Project Component Details/Planning

**Demographic Survey**

* age
* time a week spent using computer, phone, tablet
* familiar with/aware of term social engineering
* prior training/courses in cyber security

**Scenarios**

* Instructions given before scenarios
* Each scenario is independent of other scenarios
* List scenarios as Scenario 1, 2, etc. instead of giving any details as to type
* Options
  + **Baiting**- Lure with an attractive offer that plays on fear, greed, curiosity of victim
    - Company labeled flash drive in parking lot/lobby/etc. at work labeled 2020 Reports
  + **Scareware**- false alarm/threats
    - Popup banner in browser “Your computer may be infected with harmful spyware programs” Offers to install tool or direct you to a malicious site
  + **Pretexting**- obtain information through series of lies usually start by building trust
  + **Phishing**- email and text messages aimed at creating a sense of urgency, curiosity or fear
    - Email to users of an online service alerts of policy violation requiring action such as password change
  + **Quid Pro Quo-** promised benefit in exchange for information
  + **Piggybacking/Tailgating-** Following someone into a restricted area without proper authorization
    - Someone asks if you could hold open the door for them. They had an emergency with their kid this morning and forgot to grab their keycard as they left.
* Questions

Example: Would you “potential action to take such as opening email or attachment”?

* Simple levels of responding maybe, definitely, etc.
* ~~Answer with~~ 
  + ~~I have never done this and wouldn’t do it.~~
  + ~~I have never done this but I would do it.~~
  + ~~I have done this and would do it again.~~
  + ~~I have done this and wouldn’t do it again.~~
* ~~Generic question (What would you do?) and more choices of answers such as~~
  + ~~I would throw out the usb~~
  + ~~I would scan it first with antivirus program~~
  + ~~I would plug it in to my computer to see if I can find out the owner,~~
  + ~~I would give it to security~~
  + ~~I would put it in lost and found~~

**Education**

* Definition of social engineering
* How social engineering is used/related to cyber security/cyber attacks
* Tips/Best Practices to use in order to avoid being socially engineered

**Scenarios Repeated Options**

* Give exact same scenarios and questions
  + To see if they change their answers after education
    - Give a summary of what attacks were present in each scenario at end
* Give exact same scenarios and ask them if this is a potential social engineering attack
  + To see if they can identify social engineering attempts after education
    - Give answer (if attack or not) after each question or at end
* Give exact same scenarios and questions but also ask if potential social engineering attack
  + Combo of above two
    - Give answer (if attack or not) after each question or at end

**Game**

* Development
  + Using GameMaker Studio 2
* Scenarios (Action Bits)
  + Email Checking
  + Door Piggybacking
  + Password Entry
  + Mobile Push Notification
  + Office Phone Call

**Post Survey**