Hacking Humans: The Only Way to Fly!

Wednesday, May 17, 2017, 4:15pm

M100G-H
Identity Paradox

Who am I?

• How do you know?
• How do I prove it to you?

Without compromising my privacy?
Ron Woerner

• InfoSec Architect, Carlson Rezidor Hotel Group
• Professor Cybersecurity Studies, Bellevue University
• >25 years corporate IT, 15+ Security
• CISSP, CISM, & Certified Ethical Hacker
• Twitter: @ ronw123
• These are my thoughts based on my studies and experiences.
• Normal caveats apply.
• Comments & questions are welcome any time.
• There’s a test and homework.
What the $%$# are we doing here?
Goals

• Show you how easy unfluence is
• Give you cr@p to think about & do
• Help you be a better security professional

• Have fun during the last session
The first principle is that you must not fool yourself and you are the easiest person to fool.

Richard P. Feynman
IT IS HARD WALKIN' ON THIS STUFF.

YEP, SON, WE HAVE MET THE ENEMY AND HE IS US.

CYBERSPACE
Why we ‘do’ security

Mind
Knowing

Heart
Telling

Soul
Feeling

Unfluence / Human Hacking

Tweet along: #Sec360
Ron Woerner – Hacking Humans
www.Secure360.org
People are human

They can’t help it.
Mindlessness
What it’s all about

People

Ron Woerner – Hacking Humans
www.Secure360.org
Influencing in a negative way

Un-fluence

Social Engineering

“The art and science of skillfully maneuvering humans to take an action that may or may not be in their own best interests.”

(Chris Hadnagy, Social Engineering, The Art of Human Hacking)
Social Engineering

Preys on qualities of human nature:
- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble
- Acting without thinking

Technology is only a tool for manipulation
The Power of Observation

Tweet along: #Sec360

Ron Woerner – Hacking Humans
www.Secure360.org
Influence & Human Behavior
Unfluence Techniques

Reciprocation
Commitment & consistency
Social Proof
Liking
Authority
Scarcity
Unfluence Techniques

- Pre-texting
- Elicitation
- Framing
Pretexting

Creating a scenario that persuades a person to provide information, access or to perform a specific action.
Pretext Planning

• Research the topic/area thoroughly
• Gain personal interests in the topic/area
• Practice new dialects or expressions
• The phone can be an effective tool
  • Create Office noise: http://www.thrivingoffice.com
  • Spoof your caller ID: www.spoofcard.com
• Keep your pretext simple
• Your efforts should appear spontaneous
• Provide the target with a logical conclusion or follow through

Tweet along: #Sec360

Ron Woerner – Hacking Humans
www.Secure360.org
Pretexting Tools of the Trade
Pretexting examples

• Stanley Mark Rifkin
  • Credited with the largest bank heist in American history

• Hewlett-Packard
  • Patricia Dunn hired a team of security specialists who hired a team of private investigators. Criminal charges were brought against Dunn and the consultants she hired.
Keeping yourself out of trouble

The FTC states that it is illegal for anyone to:

- Obtain false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit lost or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else’s customer information using false, fictitious or fraudulent statement or using false, fictitious or fraudulent documents, or forged, counterfeit, lost or stolen documents.
Framing

• Altering the way we perceive and react to the world

• If a baseball and a bat cost $1.10 together, and the bat costs $1.00 more than the ball, how much does the ball cost?
Diversion – A Manipulation Technique

- Having a cover story when caught can go a long way in a target granting access

- Diverting the target’s attention away from the problem can redirect his concern

Tweet along: #Sec360

Ron Woerner – Hacking Humans
www.Secure360.org
The Rules of Embedded Commands

Embedded commands work well if they are:

- Short – 3 to 4 words
- A slight emphasis is needed. Example: Act now!
- Hide them within a normal sentence
- Facial and body language support the commands
The Rules of Embedded commands

Good examples are:

“Buy Now!”
“Follow me!”

Exploit writers use padding, or extra characters which do not interrupt the execution but give room for the malicious code:

Examples are:

“A person can……”
“How do you feel when…..”

The statements invoke an emotion or thought which allows an injection of code into the subconscious.
Embedded Commands Cont.

**Use quotes or stories:**
The unconscious mind processes stories as direct instructions. Quoting is a line adding power or weight.

**Use negation:**
Similar to reverse psychology
Telling a person that something is not important or relevant make the unconscious mind pay extra attention to the command, even if it not warranted. The mind will make a decision if it is important or not.
Embedded Commands Cont.

*Make the listener use their imagination:*

Use phrases that make the listen think like: “What happens if....”

The listener’s unconscious mind processes the statement directly without context.

Example of telling someone: “Do not imagine a red cow”

The human subconscious imagines a red cow first to tell yourself to not to think about it.

Caution: Overemphasis of tones and words may turn off your subject.
The Human Buffer Overflow

• Software hackers are looking for memory space they can use to inject commands
• Overwhelm a program to reach its limits and crash
• Humans have preprogrammed responses to certain scenarios it
• Once we hit our limits, we stall and stutter but not crash

Try the exercise on the next slide
Try and read the **color** of the word, not what the word **spells**..
Elicitation

SE obtains information, then uses it to motivate the target the SE wants to occur.

Use info to motivate the target the SE wants to occur.

Target takes an action
Why Elicitation Works

- Desire to be polite
- Reaction to being praised
- Ego
- Trustworthiness
Elicitation Main Steps

Be Natural

Establish Trust

Educate Yourself

Appeal to target’s ego
Tools of the Trade

Google
SEToolkit
Cree.py
Metasploit
TheHarvester
Evil
Our Twisted Minds
Elicitation Techniques

• Mutual interest
• Simple flattery (Ego)
• Quid pro quo (volunteer information)
• Exploit the instinct to complain
• Naïve mentality
• Purposefully erroneous statement
• Silence
• Alcohol
Six Ways to Make People Like You

1. Become genuinely interested in other people
2. Relax and smile
3. Remember and use other people’s names
4. Listen – concentrate on actively listening
5. Talk in terms of the other person’s interests
6. Make the other person feel important
Building Rapport

• Establish trust
• Be Genuine about Wanting to get to know People
• Take Care with your Appearance
• Be Aware of how you affect people
• Develop your Curious Side

» Be a good listener
» Keep the Conversation off Yourself
» Remember That Empathy is key to Rapport
» Be Well Rounded in your General Knowledge
» Find Ways to Meet People’s Needs

Tweet along: #Sec360
Other Rapport - Building Techniques

• Breathing at the Same Rate as your Target
• Matching your Target’s Vocal Tone and Speech Pattern
• Matching Your Target’s Body Language
Cressey’s Fraud Triangle

ACCESS

INTENT

FRAUD

KNOWLEDGE
What do we do???

• Universal Participation
• Training and Awareness
• Ask for help
• If you see something, say something
• …
Who Owns the Headache?

Tweet along: #Sec360

Ron Woerner – Hacking Humans
www.Secure360.org
Homework

• Social Engineer . org - http://www.social-engineer.org/
• Business Balls - http://www.businessballs.com/
• Johnny Long – Defcon 15, No Tech hacking, https://www.youtube.com/watch?v=5CWrzVJYLWw

Tweet along: #Sec360
Practice:

Get out of your chair
What it’s all about

People
Seek first to understand – then to be understood.  - Dr. Stephen Covey

People don’t care how much you know until they know how much you care.  - Dr. John Maxwell

You’ll have more fun & success helping other people achieve their goals than you will trying to reach your own goals first.  - Dale Carnegie
Ron Woerner, CISSP, CISM

@ ronw123
ronw2007 (at) gmail.com

I HAVE NO SPECIAL TALENTS. I AM ONLY PASSIONATELY CURIOUS.

-ALBERT EINSTEIN