Social Engineering
ORMIA Specialized Course

Robert Tracey, Gabriel Zaconeta
May 18, 2016
Agenda

- Hacking Humans & Introduction to Social Engineering
- Social Engineering Types
- Examples of Recent Social Engineering Attacks
- Tips To Protect Yourself
- What Can We Do? Awareness!
- Considerations for Auditing
Hacking Humans
Hacking Humans

Advantages

• Very low risk with high reward potential.
• Employees/Insiders already have access to sensitive materials – no technical knowledge to acquire this access as needed as with ‘traditional hacking’.
• Highly flexible – can target specific marks or an entire organization.
Types of Social Engineering
Types of Social Engineering

Phishing
- Uses E-Mail / fictitious webpages.
- Targeted phishing is known as ‘spear-phishing’.

Pretexting
- Uses prefabricated scenarios – can be in person or over phone.
- Example: A scammer posing as IT to extract login details.

Baiting
- Uses software downloads / physical media.
- Example: USB sticks with materials from a Conference.

Blackmailing
- Uses sensitive details of individuals for leverage.
- Can also be used with malware (example: US DoJ Virus).
- This may be a potential outcome of the OPM Hack.
Social Engineering via Email

**What you Need**

- Mailing Lists of target individuals and institutions -or- company’s email naming convention (e.g. firstname.lastname@company)
- Basic information about the target
- Servers / Bot Farms for mass-phishing attacks (e.g., bank phishing scams)

**Skill Level:** Low

**What you Get**

- A percentage of targets will generally fall for the scam
- Gain user credentials, financial information – can steal directly from individual or leverage for future theft
- Gain details around the organization or push malware to the organization

**Damage Level:** High
Social Engineering via Voice

Pretexting
• Uses prefabricated scenarios – can be in person or over phone.
• Example: A scammer posing as IT to extract login details.

What you Need
• Calling Lists of target individuals and institutions – harder to get than email addresses
• Trick: Get Area Code – Exchange and start calling all of them
• Basic information about the target
• VoIP Services / Untraceable phone connections
• Robo-calling is also feasible but less effective

Skill Level: Moderate

What you Get
• Depending on level of effort made, can get in depth information being sought such as passwords, identification details (SSNs, CC numbers), or sensitive details about the organization
• More effective in forcing action from the targets (e.g., can pose as an important individual)

Damage Level: High
Baiting

- Uses software downloads / physical media.
- Example: USB sticks with materials from a Conference.

What you Need

- Malware designed for the purpose (can produce individually or obtain existing malware)
- Delivery mechanism (USB drives, freeware applications, etc.)
- Emerging Example: Mobile Application Freeware

Skill Level: Low to Moderate

What you Get

- Depending on attractiveness of the software (“bait”) can have a very high degree of penetration of the malware
- Obtain user credentials, local session information – all can be used for other attacks
- Can also be done to simply cause damage

Damage Level: High
Blackmailing (Severe Social Engineering)

Blackmailing

- Uses sensitive details of individuals for leverage.
- Can also be used with malware (example: US DoJ Virus).
- This may be a potential outcome of the OPM Hack.

**What you Need**

- High degree of information on the target individual – this isn’t something that can be delivered ‘en masse’
- Strong communication skills – need to be able to manipulate the target to the desired outcome
- Untraceable source – advantage of remote blackmailing is it is hard to get back at the attacker

**Skill Level:** High

**What you Get**

- If successful, whatever you are trying to get (money directly from individual, highly sensitive information relating to job, etc)
- Blackmail can range in levels of sophistication and severity (e.g., from using basic doxxing to espionage)

**Damage Level:** Very High
Examples of Social Engineering Attacks
Examples of Social Engineering Types

- Difficult to recognize phishing attacks from legitimate emails and websites.
- External threats establishing trust and confidence with targets.
- Historically, employees have been the source of most security issues in organizations.
- Social engineering attempts can be carried out over long periods of time.
Phishing Example

- Personal AOL email account of CIA Director, John Brennan, hacked through gaining information from Verizon.
- Social Engineering techniques used against both Verizon and AOL to gain access.
- Hacker obtained work-related information Brennan forwarded to his personal account.

**Whaling Example**

- Whaling, the social engineering grift typically involves a hacker masquerading as a senior executive asking an employee to transfer money.
- This is a pure social engineering hack targeting relationships between employees. Whaling fraudsters either gain access to an executive's email inbox, or email employees from a fake domain name that appears similar to the legitimate domain name.
- The intended recipient is asked to take some action, such as moving money from a corporate account to an account the fraudster has set up, Malone says.
Spying and Eavesdropping Example

- Spyware on your cell phones.
- Determining if your phone contains the spyware can be difficult. The spyware app could be installed to look like another app or file.

---

**FBI Arrests StealthGenie Mobile Spyware App Maker, Disables Website**

The maker of a smartphone app that could surreptitiously monitor calls, texts, and videos on mobile phones was indicted in Virginia for allegedly conspiring to advertise and sell the spyware application.

Hammad Akbar, the chief executive officer of Pakistan-based InvoCode Pvt Ltd, the company that advertised and sold StealthGenie online, was arrested in Los Angeles Saturday, September 27. The 31-year-old Pakistani man was charged with conspiracy and sale of a surreptitious interception device. StealthGenie spyware could intercept communications to and from mobile phones and was marketed as largely undetectable and untraceable.

In announcing the charges, officials said the spyware technology could be employed to invade the privacy of unwitting victims. Purchasers of the app would need only a few minutes to download and install it on a victim’s mobile phone for full access to the phone’s communication functions.
Blackmail Example

- Threats of disclosing sensitive information or widespread cyber attacks unless payment of lump sums.
- Cyber-extortion has become an emerging tool for criminals to hold businesses against their will. Threatening them with widespread spamming and other Internet-based attacks.

---

**New York Field Office**

**Manhattan U.S. Attorney Charges California Man with Cyber-Extortion of New York-Based Insurance Company**

**U.S. Attorney's Office**

March 08, 2010

**Southern District of New York**

(212) 637-2600

PREET BHARARA, the United States Attorney for the Southern District of New York, and GEORGE VENIZELOS, the Acting Assistant Director-in-Charge of the Federal Bureau of Investigation's New York Field Division ("FBI"), announced that ANTHONY DIGATI was arrested on March 6, 2010, on charges of attempting to extort approximately $200,000 from a New York-based life insurance company by threatening to make false public statements and transmit computer spam in an effort to damage the reputation of the company and cost it millions of dollars in revenue.
Tips to Protect Yourself
Suggested Tips to Avoid Being Phished

- Keep your email, web, and endpoint security up to date.
- Even trusted email senders can be compromised.
- Colleagues may innocently send infected links or files to download.
- Just because an email looks good doesn't mean it's legitimate. Beware of emails that are badly formatted or contain misspellings (especially from well-known companies).
- While some email addresses are obviously from a phony third-party site, it's easy for sophisticated scammers to make an email address look similar to a legitimate domain.
- Your safest choice is to independently confirm requests by reaching out to the main source.
Questionable Websites - Important Reminders

Beware of websites or emails that:

- Asks for personal information such as credit card number, PIN number, bank account number, an account password, mother’s maiden name, or social security number.
- Does not use SSL (no https).
- Uses suspicious or forged URLS.
- Has poor resolution.
- Has misspelled words, grammatical errors, etc.
- Uses smaller windows within a normal sized webpage.
- Uses the title page as “Random Account Verification”.
- Uses an IP address (ex. 123.23.34.2) instead of a text URL (e.g.www.help.home.gov)
### E-mail Warning Signs

12 warning signs will help you recognize a fake email:

1. The email contains information that could be obtained from social networking sites.
2. There is a hyperlink in the email.
3. The email refers to a current news event.
4. The “tone” of the email from a friend or colleague doesn’t sound quite right.
5. The email requires immediate action.
6. The email doesn’t address you by name or include part of your account number.
7. The email does use your name, but it still seems suspicious.
8. The email requests personal data.
9. The email asks you to update your username and/or password.
10. The email is poorly formatted and/or uses poor grammar.
11. The email “looks” official but contains other warning signs.
12. Be suspicious of hyperlinks that are made up of words or phrases instead of a valid website name.
Summary

- Protect your password and never share it with anyone.
- Be wary of how social engineers are gathering information from Facebook and other social networking sites.
- Keep in mind the sensitivity of the information you deal with regularly.
- Executives are especially lucrative targets because of their wide variety of contacts and knowledge.
- Never provide an unknown person with information regarding other employees.
- Don’t say “yes” just to get the person off the phone.
- Don’t give away seemingly unrelated bits of information.
- Refer inquiries for Bank information to management if you are uncertain about the identity and need to know of the requester.
- Report password compromise or suspicious behavior to the National Service Desk and your management.
What Can You Do? BE AWARE!
What Can We Do? (Rob)

**Defense against the Four Types**

- Phishing / Spear-Phishing can be defended through careful scrutiny of email and webpages.
- Pretexting can be defended with skepticism.
- Baiting can be defended with skepticism and virus/malware defense tools. (for personal use, I recommend VirusTotal).
- Blackmailing can be defended with skepticism and in severe cases, law enforcement. I strongly recommend locking down your social media presence as this is a ripe source for blackmail / ‘doxxing’.
Considerations for Auditing
Audit Considerations

- Does your organization…
  - Have adequate awareness training?
  - Have protections against unsolicited emails and phone calls?
  - Have controls over installation and use of external media?
  - Have a support line for individuals that are attacked?
  - Do mock social engineering exercises?
Audit Considerations

- Does your organization have a Security Awareness Program for social engineering?
  - Evaluate effectiveness & reach of training & communications
  - Determine how effectiveness of program is evaluated

- Test to verify efficacy of Malicious Email Filtering by:
  - % blocking of malicious emails
  - Frequency/types of filters updated based on incidents

- How is your organization managing Incidents?
  - Is there an accurate, complete list of incidents?
  - Analysis of nature and severity?
  - Remediation effectiveness and completeness?
Designing a mock social engineering exercises

- Plan the social engineering campaign – In House vs External
- Design a phishing/pretexting attack to test the user base
- Determine scope of users to test
- Execute the campaign – consider reporting to the user immediately if they fell for it (improves awareness)
- Collect statistics (who fell for it, who ignored it, who reported it)
- Perform analytics (what types of users are falling for the attack and what types are reporting it)
- Perform the campaign over time, track progress
- Adjust Information Security awareness program based on results
Questions & Answers