Defending Against Social Engineering

Tactics to help prevent a successful social engineering attack

u6350995

What is Social Engineering?

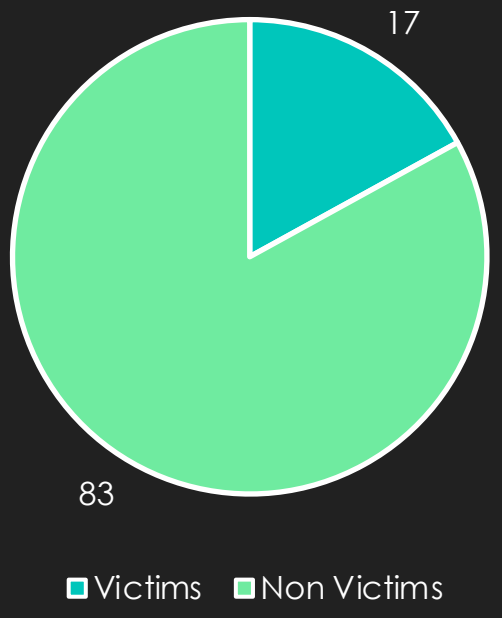
"Hacking attempts focused on human vulnerabilities in a system instead of lapses in software or hardware."





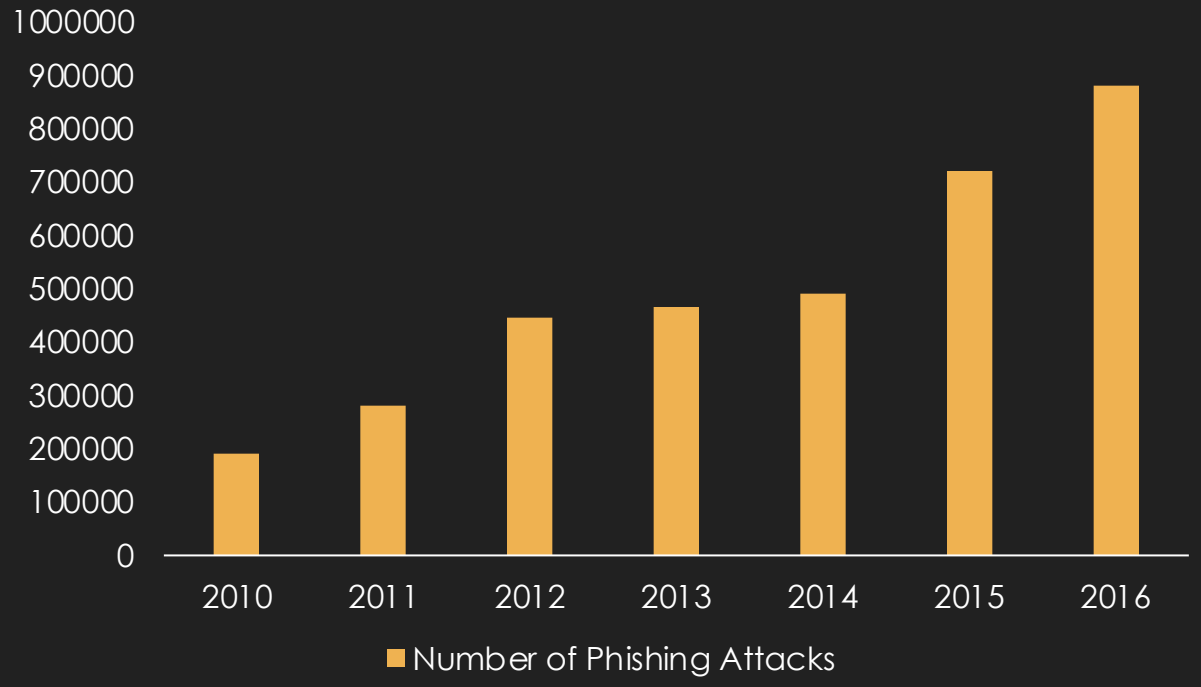
Facts and Figures

Victims of Social Engineering



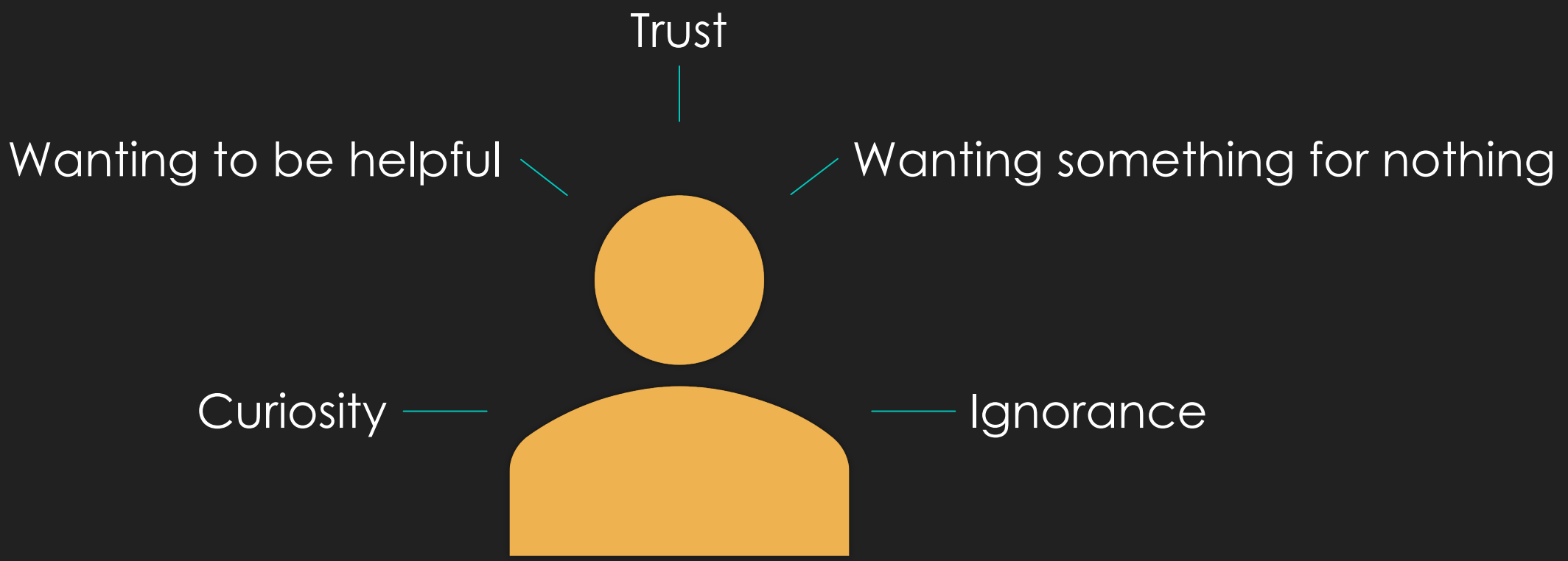
(Ashford, 2018)

Number of Phishing Attacks



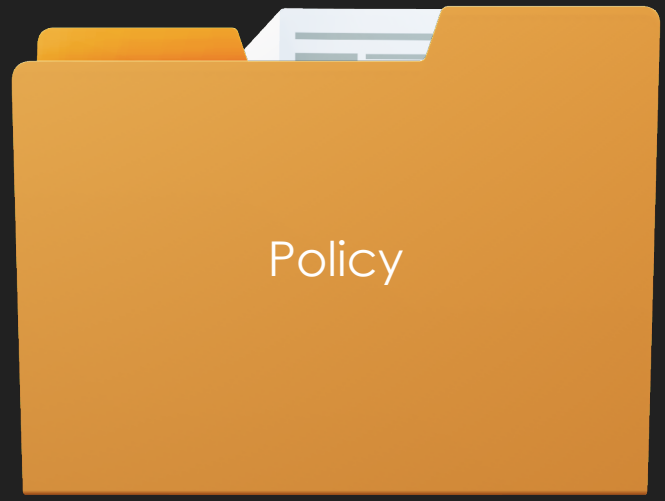
(Gupta et al, n.d.)

Why is it so Successful?

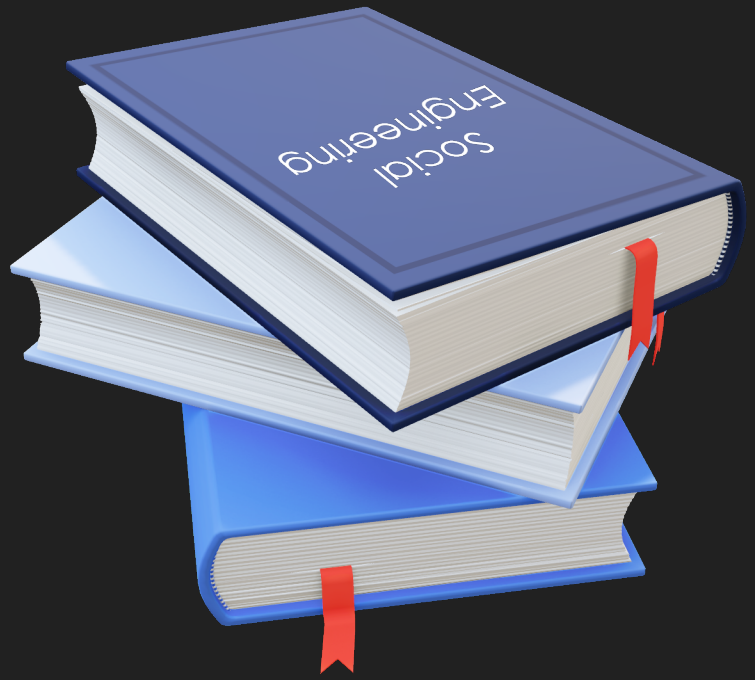


Tactic 1: Policy and Rules

- Policies can include protocols about many things like:
  - Password rules
  - Destroying of information
  - Approval of access
- Ensuring employees follow all protocols and policies is a must
- Policies can minimise damages from successful attacks



Tactic 2: Training and Knowledge



- Ensure everybody is aware of what social engineering can look like
- Ensure all training is up to date with newest attack techniques
- Ensure training is revisited so it's fresh in everyone's mind and easily remembered

Tactic 3: Traps and Tricks

- Traps rely on a great foundation of policies and training
- Land mines must be undetectable by social engineers to be effective

Summary

- Ensure to have a solid policy in place that's followed
- Keep knowledgeable about social engineering attacks
- Leave land mines throughout processes to catch any attackers