



| Social Engineering

Nathan Sportsman

Founder and Chief Executive Officer

Agenda

❖ Strategy

- Know Thy Self
- Know Thy Enemy

❖ Tactics

- Remote Attacks
- Onsite Attacks

❖ Case Studies

- Case Study I
- Case Study II

“All men can see these tactics whereby I conquer, but what none can see is the strategy out of which victory is evolved.”

STRATEGY

Know Thy Self

- ❖ Social engineering is the exploitation of human behavior and trust
- ❖ Techniques can be learned quickly, but success depends on more than methodology
- ❖ Self confidence, quick thinking, and cool headedness are harder to master
- ❖ Practice, practice, practice

Confidence

❖ Eye contact

- Looking away or down is a sign of lying or nervousness
- As the other person speaks, look them in the eye
- When speaking, long eye contact is unnatural
- Break away and reestablish eye contact as you talk

❖ Body language and presentation

- Body languages speaks more than words
- Be mindful of posture and don't forget to smile!

Confidence

❖ Speaking

- Slowly and clearly, do not mumble
- Watch for stuttering or shakiness in voice

❖ When challenged

- Remain calm and don't panic
- Have backup responses ready

“You must believe in yourself!”

Friendliness

- ❖ Being friendly and polite yields the best results
 - Performing favors and being complimentary generates trust
- ❖ Acting lost and pretending ignorance is also effective
- ❖ Using rank, threats, frustration, or any other coercive means is least effective

Patience

❖ Establish relationships

- Do not ask for large requests upfront
- Ask for small, innocuous favors at first
- Build a relationship and sense of cooperation
- Gradually lead into the end objective

❖ Build a network

- Obtain small pieces of information from different people
- Use the theory of "social proof" to turn a single victim into multiple victims
- Use information learned to obtain new information

“Opportunities multiply as they are seized.”

In The Moment

- ❖ Skilled deception requires "playing a role"
- ❖ Same skills as successful acting
 - Speak loud and slow
 - Appear effortless
 - Believe your own deception

In The Moment

- ❖ Have a back story
 - Don't tell it to the victim, tell it to yourself
- ❖ Maintain emotional integrity
- ❖ *"In the end, it can't look like acting."*

Work In Tandem

- ❖ Working in pairs or threes has several advantages over working alone
- ❖ Mutual validation
 - A lone person who is unrecognized by staff can draw suspicion
 - Two people unrecognized to the group, but recognized to one another, causes assumptions
 - Three also works well with one person leading and two people behind conversing, paints a much more natural scene

Work In Tandem

❖ Designated lookout

- Working in teams allows a lookout to be assigned
- One can watch for potential issues, while the other performs the task

❖ Collaboration

- Teams can play off of one another during a social engineering effort

Use What You Have

- ❖ Use humor, attractiveness, or any other physical and personality strengths you may have
 - Halo effect
- ❖ Different scenarios can be used depending on the social engineers gender
 - Returning from or on maternity leave
- ❖ Targeting opposite gender from that of the social engineer is often easier

Know Thy Enemy

- ❖ Obtain as much knowledge about the target organization prior to the engagement
 - The more research you do the more successful you will be
- ❖ A wealth of information can be obtained online
- ❖ Preliminary information can also be obtained from the employees

Company Website

- ❖ Obvious method of targeted information gathering
 - Company background
 - Executive names and biographies
 - Generic emails such as sales, careers, info
 - Obtain employee names from request / response
 - Company addresses & phone numbers
 - Open job requisitions

- ❖ Affiliate and partner information also useful
 - Sometimes its easier to impersonate a new employee or contractor / partner than an actual employee
 - If successful, access provided will probably be limited

Job Postings

- ❖ Often available on the company site, but also available on job posting sites such as monster.com, dice.com, hotjobs.com
- ❖ IT job postings list technology proficiency requirements
 - Provide a window into the technologies in use within the corporate network environment
- ❖ Provides a vehicle into the building, e.g. an onsite interview

Social Networking Sites

- ❖ Many social networking sites allow you to search for users by employer

- ❖ LinkedIn.com is a popular professional social networking site
 - Useful for obtaining a list of current employees
 - Not all profiles are up to date!
 - Employee status will have to be verified
 - Useful in identifying which employees likely know each other
 - Avoid impersonation attempts between employees that know one another!
 - Useful in identifying organizational hierarchy

Social Networking Sites

- ❖ Facebook / MySpace, may also provide additional information
 - Personal information can provide insight to probable passwords or answers to security questions

Business Contact Information Sites

- ❖ Some sites such as jigsaw.com allow you to barter business contacts for sales leads
- ❖ For every contact you add you are allowed to download another contact
- ❖ Contact information which includes name, title, email, address, and phone number can also be purchased
- ❖ Extremely useful for email and phone number harvesting

Phone Calls

- ❖ Validate the names that have been obtained are current employees
- ❖ Map department ranges
 - Extensions are generally assigned in an organized way that correlates to physical locations
 - Employees within a department generally sit next to one another

Phone Calls

- ❖ Obtain at least one direct number from an employee
 - Generally their 4 digit extension is the last four digits of their direct number
 - The prefix of employee numbers and the main number can and usually do vary

Email Conventions

- ❖ Companies generally follow a common naming convention for email addresses (often the employees username too)
 - Various permutations:
 - john@ (typical at small orgs)
 - jsmith@ (typical at small orgs)
 - smith@ (typical at small orgs)
 - john.smith@ (typical at large orgs)
 - john_smith@ (typical at large orgs)
 - john_d_smith@ (second dup employee in large org)
- ❖ Most mail servers do not implement a catch all account and will bounce emails to invalid addresses

Email Conventions

- ❖ Choose a name of a valid employee and send an innocuous email using the various naming conventions
- ❖ The email that does not bounce is the syntax the company uses
 - Some mail servers will not bounce unknown addresses. You'll have to illicit a user response in this case

Whois And Reverse Lookups

- ❖ Whois used to obtain company IP ranges which are then scanned for web servers
- ❖ Reverse DNS used to narrow list of interesting web portals
- ❖ Companies often have hidden corporate portals for past and present employees
 - Verification information can be as little as employee name and date of birth

“Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.”

TACTICS

Remote Attacks

- ❖ Easier to execute and less knowledge required
- ❖ Less risk of discovery compared to onsite attacks
- ❖ Easier to become proficient

Caller ID Spoofing

- ❖ Spoof phone number to create false sense of trust
- ❖ Services are available to spoof caller ID
- ❖ Telespoof.com is a popular spoof service
 - Easy to use – works like a calling card
 - Inexpensive
 - \$10 for 60 minutes of talk time

Employee Calling

- ❖ When obtaining sensitive information such as passwords, target specific groups
- ❖ Select non-IT employees and those less inclined to question
 - e.g. Sales, Marketing, Accounting

Employee Calling

- ❖ If the employee is uncooperative or suspicious do not push the issue or hang up
 - Avoid alerting the rest of the organization that a social engineering effort is underway!
 - Say that you have another call and will call back
 - Thank them and do not wait for a response

Fooling Helpdesk

- ❖ Helpdesk can give you a tons of information - they are there to help after all!
- ❖ Internal helpdesk number may have to be obtained from an employee
 - This can be done with a quick phone call
 - Pretend you are trying to reach helpdesk and ask for the extension

Fooling Helpdesk

- ❖ Information gathered from helpdesk depends on your end goal
 - Employee password resets
 - Understanding the new hire process
 - Information to help impersonate helpdesk in future calls
- ❖ Remember small amounts of information at a time!

Voicemail Hacking

- ❖ When new employees first start they are sometimes given a default voicemail PIN
 - Temporary PIN is usually trivial such as 1234
 - If the user is not forced to select a new PIN, it is often left unchanged
- ❖ People themselves often choose weak PINs
 - Easy to remember PINS, PII PINs, e.g. some portion of birthday – usually the year! Try 19xx
 - Review any undeleted messages
 - Do not forget to remark new messages as unread!

Phishing

- ❖ Register a domain that is similar to company name
 - www.myspace.com vs. www.rnyspace.com
 - www.compname.com vs. www.compname-security.com
- ❖ Create a page with form fields requesting whatever information you are targeting
 - Usernames
 - Passwords
 - Employee IDs

Phishing

- ❖ Send emails to employees
 - Avoid IT employees
 - Results can be improved with quick phone call to the target before the phishing attack
- ❖ Consider using pretext like "Password Strength Survey" or "Vulnerability Patch Update"
- ❖ Can also copy HTML directly from intranet or similar site and change FORM target

Onsite Attacks

- ❖ Requires additional preparation and planning
- ❖ Attacks are more unnerving than remote attacks
- ❖ Higher risk level of detection
 - Misunderstanding could lead to detainment and arrest
 - Make sure you have a get out of jail card from executive management handy at all times

Tailgating

- ❖ Piggy backing another employee's swipe to obtain access to an otherwise restricted area
- ❖ Employees often will not challenge people following them in
 - They might even hold the door open!

Dumpster Diving

- ❖ Organizations with shredding policies are still susceptible to lazy employees
- ❖ People have a tendency to throw things into their office trash bin rather than the secured bins where they will be shredded

Dumpster Diving

❖ Information found can include:

- IT account information
 - Usernames
 - Passwords
- Personally identifiable information (PII)
 - Names
 - Social security numbers
 - Account numbers
- Sensitive company information
 - Intellectual property
 - Earnings statements
 - Internal company emails
 - Customer information

USB Drives and CDs

- ❖ Install scripts / programs with phone home capabilities to remotely record when a CD or USB drive is accessed
- ❖ DLL injection into the browser is one way to exfiltrate data
- ❖ Make use of the auto-run feature
 - After the spread of Conficker via infect USB drives, Microsoft is removing the feature from Windows

USB Drives and CDs

- ❖ Create enticing CD labels and program names
 - Company Name Merit Increases Quarter / Year
 - Company Name Layoffs Quarter / Year
 - Negative labels provide better results
 - Validate with client which labels are to be used beforehand

- ❖ Distribute in high traffic areas such as:
 - Break rooms
 - Cafeterias and kitchens
 - Restrooms
 - Smoking areas

USB Drives and CDs

- ❖ Similar approach with USB drives, except labeling not usually possible
- ❖ Direct social engagement can be used to get victim to insert USB drive
 - "Can I print a boarding pass?"
- ❖ Can simply plug the USB drive into an unattended computer
- ❖ USB drives can automatically wipe themselves to eradicate evidence of compromise

Impersonation

❖ Interns or co-ops

- People are less surprised they do not know who you are
- Lost! Help!

❖ Interview candidate

- Announcing you have arrived early allows you to watch processes for badge in, forgotten badges, and PINs
- May allow you access to other areas of the building if you request bathroom or break room
- May also be watched more carefully by staff

Impersonation

❖ Regular employee

- Higher risk of someone knowing the person
- May give you additional access to the building

❖ Contractor / Handy Man / Building Maintenance

- POC usually required
- Least effective

Custodial Staff

- ❖ Often outsourced and one of the weakest links
- ❖ Least educated on security matters, and yet has access to most areas of the buildings

Custodial Staff

- ❖ Some organizations train security and custodial staff not to bother or question executives
 - Simply showing up in a suit can get you what you want!
- ❖ Full blown social engineering efforts will often try to get the social engineer hired on as a janitor
 - Generally easy placement with no background check

“Let your plans be dark and as impenetrable as night, and when you move, fall like a thunderbolt.”

CASE STUDIES

Case Study I

1. Research began on target company and a list of employees was obtained
 - Primary resource was linkedin.com
2. An employee name was selected and their employment status was verified
 - Employee who typically arrives later than most was needed. For this reason employee with job title of developer was selected
 - Employment status verified by contacting main number and requesting extension of employee

Case Study I

3. Over the next few days employee, John Doe, was called at various times in the morning to determine when they arrived
4. Once patterns established, John was called one last time before entering the building to ensure he had not arrived yet
5. Consultant entered building and announced himself as interview candidate to see John

Case Study I

6. Receptionist attempted to contact John Doe and then asked consultant to have a seat and wait

7. During this time social engineer observed process for badge in including the process for when an employees forget their badge
 - They were required to give a valid name
 - A dollar was given to the receptionist

Case Study I

8. After enough information was gathered and enough time passed, the consultant asked the receptionist if he could use the bathroom.
 - The bathroom was further into the interior of the building beyond the HID access doors.
9. The receptionist buzzed the consultant into the building unescorted.
10. The consultant only had enough time to leave trojaned CDs and USB drives in the bathroom and break area before returning to the lobby

Case Study I

11. After waiting a little longer the consultant stated he was going out to smoke and did not return
12. The trojanned CDs and USBs may have provided the access to the network the needed, but there was no guarantee
13. The consultant returned at lunch time the following day when a stand in reception was available and stated during his lunch break he had left his badge at home. The consultant gave a name and placed a buck on the counter.

Case Study I

14. The consultant was then given a temporary badge that gave him access to all building floors

Case Study II

1. Consultant waited in the back of the building for custodial staff to take out the trash
 - The consultant had on the appropriate attire and looked like he could work there
2. Consultant stated he had left his badge and phone in the building and needed someone to keep him back in

Case Study II

3. No verification was requested and staff member opened any door he requested
 - Once the consultant was satisfied with the area of the building he was in, he was left alone

4. The consultant then located the data center
 - Access to the data center required a badge and a PIN
 - The consultant found a conference adjacent to the data center and waited

Case Study II

5. Another staff member eventually accessed the data center for cleaning
 - The staff member immediately closed the door behind him and the consultant could not get in
6. Eventually a second staff member came to do more involved cleaning and left the door open while he did so
7. The consultant walked into the data center unchallenged and accessed whichever open terminal he wished

| Social Engineering

Nathan Sportsman

Founder and Chief Executive Officer

“All warfare is based on deception.”

