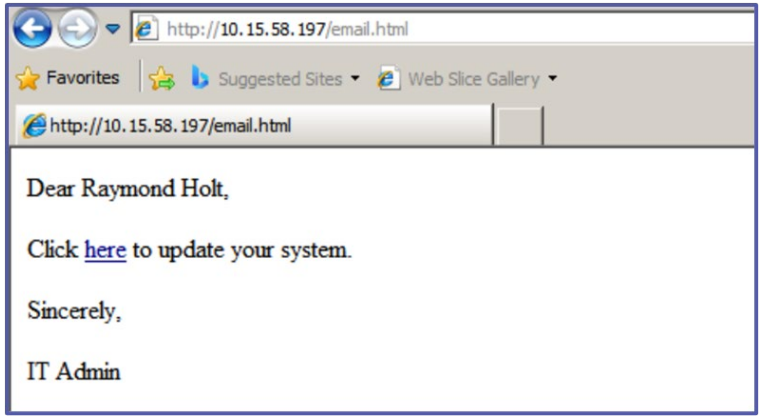
Cybersecurity

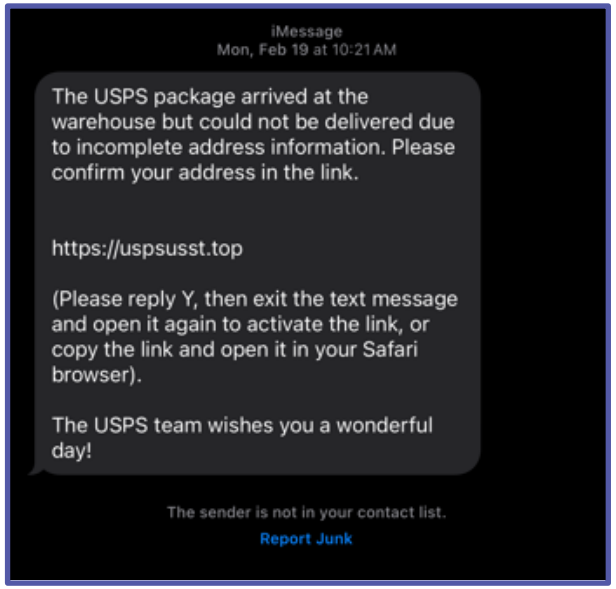
2.2.2 - Principles of Social Engineering

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Social Engineering

- Using social interactions, such as relationships, persuasion, and body language, to gain access to secretive or personal information or persuade someone to perform an action.
- Can be a single person or a group working together
- Can be performed in-person or though technical means such as texting, email, and social media



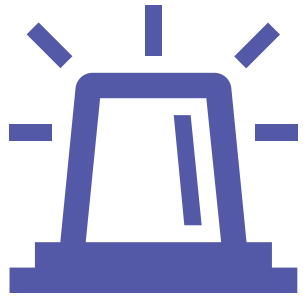


Principles of Social Engineering

- Authority
  - The malicious actor acts as an authority figure to gain information
    - “Don’t you know who I am?!”
    - “This is the police!”
- Intimidation
  - Exploits fear, usually with the idea that there are repercussions if you do not comply, or if you don’t help, bad things happen.
- Consensus/Social proof
  - Make it seem routine or as if everyone is performing the action
    - “This isn’t the first time we’ve done this.”
    - “Jose in IT did this for me last time.”

Principles of Social Engineering

- Scarcity
  - Limited time to decide or a limited opportunity to get a prize or have a task completed
- Urgency
  - You must act now with no time to think about the outcome
- Familiarity/Liking
  - Someone you know, we have common friends
    - “John put me in touch with you”
- Trust
  - Someone who is safe or is simply performing their duty
    - “I’m from IT. I’m being helpful. Let me help you.”



Defending Against Social Engineering

- Look for the principles discussed or warning signs:
  - Authority
  - Intimidation
  - Consensus/ Social Proof
  - Scarcity
  - Urgency
  - Familiarity/ Liking
  - Trust
- Recognizing key words and phrases such as “Act now,” “Supplies are limited,” “You were chosen as a winner,” etc. are all potential clues to a social engineering attack.