

## Chapter 4: Phishing and Identity Theft

**Phishing and Identity Theft:** Introduction, methods of phishing, phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft Textbook:1 Chapter 5 (5.1. to 5.3)

### Learning Objectives

- 1. Learn about Phishing and its related techniques
- 2. Understand different methods of Phishing
- 3. Get an overview about 3P's of Cybercrime
- Phishing, Pharming, Phoraging
- 4. What is spear phishing? How to avoid being victim of this ?
- 5. Overview of whaling
- 6. Learn about identity (ID) theft and understand ID theft as a major threat to businesses.
- 7. Understand “Myths and Facts” about ID theft.
- 8. Understand different types of ID thefts
- 9. Learn about different techniques of ID theft.
- 10. Understand about countermeasures for ID theft.

### 4.1. Introduction

- Phishing is a one of the methods towards enticing netizens to reveal their personal information that can be used for identity theft.
- ID theft involves unauthorized access to personal data.
- Section 66C of the IT Act states that “whosoever fraudulently dishonestly make use of the electronics signature, password or any unique identification features of any other person → shall be punished with imprisonment of three years. And shall also be liable for fine which extend to one lakh rupees.”
- Section 66D of the IT Act states that “whoever, by means for any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend up to three years and also liable for fine up to which extend to one lakh rupees.”
- Phishing is a social engineering tactics to trick users into revealing confidential information.

### Statistics about Phishing

- Phishing map available on [www.avira.com](http://www.avira.com)
- Virtual lab monitors the evolution of E-mail Phishing across the globe.
- The graphical illustrations available on [www.m86security.com](http://www.m86security.com)

→ Monitors origin from where Phishing E-mail are sent.

→ Facebook, HSBC (*Holdings plc is a British multinational universal bank and financial services holding company*), PayPal and Bank of America → targeted organization.

→US, India and China are → Targeted Countries.

3. Phishing attacks are monitored on a daily basis and displayed on [www.phishtank.com](http://www.phishtank.com)

4. According to May 2009 Phishing Monthly Report compiled by Symantec Security Response Anti -Fraud Team

→ Total 3,650 non-English Phishing websites were recorded in the month of May 2009.

→ Phishing URLs are categorized based on the top-level domains (TLDs). The most used TLD in Phishing websites during the month of May 2009 were ".com", ".net" and ".org" comprising 50%, 9% and 5%, respectively.

Phishing Activity Trends Report of Q4-2009 published by Anti-Phishing Working Group (APWG,) states the Phishing attack trends and statistics for the quarter. It is important to note that:

Financial organizations, payment services and auction websites are ranked as the most targeted industry.

Port 80 [HTTP] is found to be the most popular port in use followed by Port 443 [S-HTTP] and Port 8080 (WEB SERVER) among all the phishing attacks.

### **APWG (Anti-Phishing Working Group)**

#### **1. Explain the functions of Anti-phishing Working Group (04M)**

- [www. antiphishing.org](http://www.antiphishing.org), is an international consortium, founded in 2003 by David Jevans
- to bring security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies together, who are affected by Phishing attacks.
- APWG has more than 3,200+ members from more than 1,700 organizations and agencies across the globe.
- To name a few, member organizations are leading security companies such as BitDefender, Symantec, McAfee, VeriSign and IronKey.
- ING Group, VISA, Mastercard and the American Bankers Association are the members from financial industry.
- APWG is focused on eliminating identity theft that results from the growing attacks/scams of Phishing and E-Mail Spoofing.
- APWG provides a platform to discuss Phishing issues, define the scope Phishing problem in terms of costs and share information about best practices to these attacks/scams.

- a).What is Phishing? Explain with examples.  
 b). Define the term Phishing with respect to Wikipedia, Webopedia and TechEncyclopedia.

## 4.2 Phishing

### Wikipedia:

- It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication

### Webopedia:

- It is an act of sending an E-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for ID theft.
- The E-Mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers that the legitimate organization already has.
- The website, however, is bogus and set up only to steal the user's information

**Tech Encyclopedia:** It is a scam to steal valuable information such as credit card and social security numbers (SSN), user IDs and passwords.

- It is also known as "brand Spoofing."
- An official-looking E-Mail is sent to potential victims pretending to be from their bank or retail establishment.
- E-Mails can be sent to people on selected lists or any list, expecting that some percentage of recipients will actually have an account with the organization.
- Is a type of deception designed to steal your identity.
- Here the phisher tries to get the user to disclose the personal information → such as credit card numbers, passwords, account data or other information's.
- Email is the popular medium of Phishing attack and such E-Mails are also called as Spams; however not all E-mails are spam E-Mails.
- Types of E-Mails → Spam E-Mails and hoax E-Mails

### Spam E-Mails and hoax E-Mails

- Spam E-Mails → Junk E-Mails
- Identical messages sent to numerous recipients.
- Grown since 1990, → Botnet network of virus infected computers are used to send 80% of spam emails.
- Types → 1. **Unsolicited bulk E-Mails (UBE)** → email sent to large quantities
- 2. **Unsolicited Commercial E-Mail (UCE)** → for commercial purpose such as advertising.

### SPAMBOTS (UBE)

- Automated computer program and/or a script developed, mostly into "C" programming language to send Spam mails.

- SPAMBOTS gather the E-Mail addresses from the internet to build mailing list to send UE.
- These are called as web crawlers, as they gather E-mail addresses from numerous websites, chatroom conversations, newsgroups and special interest group (SIG) postings.
- → It scans for two things a) hyperlinks b) E-Mail addresses.
- The term SPAMBOT is also sometimes Used with reference to a program designed to prevent spam to reach the subscribers of an Internet service provider (ISP).
- Such programs are called E-Mail blockers and/or filters.

### **CAN-SPAM Act**

- The CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th US Congress).
- United States' first national standards for the sending of commercial E-Mail and requires the Federal Trade Commission (FTC) to enforce its provisions.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.
- The CAN-SPAM Act is commonly referred to as the "You-Can-Spam" Act because the bill explicitly legalizes most E-Mail Spam.
- In particular, it does not require E-Mailers to get permission before they send marketing messages.
- It also prevents states from enacting stronger anti-Spam protections, and prohibits individuals who receive Spam from suing spammers.

a). Differentiate between Spam and Hoax mails

### **Spam E-Mails popular medium of Phishers to scam users**

- 1. **HSBC, Santander, Common Wealth Bank** → International bank having large customer base, phishers dive deep in such ocean to attempt to hook the fish.
- 2. **eBay** → auction site often mimicked to gain personal information
- 3. **Amazon** → It was the top brand to be exploited by phishers till July 2009.
- 4. **Facebook** → Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mails.

### **Tactics used by Phishers to attack the common people using E-Mails asking for valuable information about himself/herself or to verify the details**

- 1. **Names of legitimate organizations:**

Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.

- 2. **From a real employee:**

Real name of an official, who actually works for the organization, will appear in the "from" line or the text of the message (or both). This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.

•

- **3. URLs that look right:**
- The E-Mail might contain a URL (i.e., weblink) which seems to be legitimate website wherein user can enter the information the phisher would like to steal.
- However, in reality the website will be a quickly cobbled copycat -a spoofed" website that looks like the real thing, that is, legitimate website. In some cases, the link might lead to selected pages of a legitimate website- such as the real company's actual privacy policy or legal disclaimer.
- **4. Urgent messages:**
- Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

**Here are a few examples of phrases used to entice the user to take the action.**

- **1. Verity your account:**
- The organization will never ask the user to send passwords, login names, permanent account numbers (PANs) or SSNs and other personal information through E-Mail.
- For example, if you receive an E-Mail message from Microsoft asking you to update your credit card Information, do not respond without any confirmation with Microsoft authorities- this is a perfect example of Phishing attack.
- **2. You have won the lottery:**
- The lottery scam is a common Phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work your part.
- The lottery scam often includes references to big companies, for example, Microsoft.
- There is no Microsoft lottery. It is observed that most of the phished E-Mails display the agencies/companies situated in Great Britain and hence it is extremely important for netizens to confirm/verify the authenticity of such E-Mails before sending any response.
- If " any-Mail is received displaying "You have won the lottery in Great Britain," confirm it on [www.gamblingcommission.gov.uk](http://www.gamblingcommission.gov.uk)
- If any E-Mail is received displaying your selection for any job into Great Britain, confirm/verify the details of the organization on [www.companieshouse.gov.uk](http://www.companieshouse.gov.uk) or on <http://www.upmystreet.com/local/uk.html>
- **3. If you don't respond within 48 hours, your account will be closed**
- These messages convey a sense of urgency so that you will respond immediately without thinking. A Phishing E-Mail message might even claim that your response is required because your account might have been compromised

**Let us understand the ways to reduce the amount of Spam E-Mails we receive**

- 1. Share personal Email address with limited people and/or on public websites-the more exposed to the public, the more Spam E-Mails will be received.
- 2. Never reply or open any Spam E-Mails. Any spam E-Mails that are opened or replied to inform the phishers not only about your existence but also about validity of your E-Mail address.
- 3. Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT for example, RajeevATgmailDOTcom. This usually prohibits

phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.

- 4 Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses for these sites but rather use E-mail addresses that are free from Yahoo, Hotmail or Gmail.
- 5. Do not forward any E-Mails from unknown recipients.
- 6. Make a habit to preview an E-Mail (an option available in an E-Mail program) before opening it.
- 7. Never use E-Mail address as the screen name in chat groups or rooms.
- 8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

### **Hoax Mails**

- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real. when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- [www.breakthechain.org](http://www.breakthechain.org): This website contains a huge database of chain E-Mails.
- [www.hoaxbusters.org](http://www.hoaxbusters.org): excellent website containing a large database of common Internet hoaxes.
- It contains information about all the scams.
- I maintained by Computer Incident Advisory Capability, Which is the division of US department of energy. Eg., “Breaking news” → Info → “Barack Obama refused to be the president of the US → E-mail Signature as CNN

#### **4.2.1 Methods of Phishing,**

Explain four types of methods used by the phishers to reveal personal information on Internet

1. Dragnet 2. Road-and-reel 3. Lobsterpot 4. Gillnet

##### **1. Dragnet**

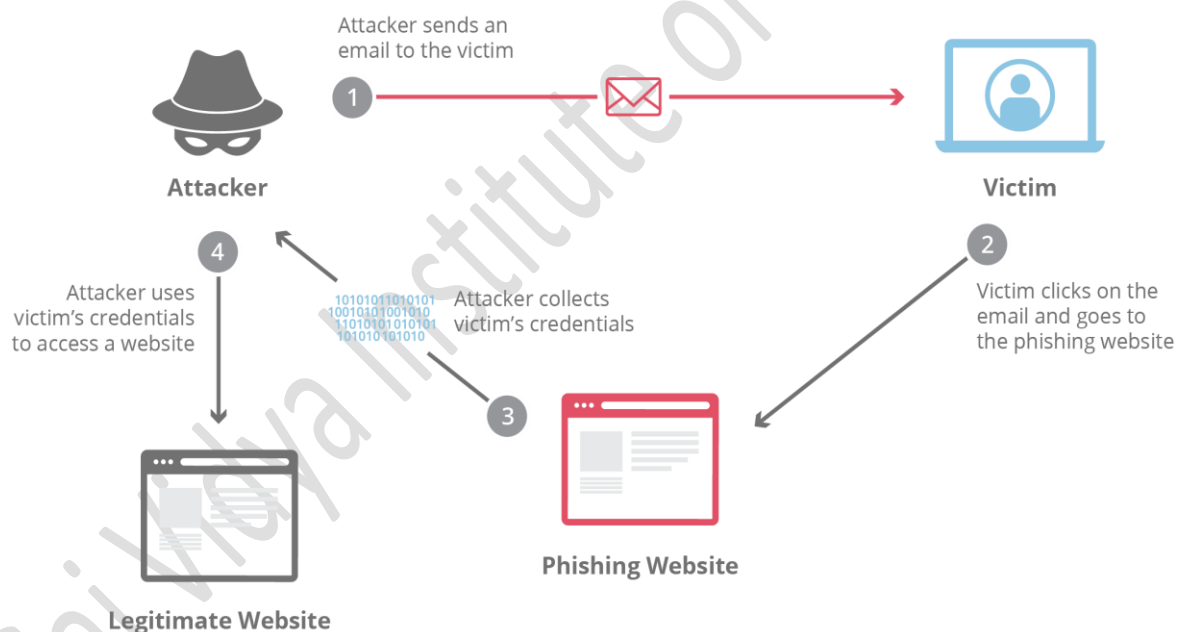
- A method involves the use of spammed E-Mails, bearing falsified corporate identification (ne., corporate names, logos and Customers of trademarks), which are addressed to a large group of people ( a particular financial institution or members of a particular auction site) to web- sites or pop-up windows with Similarly falsified identification.
- Dragnet phishers do not identify specific prospective victims in advance.
- Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims-typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop- up windows where they are requested to enter bank or credit card account data or other personal data.

## 2. Road-and-reel

- In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.
- For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the "sale" and the information is available to the phisher easily.

## 3. Lobsterpot

- This method focuses upon use of spoofed websites.
- It consists of creating of bogus/ phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out.
- These attacks are also known as "content injection Phishing."
- Here the phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears as legitimate website similar to official site. These fake sites are spoofed websites.
- Ones the netizens is into the one of these spoofed sites, he/she might willingly send personal information to the con artist. Then they use your information to purchase goods, apply new credit card or to steal your identity.



## 4. Gillnet

- This technique relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites.
- They can, for example, misuse browser functionality by injecting hostile content into another site's pop-up window.
- Merely by opening a particular E-Mail or browsing a particular website, netizens may have a Trojan Horse introduced into their systems.
- In some cases, the Malicious Code will change settings in user's systems so that users who want to visit legitimate banking websites will be redirected to a look-alike Phishing site.

- In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then they transmit those data to phisher for later illegal access to user's financial accounts.

**Box 1:**

Explain the following attack against the legitimate website.

- Website Spoofing
- XSS-Cross site Scripting
- XSRF- Cross scripting Request Forgery

**Website Spoofing (attack launched on legitimate Webpage)**

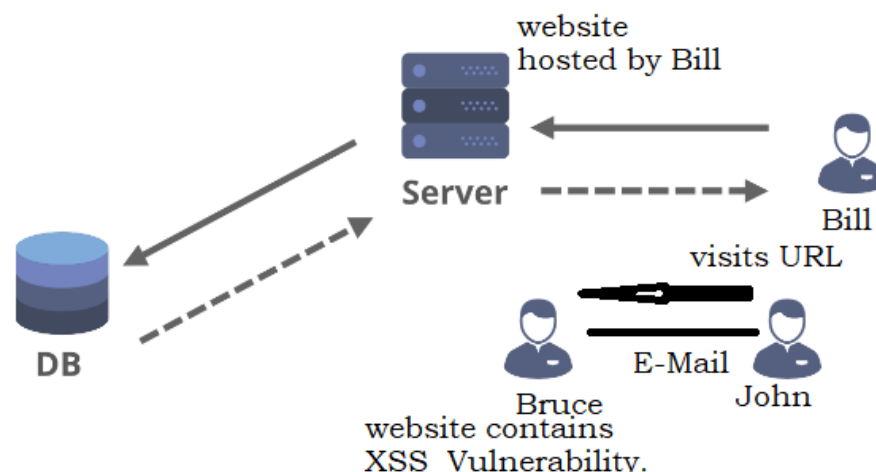
It is an act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization.

Normally, the website will adopt the design of the target website and it sometimes has a similar URL.

**XSS (Cross Site Scripting) (attack launched on legitimate Webpage)**

**Cross-site scripting (XSS):** XSS is a type of computer security vulnerability typically found in web applications that enable malicious attacker to inject client-side script into webpage viewed by other users.

An exploited cross-site scripting vulnerability can be Used by attackers to bypass access controls Such as the same origin policy.

**Cross Site Scripting(XSS)****XSRF Cross-site request forgery (attack launched on legitimate Webpage)**



CSRF is also known as a one-click attack or session riding (abbreviated as CSRF or XSRF) and is a type of malicious exploit of a website where by unauthorized commands are transmitted from a user that the website trusts.

Unlike cross-site scripting (XSS), which exploits the trust a user has on a particular site, CSRF exploits the trust that a site has in a user's browser.

### **Phishing vis-à-vis Spoofing**

- 1. Phishing is used to get the victim to reveal valuable (or at times invaluable) information about him/her. Phishers would use Spoofing to create a fake E-Mail.
- 2. Spoofing is not intended to steal information but to actually make the victim do something for phishers.
- 3. Phishing may, at times, require Spoofing to entice the victim into revealing the information about Spoofing does not always necessarily result in Phishing someone else's account

### **The Combined Attack - Phishing and Spoofing**

- Phisher sends an E-Mail, during Income Tax return filing period, from an official looking IT (Income Tax) account which is spoofed.
- The E-Mail would contain URL to download a new tax form that was recently issued.
- Once the victim clicks the URL a "virus cum Trojan Horse" is downloaded to the victim's system.
- The IT Form may seem official, but like a Trojan Horse, the payload has already been delivered.
- The virus lies in wait, logging the actions of the victim.
- Once the victim inputs certain keywords, like bank names, credit card names, social networking websites and so forth, it logs the site and the passwords used.
- Those results are flagged and sent to the phisher.
- The virus could then gather the user's E-Mail contacts and send a fake E-Mail to them as well, containing the virus.
- The phisher now has gained the required personal information as well as virus was sent, downloaded and spread to entice other netizens.

### **4.2.2. Phishing Techniques [UFWFSP]**

Discuss the various techniques used by Phishers to launch Phishing attacks  
OR  
Discuss the different Phishing techniques?

- 1. URL (weblink) Manipulation
- 2. Filter Evasion
- 3. Website Forgery
- 4. Flash Phishing
- 5. Social Phishing
- 6. Phone Phishing

## 1. URL (weblink) manipulation

- URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website.
- In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of `www.abcbank.com`, URL is provided as `www.abcbank1.com`.
- Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens.
- This makes a big difference and it directs users to a fake/bogus website or a webpage.

## Homograph Attack

- It is used by Phisher to attack on Internationalized Domain Name (IDN) to deceive the netizens by redirecting them on the phony website which look like the original website.
- ASCII has several characters and/or pairs of characters which look alike,
- Eg. 0 and "O". "l" (L lower case) and I("i" alphabet in uppercase ) [GOOGLE.COM can be registered as G00GLE.COM]
- Microsoft.com or /rnicrosoft.com
- Phisher could create and register a domain name which appears almost identical to an existing domain and takes netizens to the Phony websites.
- Phisher could easily record password or account details though spoofed websites, while passing traffic through the original websites.

## 2. Filter Evasion

- This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
- Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is not enabled by default.
- Firefox 2.0 and above has inbuilt "Google Phishing filter." duly licensed from Google. It is enabled by default.
- The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.

## 3. Website forgery

- In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands.
- As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily.
- Another technique used is known as "cloaked" URL-domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.

#### 4. Flash Phishing

- Anti-Phishing toolbars are installed/enabled to help checking the webpage content for signs of Phishing, but have limitations that they do not analyse flash objects at all.
- Phishers use it to emulate the legitimate website.
- Netizens believe that the website is "clean" and is a real website because anti-Phishing toolbar is unable to detect it.

#### 5. Social Phishing

- Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
- The victim calls the bank on the phone numbers displayed in the mail.
- The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
- Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity".
- Phisher gets the required details swimmingly.

#### 6. Phone Phishing

- Phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords.
- Mishing- Mobile Phishing attacks (Vishing and Smishing)

#### Innovative Phishing Attack Launched through Android Market

- Android: It is an open-source operating system (OS) for mobile phones and is based on Linux Kernel.
- Its popular due to the release of Google's Nexus One Phone.
- Its Market is as popular as iPhone App Store. →22,000 applications available
- <https://news.spoftpedia.co> → a malware writer succeeded to list a rogue Phishing application called 09Droid on the Android Market website.
- It found shell for mobile application, but later came to know that its being used to steal Online Banking credentials.
- Travs Credit Union (TCU) issued an alert to all consumers regarding this malware injection through 09Droid. →Application was stealing financial information of consumers.

#### 4.2.3 Spear Phishing

What is spear Phishing? Explain with examples.

**OR**

What is Whaling? Explain the difference between Whaling and Spear Phishing.

- It is method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.

- Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group.
- The message might look like as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company it could include requests for usernames or passwords.
- Unfortunately, through the modus operandi of the Spear phishers, the E-Mail sender information has been faked or spoofed.
- While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company's entire computer system.
- If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.
- Spear Phishing also describes scams that target people who use a certain product or website.
- Scam artists use any information they can to personalize a Phishing scam to as specific a group as possible.
- Thus, "Spear Phishing is a targeted E-Mail attack that a scammer sends only to people within a small group, such as a company".
- The E-Mail message might appear to be genuine, but if you respond to it, you might put yourself and your employer at risk.
- You can help avoiding Spear Phishing scams by using some of the same techniques you have already used to help avoid standard Phishing scams

#### Whaling

- It is a Specific form of Phishing and/or Spear Phishing.
- Targeting executives from the top management in the organizations, in private companies.
- The objective is to swindle the executive into revealing confidential information.
- E-Mails sent here are designed to masquerade as a critical business E-Mail sent from a legitimate business authority.
- It has falsified industry wide concern and is meant to be tailored for executives.
- Whaling Phisher have forged official looking FBI subpoena E-mails. And claimed that manager needs to click a link and install special software to view subpoena.
- In 2008 FBI 20,000 corporate CEO were attacked. More than 2000 people clicked on the whaling link. Linked software was a keylogger that secretly recorded the CEO passwords and forwarded those passwords to the Phisher men.

#### Avoiding Spear Phishing Scams

1. Never reveal personal or financial information in a response to an E-Mail request, no matter who appears to have sent it.
2. If you receive an E-Mail message that appears suspicious, call the person or organization listed in the From line before you respond or open any attached files.
3. Never click links in an E-Mail message that requests personal or financial information. Enter the web address into your browser window instead
4. Report any E-Mail that you suspect might be a Spear Phishing campaign within your company.
5. You can use the phisher filter-it scans and helps identify suspicious websites, and provides up-to the hour updates and report about known phishing sites.

#### **4.2.4. Types of Phishing Scams**

Explain the different types of Phishing scams.

OR

**Discuss various types of Phishing Scams. (10M)**

##### **1. Deceptive Phishing →**

- Phishing scams started by broadcasting deceptive E-Mail messages with objective of ID theft.
- E-Mails are broadcasted to a wide group of netizens asking about the need to verify banking account information/system failure requiring users to re-enter their personal information.
- The netizens easily get enticed and reveal their information by responding to these E-Mails and/or clicking on weblinks or signing onto a fake website designed by the phisher.

##### **2. Malware-based Phishing →**

- It refers to scams that involve running Malicious Code on the netizens system.
- Malware can be launched as an E-Mail attachment or as a downloadable file from a website or by exploiting known security vulnerabilities.
- For example, small and medium businesses are always found to be ignorant to keep their operating systems (OS) antivirus software up to date with latest patch updates released by vendors.

##### **3. Keyloggers →**

- A small integrity program to steal information sends to phisher, keylogger log, to the phisher through the Internet.
- The keyloggers can also be embedded into netizen's browser as a small utility program which can start automatically when the browser is opened or can be embedded into system holes as device drivers.

##### **4. Session hijacking →**

- It is an attack in which netizens' activities are monitored until they establish their bonafide credentials by signing into their account or begin the transaction and at that point the Malicious Code takes over and comport unauthorized actions such as *transferring funds without netizen's knowledge*.

##### **5. In-session Phishing →** another parallel session in the same browser.:

- It is a Phishing attack based upon one web browsing session being able to detect the presence of another session (such as visit to an online banking website) on the same web browser and then a pop-up window is launched that pretends to be opened from the targeted session

##### **6. Web Trojans →**

- Pops up to collect netizen's credentials and transmit them to the phisher while netizens are attempting to log in. Such pop-ups are usually invisible

##### **7. Pharming →** I

- It is a new threat evolved with a goal to steal online identity of the netizens and Pharming
- Is known as one of the "P" in cybercrime
- In Pharming, following two techniques are used:
  - **Hosts file poisoning:**
  - The most popular operating system (OS) in the world is Windows and It has "host names" in their "hosts" file.

- A simple text file was used in web address during early days of the Internet. (before DNS)
- Phisher used to "poison" the host file to redirect the netizen to a fake/bogus Website, designed and developed by the phisher, which will "look alike the original website, to Steal the netizen's personal information easily.
- **DNS-based Phishing:**
- Phisher tampers with a DNS so that requests for URLs or name service return a fake address and subsequently netizens are directed to a fake site.
- Netizens usually are unaware that they are entering their personal confidential information in a website controlled by phishers and probably not even in the same country as the legitimate website.
- DNS-based Phishing is also known as DNS hijacking.
- Along with this attack Click Fraud is an advanced form of technique evolved to conduct Phishing scams.

#### **8. System configuration attacks:**

- Phisher intrude into netizens system to modify settings for malicious purposes.
- For example, URLs saved under favourites in the browser are modified to redirect the netizen to a fake/bogus "look alike" websites (i.e., URL for a bank can be changed from "www.xyzbank.com to www.xyzbanc.com.).

#### **9. Data theft →**

- Critical and confidential data getting stolen is one of the biggest concerns in the modern times.
- As more information resides on the corporate servers and the web attackers have a boom time because taking away/copying information in electronic form is easy.
- Unsecured systems are often found to be inappropriately maintained from cybersecurity perspective.
- When such system is connected, the web servers can launch an attack with numerous methods and techniques. Data theft is used in business espionage.

#### **10. Content injection Phishing:**

- In these types of scams, phisher replaces the part of the content of a legitimate website with false content.

#### **11. Man-in-the middle Phishing:**

- Phisher is positioned himself in between the netizens and legitimate website or system.
- Phisher records the input being provided by the netizen but continues to pass it on to the web server so that netizens transactions are not affected.

#### **12. Search engine Phishing:**

- It occurs when phishers create websites with attractive sounding offers (often found too good to be true) and have them indexed legitimately with search engines.
- Netizens find websites during their normal course of search for products or services and are trapped to reveal their personal information.
- For example, phishers set up fake/ bogus banking websites displaying an offer of lower credit costs or better interest rates than other banks offer of lower credit costs or better interest rates than other banks.

### 13. SSL certificate Phishing:

- Phishing is an advanced type of scam. Phishers target web servers with SSL certificates to create a duplicitous website with fraudulent webpages displaying familiar "lock" icon.
- It is important to note that, in such types of scams, SSL certificates are always found to be legitimate as they match the URL of the fake pages that are mimicking the target brands but in reality, had no connection to these brands displayed.
- It is difficult to recognize such websites; however, smart netizens can detect such deception after reviewing the certificate and/or whether the website has been secured with an extended validation SSL certificate.

### Three P's of Cybercrime -Phishing, Pharming & Phoraging

- **Pharming:** It is an attack aiming to redirect a website traffic to another bogus websites.
- Pharming is a neologism based on farming + Phishing.
- Concern for businesses hosting E-Commerce and Online banking websites.
- Here attacker cracks vulnerability in an ISP, DNS server and hijacks the domain name of a commercial site.
- **Phoraging:** It is defined as a process of collecting data from many different online sources to build up the identity of someone with the ultimate aim of committing the identity theft.
- It is information diving-searching for information.
- Now a days looking for matrimonial sites, social networking sites for professional to reveal personal information.
- **Advanced Form of Phishing- Tabnapping or Tabjacking**
- Tabs are web browser tabs.
- Browser Tabs that are not in use are called as napping.
- Most often netizens work with multiple tabs, open with multiple web browsing sessions on each one. Its takes hour together time.
- Phishers have identified a way to invade the browser tabs and change it to a page designed to steal information.
- If a page is ideal for a particular time period, and then phisher redirects the victim to a phished webpage.
- Phisher judge the idle webpages based on mouse movement, scroll bar movement and keystrokes.
- Websites from banking/financial institutes as well as popular sites like Gmail, Facebook, Instagram, WhatsApp are the primary targets.

### **DNS Hijacking (session hijacking)**

- **DNS Hijacking:** It is also known as DNS redirection and it is the practice of redirecting the resolution of Domain Name Server (DNS) names to rogue DNS servers.
- An illegal change to a DNS server directs URL to a different website.
- In some cases, new websites URL may have done one different letter in the name that might go unnoticed. The bogus website might offer similar and/or competing products for sale.
- DNS is used to interpret domain names such as www. <domainname>.com into an IP address. The IP address consists of numbers such as xxx.xx.xxx.x (192.60.168.1) that give a domain a unique identification

- It is used by attacker with malicious intent who redirect or hijack the DNS addresses to bogus DNS servers for the purpose of injecting malware into your PC, Promoting Phishing scams, advertising on high traffic website and other criminal related activity.
- DNS hijacker use Trojan to exchange the legitimate DNS server assignment by the ISP with a manual DNS server assignment from a bogus DNS server.
- When netizens visit the reputable websites with legitimate domain names, they are automatically hijacked to a malicious website that is disguised as the legitimate one.
- Switch from the legitimate DNS server to bogus DNS server goes unnoticed by both the netizens and the legitimate website owner.
- This opens up the malicious website to perform any criminal act that the phisher wishes because the netizens thinks that they are in the real website.

### **Click Fraud (session hijacking)**

- It is a type of Internet crime that occurs in pay-per-click online advertising when a person automated script or computer program imitates a legitimate user of a web browser clicking on an advertisement (ad) for the purpose of generating a charge per click without having actual interest in the target of the ad's link.
- Click Fraud is the subject of some controversy and increasing litigation because of the advertising networks being a key beneficiary of the fraud.
- It is an illegal practice that occurs when individuals click on a website click through advertisements to increase the payable number of clicks.
- Illegal click can be performed by clicking the Advertising hyperlinks or by using automated software or online Bots that are programmed to click these banner ads and pay per click text ad links.
- Research has indicated that Click Fraud is perpetrated by individuals who use Click Fraud to increase their own personal banner ad revenues and also by companies who use Click Fraud as a way to deplete a competitor's advertising budget.
- Visit the weblinks mentioned below to explore more on Click Fraud:
  1. Exposing Click Fraud: <http://news.cnet.com/Exposing-click-fraud/2100-10243-5273078>
  2. The dark side of online advertising. [http://www.businessweek.com/magazine/content/06\\_40/b4003001.html](http://www.businessweek.com/magazine/content/06_40/b4003001.html)

### **SEO (Search Engine Optimization) Attacks Beware While Searching through Search Engines**

- SEO is the practice of maximizing the volume or quality of traffic to a website from search engines Techniques used for Black hat SEO attacks
- Techniques used for Black hat SEO attacks
  1. Fake antivirus
  2. SEO page
  3. SEO poisoning
  4. Black hat SEO kits

### **Distributed Phishing Attack (DPA)**

- It is an advanced form of Phishing attack that works as per victim's personalization of the location of sites collecting credentials and a covert transmission of credential to a hidden coordination centre run by the phisher.
- Here a large number of fraudulent web hosts are used for each set of lured E-Mails.



#### 4.2.5 Phishing toolkits and Spy phishing

Explain Phishing Toolkits with examples.

A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics displayed on these websites.

These developed by individual or groups and sold for money.

Phisher use hypertext pre-processor (PHP) to develop the phishing kits.

These are Do-It Yourself Phishing kits-information sent to recipients other than the authors of Phishing kits) other than the intended users.

#### Distributed Phishing Attack (DPA)

- It is an advanced form of Phishing attack that works as per victim's personalization of the location of sites collecting credentials and a covert transmission of credential to a hidden coordination centre run by the phisher.
- Here a large number of fraudulent web hosts are used for each set of lured E-Mails.

#### 4.2.5 Phishing toolkits and Spy phishing

- A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics displayed on these websites.
- These developed by individual or groups and sold for money.
- Phisher use hypertext pre-processor (PHP) to develop the phishing kits.
- These are Do-It Yourself Phishing kits-information sent to recipients other than the authors of Phishing kits) other than the intended users.
- Rock Phish: It is a Phishing toolkit popular in the hacking community since 2005. It allows non-techies to launch Phishing attacks.
- The kit allows a single website with multiple DNS name to host a variety of phished webpages, covering numerous organizations and institutes
- Xrenoder Trojan Spyware: It resets the homepage and/or the search settings to point to other websites usually for commercial purposes or porn traffic.
- Cpanel Google: It is a Trojan Spyware that modifies the DNS entry in the host's file to point to its own website.
- If Google gets redirected to its website, a netizen may end up having a version of a website prepared by the phisher.

#### 4.2.6 Phishing countermeasures

What are countermeasures to prevent malicious attacks. (06M)

1. The countermeasures will prevent malicious attacks that phisher may target to gain the unauthorized access to the system to steal the relevant personal information about the victim, from the system.
2. It is always challenging to recognize/Judge the legitimacy of a website while Googling (i.e., surfing on the Internet) and find it more intriguing while downloading any attachment from that particular website.

3. explained in Table 4.1
4. Table 4.1 How to avoid being victim of Phishing attack

SL. NO.	Security Measures
1	Keep antivirus up to date
2	Do not click on hyperlinks in E-Mails
3	Take advantage of anti-Spam software
4	Verify https (SSL)[ secure Socket layer ]
5	Use anti-Spyware software
6	Get educated
7	Use the Microsoft Baseline Security Analyzer (MBSA)
8	Firewall
9	Use backup system images
10	Do not enter sensitive or financial information into pop-up windows
11	Secure the hosts file
12	Protect against DNS Pharming attacks

### **How to Judge/Recognize Legitimate Websites**

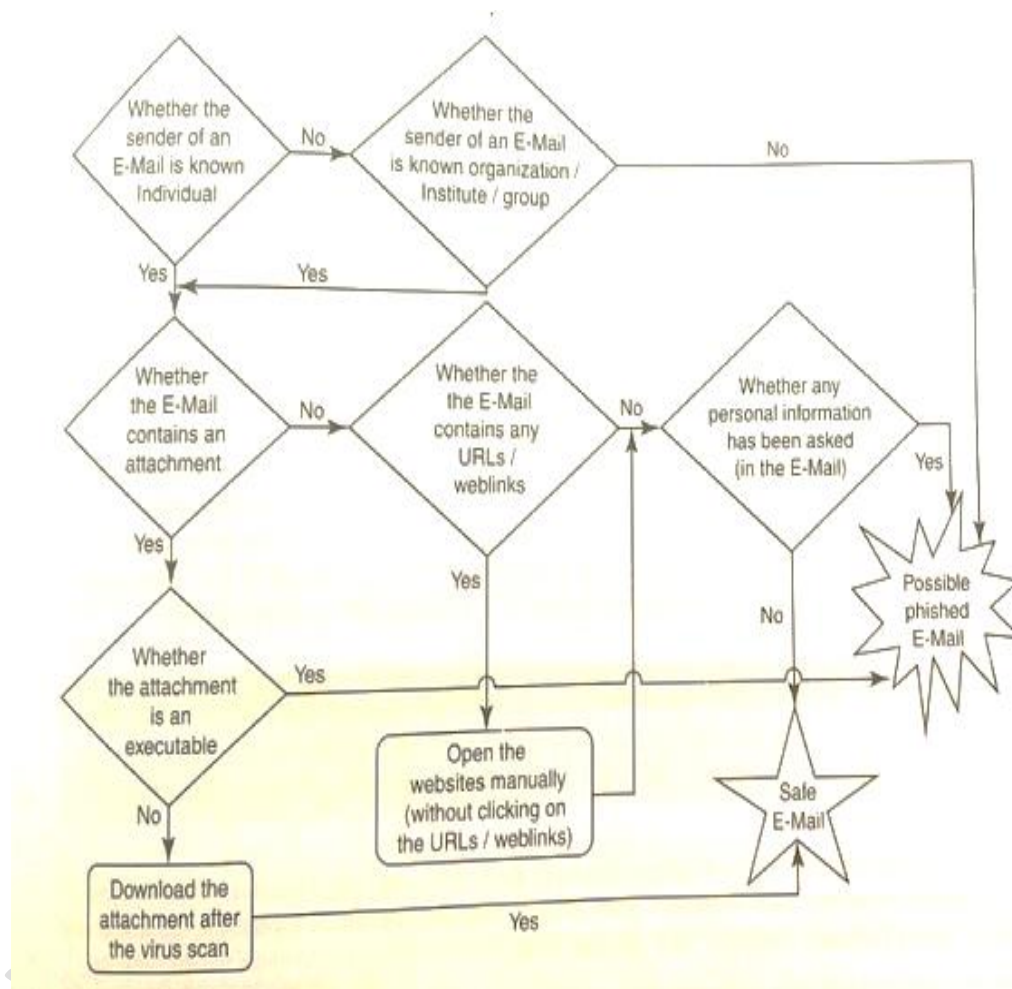
- ScanSafe ([www.scansafe.com](http://www.scansafe.com)) was the first company in the world to offer web security. Scandoo ([www.Scandoo.com](http://www.Scandoo.com)) scans all search results' to protect the user from visiting false websites (i.e., websites that spread malicious viruses or Spyware as well as protecting the user from viewing offensive content).
- Presently this Site is not available as improvements for add-on features based on users' feedback is underway.
- McAfee Site Advisor software ([www.siteddvisor.com](http://www.siteddvisor.com)) is a free web security plug-in that provides the user with red, yellow and green website security ratings based on the search results.
- These ratings are based on tests conducted by McAfee after looking for all kinds of threats such as to name a few Phishing sites, E-Commerce vulnerabilities, browser exploits, etc.

### SPS (Sanitizing Proxy System) Algorithm to Thwart Phishing Attacks

- Phishing attack comprised two phases: a) attraction and b) acquisition
- Characteristics of SPS:
  1. Two-level filtering
  2. Flexibility of the rule set

3. Simplicity of the filtering algorithm
4. Accountability of HTTP response sanitizing
5. Robustness against both misbehavior of novice users and evasion techniques

Explain the flowchart of Phishing attacks.



**Fig: Phishing Attack flow chart**

### 4.3 Identity Theft

What is identity theft? Explain with examples. (08M)

How can information be classified? (06M)

What are the different techniques of Identity theft?(08M)

- It happens when someone uses your personally identifying information. Like your name, social security number, or credit card number, without your permission to commit fraud or other crimes.

- OR
- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 60D)
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Theft Resource Center (ITRC), with the objective to extend the society to spread awareness about this fraud

#### **FTC→ Mentioned the Prime Frauds**

- Credit card fraud (26%): The highest rated fraud that can occur is when someone acquires the victims credit card number and uses it to make a purchase.
- Bank fraud (17%): Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft.
- Employment fraud (12%): In this fraud, the attacker borrows the victim's valid SSN to obtain a job.
- Government fraud (9%): This type of fraud includes SSN, driver license and income tax fraud.
- Loan fraud (5%): It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.

#### **Identity Theft Information**

- 66% of victim's personal information is used to open a new credit account in their name.
- 28% of victim's personal information is used to purchase cell phone service.
- 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief.

#### **Identity Theft Resource Center (ITRC)**

- Identity Theft Resource Center (ITRC) is a non-profit, nationally respected organization situated at San Diego, CA USA dedicated exclusively to the prevention of identity theft.
- The ITRC provides support to the society for public education about identity theft.
- The organization also provides advice to governmental agencies, law enforcement agencies and business organizations about evolving and growing threat of identity theft.

Myth	Fact
There's no way to protect yourself from identity theft	The risk of identity theft can be minimized by taking preventive measures.
Identity theft is only a financial crime	Other identity theft also available and are dangerous, medical ID theft of Personal medical record, for false insurance claims.
It's my bank's fault if I become a victim of identity theft	Majority identity theft begins elsewhere, PI may be stolen from lost or stolen wallet, check book, credit or debit card (low tech tool) High tech tool, hacking, Phishing, skimming)
It is safe to give your personal information over the phone if your caller ID confirms that it is your bank	Caller ID Spoofing can be done, don't give any information to any one.
Checking your credit report periodically or using a credit monitoring service is all you need to do to protect yourself from identity theft.	One can get free credit report in the US from each of the credit bureaus from <a href="http://www.AnnualCreditReport.com">www.AnnualCreditReport.com</a>
My personal contact information (mailing address, telephone number, E-Mail address, etc.) is not valuable to an identity thief.	Any information that could be used by a thief to impersonate you should be protected.
Shredding my mail and other personal documents will keep me safe.	Shredding documents that contain personal information before you throw them away is a great way to protect yourself from "dumpster diving," which occurs when attackers search the trash for personal information.
I don't use the Internet, so my personal information is not exposed online.	Your personal information appears in more places than you might realize whether its your medical records, a job application or a school emergency contact form. Many of these records are kept in electronic databases and transmitted online.
Social networking is safe.	They can be dangerous when it comes to your identity..

	privacy controls offered by most of these sites, and use common sense.
It is not safe to shop or bank online	Like social networking, shopping and banking online are safe as long as you use common sense and make good choices about where and how you do it. Observe the webpage is legitimate.

#### **4.3.1. Personally Identifiable Information (PII)**

The fraudster always has an eye on the information which can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. PII has four common variants based on personal, personally, identifiable and identifying.

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity :

1. Full name,
2. National identification number (e.g., SSN
3. Telephone num
4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

Identify an Individual.

- 1. First or last name;
- 2. age;
- 3. country, state or city of residence;
- 4. gender;
- 5. name of the school/college/workplace
- 6. job position, grades and/or salary;
- 7. criminal record.

Classification of Information can be of two types namely:

#### **Non-classified information**

1. Public information (public record)
2. Personal information (addresses, telephone numbers, E-mail addresses)
3. Routine business information
4. Private Information (SSN, credit card numbers and other financial information.)

5. Confidential business information (sales plans, patentable innovation, new product plans)

### **Classified information**

- **Confidential** → Information about strength of armed forces and Technical Information about weapons
- **Secret** → National security policy, military plans or Intelligence operations
- **Top Secret** → Damage national security, vital defence plans and cryptographic Intelligence system

### **4.3.2 Types of Identity Theft**

#### ***What are the different types of Identity theft?***

- 1. Financial Identity Theft
- 2. Criminal Identity Theft
- 3. Identity Cloning
- 4. Business Identity Theft
- 5. Medical Identity Theft
- 6. Synthetic Identity Theft
- 7. Child Identity Theft

### **Financial Identity Theft**

- In total, 25 types of financial ID thefts are investigated by the US Secret Service.
- Financial identity occurs when a fraudster makes a use of someone else's identifying details, such as name, SSN and bank account details, to commit fraud that is detrimental to a victims finances.

### **Criminal Identity Theft**

- It involves taking over someone else's identity to commit a crime such as enter into a country, get special Permits, hide one's own identity or commit acts of terrorism. These criminal activities can include:
  - 1 Computer and cybercrimes;
  - 2. organized crime;
  - 3. drug traffickings
  - alien smugglings
  - 5. money laundering.

### **Identity Cloning**

- Identity cloning may be the scariest variation of all ID theft.

- Instead of stealing the personal information for financial gain or committing crimes in the victims name, identity clones compromise the victims life by actually living and working as the victim.
- ID clones may even pay bills regularly, get engaged and married, and start a family.
- In summary, identity cloning is the act of a fraudster living a natural and usual life similar to a victim's life, may be at a different location.

### **Business Identity Theft**

- "Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance n
- comparison with individual's ID theft
- A fraudster rents a space in the same building as victims office
- A fraudster rents a space in the same building as victims office
- Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams.

### **Medical Identity Theft**

- India is known for medical tourism.
- Thousands of tourists visit India every year, getting their medical problems attended (surgeries, total health check-up Kerala massage etc.,)
- Because of Good Quality and Reasonable in Price in medical services.
- protected health information (PHI).
- The stolen information can be used by the fraudster or sold in the black market to people who "need them."

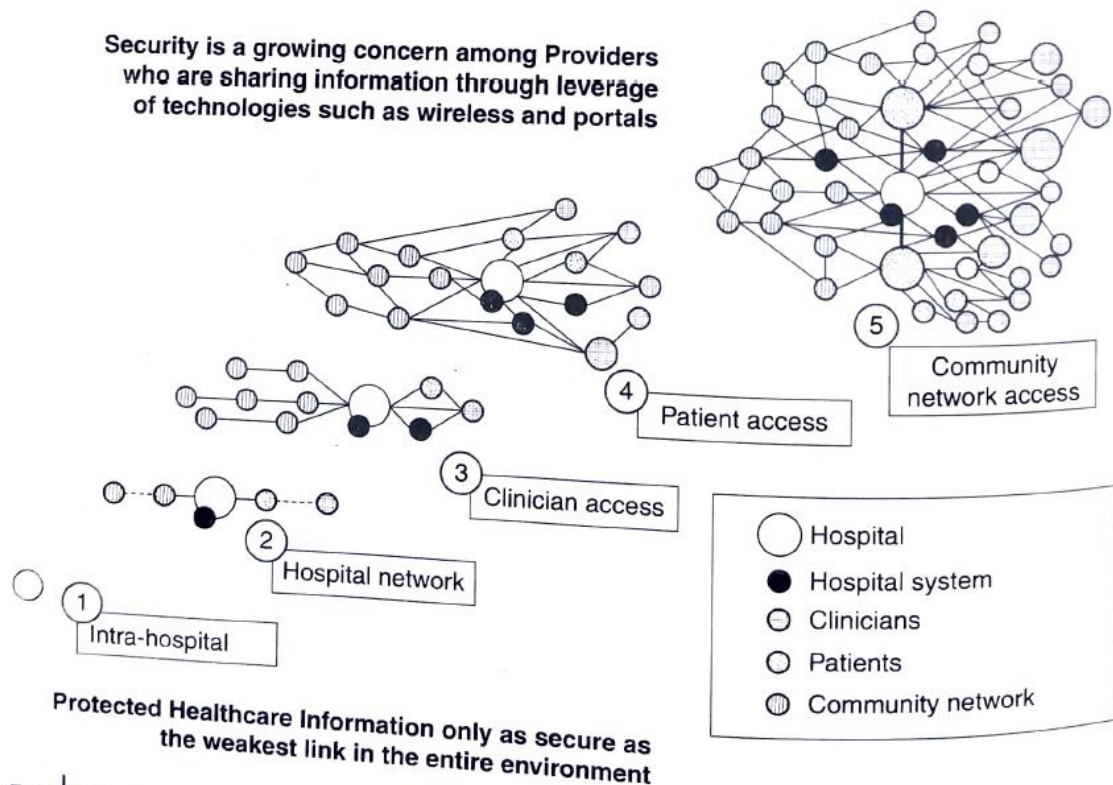
### **Synthetic Identity Theft**

- This is an advanced form of ID theft in the ID theft world.
- The fraudster will take parts of personal information from many victims and combine them.
- The new identity is not any specific person, but all the victims can be affected when it is used.

### **Child Identity Theft**

- Parents might sometimes steal their children's identity to open credit card accounts, utility accounts, bank accounts and even to take out loans or secure leases because their own credit history is insufficient or too damaged to open such accounts.





**Fig.** Medical domain interconnected entities

### 4.3.3 Techniques of ID Theft

#### Human-based methods

- **Direct access to information:** People who have earned a certain degree of trust (ex., house cleaners, babysitters, nurse, friends or roommates) can obtain legitimate access to a business or residence to steal information.
- **Dumpster diving:**
  - Retrieving documents from trash bins is very common and is called dumpster diving.
- **Theft of a purse or wallet:** Wallet often contains bank credit cards, debit cards, driving licence medical insurance identity card and what not.
- Pickpockets work on the street as well as in public transport and exercise rooms to steal the wallets and in turn sell the personal information.
- **Mail theft and rerouting:**
  - It is easy to steal the postal mails from mailboxes, which has poor security mechanism and all the documents available to the fraudster are free of charge, for example, Bank Mail (credit cards and account statements), administrative forms or partially completed credit offers.
  - The fraudster can use your name and other information that may prove to be harmful for an individual in the near future.
  - Therefore, return items to the sender or request a change of address.

- **Shoulder surfing:** People who loiter around in the public facilities such as in the cybercafes, near ATMs and telephone booths can keep an eye to grab the personal details.
- **False or disguised ATM (skimming):** Just as it is possible to imitate a bank ATM, it is also possible to install miniaturized equipment on a valid ATM.
- This equipment (a copier) captures the card information, using which, duplicate card can be made and personal identification number (PIN) can be obtained by stealing the camera films.
- **Dishonest or mistreated employees:** An employee or partner with access to the personal files, salary information, insurance files or bank information can gather all sorts of confidential information and can use it to provide sufficient damage.
- **Telemarketing and fake telephone calls:** This is an effective method for collecting information from unsuspecting people. The caller who makes a "cold call" (supposedly from a bank) asks the victim to verify account information immediately on the phone, often without an explanation or verification. This attack is known as Vishing.

#### **Computer-based technique**

These techniques are attempts made by the attacker to exploit the vulnerabilities within existing processes and/or systems.

- **Backup theft:** In addition to stealing equipment from private buildings, attackers also strike public facilities such as transport areas, hotels and recreation centres. They carefully analyse stolen equipment or backups to recover the data.
- **Hacking unauthorized access to systems and database theft:** Besides stealing the equipment and/or hardware criminals attempt to compromise information systems with various tools, techniques and methods to gain unauthorized access to download the required information.
- **Phishing:** It is an attack that attempts to steal money or identity by getting victim to reveal personal information.
- **Pharming:** It is a scamming practice in which malicious code is installed on a personal computer or server misdirecting users to fraudulent websites without their knowledge or consent. User will input information unknowingly.

#### **4.3.4 Identity Theft: Countermeasures**

How to prevent being a victim of Identity theft?

- Identity Theft is growing day-by-day
- We need to keep the credit card and PIN safely
- Always Vigilant and take optimum care towards protecting the self-identity

SL. NO	Security Measures
1	Monitor your credit closely
2	Keep records of your financial data and transactions
3	Install security software
4	Use an updated Web browser
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages.
6	Store sensitive data securely
7	Shred documents
8	Protect your PII
9	Stay alert to the latest scams

#### 4.3.5 How to Efface Your Online Identity

- Protect identity is important for netizens, by erasing the footprint on the internet.

SL.NO	How to protect/efface your online identity
1	<a href="http://www.giantmatrix.com">www.giantmatrix.com</a>
2	<a href="http://www.privacyeraser.com">www.privacyeraser.com</a>
3	<a href="http://www.reputationdetender.com">www.reputationdetender.com</a>
4	<a href="http://www.suicidemachine.org">www.suicidemachine.org</a>
5	<a href="http://www.seppukoo.com">www.seppukoo.com</a>