Security+ Chapter 4:

Social Engineering

Justin McAfee | iaintshootinmis

Twitter | Github

Who am I?

- Former Psychological Operations Specialist

- Current Incident Response professional for a Global Food and Beverage Supplier

- Husband, Dad, and National Park Enthusiast

What's in it?

- Methods of Persuasion
- Social Engineering Techniques
- Password Attacks
- Physical Attacks

Methods of Persuasion

7 types of Persuasion

- Authority
- Intimidation
- Consensus
- Scarcity
- Familiarity
- Trust
- Urgency

Authority

Abuses the idea that most people will obey people who appear to be in charge or knoweledgable, regardless of whether they actually have authority.

Attackers may imitate an authority figure to gain compliance.

BazaarCaller is a common scam where threat actors claim to be calling from Microsoft to elicit the targets compliance.

Intimidation

Abuses the idea that the attacker has some ability to harm the target whether physically, or through legal or financial means.

Attackers may combine persuasion types.

Scammers often imitate the FBI or Police department to convince targets they have outstanding warrants that can go away for a small "fee"
Or that they are the IRS contacting the user about a very big tax problem that could result in their arrest.

Consensus

Targets a users feeling of belonging. This can be effectively used by showing that others are also participating in the activity.

Threat actors may use the name of other users who fell for a social engineering attack to legitimize their behavior.

```
"You can check with Susan, we worked with her on this issue previously."
"Susan, did you work with Microsoft?"
"Yeah, they got me all squared away!"
```

Scarcity

Used in advertising and other scenarios to make something more desirable by describing its rarity

Plays on the targets FOMO - Fear of Missing Out

Think QVC but with bad guys

Familiarity

This persuasion technique is one of the single most effective and depends on you having familiarity (and likely Trust) with an organization or individual

Smishing campaigns often target Familiarity by sending spoofed messages from a familiar number, a boss, colleague, or friend.

Trust

Like familiarity, expects the target has a certain *implicit* trust with the personality the threat actor is immitating and uses that trust to build ever increasing compliance

Famed Televangelist Peter Popoff used this technique in his "Send a dollar" scheme

Urgency

Simply put, something must be done **now** and the target must be the person to do it

Used most often in combination with Intimidation and Authority

React v Proactive

These techniques work because humans are bad at reacting. Reacting is based on emotional instead of logical responses and tend to degrade our logical, empirical, and critical thinking skills.

Unless a situation is life-threatening, remember to Stop. Think. Act.

For more information on the topic, check out Maslov's Heirarchy of Needs and the combination of Persuasion Techniques with each level of the Heirarchy

Social Engineering Techniques

8 Techniques

- Phishing
- Credential Harvesting
- Website Attacks
- Spam
- In-Person Techniques
- Identity Fraud & Impersonation
- Reconnaissance & Impersonation
- Influence Campaigns

Phishing

A broad category to describe obtaining information (usernames, passwords, credit card #s, PINs) illicitly
Defense: User Awareness Training

- Phishing - usually specific to email
- Smishing - SMS (text) messages
- Vishing - Phone calls
- Spear Phishing - Targeting specific users to gain specific access or create a specific impact
- Whaling - aimed at executives and senior employees, think VPs, C-suite and "biggest fish in the pond"

Credential Harvesting

Process for collecting usernames and passwords
Defense: Multifactor authentication and encryption of credential stores, monitoring of anomalous user activity (Impossible travel, new devices, new locations)

- Often accomplished through phishing
- Can occur through theft of credential stores (databases of username and password combinations)
- Used to gain access to systems as legitimate users

Website Attacks

Attacks against websites to perform credential harvesting or deploy malware

- Pharming - technically expensive attack to redirect users from legitimate site to malicious site (usually envolving a DNS alteration)
- TypoSquatting - Using website name misspellings to trick users (e.g.; Gogle[.]com, Microsorft[.]org)
- Watering Hole - Targeting websites that the target will visit. Often used against politicians and industry leaders (targeting InformationSecurity Today would likely give access to the accounts of [illegible]d CISOs)

Spam

Trash emails often utilize persuasion techniques to attempt to get you to buy a product, click a link, or download a file.

Additionally SPIM (Spam over Instant Messaging) - exactly what it sounds like. This is nonsense, remember it for the test and if I ever hear you say it I'll ridicule you endlessly.

In-Person Techniques

- Dumpster Diving - Digging through trash for information. Some companies combat this with Secure Disposal Services
- Shoulder Surfing - looking over user's shoulder or using reflective surfaces to see their credential entries. Often combated with polarized screen covers on devices
- Tailgating - Following another legitimate user through a physical barrier, door, or turnstile, etc... Prevented by "meat grinders"

Eliciting Information

Leading targets to discuss topics without their knowledge

Prepending....

- Adding information to Email details to trick anti-spam tools
- Adding information as part of another attack to manipulate the outcome
- Leading conversations to related topics to gain info about specific topics

Identity Fraud & Impersonation

- Pretexting - using pretend situations to justify contacting a target
- Identity theft - pretending to be a specific person or role to gain access or compliance
- Hoaxes - Social media may be leveraged by attackers to create anxiety or interest in intentionally fake stories/situations
- Invoice scams - Sending fake invoices to real companies in hopes of exploiting poor Accounts Payable processes

Reconnaissance & Impersonation

Gathering information about a target through impersonation and social engineering

- Making phone calls, sending emails, or sending letters to gain information
- Can be on-site and in-person as well

  Reconnaissance also means any collection of information broadly across physical and digital means

Influence Campaigns

- Social media leveraged to create a certain belief and ultimately action on behalf of a target
- Coupled with Social media, and other online mediums
- Part of Hybrid Warfare - Competition, short of kinetic action (physical world combat) that include cyberwarfare, propaganda and information warfare

Password Attacks

- Brute Force
- Password Spraying
- Dictionary Attacks

Brute Force

Attempting lots of passwords until one works

- Can be done manually
- Can be done with great complexity given rule sets and advanced automation
- targets one or few accounts with MANY password attempts

Password Spraying

Attempting a single or few passwords against MANY accounts

- Can be done manually
- Most often done with advanced automation
- Threat actors may pair information from reconaissance to identify emails, usernames, etc...

Dictionary Attacks

Attempting a set of known or expected "good" passwords against accounts

- RockYou.txt contains the passwords of 32million users of former software company Rockyou
- Extremely well known and easily accessible lists of *known* passwords across all commonly spoken languages, English, Spanish, French, Chinese, and Japanese

Password Cracking

- Offline
  Attackers may perform attacks against a cached copy of a stolen credential store.
  Hashed passwords specifically may be target with Rainbow tables (discussed in Chapter 1, hashes)
  Rainbow tables are a massive list of all *possible* combinations
- Online
  Attackers may perform attacks against live systems. These are quickly identified by seeing many failed login attempts with the same password or same login location, or many failed attempts by a single user.

Malicious Flash Drives/Malicious USB Cables

May be dropped or delivered

- Autorun - Normal USB storage devices with malicious scripts that execute on plug-in
- BadUSB - Single board computers with malicious code that may have collection, injection, and wireless networking capabilities
- USB Rubber Duck - Emulates a input device (like a mouse or keyboard) to execute preprogrammed scripts on input
- O.M.G. Cable - Single board computers embedded into USB cables, most commonly used on Apple devices. Allow inject of malicious

Card Cloning

Used to target RFID and payment magnetic stripe cards

- Often performed by *skimming* using hidden or fake card readers or social engineering to gain access to a card

Previously scammers have supplied card skimmers to restaurant employees to take cards out of customer view and skimming/cloning them while processing the users bill

Supply Chain

Attackers target the manufactures of devices, including integrated circuits, computer systems, etc...

- US Government has both used this technique and attempts to protect the US from these attacks through the Department of Defense's Trusted Foundry program.

Many companies purchase direct from manufacturer to avoid supply chain attacks or issues

Check on Learning

- What is tailgating?
- What are some commmon phishing techniques? Which target senior employees?
- You receive a text from your CEO asking for help! What persuasion technique is this? Bonus: What phishing technique is it?