# CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

# Social Engineering (Part1)

- Definition
- Purpose
- Very commonly seen tricks in the social engineering
    - A couple of “principles” to conduct a social engineering
- A case study
    - A very old trick but it is still useful
    - A real case happened to my friend, many years ago
- Can ChatGPT helps bad guys in Social Engineering?

(TBD, in the next meeting)

- It lowered the difficulties for those “not very well-educated” criminals

# Definition

- In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information.
- Most of the time, because of the “lack-of-knowledge”, people easily take the bait

# Purpose

- $ and $
- User name / password
- Collecting your personal information
    - There is a “rising tide” of such a kind of activities
    - They are just trying everything to get the useful information from you
    - Sell your information to other hackers
    - Or use this information for next wave of social engineering
    - They can pretend to be the sales person from insurance companies
    - They can pretend to be the HR personnel (head hunter) from some human resource companies or some big companies
    - They can easily do that, because it is super easy to use a “fake phone number” in the VoIP

# Very commonly seen tricks in the social engineering

- All you need to do is
  - Collect the information, try to find out the target. Because different target has very different stakes, or something they really cared about.
    - Senior citizen or young people?
    - Local student or international student?
    - Female or male?
  - Make up a story and try to make everything looks reasonable
    - The story has to be logically perfect
  - Try to setup all the hardware / software if it is needed
  - Let’s do the role playing!
    - Hire the different bad guys to do their jobs (depends on different “story”). You might need these person.
      - Local cops? Prosecutor? Banker? DHS or USCIS official? Embassy officials in the US

# A couple of “principles” to conduct a social engineering

- Key principals (from Wikipedia, and this is very common in the social engineering textbooks)
  - **Intimidation (very common)**
    - Attacker (potentially disguised) informs or implies that there will be negative consequences if certain actions are not performed.
    - Example1: If you do not …, I will tell your manager.
    - Example2: If you do not …, we will hire a lawyer to sue you.
    - Example3: If you do not …, we will quickly invalidate your foreign student status in the US.

# A couple of “principles” to conduct a social engineering

- **Urgency (very common)**
  - Example1: We have special sales in our store today and everything is 50% off. We have this and that…, if you want to buy something, may I have your name and address?
  - Example2: I’m the Dean of some college in the Truman and you have a job to go to a Zoom meeting. Please send me your phone number or email
- **Consensus/Social proof**
  - Example1: See? We have several customers they can successfully reduce their health insurance by 20% yearly. Would you like to purchase our insurance?
- **Authority**
  - Example1: I’m the information security officer of this company and I found you use the computer and network of our company to chat with your friends. Give me your email account and password so I can update your security policy.

# A couple of “principles” to conduct a social engineering

- When an attack is performed, they hackers like to mix several altogether and is not limited to only one principle.
    - For example, **Intimidation + Urgency**

# A case study --- A very old trick but it is still useful

- Like I said, for hackers they like to take advantage of the people from their “lack-of-knowledge”
- For example, sometimes, when we are performing a Google search, it is likely we might get into some small websites.
  - Those websites **might get compromised already** and the owner are not aware of that
  - Assuming there is a guy, who is not the computer science student, noticed a Javascript pop-up, saying…
    - Your password in Gmail account is expired, please login again.
    - Are you sure this kind of Javascript pop-up is from Google Gmail? ^_^

# A real case happened to my friend, many years ago

- I got one good friend and he used to be my room mate 8 years ago.
  - That happens in my 1st year being a Ph.D student
- My room mate, who just traveled back from my country
- One day, he got a “mysterious” phone call. The one who said he is the official from DHS or USCIS (I didn’t remember that exactly)
- The person “enumerated” several violations
  - Your SSN was used by someone in doing some other illegal activities.
  - Your bank account was related with cases in money laundering.
  - You…
  - There will be a local police call you after within 10 minutes…
- My friend “Googled” the phone number and he found the phone number seems “real”

# A real case happened to my friend, many years ago

- After 10 minutes later, an incoming phone call is from the city police!
    - The phone number is “correct” (My friend Googled the phone number)
    - The police said, they just got notified from the officials. My friend is likely get involved in money laundering.
    - Based on all of these things, they have reasons to “invalidate” my friend’s status being an international student.
    - The cop said they can hire a lawyer to defend for my friend but he has to pay some $$ for the lawyer first.
- The interesting thing is, their speaking is totally who they are !
    - Midwest American accent!
    - The guy who plays the role being a police officer. The way of his saying totally sounds like a law enforcement person or a retired soldier.
- My friend freaked out and he called lots of his friend for help
    - By the way, he is not the CS major student ^_^

# A real case happened to my friend, many years ago

- Finally, I told my friend. You can try to make a call to the city police to verify this.
- It is eventually proved to be a scam, targeting the international student in the college town.