SMVS
Page No.
Date : / /

Phishing and Identity Theft

* Phishing :

=> Phishing is a type of cybersecurity attack that attempts to obtain data that are sensitive.

Phishing attacks usually involve Fradulent message sent via mail, social media or text message.

This message ofter appear to come from a legitmate source such as Bank or a trusted contact.

Attacker use various Method to get this trusted entities.

=> Phishing Method/Technique/Scames :

This are the main Types of Phishing Attack.

1 Email Phishing :

Most comman type of phishing where attacker send the fraudulent

emails that appear from the trusted sources.

Using this Attack, Attacker try to gain login credentials or personal information.

2 Spear Phishing:

In this Attack, Attacker aimed one organization or individuals and use detailed information about victim to create personlized message.

Using This Attack, Attacker try to gain access to sensitive information.

3 Clone Phishing:

In this Attack, Attacker create a nearly identical copy of the legitimate email or website.

Using This Attack, Attacker try to force victim into interacting with malicious content.

SMVS
Page No.
Date : / /

4 Voice Phishing :

This Phishing carried out over the phone where attacker impersonate legitimate entities to gain the sensitive information.

Attacker Try to gain personal or financial information.

5 SMS Phishing :

Phishing Scams delivered via SMS text message that include malicious links or requests for personal information.

Message may appear to be from bank or trusted entities.

6 Social Media Phishing :

This Phishing carried out through Social Media where Attacker create fake accounts or send deceptive message.

Attacks may involve Friend request, direct message or fake posts.

SMVS
Page No.
Date : / /

7 Spy Phishing :

Spy Phishing is also know as Spyware Phishing in which attacker try to install Spyware or malicious software on victim's device.

Attackers send phishing email, messages or links that appear from trusted entities.

When Victim interacted with the link or message, install spyware or malicious software on the victim's device.

=> Preventive Measure of Phishing :

1 Educate and Train Users :

Conduct regular training sessions for employee to recognize phishing attempts and understand how to respond.

2 Implement Email security Measures:

Use Advanced email Filtering

SMVS
Page No.
Date : / /

solution to detect and check phishing emails.

3 Use Strong Authentication Method :

Use Multi-Layer Authentication to add extra layer of security.

4 Maintain Up-to-Date Security Software :

Use reputable antivirus and anti-malware software and keep it updated.

5 Secure Communication Channels :

Ensure that website use HTTPS to encrypt data transmitted between user and website.

6 Verify Suspicious Requests :

If you receive unexpected request than verify with organization or person.

SMVS
Page No.
Date : / /

7 Regular Audits:

Perform Regular security audit and assessments to identify vulnerabilities.

8 Safe Practices:

Encourage safe online practices such as not sharing personal information to unsecured channels.

* Identity Theft

=> Identity Theft is the unauthorized use of someone's personal information.

Attacker try to get and use Social security number, credit card details or other identifying data.

Using this Information, Attacker can commit fraud or other cimes.

SMVS
Page No.
Date : / /

=> Types of Identity Theft:

1 Criminal Identity Theft:

Attacker use to someone other person's identity during the commission of a crime.

2 Senior Identity Theft:

Attacker use Senior person and sent information that looks to be actual and then their personal information gether.

3 Driver's License Identity Theft:

Attacker use someone else's driver's lincense information to commit fraud or other illegal activities.

4 Medical Identity Theft:

Occurs when someone use another person's medical information to obtain medical services or prescription drugs.

5 Tax Identity Theft:

Involves using someone's personal information to file fraudulent tax return and claim refunds.

6 Social Security Identity Theft:

Involves the misues of someone's social security number to commit fraud.

7 Synthetic Identity Theft:

Combines real and fake informatio to create a new identity.

8 Financial Identity Theft:

Involves stealing someone's financial information such as bank account details to make unauthorized transaction.

SMVS
Page No.
Date : / /

=> Techniques of Identity Theft

1 Pretext Calling :

Attacker use voice phishing and calling victims and pretending to be someone they are not.

2 Mail Theft :

Involves stealing mail from public mailboxes to obtain personal and financial information.

3 Phishing :

A technique where attacker send fradulent emails that appear to come from trusted entities.

4 Internet-based Attack :

Exploits the internet to execute various identity theft techniques including spyware and fake website.

5 Dumpster Diving:

The practice of sifting garbage or recycling to obtain or find document containing personal information.

6 Card Verification Value (CVV) Code Requests:

Involves attackers attemping to obtain the CVV number from credit or debit card.

=> Prevention From Identity Theft:

1 Secure Personal Information:

2 Protect Digital Information

3 Monitor Financial Accounts

4 Be Cautious with Personal Information.

5 Be awere of Phishing and Scams

6 Secure Your Digital Devices

SMVS
Page No.
Date : / /

7 Secure Online Accounts

8 Manage Personal Information

9 Take Action if You are victim