Social Engineering – Hacking the Human Element

CliftonLarsonAllen

cliftonlarsonallen.com

Agenda

- Explain attacker motivations
- Identify Social Engineering techniques
- Identify sound security measures to protect critical assets
- Summarize key areas of control your organization should have in place to improve the security posture

Social Engineering Risks

Social Engineering

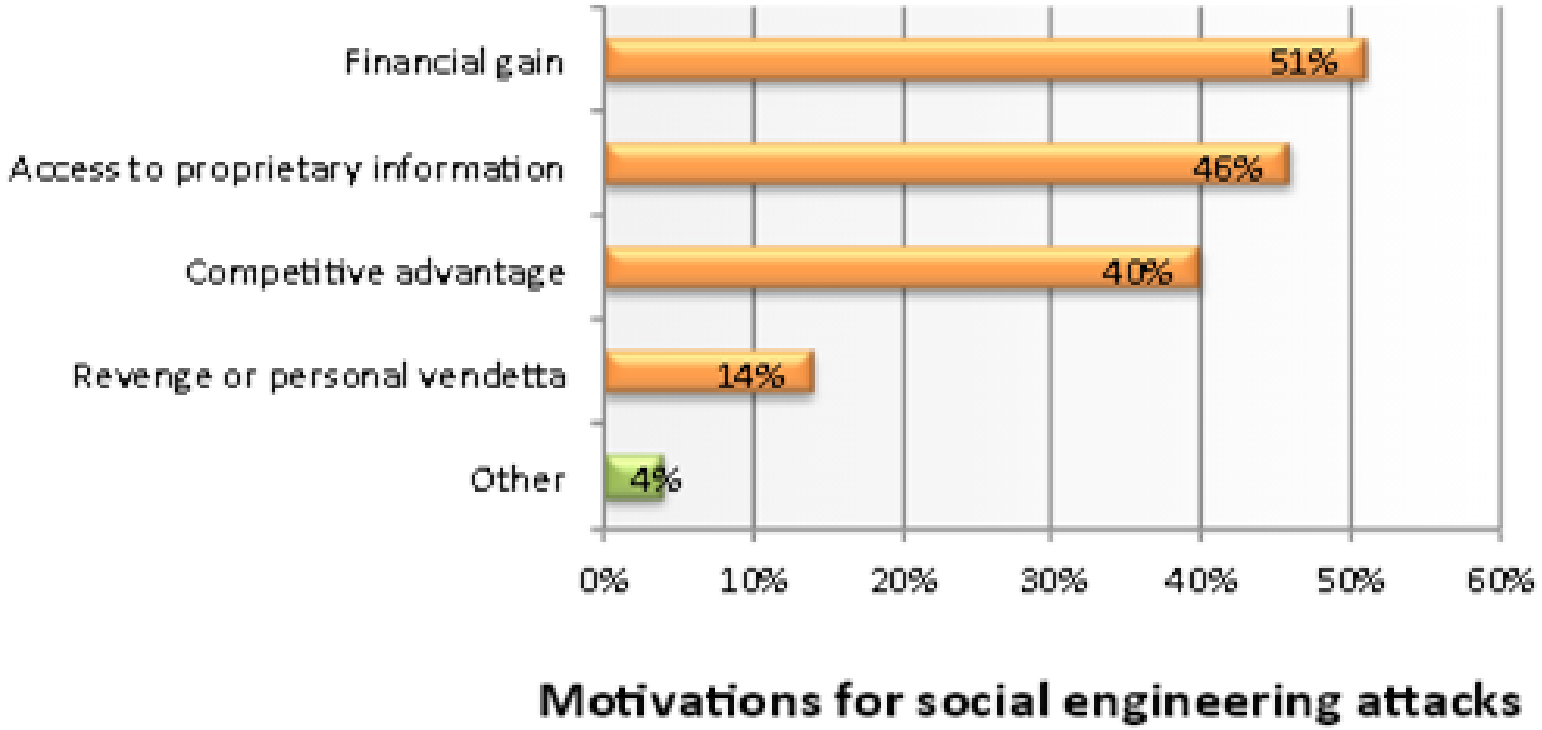
- Hacking the human
  - Simply put, Social Engineering is the exploitation of human nature.

- Highest risk for these attacks?
  - New employees [60%]
  - Contractors [44%]
  - Executive assistants [38%]

Case Study

- London gang used social engineering to gain physical access to a bank
- Installed a KVM switch attached to a wireless router
- Exploited remote access to observe and understand
- Stole two million / 125 thousand dollars during two separate heists
- Stole high value credit cards
    - Over 1 million in fraudulent purchases

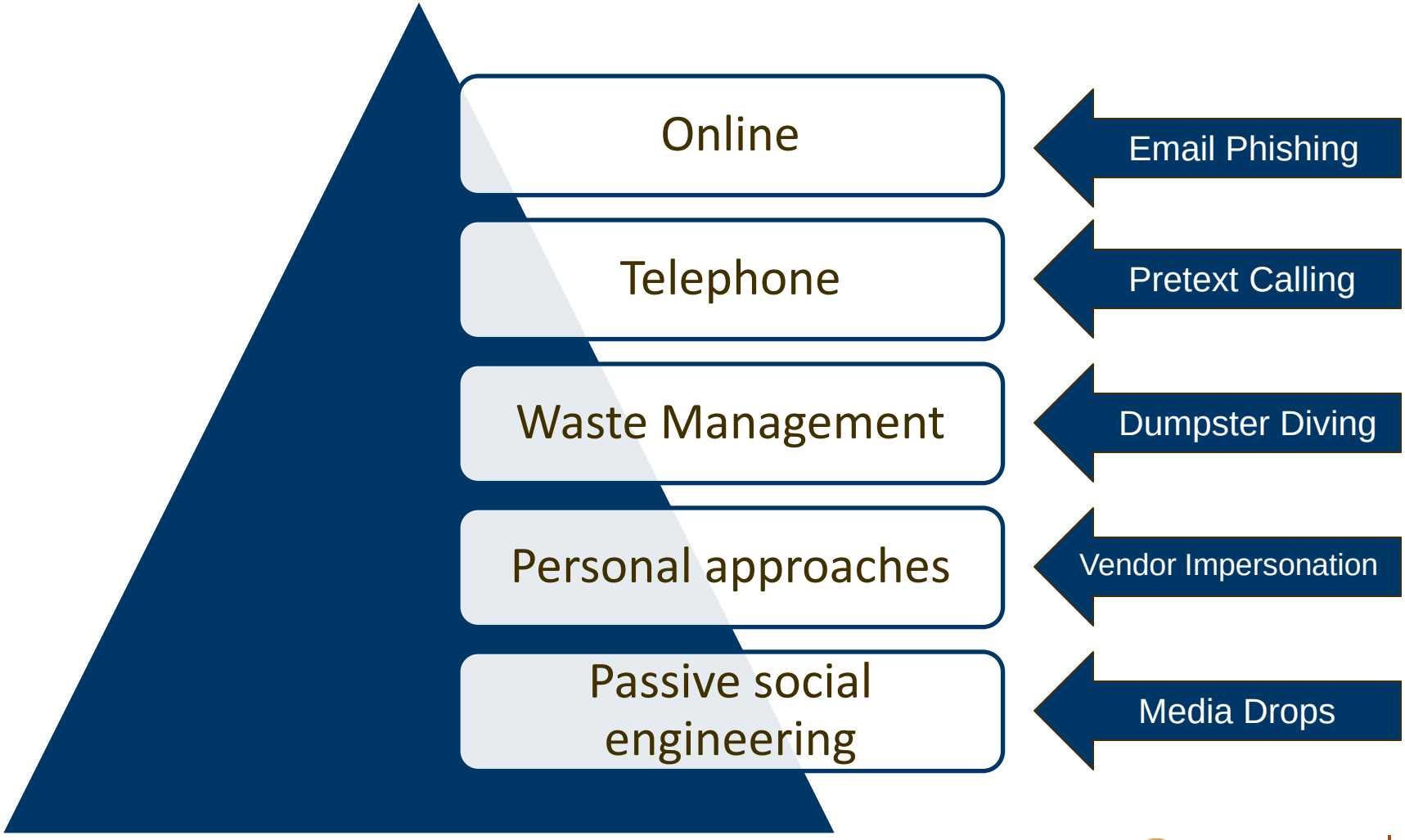
Motives



Motivations for social engineering attacks

- Motivators include knowledge, curiosity, ego, social acceptance and pure entertainment

Several different attack vectors



Information Gathering

- The ***information gathering*** process is critical. The internet can provide a host of information essential to performing a successful social engineering attack
- Google images
  - Facility access, entrances
  - Type of access control used
  - Employee information
- Social Media
- Information is a dangerous weapon. Adds legitimacy where there is none

Google Hacking

- Employee Enumeration
  - The Harvester (Edge-Security)
  - Whois lookups
  - Social Media
- Facility/Systems Information
  - Google Hacking Database

Social Engineering Techniques

Tailgating

- Gaining access to a physical access facility by means of coercion or manipulation or simple entry
- Total bypass of physical security
- Employees and vendors avoid confrontation
- Attributed to deficient or lack of access restriction, lack of security awareness

"Cigarettes are a social engineer's best friend."

Tailgating

Stop for video

Shoulder Surfing

- Direct observation
- Effective in public areas
- Access to confidential information
- Attributed to deficient privacy features, improperly restricted areas
- Privacy screens required in public areas in some industries

Vendor Impersonation

- Attempting to gain access by posing as a trusted source
- Used to gain ***trusted*** access to restricted areas
- Typically uses a pre-text (Call or email)
- Fake identification is often provided on first contact
  - Business cards can be faked easily
- Simple call back is the best defense
  - One minute of inconvenience can stop a potential breach

Phone Calls

- Objectives:
  - Gain sensitive information
  - Persuade to perform an action outside of job function
- Iterative process
- Prior information gathering is critical
- Successful due to misunderstanding or failure to apply administrative policies

Phone Calls

Stop for call recording

Dumpster Diving

- Looking for information discarded by company employees
- Typically done after hours
- Reconnaissance has likely been done prior to attack
- Attributed to lack of access restrictions, deficient disposal procedures

"One man's trash is another man's treasure."

Mitigating the Risks

Simulation and Training

- Employee awareness training
  - Policies/Procedures
  - Hands on simulated training
- Annual Testing (If not more)
  - Performed by a third party vendor

Visitor Control

- Guards
  - Human eyes are often better
- Visitors announced and escorted
- Sign visitor log
- Wear visitor badge (preferably automated access control)
- Implement compensating controls

Controlling Paper

- Locked shred bins
- Vendor picks up and shreds onsite
- Certificate of destruction is provided
- Clean desk policy
- Random walkthrough for compliance
- Employee awareness
- Secure dumpster area

Defense in Depth

- The concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack.
- ***Not enough to just secure your network***

Summary

- Layered security is best
- Management buy in
- Security awareness is key
- Validate your security
- Never stop training

Brett DeWall
Senior Consultant, Information Security
Brett.dewall@claconnect.com
507-272-8904

Zac Davis
Consultant, Information Security
Zachary.davis@claconnect.com
763-843-0163