* **Social Engineering:**
  + The practice of manipulating people through a variety of strategies to accomplish desired actions.
  + Social Engineers work to influence their targets to take actions that they might not otherwise have taken.
  + A number of key principles are leveraged to successfully social engineer an individual. 7 main ones are:
    - **Authority:**
      * Relies on the fact that most people will obey someone who appears to be in charge or knowledgeable, regardless of whether they are.
        + A social engineer may claim to be a manager, government official, or someone with authority.
    - **Intimidation:**
      * Relies on scaring or bullying an individual into taking a desired action. The individual who is targeted will feel threatened and respond by doing what the social engineer wants them to do.
    - **Consensus (Social-Spoofing):**
      * Consensus-based social engineering uses the fact that people tend to want to do what others are doing to persuade them to take an action.
        + An example is to claim everyone at your department has already clicked a link, so you should too because it’s safe.
    - **Scarcity:**
      * Used in scenarios that make something more desirable because it may be the last one available.
    - **Familiarity:**
      * Rely on you liking the individual or even the organization the individual is claiming to represent.
    - **Trust:**
      * Similar to familiarity, relies on a connection with the individual they are targeting. However, trust relies on targets thinking that something is normal and thus familiar.
        + Social engineers must build a connection with their targets so that they will take actions that they want them to take.
    - **Urgency:**
      * Relies on create a feeling that action must be taken quickly due to some reason or reasons.
  + Many of these key principles create situations where targets will typically want to respond rather then clearly think out the situation first then respond accordingly.
    - A key part of social engineering is understanding targets, **how humans react, and how stress reactions** can be leveraged to meet a goal.
* **Social Engineering Techniques:**
  + **Phishing:**
    - A broad term used to describe the fraudulent acquisition of information, often focuses on credentials like usernames and passwords, as well as sensitive personal information like credit card numbers and related data.
    - **Typically done over email.**
      * **Smishing:**
        + Phishing via SMS (text) messages.
      * **Vishing:**
        + Phishing via telephone.
      * **Spear Phishing:**
        + Phishing which targets specific individuals or groups in an organization to gather desired information or access.
      * **Whaling:**
        + Spear phishing that targets senior employees like CEOs and CFOs
    - Can typically be countered with training and awareness, but some tools also can detect if an email is a phishing attempt.
  + **Credential Harvesting:**
    - The process of gathering credentials like usernames and passwords.
      * Often performed via phishing attacks but can be accomplished through system compromise resulting in the acquisition of user credentials or system credentials.
    - Once credentials are harvested, attackers can leverage them for further attack with financial attacks being a top target.
      * Multifactor authentication (MFA) and user awareness + technical tools help prevent this from escalating.
  + **Website Attacks:**
    - **Pharming:**
      * Redirect traffic away from legitimate websites to malicious versions.
        + Require a successful technical attack that can change DNS entries on a local PC or on a trusted local DNS server, allowing the traffic to be redirected.
    - **Typosquatting:**
      * Use misspelled and slightly off but similar to the legitimate site URLs to get people to websites they didn’t intend to be at.
        + Can be used for ad traffic or drive sales of similar but not legitimate products.
    - **Watering Hole:**
      * This technique does not redirect users, but targets users based on the user’s frequently visited sites.
        + Then, the attacker can compromise the website or set up advertising networks.
  + **Spam (Unsolicited or Junk Email):**
    - As the name implies, just sending a bunch of unsolicited mail. The success of it comes from the fact that if you send enough tempting messages to enough people, there is going to be someone who falls for it.
    - **Spam over Instant Messaging (SPIM):**
      * Instant messaging spam, not very common though.
  + **In-Person Techniques:**
    - **Dumpster Diving:**
      * Not really a social engineering technique but is very effective at retrieving potentially sensitive information from dumpsters.
    - **Shoulder Surfing:**
      * The process of looking over a person’s shoulder to capture information like passwords or other data.
      * This can include any other way of looking at a person logging into a system such as looking at a mirror.
        + Things like polarized security lenses over screens can help prevent shoulder surfing in public places.
    - **Tailgating:**
      * A physical entry attack that required simply following someone who has authorized access to an area so that as they open secured doors you can pass through as well.
    - **Eliciting Information (Elicitation):**
      * Technique used to gather information without targets realizing they are providing it.
        + Includes flattery, false ignorance, or even acting as a counselor or sounding board for all common elements of an elicitation effort.
        + Talking a target through things, making incorrect statements so that they correct the person eliciting details with the information they need.
      * Ideally, a social engineering target will never realize they provided more information than they intended to.
    - **Prepending:**
      * Can mean one of three things:
        + Adding an expression of phrase, such as adding “SAFE” to a set of email headers to attempt to fool a user into thinking it has passed on antispam tool.
        + Adding information as part of another attack to manipulate the outcome.
        + Suggesting topics via a social engineering conversation to lead a target toward related information the social engineer is looking for.
  + **Identity Fraud and Impersonation:**
    - **Pretexting**:
      * The process of using a made-up scenario to justify why you are approaching an individual.
      * Often used to make the impersonator sound more believable.
      * However, it can be easy to counter if the target asks for identity verification.
    - **Identity Fraud (Identify Theft):**
      * The use of someone else’s identity.
        + Typically used for financial gain, but can be used by social engineers.
        + **Impersonation:**

When you act like someone else, can be a limited form of identity fraud.

* + - * + **Hoaxes:**

A common occurrence where fake news and information is spread. Social media plays a large role in many modern hoaxes, and social engineers may leverage them.

* + - * + **Invoice Scam:**

Involves sending fake invoices to organization in the hopes of receiving payment. Can be both electronic or physical, relying on the recipient not checking to see if it is legitimate.

* **Reconnaissance and Impersonation:**
  + Social engineering is a great way to gather information and thus is often used as part of reconnaissance effort. Social engineering can be used during phone calls, email, and other means of contact to elicit more information about a target than is publicly available. At the same time, on-site and in-person reconnaissance efforts use social engineering techniques to gain access, gather information, and bypass security systems and processes.
    - However, **reconnaissance** just broadly means to gather information about a target.
* **Influence Campaigns:**
  + As cyberwarfare and traditional warfare have continued to cross over in deeper and more meaningful wats, online information campaigns focused on social media, email, and other online-centric mediums.
    - Related is **hybrid warfare**, which includes competition short of conflict and may include active measures like cyberwarfare as well as propaganda and information warfare.
  + Influence campaigns are not the exclusive domain of cyberwarfare, however. Individuals and organizations conduct influence campaigns to turn public opinion in directions of their choosing. Even advertising campaigns can be considered a form of influence campaigns, but in general, most are associated with disinformation campaigns.
    - In general, it is important to understand the tightly coupled roles of influence campaigns and social media as part of hybrid warfare efforts by nation-state actors of all types.
* **Password Attacks:**
  + There are many ways other than social engineering and malware to obtain passwords:
    - **Brute-force attacks:**
      * Iterates through passwords until they find one that works.
      * Sometimes use a password list but can also use complex algorithms that mix word lists and other characters to account for complexity password rules.
    - **Password Spraying:**
      * A form of brute-force that attempts to use a single password or small set of passwords against many accounts.
        + Pretty good against targets that may use a specific default password or set of passwords, such as a sports team’s fan website which will have names of players and numbers.
    - **Dictionary Attack:**
      * Another form of brute-force that uses a list of words.
        + **John the Ripper** is a popular tool with word lists built in.
  + Regardless of password attack mechanism, and important differentiator between attack methods is whether they occur **online**, and thus against a live system that may have defenses in place, or if they are **offline** against a compromised or captured password store.
    - If you can capture hashed passwords from a password store, tools like rainbow tables can be very useful.
      * **Rainbow tables** are an easily searchable database of precomputed hashes using the same hashing mythology as the captured password file.
    - You can also use a password cracker against a password file as tools like Jack the Ripper can brute-force and dictionary attack different password storage formats.
    - In general, the best course of action to defend against these attacks is to use a well-constructed password that has never been hashed before. Additionally, using a **“salt and pepper”** technique where you add some more characters to an already hashed password makes it hard for a rainbow table to be used.
* **Physical Attacks:**
  + Social engineering and on-site penetration testing often go hand in hand, and thus the physical side of social engineering has its own sets of tools and techniques:
    - **Malicious Flash Drive:**
      * Attacks like these falls in two categories:
        + Attacker drops a flash drive around an area that the target may walk past, and hope the target plugs it into their computer.

Sometimes, the drive will be labeled with interesting text like “performance reviews” or “financial planning” to make it entice yet still innocent.

* + - * + They can also sometimes effectively act as a Trojan, where the devices are shipped and delivered with malware included either from the factory or through modifications made in the supply chain.

This is possible for any type of USB-connected device, not just thumb-drives.

* + - **Malicious USB Cables:**
      * These also exist but they are uncommon because require dedicated engineering to build and mostly show up in common USB appliances like keyboards or mice.
        + These can either install malware or be a keylogger.
    - **Card Cloning:**
      * Focus on capturing information from cards like RFID and magnetic stripe cards often used for entry access.
      * **Skimming:**
        + Attacks that use hidden or fake card readers or social engineering and hand-held readers to skim cards, and then employ cloning tools to use credit cards and entry access cards for their own purposes.
      * Card cloning can be difficult to detect if the cards do not have additional built-in protection such as cryptographic certificates and smart chips that make them hard to clone.
        + Magnetic stripe and RFID-based cards that can be easily cloned can be detected only by visual inspection to verify they are not the original card.
    - **Supply Chain Attacks:**
      * Attempt to compromise devices, systems, or software before it even reaches the organization.
        + The US operates the **Trusted Foundry** under the auspices of the U.S. Department of Defense to ensure that the supply chain for classified and unclassified integrated circuits, devices, and other critical elements are secure and that manufacturers stay in business and are protected to ensure devices remain trusted.
      * For individual organizations, supply chain security is much harder but buying from trusted vendors is the only solution.
* Moving to the cloud changes which attacks you are likely to worry about in a number of cases, as well as which controls you can deploy and manage.
  + Since most people outsource their cloud services to a provider, they may operate in a potentially more secure datacenter, but the ability to audit and secure the physical data yourself is no longer in your control.