Agenda

• What is Social Engineering and Why it’s so Effective
• Social Engineering Cycle
  • Investigation
  • Hook
  • Play
  • Exit
• Social Engineering Tactics
  • Digital
  • In Person
  • Phone
• Social Engineering Healthcare Scenarios
• Mitigations
• HC3 Contact Information
• References

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Social Engineering (SE) is the art of human hacking

- Key Tenants are manipulation, influence, urgency, and deception
- Exploits human psychology and susceptibility to maneuver victims into disclosing sensitive information
- Use various tactics techniques and procedures to procure information
- Recognizes humans are first line of defense and are the weakest link

General Traits of Social Engineers

- Extremely Confident
- Charismatic
- Intimidators
- Expert conversationalist
- Act and look like they belong
- Amicable
- Appease targets self interest
- Appear non-threatening
- Masters of non-verbals
- Amoral and Callous Attitude

Find out about the famous Kevin Mitnick, Once one of the FBI's Most Wanted because he hacked into 40 major corporations just for the challenge.

Image: BAE
Why is Social Engineering so Effective

• **Taking Advantage of Our Tendency to Simplify**
  
  Humans have a deep-seated desire to keep things simple. We find patterns that help us take complex tasks and simplify them
  
  • This simplification is what makes social engineering so effective and scary because it bypasses our ability to reason
    
    • Attackers don’t have to come up with elaborate backstories that can stand up to scrutiny. Their goal is to keep us from looking too closely

• **Thinking is Hard**
  
  Mental exertion, like physical exercise, takes energy, we don’t run our conscious minds at full tilt every day because it would be exhausting

  • The brain naturally looks for opportunities to take pressure off of our conscious mind and offload it to our subconscious or unconscious as a habit through a process called conditioning

  • Because conditioning happens at the subconscious or unconscious level, when a habit is triggered it can cause us to ignore other information associated with it. This is because our subconscious perceives it as unimportant. This reflex is what social engineers take advantage of, which we call, being on ‘autopilot’.
Why is Social Engineering so Effective

- **Timing is Everything**
  - Humans vary in how attentive they are over time.
    - This is due to a combination of biological factors (ex: tiredness, hunger, stress) and mental/environmental factors (ex: distraction, information overload, boredom).
    - It’s common for SE’s to target times of day where people are most commonly going to be distracted.
  - To summarize these points consider the following:
    - “It’s 4:45 on Friday afternoon. Jerry has had a heck of a week and is counting down the minutes until 5 PM hits so he can clock out for some well-deserved R&R. Suddenly, an email hits his inbox.
      - “URGENT!” the message from the CEO says. “I need you to complete this wire transfer for me. It’s very important!” Jerry was so close!
    - He decides to just get this out of the way. After all, it’s the only thing standing between him and the weekend! Jerry is so focused on getting out the door that he doesn’t notice the from address on the email is unusual.
    - This won’t be discovered until Monday morning, when the CFO calls Jerry into his office to ask why he wired $25,000 to an organization that doesn’t exist.”
Social Engineering Cycle

Preparing the ground for the attack:
- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Closing the interaction, ideally without arousing suspicion:
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.
Digital Social Engineering Tactics

- Pretexting
  - The SE presents themselves as someone else with a plausible scenario in order to obtain information, they will target people with direct or indirect ties to their victim.

- Threatening/Blackmail
  - The SE commits (or pretends to commit) a low-level attack against an individual. The SE informs the user that they will lose their job and face legal ramifications if they don’t follow their instructions. E.G. sextortion powered by deep fakes.

- Phishing
  - The SE fakes an IT help desk account, mimics your brand look, and even purchases a domain like your own. They offer a password reset form, complete with an old password field — which is what the SE needs to gain entry into the account. They will use this to access the network or the person’s machine in order to go deeper into the network.
Digital Social Engineering Tactics

- **Typo-squatting**
  - The SE buys domain names and squats on them, matching a brand’s look and feel. Usually the domain is only a character or two off of the main brand’s domain.
  - If the site typically has a download, they can include malware with the executable file. This can include “scareware,” which uses popups and notifications on the target’s computer to require payment for access to the program. When a user fills out a form, they will use the login credentials to cause harm.

- **Device Leave Behind – Baiting**
  - The SE leaves a USB drive, CD, phone or other storage device around an office and writes a tempting label on it. If someone finds a USB drive, they’ll just start to use it on their own.
  - To make sure the user thinks the storage device is legit, the SE might place music files on there, along with other files on the storage device that sound enticing to click. Once accessed, the malicious code is launched.

![Anomali Image](image1)

POSSIBLE MALICIOUS KEYWORD DOMAIN EXAMPLES FOR ANOMALIBANK.COM:
- anomalibank.com ✓
- update-anomalibank.com ❌
- anomalibank-alert.x7462e7.com ❌
- wwwanomalibanksecure.com ❌

POSSIBLE TYPO DOMAIN EXAMPLES FOR DOMAIN.COM:
- domain.com ✓
- domainan.com ❌
- domains.com ❌
- domainln.com ❌
- domain.cm ❌

![Zakird Image](image2)

Image: Anomali
Image: Zakird
Digital Social Engineering Tactics

• Social Media Based Social Engineering
  • The SE either builds a brand that looks legit or mimics the target company’s site and brand. From here, SE perform “news-jacking,” where they retweet or use a hashtag to join a conversation. The SE then piggybacks on high profile stories surrounding their targets and push out a link to a phishing site where they can get users to take actions that might compromise their login or other information.
  • The SE gains access into your account and sends out shared links to surveys and games to your friends. In addition, the SE may take a more relationship-based approach and follow up on existing messages with your friends, who are their ultimate targets, offering them a link to a phishing site.
  • On professional social media sites like Linkedin, a SE will pretend to be a recruiter for a company. They’ll send you a private message and inform you about a position at a well respected company that sounds incredible. They’ll send you to a phishing employment site, where they gather a bunch of information, and require your social security number for background check purposes.
  • Social media is an easy way for hackers to go phishing for unsuspecting users, and it’s becoming more prevalent because there are so many attack methods.
In-person Social Engineering Tactics

- Neuro-Linguistic Programming (NLP)
  - This is a social engineering tactic you’ll sometimes see salespeople perform to get clients to like them. SE use it in the same way. Once the SE gets physically close to the target, the SE will match the voice, tone and body language of their victim.
  - NLP helps SEs build a rapport with the target and subtly steer the conversation. The SE will use industry or company jargon to help close the deal and get the info they need. This helps make them seem like an authority. The SE can simply try to bribe, threaten or even straight up solicit information from their target.

- Classic Piggyback
  - This is an in-person social engineering attack that typically happens at large organizations. The SE will scout outdoor social locations and then join the group, maybe even asking people what department they work in and striking up a casual conversation. When the group goes in, the SE follows the employees.

Image: Cyber Peace Corp
In-person Social Engineering Tactics

• The Cable Guy
  • The SE will dress up as technician and report to the front desk. They'll ask to be escorted to IT in order to work on the wiring or some other connection issue on the company’s end. In this scenario, the SE might not even have to chat with someone in IT, as they may be shown to where they’re needed.
  • The SE might apologize for being late or take a fake phone or radio call from their boss. When the SE is alone, he can carry out his plan.

• Rogue Employee(s)
  • Where the SE gets a low-level job at a company with just enough access to their marks. Another alternative involves bribery and solicitation to perform these actions.
  • Once they have a position in the office, either on their own or through a surrogate user, they can access open workstations or perform any number of malicious activities.
Phone Social Engineering Tactics

- Vishing
  - Voice Phishing aims to get prospective victims to share personal or financial information. A malicious actor aims to get you to comply with what, under normal circumstances, would be considered unrealistic demands through creating a situation that creates an emotional response such as fear, urgency, curiosity, or even excitement.
  - With Technology, SE can impersonate voices of targets, E.G. A CEO to secretary for further gain

Click this link to see an video example of Vishing
https://www.youtube.com/watch?v=lc7scxvKQOo
Phone Social Engineering Tactics

- **SMiShing**
  - Uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. Like phishing, the SMiShing message usually asks for your immediate attention.

- **Charitable Donation Calls or text messages**
  - SEs will exploit our generosity with phony requests for donations to charitable causes which includes payment instructions on how to send money to the hacker.
  - By researching you on social media, a SE can figure out what charitable causes, disaster relief efforts, or political campaigns you are likely to support. They will use this information to craft messages aligned with your ideals. SE will take advantage of any current events, conferences, etc.

Image: SMiShing Examples
SOCIAL ENGINEERING IN HEALTHCARE

Image: Security Metrics
Social Engineering Scenarios in HealthCare

• The Dumpster Dive
  • Sometimes hospitals don’t dispose of sensitive documents properly. Take a hospital with an offsite IT staff. If the hospital receives invoices and doesn’t shred them, a SE could go through that trash and find sensitive information about new hospital computers. Even better, he could find the names of the IT personnel that installed the new computers.

• The Name-Drop
  • A SE goes up to a help desk, “Hi, my supervisor, Kent, has requested a change to a system in my department; it’s been having problems. I need to get on one of your computers.” He’s in a big hospital, so the staff believes him, especially since he gives a supervisor’s name. The staff grants that request without a second thought. He has access to a computer that may have PHI and other data.

• The Walk-In
  • The SE walks into the hospital, dressed up as a fake IT or nurse or in a suit or as a third party vendor or essential someone that looks like they visit your location. They will have a reason as to why they are there and proceed to try and enter your facility. Once in, they will continue with their nefarious plan.
• The Pointed Question
  - A SE asks a staff member pointed questions, masking them as casual inquiries. The staff member then unwittingly gives her valuable information, such as his supervisor’s name, his username, the supervisor of the department, etc. After a few more questions, she now has enough information to call up a different department, name-drop and then get more information.

• Tailgating
  - A SE shows up at the employee entrance carrying an armful of donut boxes. A clueless but helpful employee holds the door open for him, and then follows him to the elevator to ask which floor he needs (all the while not even noticing he doesn’t have an employee badge).

• Threatening
  - A SE calls in, acting as the secretary of one of the hospital’s most important doctors. His boss is having problems accessing the system and he demands to know why. Acting rushed and annoyed, he demands access into the system.

• The Unlocked Computer
  - A SE walks into a hospital. He confidently goes into an office that’s unlocked and sits down at the computer. The computer is unlocked and he now has access to all kinds of data. He starts going through information and installs malware on that computer to steal more information later.
Mitigations

• **Make each department accountable for security:** For most hospitals, it’s impossible for the C-Suite to train everyone about security. Every department head should constantly discuss security with employees.

• **Slow Down:** Slow down and evaluate the situation with a clear mind before rushing into anything. SE’s want you to rush to action before you notice any potential red flags.

• **Take advantage of resources:** See the reference slides for further information and resources available to you. Research and learn!

• **Test your staff:** The best way to learn security techniques is to practice them. Get your staff used to social engineering attempts by pretending to be a social engineer (or hire an ethical social engineer). See what they do, and debrief them after.

• **Boost your physical security:** Keep computers locked, use screensavers, watch your devices, and lock offices when not in use. Taking small measures will help prevent social engineers from easy access.

• **Proper Regular Staff Training:** Train your staff to be aware, suspicious, and verify requests. It’s critical to your patient data and organization’s brand that your staff members know how to address social engineering. Onboard and annual training isn’t enough!! Schedule quarterly, or even monthly training.
Check out some previous HC3 briefs to see more about


**Product Evaluations**

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

**Requests for Information**

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV) or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
References

- 2018 AEP Vulnerabilities of Healthcare IT Systems

- Healthcare Recognize Social Engineering Techniques
  https://www.securitymetrics.com/blog/healthcare-recognize-social-engineering-techniques

- Disaster Tips on Cyber and Social Engineering Scams
  https://h-isac.org/disaster-tips-on-cyber-and-social-engineering-scams/

- Social Engineering Training What Your Employees Should Know
  https://www.securitymetrics.com/blog/social-engineering-training-what-your-employees-should-know

- Be Cyber Smart Common Scams
  https://www.dhs.gov/be-cyber-smart/common-scams

- Your Business Prepared Physical Security Threat
  https://www.securitymetrics.com/blog/your-business-prepared-physical-security-threat

- Become Cyber Savvy Protect Against Phishing Attacks

- DHS TIPs ST04-014
  https://www.us-cert.gov/ncas/tips/ST04-014

- Deepfakes and Cheap Fakes

- How I Socially Engineer Myself into High Security Facilities
References

- Social Engineering is No Friend to Small Business
  https://blog.twinstate.com/cybersecurity/social-engineering/social-engineering-is-no.friend.to.small.business

- Employee Data Security Training What You Should Do

- What is Social Engineering Tactics
  https://heimdalsecurity.com/blog/what.is.social.engineering.tactics/

- Social Engineering Attacks
  https://securitytrails.com/blog/social-engineering.attacks/

- What is Social Engineering
  https://www.knowbe4.com/what.is.social.engineering/

- Recognizing Social Engineering
  https://www.twinstate.com/recognizing-social-engineering-11-tips.to.identify.an.attack/

- Fraudsters Use AI to Mimic CEOs Voice
  https://www.wsj.com/articles/fraudsters-use.ai.to.mimic.ceos.voice.in.unusual.cybercrime.case.11567157402

- Social Engineering Attacks
  https://www.smartfile.com/blog/social-engineering.attacks/

- Brain Hacking Nobody Time for That
  https://info.phishlabs.com/blog/brain.hacking.nobody.time.for.that

- Know the Risk Raise Your Shield
  https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk.raise.your.shield/ncsc.awareness.materials