Phishing and Identity Theft

Introduction

Phishing is one of the methods toward enticing netizens to reveal their personal information that can be used for identity (ID) theft. ID theft involves unauthorized access to personal data. Section 66C of the Indian IT Act states that "whosoever fraudulently dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh." Section 66D of the Indian 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 to three years and shall also be liable for fine which extend to one lakh rupees." "Phishing" is the use of social engineering tactics to trick users into revealing confidential information.

Phishing has become a universal phenomenon and a major threat worldwide that affects not only individuals but also all industries and businesses that have an online presence and do online transactions over the Internet.

The statistics about Phishing attacks/scams proves Phishing to be a dangerous enemy among all the methods/techniques, because the prime objective behind these attacks is ID theft.

Phishing

The word Phishing comes from the analogy that Internet scammers are using E-Mail lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. As hackers have a tendency of replacing "f" with "ph" the term Phishing came into being.

Let us take a look at some definitions of the term "Phishing."

1. **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.
2. **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 users' information.

3. **TechEncyclopedia:** 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.
In summary, Phishing is a type of deception designed to steal your identity (i.e., a kind of ID theft fraud). In Phishing schemes, the phisher tries to get the user to disclose valuable personal data – such as credit card numbers, passwords, account data or other information – by convincing the user to provide it under false pretenses. E-Mail is the popular medium used in the Phishing attacks and such E-Mails are also called as Spams; however, not all E-Mails are spam E-Mails. It is important to understand these types of E-Mails with which we deal everyday.

We will discuss two such E-Mails:
(A) Spam E-Mails
(B) hoax E-Mails.

A. Spam E-Mails Also known as “junk E-Mails” they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets , networks of virus-infected computers, are used to send about 80% of Spam.
Types of Spam E-Mails are as follows:
1. **Unsolicited bulk E-Mail (UBE):** It is synonym for SPAM – unsolicited E-Mail sent in large quantities.
| SPAMBOTS SPAMBOT is an 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 lists to send unsolicited E-Mail. SPAMBOTS are also known as web crawlers, as they gather E-Mail addresses from numerous websites, chatroom conversations, newsgroups and special-interest group (SIG) postings. SPAMBOT begins its scan on a webpage and search for two things: (a) hyperlinks and (b) E-Mail addresses. It gathers and stores E-Mail addresses and crawls (i.e., follows) through each hyperlink to a new page to gather E-Mail addresses.

2. **Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising.

Spam E-Mails proved to be a popular medium for phishers to scam users to enter personal information on fake websites using E-Mail forged to look like as if it is from a bank or other organizations such as:

1. **HSBC, Santander, CommonWealth Bank:** International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fish.
2. **eBay:** It is a popular 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-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

The E-Mail will usually ask the user to provide valuable information about himself/herself or to "verify" information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:

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. **"Verify 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 on your part. The lottery scam often includes references to big companies, for example, Microsoft. There is no Microsoft lottery.

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 E-Mail address with limited people and/or on public websites – the more it is 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.

B. **Hoax E-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. It is difficult sometimes to recognize whether an E-Mail is a "Spam" or a "hoax." The websites mentioned below can be used to check the validity of such "hoax" E-Mails – for example, chain E-Mails.

1. www.breakthechain.org: This website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails (e.g., from "lottery schemes" to "your wish will come true" E-Mails). One can search the subject line of such an E-Mail or a couple of key words on this website to know whether it is a Spam E-Mail or a legitimate E-Mail.

2. www.hoaxbusters.org: This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy. Hoaxbusters contains information almost about every scam, legend and frivolous warning that exists on the Internet. For example, mail with the subject as "Breaking News" may contain the text as "Barack Obama refused to be the president of the US" and will end with the E-Mail signature as "CNN."

Methods of Phishing

Let us understand the most frequent methods used by the phishers to entice the netizens to reveal their personal information on the Internet.

1. **Dragnet:** This method involves the use of spammed E-Mails, bearing falsified corporate identification (e.g., corporate names, logos and trademarks), which are addressed to a large group of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites 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. **Rod-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:** Th is 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." 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 to be a legitimate website or possibly a pop-up window that looks exactly like the official site. These fake sites are also called "spoofed" websites. Once the netizen is into one of these spoofed sites, he/she might unwittingly send personal information to the con artists. Th en they often use your information to purchase goods, apply for a new credit card or otherwise steal your identity.

Website Spoofing, XSS and XSRF Website Spoofing: It is the 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.

Cross-site scripting (XSS): XSS[15] is a type of computer security vulnerability typically found in web applications that enable malicious attackers to inject client-side script into webpages 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 request forgery (XSRF): XSRFis 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 whereby 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 but 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. 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, and then transmit those data to phishers for later illegal access to users' financial accounts. We will discuss more on this in the next section while understanding Phishing techniques used by phishers.

Phishing Techniques

In this section we will discuss common ways, the techniques used by phishers to launch Phishing attacks.

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 diff erence of one or two letters in the URLs, which is ignored by netizens. Th is makes a big diff erence and it directs users to a fake/bogus website or a webpage. See below to know about an advanced Phishing attack known as homograph attack.

Homograph Attack The meaning of homograph is that two words are spelled the same way but differ in meaning (e.g., fair). Phishers use homograph attack on the 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, for example, "0" (zero) and " O " (o alphabet in uppercase), "1" (L alphabet in lowercase) and "I" (i alphabet in uppercase). For example, the original website www.GOOGLE.com can be registered as www.G00GLE.com.

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 lter," duly licensed from Google. It is enabled by default.

• The Opera lter 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 (see Table) to help checking the webpage content for signs of Phishing, but have limitations that they do not analyze 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:** We have explained “Mishing” – mobile Phishing attacks (“Vishing” and “Smishing”). Besides such attacks, 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.

Phishing Attack Launched through Android Market Android: It is an open-source operating system (OS) for mobile phones and is based on Linux kernel. This OS has recently gained popularity with the release of Google’s Nexus One phone. The Android Market is similar to iPhone App Store. Currently, around 22,000 applications are available on the Android Market.

Spear Phishing

“Spear Phishing” is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. 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 (such as the person who manages the computer systems); 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. Th us, “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

| **Avoiding Spear Phishing Scams** There are few precautions you can take to avoid making yourself a victim of Phishing scam:

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 Phishing filter – it scans and helps identify suspicious websites, and provides up-tothe-hour updates and reports about known Phishing sites.

Whaling

This is a specific form of "Phishing" and/or "Spear Phishing" – targeting executives from the top management in the organizations, usually from private companies. Th e objective is to swindle the executives into revealing confidential information. Whaling targets C-level executives sometimes with the help of information gleaned through Spear Phishing, aimed at installing malware for keylogging or other backdoor access mechanisms.

Note: The names given to various Internet scams are found to be amusing. Whaling may have been derived from the fact that the people targeted are top-ranking executives. The difference between Spear Phishing and whaling appears to be a bit cloudy. It seems, whaling involves more extensive reconnaissance about the target rather than the target being enticed to be a victim of Spear Phishing attack.

E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent from a legitimate business body and/or business authority. Th e content of an E-Mail usually involves some kind of falsified industry-wide concern and is meant to be tailored for executives.

Types of Phishing Scams

We have seen how phishers use numerous methods and techniques to launch Phishing attacks. The prevalent types of Phishing scams are .

1. **Deceptive Phishing:** Phishing scams started by broadcasting deceptive E-Mail messages with the 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/fictitious account charges and/or undesirable account changes/new free services requiring quick action. Th e 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:** Malware can embed a keylogger to track keyboard input and send relevant information, maybe the 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 files as device drivers.

4. **Session hijacking:** It is an attack in which netizens' activities are monitored until they establish their bona fide 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. See Box 5.9 to know more about "advanced form of Phishing."

| **Advanced Form of Phishing – Tabnapping or Tabjacking** Tabs are the web browser tabs and browser tabs that are not in use are called as napping. Most often, netizens work with multiple tabs open with different Web-browsing sessions on each one. In fact, netizens go hours without even realizing that, they have multiple tabs open. When a netizen visits legitimate website such as banking website and opens a genuine webpage and that webpage is not used, that is, it is kept idle for some time because may be netizen starts surfing other website (i.e., Googling) then, and when the netizen returns back to banking webpage, he/she gets redirected to phished webpage and he/she does not notice it, as he/she never closed the tab. Phishers have identified a way to invade the browser tabs and change (i.e., replace) it to a page designed to steal the personal information. This is done by checking whether the webpage is idle 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, Orkut, Facebook and Yahoo are primary targets. For example, netizen opens a tab to view the bank account. Netizen login on the website with his/her user ID and password and then go to another tab. While working with the other tab, phisher replaces the legitimate bank site webpage with a cloned login page developed to steal personal information. When he/she goes back to the tab, bank website, netizen assumes the webpage has timed out and hence requesting you to re-enter your password. If you do then you give the hacker access to your account.

5. In-session Phishing: 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. Netizen believes this pop-up window is being a part of the targeted session and is used to steal netizen's personal information/data in the same way as with other Phishing attacks. Th e advantage of in-session Phishing attack is the phisher does not need the targeted website to be compromised but to rely on modern web browsers to support more than one session.

6. Web Trojans: It 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: 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:

• Th Hosts file poisoning: e 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 (i.e., URL of website) during early days of the Internet [(i.e., before undertaking a DNS (Domain Name Server) lookup)]. 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 .

Three Ps of Cybercrime – Phishing, Pharming and Phoraging

1. Pharming: It is an attack aiming to redirect a website’s traffic to another bogus website. The term Pharming is a neologism based on “farming” and “Phishing.”. Pharming has become a major concern for businesses hosting E-Commerce and online banking websites. In Pharming, an attacker cracks vulnerability in an Internet service provider’s (ISP) DNS server and hijacks the domain name of a commercial site. Therefore, anyone going to the legitimate site is then redirected to an identical but bogus site. Antivirus softwares and Spyware removal softwares cannot protect against Pharming. The most efficient way to prevent Pharming is to ensure using secure web connections like HTTPS to access websites such as banking or financial institutions and at the same time accept the valid public-key certificates issued by trusted sources. A certificate from an unknown organization or an expired certificate should not be accepted.
2. Phoraging (pronounced foraging): 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 identity theft.

8. System reconfiguration attacks: Phisher can intrude into the netizens’ system (i.e., computer) to modify the settings for malicious purposes. For example, URLs saved under favorites in the browser might be modified to redirect the netizen to a fake/bogus “look alike” websites (i.e., URL for a website of 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 and more information resides on the corporate servers and the Web (including what happens with “cloud computing”), attackers have a boom time because taking away/copying information in electronic form is so easy! Unsecured systems (e.g., computers enabled with the Internet facility and with inappropriate security settings) are often found to be inappropriately maintained from cybersecurity perspective. When such systems are connected, the web servers can launch an attack with numerous methods and techniques. Data theft is a widely used approach to business espionage. Phishers can easily make profit from selling the stealth confidential communications, design documents, legal opinions and employee-related records to those who may want to embarrass or cause economic damage to competitors.

10. Content-injection Phishing: In this type of scam, phisher replaces part of the content of a legitimate website with false content to mislead the netizen to reveal the confidential personal information. For example, Phisher may insert Malicious Code to capture netizen's credentials that can secretly collect information and send it to phisher.

11. Man-in-the-middle Phishing: In this type of attack, phisher positions himself between the netizen and the 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 aff ected. Later on phisher can either sell or use the information or credentials collected when the user is not active on the system. Th is attack is very difficult to detect compared to other forms of Phishing.

12. Search engine Phishing: It occurs when phishers create websites with attractive sounding off ers (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 off er of lower credit costs or better interest rates than other banks. Netizens who use these websites to save or make more from interest charges are encouraged to transfer existing accounts and enticed to giving up their details.

13. SSL certificate Phishing: It is an advanced type of scam. Phishers target web servers with SSL certifi- cates 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.

Distributed Phishing Attack (DPA)

We learned that the most common Phishing attack is launched using an E-Mail and fraudulent webpage/website to web host structure. Phisher sends lure E-Mails that entice the victim to follow the URLs displayed in the E-Mail which directs him/her to the phisher's website. As the victim is unable to verify/ check legitimacy of the webpage/website, he/she submits personal information. Most often, the Phishing messages and webpages/websites masquerade as banks/financial institutions, government agencies or some other trustworthy entity that could probably ask for personal information. Distributed Phishing attack 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 credentials to a hidden coordination center run by the phisher.

In this attack a large number of fraudulent web hosts (i.e., servers controlled by the phisher) are used for each set of lured E-Mails. Each server collects only a tiny percentage of the victim's personal information. This minimizes the possibility that the phisher shutdown the fraudulent web host within hours of initial mailing due to risk of detection of the origin of the fraudulent E-Mail. Each victim is referred to a unique webpage and in the extreme case the benefits of detection are kept minimum. Even if the victim recognizes the fraudulent E-Mail as a component of a Phishing attack, disabling the web server and/or the weblink to the fraudulent web server will not prevent any other potential victims from being betrayed of their personal information. Phishers launch attacks through thousands of servers using collections of compromised systems such as Botnets and/or zombies .

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 diff erent brands including the graphics (i.e., images and logos) displayed on these websites. Phishing toolkits are developed by groups or individuals and are sold in the underground economy. These sophisticated kits are typically difficult to obtain, are quite expensive, and are more likely to be purchased and used by well-organized groups of phishers, rather than average users.

Phishers use hypertext preprocessor (PHP) to develop the Phishing kits. PHP is a general purpose scripting language that was originally designed for web development of dynamic webpages. PHP code is embedded into the HTML source script and interpreted by a web server with the help of a PHP processor module. Most of the Phishing kits are advertised and distributed at no charge and usually these free Phishing kits – also called DIY (Do It Yourself) Phishing kits – may hide backdoors through which the phished information is sent to recipients (may be to the authors of Phishing kits) other than the intended users.

Following are few examples of such toolkits:

1. **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 names to host a variety of phished webpages, covering numerous organizations and institutes.

2. **Xrenoder Trojan Spyware:** It resets the homepage and/or the search settings to point to other websites usually for commercial purposes or porn traffic.

3. 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.

Note: DIY (Do It Yourself) Phishing kits that are available and/or distributed free of cost, aim not only just to steal personal information but also to infect the system with malware by embedding client-side vulnerabilities.

Phishing Countermeasures

The countermeasures explained in Table 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. 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 (see KRESV test in Appendix C in CD). Box 5.13 explains about "How to recognize legitimate websites," while surfing on the Internet.

Table 5.1 | How to avoid being victim of Phishing attack

Sr. No.	Security Measures	Brief Description
1	Keep antivirus up to date	Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. Th is can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
2	Do not click on hyperlinks in E-Mails	It should always be practiced that, in case an E-Mail has been received from unknown source, clicking on any hyperlinks displayed in an E-Mail should be avoided. Th is may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check out the link, manually retyping it into a web browser is highly recommended.
3	Take advantage of anti-Spam software	Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-Spam software, many types of Phishing attacks are reduced because the messages will never end up in the mailboxes of end-users.
4	Verify https (SSL)	Ensure the address bar displays "https://" rather than just "http://" along with a secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double-clicking the lock to guarantee the third-party SSL certificate that provides the https service. Always ensure that the webpage is truly encrypted.

5	Use anti-Spyware software	Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti-Spyware software can often detect the problem and provide a fix.
6	Get educated	Always update the knowledge to know new tools and techniques used by phishers to entice the netizens and to understand how to prevent these types of attacks. Report any suspicious activity observed to nearest cybersecurity cell.
7	Use the Microsoft Baseline Security Analyzer (MBSA)	The netizens on the Microsoft platform should use MBSA to ensure the system is up to date by applying all the security patches. MBSA is a free tool available on Microsoft's website. This protects the IT systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in Phishing attacks.
8	Firewall	Firewall can prevent Malicious Code from entering into the system and hijacking the browser. Hence, a desktop (software) such as Microsoft's built-in software firewall in Windows-XP and/or network (hardware) firewall should be used. It should be up to date in case any cybersecurity patches have been released by the vendor.
9	Use backup system images	Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play.
10	Do not enter sensitive or financial information into pop-up windows	A common Phishing technique is to launch a bogus pop-up window when someone clicks on a link in a Phishing E-Mail message. This window may even be positioned directly over a legitimate window a netizen trusts. Even if the pop-up window looks official or claims to be secure, entering sensitive information should be avoided because there is no way to check the security certificate. .
11	Secure the hosts file	The attacker can compromise the hosts file on desktop system and send a netizen to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe.
12	Protect against DNS Pharming attacks	This is a new type of Phishing attack that does not Spam you with E-Mails but poisons your local DNS server to redirect your web requests to a different website that looks similar to a company website (e.g., eBay or PayPal).

How to Judge/Recognize Legitimate Websites 1. ScanSafe (www.scansafe.com) was the first company in the world (founded in 2004) to offer web security. Scandoo (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. 2. McAfee SiteAdvisor software (www.siteadvisor.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.

We learned that "E-Mail" is the popular medium used by phishers to entice the netizens; every netizen should imbibe it while responding to the received E-Mails. Hence, it is very important for the netizens who are not IT savvy (i.e., Techies – IT Professionals) but are Internet savvy (i.e., continuously surfing on the net) to discover the phished E-Mails. Figure shows a simple flowchart explaining how to distinguish between a legitimate E-Mail and a phished E-Mail.

SPS Algorithm to Thwart Phishing Attacks

Th e proposal of system based on a simple filtering algorithm, Sanitizing Proxy System (SPS), has been suggested under the white paper by the authors Daisuke Miyamoto, Hiroaki Hazeyama and Youki Kadobayashi from Nara Institute of Science and Technology, Japan.

The key idea behind SPS is that web Phishing attack can be immunized by removing part of the content that entices the netizens into entering their personal information. SPS sanitizes all HTTP responses from suspicious URLs with warning messages; however, netizens will realize that they are browsing Phishing sites. The white paper describes SPS filtering algorithm in simple 20 steps and dictates how it can be built in any proxy system, such as a server solution, a personal firewall or a browser plug-in. The Phishing attack comprised two phases: (a) attraction and (b) acquisition. E-Mail Spoofing attracts netizens, as if it has been sent by a legitimate individual/organization. To acquire personal information, the spoofed E-Mail entices the netizens to execute the attached crimeware, such as a keylogger or a redirector, or to access a "spoofed" website.

Th e white paper summarizes the characteristics of SPS in the following points:

1. Two-level filtering: SPS employs two-level filtering composed of strict URL filtering and HTTP response sanitizing. By combining two filtering methods, netizens can be protected from revealing their personal information on Phishing sites.
2. Flexibility of the rule set: By filtering HTTP responses, the algorithm distinguishes between legitimate websites and other suspicious websites based on a rule set written by the operator of SPS.
3. Simplicity of the filtering algorithm: A simple two-level filtering algorithm can be described into 20 steps and can easily apply the SPS functions into existing proxy implementations, browser plugins or personal firewalls. SPS can be based on two diff erent open-sourced proxy implementations to prove the simplicity and availability of the two-level filtering algorithm.
4. Accountability of HTTP response sanitizing: SPS prevents netizens from disclosing their personal information to Phishing sites by removing malicious HTTP headers or HTML tags from HTTP responses. SPS can also alert netizens about requested webpage containing suspicious parts that are under threat at the time of Phishing attacks.
5. Robustness against both misbehavior of novice users and evasion techniques: An SPS built-in proxy server can protect netizens from almost all deceit cases of web Spoofing, regardless of netizen's misbehavior and evasion techniques used by the phisher.

Identity Theft (ID Theft)

This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits . The person whose identity is used can suff er various consequences when he/she is held responsible for the perpetrator's actions. In many countries, specific laws make it a crime to use another person's identity for personal gain. As mentioned in the "introduction" section, ID theft is a punishable off ense under the Indian IT Act (Section 66C and Section 66D).

Th e statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Th eft Resource Center (ITRC), with the objective to extend the support to the society to spread awareness about this fraud.

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.

| Identity Theft Resource... (Continued) 1. During December 1999, Linda and Jay Foley founded the ITRC, under the umbrella of Privacy Rights Clearinghouse, originally named Victims of Crimes Extended Services (VOICES). 2. In Spring 2000, the name of the organization was changed to the Identity Theft Research Center (ITRC) and was headed by Linda Foley. 3. During 2001, Jay Foley joined the ITRC as a full-time director. 4. In 2007, ITRC staff developed and published a completely new website www.idtheftcenter.org, which is a Google ranked 7 website.

According to 2010 Report published by Javelin Strategy & Researchthe number of "identity fraud victims" were increased by 12% during 2009 and "amount of fraud" increased by 12.5%.

Key statistics noted about total identity frauds in the US are as mentioned below:

1. Th e total fraud amount was US$ 54 billion.
2. Th e average amount spent by the victim was US$ 373 and the time of 21 hours to resolve the crime.
3. In total, 11.1 million adults were found to be victims of ID theft, which amounts to 4.8% of the population being a victim of identity fraud in 2009.
4. 13% of identity frauds were committed by someone who the victim knew.
5. Online methods accounted for only 11% of ID theft in 2009.
6. Offline methodology such as stolen wallets and paperwork account for almost half (43%) of all ID thefts.

Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.

1. Credit card fraud (26%): Th e highest rated fraud that can occur is when someone acquires the victim's credit card number and uses it to make a purchase.
2. 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. Chapter 11 (see Section 11.4.1) provides many illustrations on banking-related frauds.
3. Employment fraud (12%): In this fraud, the attacker borrows the victim's valid SSN to obtain a job.
4. Government fraud (9%): Th is type of fraud includes SSN, driver license and income tax fraud.
5. 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.

Personally Identifiable Information (PII)

Th e 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 number and mobile phone number;
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.

The fraudster may search for following about an individual, which is less often used to distinguish individual identity; however these can be categorized as potentially PII because they can be combined with other personal information to 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.

The information can be further classified as

(a) non-classified and

(b) classified.

1. **Non-classified information**

- Information that is a matter of public record or knowledge. Public information:
- Information belongs to a private individual but the individual commonly Personal information: may share this information with others for personal or business reasons (e.g., addresses, telephone numbers and E-Mail addresses).
- Business information that do not require any special protection Routine business information: and may be routinely shared with anyone inside or outside of the business.
- Information that can be private if associated with an individual and Private information: individual can object in case of disclosure (e.g., SSN, credit card numbers and other financial information).
- Information which, if disclosed, may harm the busi- Confidential business information: ness (e.g., sales and marketing plans, new product plans and notes associated with patentable inventions).

2. **Classified information**

- Information that requires protection and unauthorized disclosure could damage Confidential: national security (e.g., information about strength of armed forces and technical information about weapons).
- Information that requires substantial protection and unauthorized disclosure could Secret: seriously damage national security (e.g., national security policy, military plans or intelligence operations).
- Information that requires the highest degree of protection and unauthorized Top secret: disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

Types of Identity Theft

Identity is stolen in order for someone to commit the crime. ID theft is related to many areas:

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

Financial ID theft includes bank fraud, credit card fraud, tax refund fraud, mail fraud and several more. 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 victim's finances. For example, the fraudster fraudulently can open a new credit card account in the victim's name and the card charges up, payment is neglected, leaving the victim with bad credit history (i.e., horrible credit score) and a world of debt. In some cases, the fraudster will completely take over a victim's identity, which enables the fraudster to easily open bank accounts, multiple credit cards, purchase a vehicle, receive a home mortgage or even find employment in the victim's name.

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 trafficking;
4. alien smuggling;
5. money laundering.

Individuals who commit ID theft are not always out to steal the victim's money or ruin victim's credit. This type of fraud/theft occurs when a fraudster uses the victim's name upon an arrest or during a criminal investigation. The personal information given by a fraudster to a law enforcement officer may include counterfeited document such as driver's license, birth certificate, etc. Unfortunately, the victim of criminal ID theft may not know what warrant has been issued under his/her name for quite some time. Th e victim will only come to know in case of being detained on a routine traffic stop and arrested due to outstanding and overdue debts. In some cases, the fraudster will appear in court for the violation and enter a guilty plea without the victim's knowledge. This may place the victim's name into countywide or state-wide criminal database with a huge blemish language on the record.

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 victim's name, identity clones compromise the victim's 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 diff erent location. An identity clone will obtain as much information about the victim as possible. They will look to find out what city and state the victim (he/she) was born in, what street he/she grew up on, where he/she attended school and what relationships he/she may have been involved in. They will also want to know information concerning the victim's parents and other family members. In a nutshell, identity clones want as much personal information about the victim as they can attain. Th is enables them to answer questions in an informative manner when they are on the move or asked about the victim's life.

Business Identity Theft

"Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance in comparison with individual's ID theft. A fraudster rents a space in the same building as victim's office. Then he applies for corporate credit cards using victim's firm name. The application passes a credit check because the company name and address match, but the cards are delivered to the fraudster's mailbox. He sells them on the street and vanishes before the victim discovers the firm's credit is wrecked.Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams. BSI is the information about the business/organization, privileged in nature and/or proprietary information which, if it is compromised through alteration, corruption, loss, misuse or unauthorized disclosure, could cause serious damage to the organization. Such information is like a "sensitive asset" for the organization.

Identity theft in the business context occurs most often when someone knocks off the victim's product and masquerades their shoddy goods as victim's. It is a kind of intellectual property theft. Nowadays, technology has made it easier for the trademarks and security devices such as holograms to be knocked off swimmingly. The consumers should no longer rely on trademarks alone to certify the authenticity of the goods and should verify their source of origin.

Medical Identity Theft

India is known to have become famous for “medical tourism.” Thousands of tourists, every year visit India with dual purpose – touring the country plus getting their medical problems attended to (surgeries, total health check, Kerala massage, etc.) because India has made name for good quality and yet reasonable priced (compared with Europe and the US) in medical services. In the process thousands of medical records of foreigners as well as locals who avail medical facility get created. This has created a boom for cybercriminals.

Healthcare facilities now are very different compared to how they were used a decade back. There are greater opportunities for protected health information (PHI) changing hands when multiple agencies are connected over computer networks and the Internet – for example, medical representatives, health officers, doctors, medical insurance organizations, hospitals, etc. to name a few (see Fig. 5.2). Medical facility providers are moving from cumbersome paper records to faster and easier file and trace electronic records; however, the concern over medical ID theft[43] is growing. The stolen information can be used by the fraudster or sold in the black market to people who “need” them. This could lead to many more cases. For example, invoice of thousands of dollars of emergency medical services was received by a man situated in Houston (Texas), who had never had any health issues, as reported in the New York Times. A fraudster had used this man’s identity for the fraudster’s emergency medical needs.

According to a 2008 Identity Theft Resource Center survey, some of the reasons why medical ID theft is particularly damaging the victims include:

1. Approximately one-third of victims of medical ID theft surveyed had someone else’s medical information or medical history on their medical record, increasing the possibility of patients being treated incorrectly because of incorrect medical records.
2. More than 10% of victims of medical ID theft surveyed were denied health or life insurance for unexplained reasons.
3. More than two-third of victims surveyed receive a bill for medical services that were provided to an imposter.

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.

Techniques of ID Theft

Identity theft can affect all aspects of a victim's daily life and often occurs far from its victims. The attackers use both traditional, that is human-based, methods as well as computer-based techniques.

1. Human-based methods: These methods are techniques used by an attacker without and/or minimal use of technology

• Direct access to information: People who have earned a certain degree of trust (house cleaners, babysitters, nurses, friends or roommates) can obtain legitimate access to a business or to a residence to steal the required personal information.

•Dumpster Diving: Retrieving documents from trash bins is very common .

• Theft of a purse or wallet: Wallet often contains bank credit cards, debit cards, driving license, 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 ATMs ("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 much explanation or verification. This attack is known as Vishing.

3. Computer-based technique:

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

- Backup theft: Th is is the most common method. In addition to stealing equipment from private buildings, attackers also strike public facilities such as transport areas, hotels and recreation centers. They carefully analyze 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: is explained
- Pharming: Pharming is explained . In summary, the attackers setup typo or matching domain names of the target (usually of popular banks and financial institutions) and install websites with similar look and feel. Hence, even if the user types-in incorrect URL (e.g., instead of www.xyzbank.com, URL is punched as www.xyzbanc.com), the user gets the website with the same look and feel. This website is not real and is hosted with the sole purpose to extract personal information from the netizen.
- Redirectors: These are malicious programs that redirect users' network traffic to locations they did not intend to visit. For example, port redirection program is loaded by compromising the server and all HTTP Port 80 requests may be redirected to attacker. The highest volume in traffic occurs with Malicious Code that simply modifies the victim's DNS server settings or the hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. Th e fraudulent DNS server replies with "good" answers for most domains. However, when attackers want to direct the victim to a fraudulent site, they simply modify their name server responses. Th is is particularly effective because the attackers can redirect any of the users requests at any time, and the users would have no idea that this is happening. It is reported that, during December 2005, such an attack was launched against HSBC Brazil, Banco Itau, Banco Banespa and Bradesco banks.
- Hardware: During March 2005, police discovered that the London office of the Japanese bank Sumitomo had been the target of a group of hackers for several months. Th e investigators initially believed that the attackers had used a Trojan. However, after several days of exploration, they found a tiny keystroke-recording device inserted where the keyboard cable connects to the back of the computer. A quick search on the Internet yields a list of a half-dozen companies that sell this type of product.

Identity Theft: Countermeasures

Identity theft is growing day-by-day and people think simple steps such as keeping the credit card and PIN safely will protect them from ID theft. One should be always vigilant and should take optimum care toward protecting the self-identity. Table explains some good tips on countermeasures for identity theft.

Table | How to prevent being victim of identity theft

Sr. No.	Security Measures	Brief Description
1	Monitor your credit closely	The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you. Watch for suspicious signs such as accounts you did not open. You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security.
2	Keep records of your financial data and transactions	Review your statements regularly for any activity or charges you did not make.
3	Install security software	Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions.
4	Use an updated Web browser	Use an updated web browser to make sure you're taking advantage of its current safety features.
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages.	Use caution even when the message appears to come from a safe sender, as identity information in messages can easily be spoofed
6	Store sensitive data securely	Just as you keep sensitive paper documents under lock and key, secure sensitive online information. This can be done through file encryption software.
7	Shred documents	It is important to shred the documents that contain personal or financial information (both paper and electronic) before discarding them. This prevents dumpster diving and, in the online world, the ability for hackers to bypass information that has not been permanently deleted from your system.