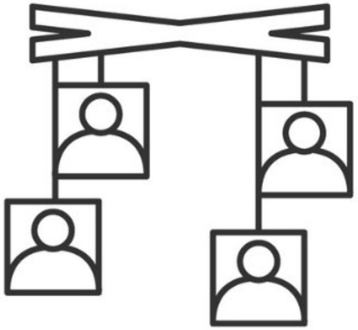
Cybersecurity

Principles of Social Engineering

CYBER.ORG

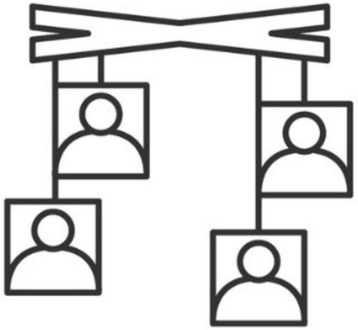
Effective Social Engineering

- Manipulating social interactions to gain access or privileged information
  - May be a team working together
  - Could be done face-to-face or online
    - “Customers” calling
    - “Suppliers” calling
    - Third party repair service (cable, elevator, fire inspection)



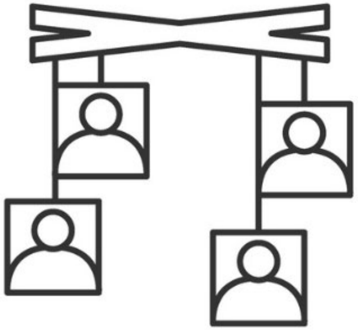
Social Engineering Principles

- Authority
  - The attacker is in charge
  - “Don’t you know who I am?!”
  - “This is the police!”
- Intimidation
  - Repercussions if you do not comply
  - If you don’t help, bad things happen.
- Consensus/Social proof
  - Make it seem routine
  - “This isn’t the first time we’ve done this.”
  - “Jose in IT did this for me last time.”



Social Engineering Principles

- Scarcity
  - Limited time to decide
  - Limited opportunity
- Urgency
  - You have to act now
  - No time to think
- Familiarity/Liking
  - Someone you know, we have common friends
  - “John put me in touch with you”
- Trust
  - Someone who is safe
    - “I’m from IT. I’m being helpful. Let me help you.”



Defending against Social Engineering

- Be on the lookout for these red flags/warning signs:
  - Authority
  - Intimidation
  - Scarcity
  - Urgency
  - Familiarity
  - Trust
- Notice these in sales tactics too
  - "Call now!" (urgency)
  - "Supplies are limited!" (scarcity)
  - "9 out of 10 agree…" (authority/trust)

How I Lost My $50,000 Twitter Username

- Naoki Hiroshima - @N
  - www.medium.com/cyber-security/24eb09e026dd
- Bad guy calls PayPal and uses social engineering to get the last four digits of the credit card on file
- Bad guy calls GoDaddy and tells them he lost the card, so he can’t properly validate. He has the last four, does that help?
  - GoDaddy let the bad guy guess the first two digits of the card
  - He was allowed to keep guessing until he got it right
  - Social engineering done really, really well

How to Steal a $50,000 Twitter Name

- Bad guy is now in control of every domain name
  - And there were some good ones
- Bad guy extorts a swap
  - Domain control for @N
  - Owner agrees
- Twitter reviewed the case for a month
  - Eventually restored access to @N
- How I lost my $50,000 Twitter Username
  - www.medium.com/cyber-security/24eb09e026dd