

1.1 Compare and Contrast different types of Social engineering techniques

<ul style="list-style-type: none">• Phishing• Smishing• Vishing• Spam• Spam over Internet messaging (SPIM)• Spear phishing• Dumpster diving• Shoulder surfing• Pharming• Tailgating• Eliciting information• Whaling	<ul style="list-style-type: none">• Prepending• Identity fraud• Invoice scams• Credential harvesting• Reconnaissance• Hoax• Impersonation• Watering hole attack• Typo squatting• Pretexting• Influence campaigns<ul style="list-style-type: none">- Hybrid warfare	<ul style="list-style-type: none">- Social media• Principles (reasons for effectiveness)<ul style="list-style-type: none">- Authority- Intimidation- Consensus- Scarcity- Familiarity- Trust- Urgency
--	--	--

Created: 2021-07-24 10:59

Tags: [#socialengineering](#)

Social engineers veil themselves in a cloak of believability -Kevin Mitnick (Famous Cybersecurity consultant/author)

Phishing: Fishing for information. Usually through face-to-face interactions and over the phone.

Smishing: A form of phishing through text messages services or apps.

- Text messages asking for response or reply. In some cases, replies could trigger a cramming event. Cramming is when a false or unauthorized charge is placed onto your mobile service plan [More info](#)
- Text messages could include a malicious hyperlink or URL
- Text messages could contain pretexts (pretexts: Investing a scenario to convince victims to divulge information)
- Text messages could include phone numbers that if called result in excessive toll charges (toll number: A regular phone number that will incur a charge for placing the call)

Vishing: Phishing done over any telephony or voice communication system

Most vishing campaigns use VoIP because they allow the attacker to be located anywhere, make free phone calls, and be able to spoof their origin

caller ID (VoIP: Making calls through internet connection instead of a regular phone line)

- Editing voice response where the vishing attacker gets the victim to answer "Yes" to a question, but then edits the recorded audio to associate the answer with a different question than was asked

Spam: Email that is undesired/unsolicited

- Countermeasures: Email filter/antivirus scanners [More info](#)
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)
 - Domain-based Message Authentication Reporting and Conformance (DMARC)
 - Secure/Multipurpose internet Mail Extensions (S/MIME)

Spam over instant messaging (SPIM): Transmission of unwanted communications over any messaging system

Spear phishing: More targeted form of phishing toward a group of individuals

- Can be crafted to seem like it originated from the CEO or other top office in an organization
- Business Email Compromise (BEC): Convincing members of company departments from a message that appears to originate from a boss, manager, or executive.

Dumpster Diving: Digging through trash, discarded equipment, or abandoned locations to obtain information about a target organization or individual

Shoulder surfing: When someone is able to watch a user's keyboard or view their display

Pharming: Malicious redirection of a valid website's URL or IP address to a fake website that hosts a false version of the original, valid site

- DNS cache poisoning
- Host file injection

Tailgating: When an unauthorized entity gains access to a facility under the authorization of a valid worker but without their knowledge.

Eliciting information: The act of gathering or collecting information from systems or people. In the context of social engineering, it is used as a research method to craft a more effective pretext

Whaling: A form of spear phishing that targets specific high-value individuals, such as the CEO.

Prepending: Adding or a term, expression, or phrase to the beginning or header of a communication.

- { Precede the subject of an attack email with RE: or FW: (Regard to/forwarded) to make the receiver think the communication is the continuation of a previous conversation
- { EXTERNAL, PRIVATE, and INTERNAL

Identity fraud: The act of stealing someone's identity.

Invoice scams: Attempts to steal funds from an organization or individuals through the presentation of a false invoice often followed by strong inducements to pay.

Credential Harvesting: Collecting and stealing account credentials.

- { Often credential collections are leaked to the general public
- { There are services that allow you to search if for sets of evidence of their own information being leaked:
 - { <https://haveibeenpwned.com/>
 - { <https://spycloud.com/>

Reconnaissance: Collecting information about a target, often for the purpose of planning an attack.

Hoax: Designed to convince targets to perform an action that will cause harm or reduce their IT security (deception)

Impersonation: Taking on the identity of someone else to use their access or authority.

- (Examples: Masquerading, spoofing, identity fraud, etc

Watering hole attack: A form of targeted attack against a region, group, or organization. The attacker searches for a common resources that they use, and infect the resource.

Typosquatting: Taking advantage of when a user mistypes the domain name or IP address of an intended resource

- (googel.com vs google.com

Pretexting: A false statement crafted to sound believable to convince the victim.

Influence campaigns: Attempting to guide, adjust, or change public opinion.

- (disinformation, propaganda, "fake news", doxing, etc...

Social Engineering Principles

The principles of social engineering attacks are designed to focus on various aspects of human nature and take advantage of them

1. (**Authority:** Most people are likely to respond to authority with obedience
2. (**Intimidation:** This uses authority, confidence, or even the threat of harm to motivate someone to follow orders
3. (**Consensus:** The social proof that a person's natural reaction is to mimic what others are doing
4. (**Scarcity:** Convince someone that an object has a higher value based on the object's scarcity
5. (**Familiarity:** This attempts to exploit a person's native trust in that which is familiar
6. (**Trust:** An attacker working to develop a relationship with a victim
7. (**Urgency:** The need to act quickly before they have time to carefully consider or refuse compliance