Cybersecurity

Security Awareness Training

SOCIAL ENGINEERING

Social engineering is the art of convincing people to reveal confidential information. Common targets of social engineering include
helpdesk personnel, technical support executives, system administrators etc.

Behaviors Vulnerable to Attacks

- Human nature of trust
- Ignorance about social engineering
- Greediness
- Comply out of sense of moral obligation

Factors that Make companies Vulnerable to Attacks

- Insufficient security training
- Unregulated access to the information
- Several organizational units
- Lack of security policies

Phases of a Social Engineering Attack

- Research on Target Company
- Select Victim
- Develop Relationship
- Exploit the Relationship

Types of Social Engineering

- Human-based Social Engineering
- Computer-based Social Engineering
- Mobile-based Social Engineering

Human-based Social Engineering

- Impersonation
- Reverse Social Engineering
- Tailgating
- Vishing
- Dumpster Diving
- Eavesdropping
- Shoulder surfing

Computer-Based Social Engineering

- Phishing
- Pop-up Window Attacks
- Spam Mail
- Instant Chat Messenger

Mobile-based Social Engineering

- Publishing Malicious Apps
- Using Fake Security Applications
- Repackaging Legitimate Apps
- SMiShing (SMS Phishing)

Insider Threats:

- Privileged User
- Disgruntled Employees
- Terminated Employees
- Accident-Prone Employees
- Third Parties
- Undertrained Staff

Type of Insider Threats

- Malicious Insider
- Negligent Insider
- Professional Insider
- Compromised Insider

Password Attacks

- **Password Cracking:** Is the process of recovering passwords from the data transmitted by a computer system or stored in it.

Types of Password Attacks

Non-Electronic Attacks - shoulder surfing, social engineering, dumpster diving
Active Online Attacks - Dictionary and Brute forcing attack; Hash injection and phishing; Trojan/Spyware/Keyloggers and Password guessing
Passive Online Attacks: Wire sniffing; Man-in-the middle attack and replay attack
Offline Attacks: Rainbow Table Attack (pre-computed Hashes); Distributed Network Attack.

How to defend against password cracking:

- do not use the same password during password change
- do not share passwords
- do not use passwords that can be found in a dictionary
- avoid storing passwords in an unsecured location
- do not use any system's default passwords

Phishing Attack

Email is an essential part or our everyday communications. It is also one of the most common methods that hackers use to attempt to gain access to sensitive information. More than 90% of data breaches start with a phishing attack. Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful attachments or divulging sensitive information, such as passwords, bank account numbers, and social security numbers.

Phishing scams can have a number of different goals. They may attempt to:

- Target your cash and payment card data
- Gain control of your computer and local network resources
- Gain access to your Computing Account and resources

Phishing scams typically attempt to take advantage of you by:

- Delivering file attachments that can infect your computer with harmful software
- Enticing you to click on links to websites that infect your computer with harmful software
- Tricking you into sharing your username and password so hackers can gain access to your network or other sites

You can identify a phishing scam by looking for email messages that:

- Create a sense of urgency
- Invoke strong emotions, like greed or fear
- Request sensitive data
- Contain links that do not appear to match legitimate resources for the organization that is contacting you

Examples of Phishing Scams

Below you will find examples of phishing scams. You can review these examples to familiarize yourself with various phishing messages.

- Password Expiration Scam using fake Company address
- Overdue Invoice
- Important Mail Notice
- Account Expiration Notice
- Unusual Sign-in Attempt
- DHL Letter Pick-Up
- Mailbox Almost Full

THANK YOU