Module - 8
Social Engineering

Social Engineering :
Psychological Manipulation of People into performing actions or divulging confidential information

Human Behaviour that lead to Social Engineering :
1. Fear 2. Urgency 3. Greed 4. Curiosity 5. Sympathy 6. Respect for Authority
7. Helpfullness

 # Types of Social Engineering :

1. **Computer Based** : No need to direct engage with victim
   Phishing Emails
   Malicious "Software Update"
   Viral Hoaxes : curious or become viral

2. **Human Based :** Attacker has to engage with the victim
   Impersonation
   Shoulder Surfing
   Tailgating

 # Reconnaissance and OSINT :

- Personal Info on companies and people can be easily discovered
- Much of it publicly available, other info can be engineered from individual
- In-Person Human Based recon can also be very effective

 # OSINT :

Open Source Intelligence (OSINT) is intelligence collected from publicly available sources. The term "open" refers to overt, publicy available sources (as opposed to convert os clandestine sources)

1. Google MAP
2. wigle.net

 # Organizational Reconnaissance :

Collecting information about an organization
- Building up a picture of the fundamentals based on basic OSINT
- Website :
  - Their Location, executives, product
- Technologies they use :
  - Observable via site, published in whitepaper or announcements
- Site Tour :
  - can provide direct access to the premises

pipl.com

 # Shoulder Surfing :

What information might be visible to casual observer ??
- Password as they're typed
- Confidential data on the screen

How might it be observed ?
- Visually via a third party
- Snapped with a camera phone

What environment pose risks ?

- Public Places (cafe's , Public Transport)
- Offices

 # Eavesdropping :

- Similar risk environment to shoulder surfing
- The threat is to information expressed verbally :
    - Passwords
    - Credit Card numbers
- Eavesdropping may also occur "on the wire"
    - Phone Tap / Man in the Middle

 # Tailgating :

The Act of Following an authorized person into an otherwise restricted area
- Door to an office building
- Pass a security point

It exploits the human weakness of helpfulness :
- It's hard for the "lead" person to reject the tailgater

This may then give the social engineer access resources such as :
- computers
- Photo copier
- Trash cans

 # Dumpster Diving :

Paper records :
- Confidential Data
- record tha could be used for impersonation or identity theft

Digital records :
- Hard Disk or thumb drives
- May Contain sensitive corporate data

-> Data breaches are a treasure trove of personal data

 # Piggybacking :

The attacker may pose as an employee and ask the authorised employee to allow him to enter along with him. He may give fake reasons like he forgot his smart badge, etc.

 # Phishing Attacks :

1. Phishing attacks are the most common form of social engineering
2. They are enormously effective
3. They exploit typical human weakness
4. Well-formed attack are enormously hard to detect and prevent

 # Phishing : It is the attempt to acquire sensitive information such as username, password, and credit card details (and sometimes, indirectly money) often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Phishing emails almost always comply with common, readily identifable patterns
- Sender and Casing
- Hyperlink Target Mismatch
- Exploiting sympathy
- Exploiting Greed
- Exploiting Fear

Phishing sites consistently exhibit suspicious traits
- Excessive information requests
- Irregular Domain Names
- Missing HTTPs : Extended Validation Certificate

 # Spearphishing :

A Phishing atrtacks specially mounted against a target organization or user, frequently tailored to the victim by representing information that us unique to them in order to build authenticity.
Spearphishing Extortion

 # Filter Evasion and Concealment Techniques :

Emails Clients and anti-virus continually evolve defences
Phishers continually evolve evasion and concealment techniques
Certain practices attempt to obfuscate the intent of the phish
- Contents are hidden behind image blocks
- Redirects : link that redirects to the phishing page , redirect also have many obfuscation technique to hide link
- Sub Domain name : Check the complete domain name
- Website Hijacking : An attacker can compromise an another legitimate website

 # Identifying Attacks with "PhishTank" :

Search your site here to get the status about your link.

 # Phishing with BEeF :
 # Creating your own Phishing attack :
use the link phish5.com to create a phishing site

 # Identity Theft and Impersonation :

1. Identity theft has a huge social cost
2. Stolen identities are an openly tradeable commodity
3. Identify theft frequently involves impersonating the victim
4. Impersonation risk every day

 # Identity Theft :

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name.

 # Impersonation :

Pretend to be someone they are not in order to get their target to do something that they don't or handover information that they don't want to share.
- Impersonate someone with authority
- Impersonate someone with Seniority
- Impersonate someone who's trusted

 # Social Engineering Countermeasures

1. Defences in the Browser and Email Client :

Explicit Defences :
Blocking of Malicious File
Warning of "deceptive sites"

Implicit Defences :
Junk/Spam Filtering
Ability to inspect Certificate

Record Destruction : If record error just thrown in the trash and not properly destroyed that presents the risk in the adversary.

Types of Records :

1. **Paper Records** :
   Shred the paper document
2. **Digital Record** :
   DBAN Software : it will delete the magnetic prints of data as well as for ssd's also
3. **Electronic Devices**
   use hammer :)

Physical Security :

2. Seperation of Duties and the Priciple of Least Privilege

1. Social Engineering
   1. Receiving a Malicious Email
   2. Browsing to the Rouge Website
   3. Victim of human-Based Social Engineering
2. Intentional Malice
   1. Disgruntled employee
   2. Financial Motivation

Separation of Duties : Separation of Duties is the concept of having more than one person required to complete the task

Principle of Least Privilege : The Principle of least privilege requires that a process, a user or a program must be able to access only the information and resources that are necessary for its legitimate purpose.

 # Multi Step and Side Channel Identity verification :

- Design the system with the expectation that the people will be compromised.
- Add Controls that are difficult to social Engineer.
- Minimize usability impact, the controls may not always be required.
- Recognize that they're not foolproof either.

 # Multi Step Verification

2FA - Two Factor Authentication
- Something you know
- Something you have

 # Logging, Auditing and Monitoring :

Who :
IP address
User Agent
What :
Resource hit
When was it Hit
Why :
Action Performed
Data Passed

 # Identity Monitoring :

- Credit Card Theft
- Credit enquiries are made under your name
- Where your personal information appears online

 # Conditioning the humans :

- People are the attack vectors - we need to condition them

- But People are fallible, volatile and frequently changing
- Most Organizational Security Training has limited effectiveness
-