagy, Social Engineering: The Art of Human Hacking, C. Long, Ed., Indianapolis, Indiana: Wiley Publishing, 2011
- C. Hadnagy. "Social Engineering: Security Through Education," 2013 [Online]. Available: <http://www.social-engineer.org/>. [Accessed March 2013]
- A. Crenshaw, "Irongeek.com," 2013. [Online]. Available: <http://www.irongeek.com/>. [Accessed March 2013]
- Paterva, "Paterva / Maltego," [Online]. Available: <http://www.paterva.com/web6/>. [Accessed March 2013]



License

This content is available under the Creative
Commons Attribution
NonCommercialShareAlike 3.0 United States
License

