5 Phishing and Identity Theft

Learning Objectives

After reading this chapter, you will be able to:

- Learn about Phishing and its related techniques.
- Understand different methods of Phishing.
- Get an overview about 3Ps of cybercrime (Phishing, Pharming and Phoraging).
- Understand what Spear Phishing is and how to avoid being victim of Spear Phishing.
- Get an overview of "whaling."
- Learn about identity (ID) theft and understand ID theft as a major threat to businesses.
- Understand "myths and facts" about ID theft.
- Understand different types of ID thefts.
- Learn about different techniques of ID theft.
- Understand about countermeasures for ID theft.

5.1 Introduction

Chapter 4 has provided an insight on how different methods and tools are used to conduct cyberoffenses and Phishing was introduced in Chapter 4 as 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. Phishing is equal parts of technology and psychology – resorted to a systematic way to exploit netizens, not only by individual attackers but also by organized criminal groups.

The statistics about Phishing attacks/scams proves *Phishing* to be a dangerous enemy among all the methods/techniques discussed in Chapter 4, because the prime objective behind these attacks is ID theft.

1. The world Phishing map available at www.avira.com[1] illustrates that the most Phishing attacks are on the rise in Asia, Europe and North America. The virus laboratory at Avira is constantly monitoring the evolution of E-Mail Phishing across the globe.

2. The graphical illustrations available on www.m86security.com[2] exhibit the following facts:
   - Monitoring of continent of origin from where Phishing E-Mails are sent. Europe is the dominant source of Phishing E-Mails.
   - Facebook, HSBC, Paypal and Bank of America are the most targeted organizations in Phishing attacks.
   - US, India and China are the most targeted countries to launch Phishing attacks.
3. The Phishing attacks are monitored on daily basis and displayed on www.phishtank.com.[3] The statistics displayed are "phishes verified as valid" and "suspected phishes submitted." It is important to note that more than five million E-Mails are identified as "verified and valid" phished E-Mails almost everyday.
4. According to May 2009 Phishing Monthly Report compiled by Symantec Security Response Anti-Fraud Team[4]:
   - Total 3,650 non-English Phishing websites were recorded in the month of May 2009 and out of these, French language Phishing sites were the most frequently recorded followed by websites in Italian and Chinese languages.
   - Phishing URLs are categorized based on the top-level domains (TLDs). The most used TLDs in Phishing websites during the month of May 2009 were ".com," ".net" and ".org" comprising 50%, 9% and 5%, respectively.
5. Phishing Activity Trends Report of Q4-2009[5] published by Anti-Phishing Working Group (APWG, see Box 5.1) 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 is found to be the most popular port in use followed by Port 443 and Port 8080 among all the phishing attacks.

This chapter aims to lay the foundation to understand Phishing and different techniques and methods of Phishing attacks. One needs to wear *HAT* and put oneself into the *SHOES* of the phisher (scammers who perpetrate Phishing scams) to understand Phishing. Phishers are also getting educated and attempt new methods and techniques to victimize netizens. Therefore, it is crucial to discuss about countermeasures to avoid becoming victim of Phishing attacks, which we have discussed at the end of this chapter. "Phishing"

Box 5.1 APWG (Anti-Phishing Working Group)

The Anti-Phishing Working Group (APWG) – 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 of the Phishing problem in terms of costs and share information about best practices to eliminate these attacks/scams.

Source: http://en.wikipedia.org/wiki/Anti-Phishing_Working_Group (9 June 2010).

attacks and "ID theft" both have an impact on individual's "privacy." Detailed discussion about "privacy" from all perspectives can be found in Ref. #2, Books, Further Reading.

5.2 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.
Source: http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp (9 June 2010).

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.[6]
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.[7]
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.[8]

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 (introduced in Section 1.5.2, Chapter 1) and (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 (explained in Chapters 1 and 2), 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* (introduced in Box 1.5, Chapter 1) – unsolicited E-Mail sent in large quantities (see Box 5.2).
2. **Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Box 5.2 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.

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* or *filters*. Such E-Mail blocker and/or filter, occasionally, may block a legitimate E-Mail message which could not be delivered to the intended recipient. This can be avoided by allowing each subscriber to generate a whitelist of specific E-Mail addresses the blocker should pass.

Source: http://en.wikipedia.org/wiki/Spambot (26 July 2010).

Box 5.3 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), signed into law by President George W. Bush on 16 December 2003, establishes the United States' first national standards for the sending of commercial E-Mail and requires the Federal Trade Commission (FTC) to enforce its provisions. The acronym CAN-SPAM derives from the bill's full name: Controlling the *A*ssault of *N*on-*S*olicited *P*ornography *A*nd *M*arketing Act of 2003. This can also be a play on the usual term for unsolicited E-Mail of this type of Spam. The bill was sponsored in Congress by Senators Conrad Burns and Ron Wyden.

Visit the weblink http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm to know more about this act (see Fig. 1.13, Chapter 1 and Section "Spam Laws" under Section 6.2.2, Chapter 6).

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. The Act has been largely unenforced, despite a letter to the FTC from Senator Burns, who noted that "Enforcement is a key factor with regard to the CAN-SPAM legislation." In 2004, less than 1% of Spam was complied with the CAN-SPAM Act of 2003 (see Example 16, Section 11.2.16, Chapter 11 in CD).

Source: http://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003 (9 June 2010).

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: [9]

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. In Chapter 7 (Section 7.14) security and privacy threats from social networking sites are discussed.

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: [10]

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. We will discuss more on this in Section 5.2.2.
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. It is observed that most of the phished E-Mails display the name of 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 E-Mail is received displaying "You have won the lottery in Great Britain," confirm it on 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 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.

Visit the weblinks mentioned below to undergo a quiz to test your Phishing IQ:

1. www.sonicwall.com/Phishing/index.html,
2. http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html

Although Phishing is categorized as Spam, it also differs from Spam. Spam attempts to sell a product or service whereas a phished E-Mail seems to be sent by a legitimate organization/institute. As Phishing and legitimate messages appear to be similar, techniques that are applied to Spam messages cannot be applied naively to Phishing messages. The purpose of a phished E-Mail is to obtain sensitive personal information about a netizen/Internet user and to do so E-Mail needs to deceive the intended recipient into believing that it is from a legitimate organization/institute. As a form of deception, a Phishing E-Mail contains no useful information for the intended recipient and thus falls under the category of Spam.

Let us understand the ways to reduce the amount of Spam E-Mails we receive.[11]

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.[12] 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. In Chapter 11 in CD, Example 16 illustrates CAN-SPAM Act Violation through E-Mail Stock Fraud (see Section 11.2.16).

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."

Visit the weblink to learn few examples of hoax E-Mails at http://www.westpac.com.au/security/fraud-and-scams/latest-hoax-email-examples

5.2.1 Methods of Phishing

Let us understand the most frequent methods used by the phishers[13] 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:** 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. See Box 5.4 to know more about other attacks launched on the legitimate websites to grab the user's personal information. These attacks are also known as "content injection Phishing." Visit http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx to see the example of a deceptive URL address linking to a scam website. 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. Then they often use your information to purchase goods, apply for a new credit card or otherwise steal your identity. Box 5.5 explains Phishing vis-à-vis Spoofing.
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.

Box 5.4 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.[14]

Box 5.4 Website Spoofing, . . . (*Continued*)

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.

1. John often visits a particular website that is hosted by Bill. Bill's website allows John to log in with a username/password pair and store sensitive information such as billing information.
2. Bruce observes that Bill's website contains a reflected XSS vulnerability.
3. Bruce crafts a URL to exploit the vulnerability, and sends John an E-Mail, enticing him to click on a link for the URL under false pretenses.
4. John visits the URL provided by Bruce while logged into Bill's website.
5. The malicious script embedded in the URL executes in John's browser, as if it came directly from Bill's server. The script can be used to send John's session cookie to Bruce. Bruce can then use the session cookie to steal sensitive information available to John (authentication credentials, billing info, etc.) without John's knowledge.

Cascading style sheets is referred to as *CSS*, hence *cross-sites scripting* is referred to as *XSS*. CSS is a style sheet language used to describe the presentation semantics (i.e., look and formatting) of a document written in a markup language such as HTML and XHTML.

Cross-site request forgery (XSRF): XSRF[16] 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 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.

1. Bill might be browsing a chat forum where another user, Bruce, has posted a message.
2. Bruce has crafted an HTML image element that references a script on Bill's bank's website.
3. In case Bill's bank keeps his authentication information in a cookie, and if the cookie has not expired, then the attempt by Bill's browser to load the image will submit the withdrawal form with his cookie, thus authorizing a transaction without Bill's approval.
4. This case displays Bill's web browser that is confused into misusing Bill's authority at Bruce's direction.

Box 5.5 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 (explained in Section 2.7, Chapter 2) 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.

5.2.2 Phishing Techniques

In this section we will discuss common ways, the techniques[17] 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 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. See Box 5.6 to know about an advanced Phishing attack known as homograph attack.
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 (see Table 5.2) 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") in Chapter 3. 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. See Box 5.7 to understand the innovative Phishing attack launched on "Android Market" website.

Box 5.6 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.G**OO**GLE.com can be registered as www.G**00**GLE.com. Another example could be www.microsoft.com could be juggled as www.rnicrosoft.com (the letter "m" has been replaced with "r" and "n"). This phenomenon opens a rich vein of opportunities for Phishing attacks. The phisher could create and register a domain name which appears almost identical to an existing domain and takes the netizen to the phony website. Phisher could send E-Mail messages displaying the URL of a phony website, purporting to come from the original site, but directing netizens to the phony website. The phisher could easily record information such as passwords or account details through this spoofed website, while passing traffic through the original website. The netizens will never be able to notice the difference, until some suspicious or unusual activity occurs with their accounts. Visit http://www.xn--goole-tmc.com/ to experience the explained phenomenon.

Source: http://en.wikipedia.org/wiki/IDN_homograph_attack (25 October 2010).

Box 5.7 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.

According to an article available on http://news.softpedia.com, a malware writer succeeded to list a rogue Phishing application called *09Droid* on the Android Market website. The application posed to be a shell for mobile banking applications, but, instead found, it is being used to obtain (steal) online banking credentials.

Travis Credit Union (TCU) issued an alert immediately, during the first week of December 2009, stating "*Your mobile device may be at risk if you downloaded an application provided by 09Droid from the Android Marketplace; applications from 09Droid are NOT an authorized or legitimate downloadable application for TCU Mobile Banking*." TCU also notified its customers through its website, Facebook page and E-Mail, although its services were not targeted by the rogue application.

First Tech Credit Union also issued a similar warning, stating "*The financial institution recommends that affected users take their phone to their mobile operator in order to make sure all traces of the malware are removed. The application attempts to steal financial information from consumers, for the likely purpose of Identity Theft*."

Source: http://news.softpedia.com/news/Phishing-Attack-Launched-from-Android-Market-131793.shtml (26 July 2010).

Phishers usually take a broad approach by sending millions of E-Mail messages that appear to come from popular banks, online auction houses and other business houses. These E-Mail messages, pop-up windows and the websites appear to be official so that they can deceive many netizens to believe that they are legitimate. Unsuspecting netizens often respond to these requests for credit card numbers, passwords, account information or other personal and financial data. According to the 2009 Consumer Reports State of the Net Survey,[18] Phishing scams cost US$ 483 million in the US. Thus, we see that Phishing scams involve fraudulent E-Mail messages or fake websites designed to steal identity. Scam artists "phish" in an attempt to persuade millions of netizens/Internet users to disclose sensitive information. Now there is a new version of

an old scam called "Spear Phishing," a targeted E-Mail attack that a scammer sends only to people within a small group, which is explained in the next section.

5.2.3 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. 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 (see Box 5.8).

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. The 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.

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. The content of an E-Mail usually involves some kind of falsified industry-wide concern and is meant to be tailored for executives.

Whaling phishers have also forged official looking FBI subpoena E-Mails and claimed that the manager needs to click a link and install special software to view the subpoena. In the case of the recent 2008 FBI subpoena whaling scam, 20,000 corporate CEOs were attacked. Approximately 2,000 of them fell for it and clicked on the whaling link, believing it would download a "special" browser add-on to view the entire subpoena document. In truth, the linked software was a keylogger that secretly recorded the CEOs passwords

and forwarded those passwords to the phisher men. As a result, each of the 2,000 compromised companies were further hacked in some way; a few of them were particularly damaged by the attacks.[19]

Although the countermeasures of Phishing are covered at the end of Phishing section, however, see Box 5.8 to understand the countermeasures for Spear Phishing.

5.2.4 Types of Phishing Scams

We have seen how phishers use numerous methods and techniques to launch Phishing attacks. The prevalent types of Phishing[20] scams are discussed in this section.

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. 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. (See Section "The Bane of Malware" under Section 9.3, Chapter 9)
3. **Keyloggers:** We have explained keyloggers in Chapter 4. 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."
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.

Box 5.8 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-to-the-hour updates and reports about known Phishing sites (see Table 5.2 and Box 5.13, Chapter 5).

Box 5.9 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.

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. The 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. To know more about this, visit http://en.wikipedia.org/wiki/In-session_Phishing (8 June 2010).

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 (see Box 5.10).

   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 (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 (see Box 5.11).
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.).

Box 5.10 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."[21]. 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.[22]

Phoraging is information diving – searching for information with the aim of identity theft whereby a phisher collects data from various sources such as social networking sites, viruses and Spyware to build up the identity of a person.

The phishers always work in a smarter way, hence nowadays they are focusing on "matrimonial sites" as well as "social networking sites for professionals" (e.g., www.linkedin.com) to reveal personal information such as date of birth, personal E-Mail address, contact details and what not as the members (i.e., users of these websites) cannot post false information on these websites!!

Box 5.11 DNS Hijacking and Click Fraud

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, particularly for the practice of Phishing or to direct users' HTTP traffic to the ISP's own web servers where advertisements are served.[23]

An illegal change to a DNS server directs URL to a different website. In some cases, the new website's URL may have one different letter in the name that might go unnoticed. The bogus website might offer similar and/or competing products for sale, or it may be a vehicle to publicly smear the reputation of the intended website.[24]

DNS is used to interpret domain names such as www.<domainname>.com (e.g., www.yahoo.com) into an IP address. The IP address consists of numbers such as XXX.XX.XXX.X (e.g., 107.60.132.4) that give the domain a unique identification. An IP address is one-of-a-kind and unique, therefore, it can be used to trace Internet activity back to the PC user as well as identify the exact location of a website. Domain names are used to identify websites because they are easier to remember than a series of numbers that make up an IP address.

DNS hijacking is used by attackers 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 websites and any other related form of criminal activity.

Once the DNS address is hijacked to a bogus DNS server, it translates the legitimate IP address or DNS name into the IP addresses of malicious websites. DNS hijacking can occur with any website large or small and turn those websites into malicious websites without the knowledge of the netizens.

As the website owners depend upon legitimate DNS servers issued by their ISP, DNS hijackers use malware in the form of a 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. The switch from the legitimate DNS server to the bogus DNS server goes unnoticed by both the netizen and the legitimate website owner. This opens up the malicious website to perform any criminal act that the phisher wishes because the netizen thinks that he/she is on the real website.

Box 5.11 DNS Hijacking . . . (*Continued*)

DNS hijacking also promotes Click Fraud with such programs as Google Adsense. As there are numerous DNS servers that are bogus, they form a network of websites which results in a lot of traffic. When there is a lot of traffic then you will find a lot of people clicking which results in Click Fraud. The attackers can rack up a lot of money with "click throughs" from programs such as Google Adsense who pay a commission for each click.

Click Fraud: 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.[25]

It is an illegal practice that occurs when individuals click on a website click through advertisements (either banner ads or paid text links) to increase the payable number of click throughs to the advertiser. The illegal clicks could be either performed by having a person manually clicking the advertising hyperlinks or by using automated software or online Bots (see Section 2.6, Chapter 2) 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.[26] Visit the weblinks mentioned below to explore more on *Click Fraud:*

1. Exposing Click Fraud: http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html (18 June 2010).
2. The dark side of online advertising: http://www.businessweek.com/magazine/content/06_40/b4003001.htm (18 June 2010).

Click forensics is the industry leader in scoring, auditing and improving traffic quality for the online advertising community. For online advertisers, traffic quality management aims to improve campaign performance. The goal is to exclude low-quality traffic, eliminate Click Fraud and improve conversion rates. Click forensics optimizes online advertising campaigns. For online publishers, traffic quality management will attract and retain advertisers and ad networks to increase spend and earnings of ad per click. Click forensics has partnered with Yahoo! Click forensics is the leader in eliminating Click Fraud and is the publisher of the Click Fraud Index and the founder of the Click Quality Council.
To know more about click forensics, visit http://www.clickforensics.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 affected. Later on phisher can either sell or use the information or credentials collected when the user is not active on the system. This attack is very difficult to detect compared to other forms of Phishing. In Chapter 11, the man-in-the-middle (MITM) attack is discussed and explained in detail.

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. 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. See Box 5.12 to know more about search engine optimization (SEO) attack, which is an advance form of technique used by the attackers nowadays.
13. **SSL certificate Phishing:** It 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.[27]

Box 5.12 SEO Attacks – Beware While Searching through Search Engines!

Search engine optimization (SEO) is the practice of maximizing the volume or quality of traffic to a website (such as a blog) from search engines via natural or unpaid search results as opposed to other forms of search engine marketing (SEM) which may deal with paid inclusion. SEO considers how search engines work and what people search for. Optimizing a website primarily involves editing its content and HTML and associated coding to increase both its relevance to specific keywords and to remove barriers to the indexing activities of search engines.[28]

Black hat SEO or spamdexing is a technique[30] which uses methods such as link farms, keyword stuffing and article spinning that degrade both the relevance of search results and the user experience of search engines. Search engines look for sites that employ these techniques to remove them from their indices.

According to security researcher Dancho Danchev, SEO attack abuses a common practice among websites – caching search queries – an activity designed to boost their rankings among major search engines, such as Google. Attackers inject common search terms and an iframe (<iframe> – HTML tag defines an inline frame that contains another document) script designed to send victims to other sites hosting Malicious Code. The search term and iframe redirect get cached in search engines such as Google.[29]

The business of using SEO techniques to infuse legitimate websites has become a huge money spinner for attackers. The attackers take advantage of hottest news/stories on the Internet to spread malware – many of them profiting from high-profile deaths and disasters; for example, the death of celebrities such as Michael Jackson have provided rich attractive content for attackers trying to take advantage of trending news stories.

Techniques used for Black hat SEO attacks

1. **Fake antivirus:** Fake security alerts are flooded to netizens to entice them into executing the Malicious Code such as Activex Controls and/or paying for a bogus security product to install them.
2. **SEO page:** Pages stuffed with erroneous keywords, usually designed to feature highly in search engine results, are attacked to misdirect netizens to rogue websites. It is also known as SEO-poisoned pages.

Box 5.12 SEO Attacks – Beware While . . . (*Continued*)

3. **SEO poisoning:** It is a process of enticing search engine into ranking an SEO page high up in the search results and these results may be manipulated results known as "poisoned."
4. **Black hat SEO kits:** These tools are used to launch and manage SEO attack. They are also known as search engine crawlers that poison search results to redirect netizens to rogue (i.e., bogus) websites. (Readers may visit http://www.blackhatseo.com to know more about this tool).

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 (explained in Chapters 1 and 2).

Visit the weblink mentioned below to know more examples of Phishing attacks launched through fake/bogus E-Mails: http://www.doshelp.com/scams-fraud/index.html

5.2.5 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 (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.[31]
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.[31]

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.

5.2.6 Phishing Countermeasures

The countermeasures explained in Table 5.1 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. This 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. This 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.

(*Continued*)

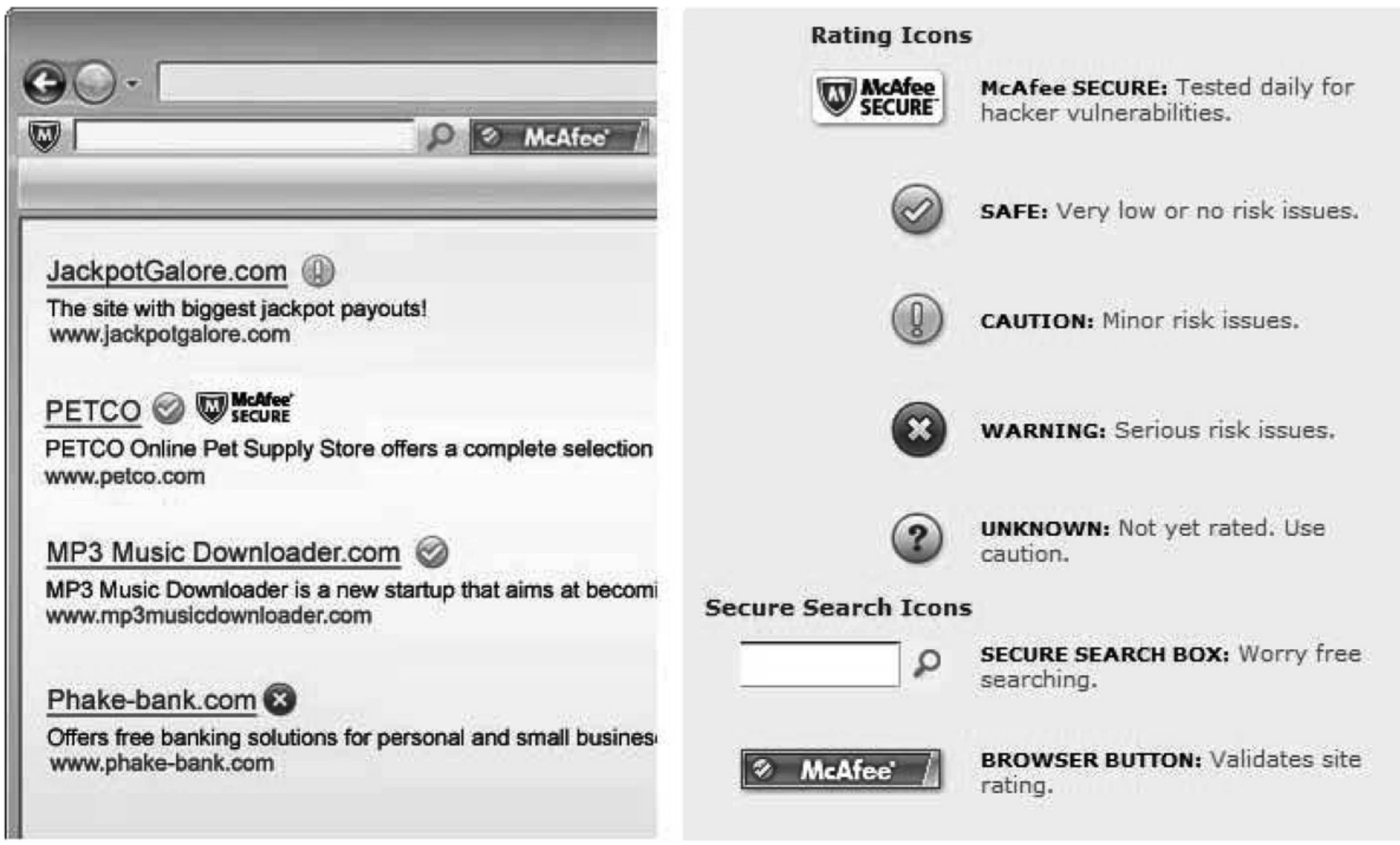
Table 5.1 | *(Continued)*

Sr. No.	*Security Measures*	*Brief Description*
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 cyber-security 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). This is explained in Box 5.11.

Source: See [32] in References section.

Box 5.13 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.



Source: http://www.siteadvisor.com/howitworks/index.html

In addition to the tools explained in Box 5.13, netizens may opt for anti-Phishing utilities (i.e., plug-ins) available for different browsers (Table 5.2) to be protected against Phishing attacks.

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 5.1 shows a simple flowchart explaining how to distinguish between a legitimate E-Mail and a phished E-Mail.

SPS Algorithm to Thwart Phishing Attacks

The 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.

Table 5.2 | Anti-Phishing plug-ins

Sr. No.	*Title*	*Website*	*Brief Description*
1	Netcraft Toolbar	http://toolbar.netcraft.com/	It offers protection from Phishing attacks.
2	TrustWatch	http://wareseeker.com/free-trustwatch/	It has a toolbar for Internet Explorer users as well as has an extension for Firefox users.
3	ScamBlocker	http://www.earthlink.net/elink/issue95/security_archive.html	It is an Earthlink Toolbar feature that helps protect users from the latest Phishing threats.
4	PhishNet 1.2	http://download.cnet.com/PhishNet/3000-2144_4-10473931.html	It protects users from web Phishing scams.
5	SpoofStick	http://www.spoofstick.com/	It helps users detect spoofed (fake) websites.
6	Google safe browsing	http://www.google.com/tools/firefox/safebrowsing/	• It is used as an extension to Firefox. • It will alert when a webpage tries asking for user's personal or financial information.
7	Windows Internet Explorer's Phishing filter	https://phishingfilter.microsoft.com/PhishingFilterFaq.aspx	• It is available in Internet Explorer 7. • It helps protect users from entering Phishing sites.

Source: See [33] in References section.

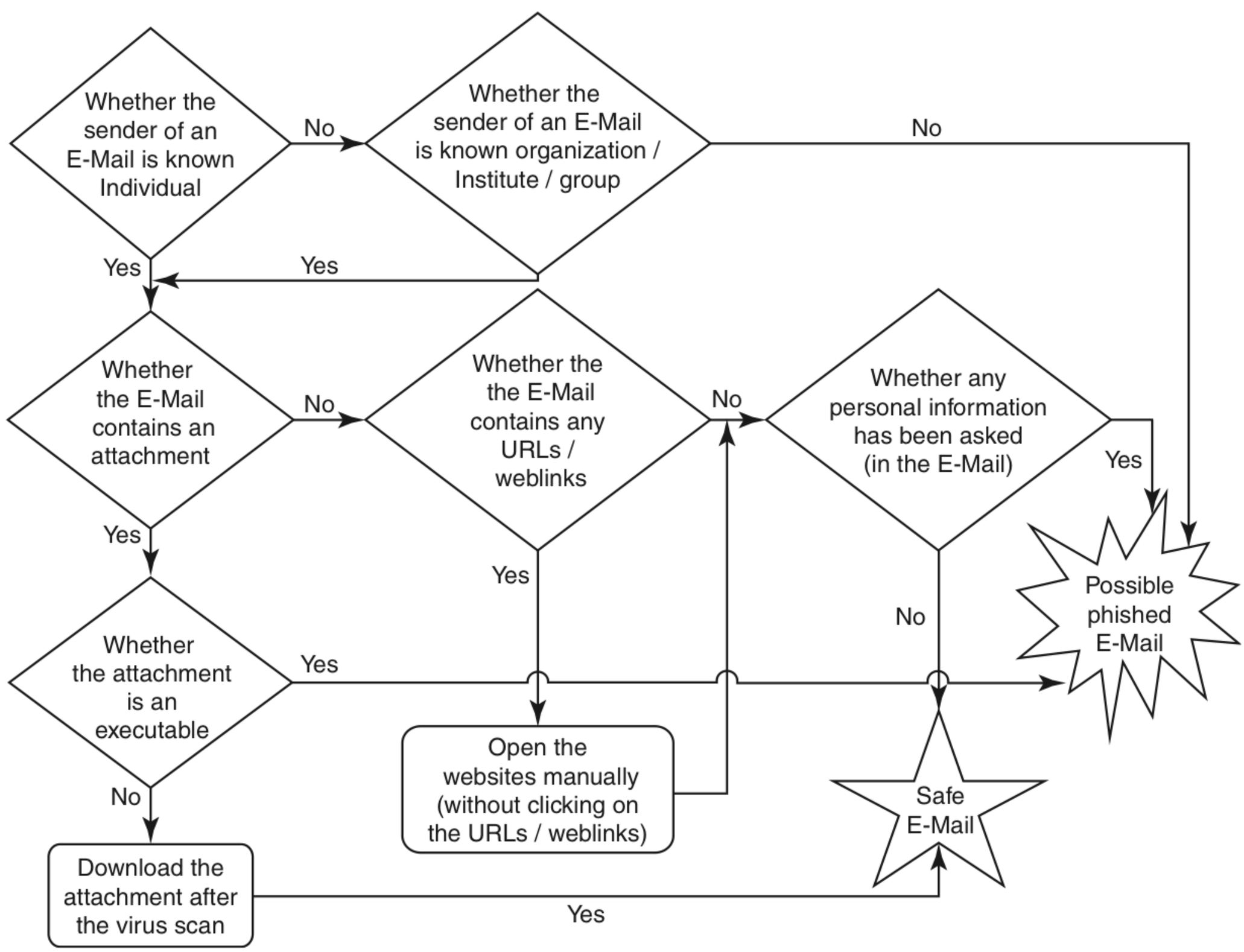


Figure 5.1 | Phishing attack – flowchart.

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.

The 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 plug-ins or personal firewalls. SPS can be based on two different 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.

5.3 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 (introduced in Section 1.5.21, Chapter 1). The person whose identity is used can suffer 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.[34] As mentioned in the "introduction" section, ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).

Visit the weblink http://njaes.rutgers.edu/money/identitytheft/default.asp to undergo a quiz on identity theft to test your awareness and to get tips to avoid to be victim of identity theft.

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 support to the society to spread awareness about this fraud (see Box 5.14).

According to 2010 Report published by Javelin Strategy & Research[35] the 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. The total fraud amount was US$ 54 billion.
2. The 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.[36]

1. **Credit card fraud (26%):** The highest rated fraud that can occur is when someone acquires the victim's credit card number and uses it to make a purchase. Chapter 11 (see Section 11.4.2) provides many illustrations on credit card frauds.
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%):** This 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.

Readers may like to visit Section 11.7, Chapter 11, where many forms of online scams are described. It is important to note the various usage of ID theft information.[37]

1. 66% of victims' personal information is used to open a new credit account in their name.
2. 28% of victims' personal information is used to purchase cell phone service.
3. 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief.

The statistics proves the importance of ID theft and the frauds related with ID theft are increasing day-by-day. ITRC, in the US, is putting enormous efforts to create awareness among the society to reduce such frauds (see Box 5.14).

Box 5.14 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.

Box 5.14 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.

Visit the weblink mentioned below to undergo the tests and quiz to know individuals preparedness toward identity theft: http://www.idtheftcenter.org/artman2/publish/c_theft_test/index.shtml

According to a September 2003 survey conducted by the FTC, an estimated 10 million people in the US found out that they were victims of ID theft in the previous year.[38] In spite of enough awareness being created and/or trainings conducted in the society, people have their own beliefs about not being a victim of ID theft fraud. Table 5.3 explains myths and facts about ID theft.

Table 5.3 | Myths and facts about identity theft

Sr. No.	*Myth*	*Fact*
1	There's no way to protect yourself from identity theft.	The risk of identity theft can be minimized by taking preventive measures such as keeping financial records duly protected and private, shredding junk mail, and keeping an eye on who sees/overlooks your personal information.
2	Identity theft is only a financial crime.	Financial identity theft is theft of information for financial gain, which is most prevalent. However, other types of identity theft are equally dangerous. For example, medical identity theft of personal medical records is used to access medical treatment or drugs, or to make false insurance claims.
3	It's my bank's fault if I become a victim of identity theft.	Some identity crime does originate with the theft of bank records or is perpetuated by lax security practices. However, the majority of identity theft begins elsewhere. Personal information may be stolen with low-technology tools such as a lost or stolen wallet, checkbook, or a debit or credit card, or more high-technology methods, such as skimming, Phishing and hacking.
4	It is safe to give your personal information over the phone if your caller ID confirms that it is your bank.	It is never safe to give personal information to unsolicited callers, no matter who they say they are. Caller IDs are easily spoofed. If you believe the caller is legitimate, hang up and call the bank back at its listed phone number.
5	Checking your credit report periodically or using a credit monitoring service is all you need to do to protect yourself from identity theft.	If anyone wants to be vigilant about identity theft, one should check their credit report regularly and one should also review their bank and credit card statements regularly. One can obtain one's free credit report in the US from each of the three credit bureaus per year from www.AnnualCreditReport.com

(*Continued*)

Table 5.3 | (*Continued*)

Sr. No.	*Myth*	*Fact*
6	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. For example, many people use their E-Mail address as a user ID for online accounts. Consider making your information available on a need-to-know basis only. Often, businesses ask for personal information they really don't need, and will simply omit information you're not willing to give.
7	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. However, relying on your shredder alone to protect you is like locking one window while leaving the rest of your house wide open. Think defensively: secure your personal information in your home, in your car and at work, and always use safe online security practices.
8	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 it's 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 sites are another good source of personal information for identity thieves. Even if you do not use them yourself, your friends or members of your family may be sharing personal information about you. Not using the Internet may offer some protection, but it won't keep you safe from online criminals.
9	Social networking is safe.	Social networking sites such as Facebook, MySpace and Twitter can be fun to use. However, they can be dangerous when it comes to your identity. These sites are used by attackers and others to steal information, trick people and promote a variety of scams. To protect yourself, avoid making personal information available to large groups of "friends," take advantage of the privacy controls offered by most of these sites, and use common sense.
10	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. Most importantly, always take care to confirm that a site is legitimate before you use it, watch out for copycat sites and keep your computer safe from viruses.

Source: See [39] in References section.

5.3.1 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 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. [Classification scheme is also explained in Chapter 9 (Section 9.11) in the context of media and asset protection.]

1. **Non-classified information**
   - **Public information:** Information that is a matter of public record or knowledge.
   - **Personal information:** Information belongs to a private individual but the individual commonly may share this information with others for personal or business reasons (e.g., addresses, telephone numbers and E-Mail addresses).
   - **Routine business information:** Business information that do not require any special protection and may be routinely shared with anyone inside or outside of the business.
   - **Private information:** Information that can be private if associated with an individual and individual can object in case of disclosure (e.g., SSN, credit card numbers and other financial information).
   - **Confidential business information:** Information which, if disclosed, may harm the business (e.g., sales and marketing plans, new product plans and notes associated with patentable inventions).
2. **Classified information**
   - **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
   - **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
   - **Top secret:** Information that requires the highest degree of protection and unauthorized 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.

5.3.2 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.

The process of recovering from the crime is often expensive, time-consuming and psychologically painful. Many a times, before a crime is detected, the fraudster is capable of running up hundreds to thousands of dollars worth of debt in the victim's name. This type of fraud often destroys a victim's credit and it may take weeks, months or even years to repair. As technology moves along and fraudsters become more advanced, financial ID theft will continue to pose a great threat to many individuals.

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. The 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.

There have been several instances where victims of criminal ID theft do not learn of an impersonation until being denied for employment or terminated from a job. This occurs when an employer conducts a criminal background search and finds that the victim has a criminal history that he/she lied about or charges that forbid him/her from working in that particular environment. When this happens, there is very little a victim can do to salvage the job, as an employer has the right to proceed with termination over entering false information on an application.

The victims of this crime are left with the burden to clear their own name in the eyes of the criminal justice system. It is very important to act quickly in order to minimize the damage and get your life back in order. What makes the process so difficult is the fact that officials working within the criminal justice system are the only ones capable of correcting the data. It is very crucial and important to contact local police department immediately in case of becoming a victim of criminal ID theft. This should be the first step in building a case and clearing your name.

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 different 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. This 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.[40] 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.[41]

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.

Visit the counterfeit gallery at the International Anti-Counterfeit Coalition website at http://iacc.org/about-counterfeiting/counterfeit-gallery/index.php to test your ability to spot fake consumer products.

Business ID theft may fuel economic and industrial espionage – which is most commonly associated with technology-heavy industries such as computer software and hardware, biotechnology, aerospace, telecommunications, transportation and engine technology, automobiles, machine tools, energy, materials and coatings and so on. See Box 5.15 to know more about industrial spy network.

The consequences of business ID theft may call for a disaster to the business, such as call out from market and damage to the reputation, and hence it is extremely important to employ countermeasures for such type of attacks (see Table 5.4).

Box 5.15 Chinese Ghost Net

China has been accused of attacking a number of groups and institutions through the use of cyber espionage, a fact which already put it high on the research team's "countries of interest" list. *GhostNet* is a spy network, accused to have been controlled from China, with the objective to hack into government and private sector companies in 103 countries.

GhostNet directs infected computers to download a Trojan known as "gh0st RAT" (also reported as Remote Access Tool) that allows attackers to gain complete and real-time control from commercial Internet access accounts located on the island of Hainan, People's Republic of China. The investigations reveal that GhostNet is capable of taking the entire control of infected computers, including searching and downloading specific files, and covertly operating attached devices such as microphones and web cameras.

This spying attack started with online espionage activities against the Tibetan community and subsequently targeted Foreign Ministries, embassies, banks and NEWS organizations across the world. Although Chinese Government has rejected all these allegations, it is reported that Foreign Ministries of Iran, Bangladesh, Latvia, Indonesia, the Philippines, Brunei, Barbados and Bhutan had been spied on remotely, and the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan were hacked.

The Toronto researchers listed the systems mentioned below as the ones they are highly confident to have been compromised:

1. Office of the Dalai Lama, India.
2. Tibetan Government in Exile, India.
3. Association of Southeast Asian Nations (ASEAN).
4. Asian Development Bank.
5. Associated Press, UK.
6. Consulate General of Malaysia, Hong Kong.
7. Department of Foreign Affairs, Indonesia.
8. Department of Foreign Affairs, Philippines.
9. International Campaign for Tibet.
10. NATO.
11. Russian Federal University Network, Russian Federation.
12. Students for a Free Tibet, US.
13. Taiwan Government Service Network, Taiwan.

If it assumed that GhostNet is a fluke and a deliberate creation of a foreign power (or the creation of a group) other than China, with the objective to search the information to sell at a profit, then there is the likelihood of many GhostNets in operation around the world, which may be operating with some specific objective. The story concludes as, GhostNet is neither the first nor the only one of its kind.

Source: http://www.darkgovernment.com/news/chinas-ghostnet/

Table 5.4 | Business identity theft – countermeasures

Sr. No.	*Facet*	*Brief Description*
1	Secure your business premises with locks and alarms	Alarm systems are effective deterrents to criminals thinking of breaking into your business, including that intent on identity theft – especially alarm systems that are monitored by a security company. Make sure that external doors have deadbolts and that exposed windows are secured with security film, bars, screens or shatter-proof glass.
2	Put your business records under lock and key	Store your physical business records, such as customer records and other data on paper, locked in filing cabinets – and lock the filing cabinets at night, or at those times during the day that you and your staff will not be "supervising" access (such as lunch time). Put copies of system and database backups and "important" business data in your safe (or in your security deposit box at the bank if you don't have an onsite safe).
3	Shred, shred and shred	Business records of any kind should never just be tossed into the trash or recycling bin where they can become a bonanza for criminals wanting to commit on identity theft; instead, all business records that you no longer have a use for should be shredded. Businesses that operate out of small and home offices can buy inexpensive shredders at any office supply store; for businesses with volumes of material to be disposed of, there are shredding services that will come and do what needs to be done. Pay special attention to the mail, a favorite source for identity theft. Anything that has your name and address on it should be shredded, and that includes most bills.
4	Be cautious on the phone	It's easy for someone to pretend to be someone they're not on the phone. Whether it's someone who wants personal information on a particular customer, or someone who claims they need to verify one of your personal accounts, don't give out information over the phone unless you can positively confirm the caller's identity. "*Information thieves and stalkers tell authorities over and over how easily they were able to obtain all sorts of valuable information simply by calling small business owners or personnel departments and asking. Posing as government agencies or credit grantors or health insurance providers, these thieves have found that a well-crafted, believable story can often get past the best locking file cabinets or password-protected computers*," warns the Better Business Bureau.
5	Limit access to your IT systems	Your computer network needs to be password protected, of course, so that anyone who wanders through your office can't just access your network. However, you also need to consider issues of internal network access. Does every employee needs to access programs or databases that may contain sensitive information? Password-protect these too and grant access on a "need-to-know" basis to help cut down identity theft.
6	Protect the IT systems from hackers	Hacking into company systems and databases appears to have become a favorite identity theft technique – perhaps because it's very easy. Your computer network needs to be protected by firewalls, which help keep out intruders by shutting out unauthorized people and letting others go only to the areas they have privileges to use. You can purchase firewalls at any computer store (or online). Another option for small or home businesses is to purchase and install a small (four to eight port) router. These often have firewall protection capability. If you're running Windows operating systems, it's also important that you keep your operating system updated, installing the various patches as they come out. Often these patches are fixes for security holes. (If you use Windows XP, you will be alerted automatically to these updates.)

(*Continued*)

Table 5.4 | (*Continued*)

Sr. No.	*Facet*	*Brief Description*
7	Create the awareness that the Internet is a dangerous place	Ordering something off the Net using a credit card is not dangerous, as long as you are placing your order through a secure site. However, there are other dangers, such as Spyware and viruses, which attempt to download automatically when you or your employees visit certain sites. If you are using Internet Explorer, make sure that you go to "Internet Options" and set the security options to a higher setting on each computer; the default is set to allow just about anything to download. Moreover, if your company has a website, be careful as to what kind of information you post on your site and how. If you are going to place sensitive information on the Net (something you should be very cautious about), such as financial data or customer databases, it needs to be password-protected and encrypted.
8	Avoid broadcasting information	"The other day while making a purchase at a computer store, an associate asked me for my phone number and popped up all my personal information on a terminal in front of him – right in plain view of five other customers! I was so curious to ask him if he wanted to read it all out loudly to make it even easier for all of them to remember it." This sort of cavalier sharing of personal information, which makes identity theft so easy, has to stop. Train your employees to be sensitive to customer information issues, making sure that they keep customer information private when they're dealing with individual customers. Turning computer screens so that they can't be viewed by anyone except the operator and other practices such as not repeating customer information loudly or not leaving files with customer information lying open on counters should be taken into consideration.
9	Create and enforce a organization-wide information security policy	The purpose of your security policy is to educate your employees about issues such as identity theft and data protection. It should include information on E-Mail policies (such as what E-Mail filters are in place and how to deal with suspicious E-Mail), computer network access, Internet use policies (such as how to increase browser security settings and safe practices, such as disconnecting from the Net after using it), customer information protection strategies and how to report incidents or violations. In other words, a manual of the issues involved with security and threats such as identity theft and what to do about them.
10	Disconnect the access of ex-employees immediately	When employees no longer work for your business, you need to be sure that their access to your computer network and company data is cut off immediately. Will all this create more trouble and expense for your small business? Yes. But unfortunately, with identity theft becoming rampant, taking these steps to prevent identity theft for you and your customers is necessary.

Source: See [42] in References section.

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.

Medical ID theft can be dangerous not only from a financial perspective as explained in the case above, but also from a medical perspective. If the fraudster has successfully stolen the victim's identity and received treatment, the record can become part of a victim's permanent medical record. For example, a patient could be unconscious after an accident. The emergency room reads that during a previous admission the "patient" indicated he/she is not allergic to the medication the doctor believes will be most beneficial for the unconscious patient. Relying on the prior medical record, the doctor administers that drug which, in reality, the patient is severely allergic to.

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.

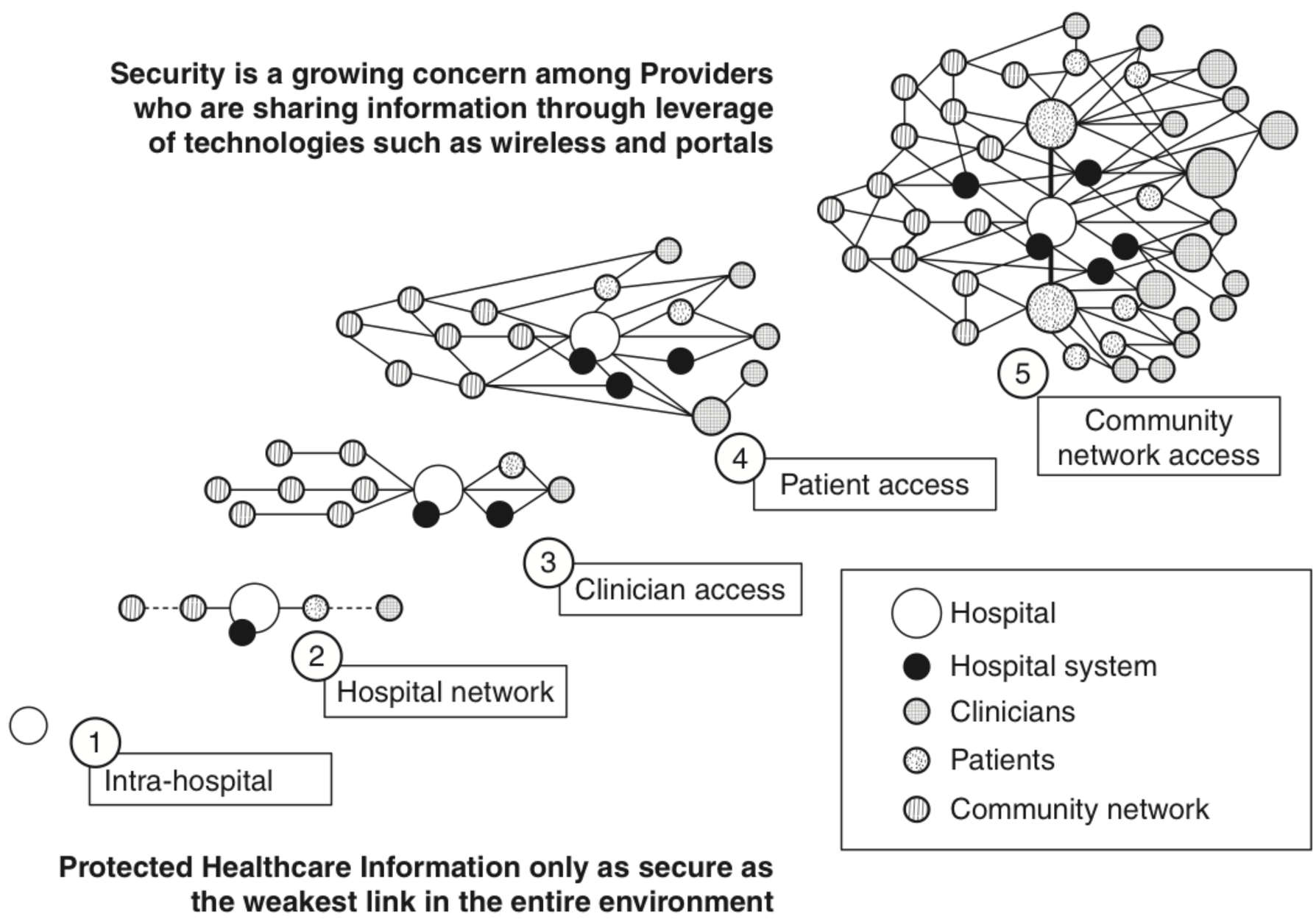


Figure 5.2 | Medical domain – interconnected entities.

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.

ModernHealthcare.com reported a noticeable spike in attempted medical ID theft. This has been confirmed during June 2008 wherein the University of Utah Hospital announced that the personal information of 2.2 million patients had been stolen.

The World Privacy Forum estimates that there are more than 250,000 cases of medical ID theft each year and acknowledges that medical ID theft is a crime that can cause great harm to the victims. Medical ID theft has been addressed by HIPAA and HITECH Acts in the US (see Box 5.16 as well as Fig. 5.2).

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.

Box 5.16 HIPAA, PHI and HITECH

The *H*ealth *I*nsurance *P*ortability and *A*ccountability *A*ct (HIPAA) enacted by the US Government in 1996, was sponsored by Senator Edward Kennedy and Senator Nancy Kassebaum. This act not only protects the Health Insurance Coverage but also detects the security and privacy of health data.

1. **HIPAA – Title I:** It regulates the availability and extent of group health plans and certain individual health insurance policies.
2. **HIPAA – Title II:** It defines numerous offenses relating to healthcare and sets civil and criminal penalties for them. It also creates several programs to control fraud and abuse within the healthcare system.

*P*rotected *H*ealth *I*nformation (PHI) is any information held by the healthcare organizations (such as hospitals, nursing homes, medical service providers and medical insurance companies) which can be interpreted broadly and includes any part of an individual's medical record or payment history.

*H*ealth *I*nformation *T*echnology for *E*conomic and *C*linical *H*ealth *A*ct (HITECH Act) is enacted as part of the American Recovery and Reinvestment Act of 2009. Subtitle D of HITECH Act dictates the privacy and security concerns associated with the electronic transmission of health information and extends the complete Privacy and Security Provisions of HIPAA to business associates of healthcare organizations (see Box 6.18, Chapter 6).

Source: http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

5.3.3 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 and explained in Chapter 2.
   - *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. This is already explained in Chapter 2.
   - *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 and it is explained in Chapter 3.
2. **Computer-based technique:** These techniques are attempts made by the attacker to exploit the vulnerabilities within existing processes and/or systems.
   - *Backup theft:* This 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 (explained in Chapter 4) to gain unauthorized access (see Box 6.1, Chapter 6) to download the required information. See Box 5.17 to know advanced form of ID theft while the victim is in travel mode.
   - *Phishing:* Phishing is explained in Section 5.2.
   - *Pharming:* Pharming is explained in Box 5.10. 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

Box 5.17 Geotagging

Geotagging is the process of adding geographical identification (such as latitude and longitude data) inside the metadata to various media such as photographs, video and/or SMS messages. Besides latitude and longitude coordinates, it can also include altitude, bearing, distance and place names. It is commonly used for photographs. Geotag information, embedded in the metadata, is stored into *E*xchangeable *I*mage *F*ile (EXIF) format or into e*X*tensible *M*etadata *P*latform (XMP) format under the photographs stored in JPEG file format. These data are not visible in the picture itself but are read and written by special programs and most digital cameras and modern scanners. The EXIF data can be read by special programs (visit www.digital-photo-software-guide.com and www.photo-freeware.net for EXIF editors), which can provide maps of the location where the photo was taken. The same geotagged photos, when shared online, can also be linked to several map services.

Risks associated with Geotagging

1. The netizens snap photographs of their families/relatives/friends during a vacation, using cell phones/digital cameras and then immediately upload them on social networking websites such as Twitter/Facebook/Orkut/Myspace. The attacker can decipher these photographs (i.e., EXIF data) to know where the victim is located when he/she took the photographs.
2. The attacker can easily find when the family is not at home and the house is vulnerable to burglary attack.
3. A simple photograph of a car parked outside the house can provide the information about the address of the home.

How to protect from Geotagging

1. Turn OFF location information into cell phones/PDAs and cameras (visit http://www.icanstalku.com/how.php to know "How to disable this configuration").
2. Refer to the manual of the device and/or consult the manufacturer of the device to disable this intrusive feature.
3. Be skeptical about uploading the photographs on social networking websites.
4. Be careful while uploading/sharing photographs of kids and spouse through E-Mails and/or uploading those on social networking websites while they may have shared with you while traveling on their own.

Source: http://en.wikipedia.org/wiki/Geotagging

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. The 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. This 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. The 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.

5.3.4 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 5.5 explains some good tips on countermeasures for identity theft.

5.3.5 How to Efface Your Online Identity

Everytime details about your identity and/or about your personal information are revealed on the Internet, you are prone to be a victim for ID theft/fraud. Hence, netizens may think to either protect their identity and/or would like to erase their identity, that is, every footprint available on the Internet. However, it is highly impossible to get one single tool that can completely eradicate each of your footprint from the Internet. Table 5.6 lists few such tools.

Table 5.5 | 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 (see Appendix C to learn E-Mail security and etiquettes).
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.
8	Protect your PII	Be cautious about giving out your personally identifiable information (PII) to anyone. Find out why the information is needed, and if it's absolutely necessary to give out. Be careful about the details you provide about yourself online, such as on social networking sites.
9	Stay alert to the latest scams	Awareness and caution are effective methods to counter fraud. Create awareness among your friends and family members by sharing security tips you learn with them.

Source: See [44] in References section.

Table 5.6 | How to protect/efface your online identity

Sr. No.	*Websites*	*Brief Description*
1	www.giantmatrix.com	**Anti Tracks:** These are set of tools that appear to be a complete solution to protect your online identity, sensitive data and maintaining the integrity of your system by hiding system's IP address, securely locking and hiding important files and folders and maintaining a healthy system performance, which keeps the system in top-notch condition.
2	www.privacyeraser.com	**Privacy Eraser Pro:** It protects Internet privacy by cleaning up all the tracks of Internet and computer activities and supports almost all popular web browsers. The main features of this utility are as follows: • Erase Browser Cache Files, Browser History, Cookies, Browser Address Bar History and Browser AutoComplete Memory. • File Shredder: Securely shred files and folders. • Cleaning Free Disk Space (Windows FAT/FAT32/NTFS). • Speed up the system.
3	www.reputationdefender.com	**MyPrivacy:** It removes your personal information such as name, address, age, phone, past address and any other related information. It also helps by continuously monitoring the Internet to remove the footprint available on the Internet.
4	www.suicidemachine.org	**Web 2.0 Suicide Machine:** It completely roots out your identity from the servers of social networking websites such as MySpace, Twitter and LinkedIn. One will have to reveal the login credentials for the corresponding web applications (webapps) to use this tool. Hence, if he/she does not need them anymore then he/she can let suicide machine eradicate the details from these webapps. It is reported that Facebook have blocked access of Web 2.0 Suicide Machine because Suicide Machine collects login credentials and scrapes Facebook pages. This has been reported as violation of Facebook Statement of Rights and Responsibilities, which has resulted into inability of suicide machine to erase your identity on the Facebook.
5	www.seppukoo.com	**Seppukoo:** It is an *anti-social network* failing to destroy your identity, specifically the footprint on the Facebook. The website is named after the "seppuku ritual suicide" practiced by ancient Japanese samurai warriors and the website draws a parallel between restoring a samurai's honor and the "liberation of the digital body." This website is operated by a group that calls itself Les Liens Invisibles, an "imaginary art group from Italy."

Summary

Phishers use different methods and techniques with one common goal of deception, to obtain personal information from the netizens. Phishers have strong technical knowledge and have innovative ideas to deceive the netizens into

1. Believing the messages are received from a trusted source.
2. Believing that the website and/or webpage is a trusted organization and/or institution.

3. Entice the Spam filter to identify that a Phishing E-Mail is legitimate.

Phishing attacks cannot be stopped with any technique and/or technology. However, good practices can reduce the prevalence of Phishing and related losses suffered from Phishing scams.

Phishing is a common form of ID theft in which the netizens are tricked into revealing confidential information about them with economic value. ID theft is increasing day-by-day and awareness and training is the key to fight against numerous attacks launched to entice the people to reveal their personal information. Besides the countermeasures, one has to be continuously vigilant while disclosing personal information and should evenly treat the risk while disclosing personal information on the Internet, while on the phone or while in person. Many scenarios and case illustrations are provided in Chapter 11 explaining Phishing scams and ID theft.

Review Questions

1. What is Phishing? Explain with examples.
2. Differentiate between Spam and hoax mails.
3. What are the different methods of Phishing attack?
4. What is Spear Phishing? Explain with examples.
5. What is whaling? Explain the difference between whaling and Spear Phishing.
6. What is identity theft? Explain with examples.
7. How can information be classified?
8. What are the different types of ID theft?
9. What are the different techniques of ID theft?
10. How to prevent being a victim of ID theft?

References

[1] To know more about the world Phishing map, visit: http://www.avira.com/en/threats/section/worldphishing/top/7/index.html (25 July 2010).

[2] Phishing statistics into graphical illustrations can be visited at: http://www.m86security.com/labs/phishing_statistics.asp (25 July 2010).

[3] To monitor Phishing attacks daily, visit: http://www.phishtank.com/stats.php (25 July 2010).

[4] May 2009 Phishing Report complied by Symantec Security Response Anti-Fraud Team can be visited at: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_05-2009.en-us.pdf (25 July 2010).

[5] Phishing Activity Trends Report of Q4-2009 published by APWG can be visited at: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf (25 July 2010).

[6] To find definition of Phishing, visit: http://en.wikipedia.org/wiki/Phishing (9 September 2009).

[7] To find definition of Phishing, visit: http://www.webopedia.com/TERM/P/phishing.html (9 September 2009).

[8] To find definition of Phishing, visit: http://www.techweb.com/encyclopedia/defineterm.jhtml?term=phishing (9 September 2009).

[9] Visit Phishing attacks launched on most reputed and popular organizations' websites at: http://www.brighthub.com/computing/smb-security/articles/64477.aspx#ixzz0qFgacNDU (9 September 2009).

[10] To know tactics employed by the phisher, visit: http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx (9 September 2009).

[11] Ways to reduce the amount of Spam E-Mails we receive: http://en.wikipedia.org/wiki/E-Mail_spam (2 December 2009).

[12] To know more about hoax E-Mails, visit: http://en.wikipedia.org/wiki/Hoax (5 December 2009).
[13] To know methods of Phishing, visit: http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions (9 September 2009).
[14] To know more about website Spoofing, visit: http://en.wikipedia.org/wiki/Website_spoofing (5 December 2009).
[15] To know more about cross-site scripting, visit: http://en.wikipedia.org/wiki/Cross-site_scripting (5 December 2009).
[16] To know more about cross-site request forgery, visit: http://en.wikipedia.org/wiki/Cross-site_request_forgery (5 December 2009).
[17] To know more about Phishing techniques, visit: http://www.brighthub.com/internet/security-privacy/articles/67339.aspx (26 July 2010).
[18] To know more about Phishing Net survey, visit: http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm (26 July 2010).
[19] To know more about whaling, visit: http://netforbeginners.about.com/od/w/f/whatiswhaling.htm (18 June 2010).
[20] To know more about Phishing scams, visit: http://pcworld.about.com/od/emailsecurity/Types-of-Phishing-Attacks.htm (6 July 2010).
[21] To know more about Pharming, visit: http://en.wikipedia.org/wiki/Pharming (9 September 2009).
[22] To know more about Phoraging, visit: http://en.wikipedia.org/wiki/Phoraging (9 September 2009).
[23] To know definition of DNS hijacking, visit: http://en.wikipedia.org/wiki/DNS_hijacking (18 June 2010).
[24] To know definition of DNS hijacking, visit: http://www.pcmag.com/encyclopedia_term/0,2542,t=DNS+hijacking&i=41622,00.asp (18 June 2010).
[25] To know definition of Click Fraud, visit: http://en.wikipedia.org/wiki/Click_fraud (18 June 2010).
[26] To know definition of Click Fraud, visit: http://www.webopedia.com/TERM/c/click_fraud.html (18 June 2010).
[27] To know more about SSL certificate forging, visit: http://www.symantec.com/connect/blogs/phishing-toolkit-attacks-are-abusing-ssl-certificates (30 July 2010).
[28] To know more about search engine optimization (SEO), visit: http://en.wikipedia.org/wiki/Search_engine_optimization (26 July 2010).
[29] To know more about search engine optimization (SEO), visit: http://www.securityfocus.com/brief/701 (26 July 2010).
[30] To know more about techniques used for Black hat SEO attacks, visit: http://www.net-security.org/secworld.php?id=9084 (26 July 2010).
[31] To know more on Phishing kits – Xrenoder Trojan Spyware and Cpanel google, visit: http://www.anti-phishing.info/phishing-kit.html (30 July 2010).
[32] How to avoid to be victim of Phishing attack – http://articles.techrepublic.com.com/510010878_115818568.tml?tag=rbxccnbtr1 (2 December 2009).
[33] To know more on anti-Phishing plug-ins, visit: http://www.brighthub.com/computing/smb-security/articles/42784.aspx (8 June 2010).
[34] To know more about definition of identity theft, visit: http://en.wikipedia.org/wiki/Identity_theft (8 September 2009).
[35] To know more about identity theft statistics, visit: http://www.spendonlife.com/blog/2010-identity-theft-statistics (30 March 2010).
[36] To know more about identity theft statistics, visit: http://www.spendonlife.com/guide/2009-identity-theft-statistics (30 March 2010).
[37] To know uses of victim information, visit: http://www.spamlaws.com/id-theft-statistics.html (18 December 2009).
[38] To know more about ID theft statistics, visit: http://www.howstuffworks.com/identity-theft.htm (2 December 2009).

[39] To know myths and facts about identity theft, visit: http://www.networksecurityedge.com/content/ten-common-identity-theft-myths-dispelled (2 December 2009).

[40] The article *Identity Theft: The 'Business Bust-Out'* can be visited at: http://www.businessweek.com/smallbiz/content/jul2007/sb20070723_261131.htm?chan=smallbiz_smallbiz+index+page_top+stories (5 January 2010).

[41] To know more on business sensitive information, visit: http://www.businessdictionary.com/definition/sensitive-information.html#ixzz13BzGtac2 (5 January 2010).

[42] To know more on business identity theft – countermeasures, visit: http://sbinfocanada.about.com/od/insurancelegalissues/a/identitytheft.htm (5 December 2009).

[43] To know more on medical ID theft, visit: http://www.webopedia.com/DidYouKnow/Internet/2009/medical_identity_theft.asp (9 June 2010).

[44] To know more on how to protect/eradicate your online identity, visit: http://www.net-security.org/article.php?id=1366 (5 January 2010).

Further Reading

Additional Useful Web References

1. To more about the article *Evolutionary Study of Phishing*, visit: http://www.cc.gatech.edu/projects/doi/Papers/DIrani_eCrime_2008.pdf (26 July 2010).
2. To know more about the article *Learning to Detect Phishing Emails*, visit: http://www2007.org/papers/paper550.pdf (26 July 2010).
3. To know more about the article *Detecting Phishing E-Mails by Heterogeneous Classification*, visit: http://digital.csic.es/bitstream/10261/21694/1/detecting.pdf (26 July 2010).
4. To know more about the article *What is Phishing?*, visit: http://antivirus.about.com/od/emailscams/ss/phishing.htm (6 July 2010).
5. To know more about tabnapping, visit: http://www.computerworld.com/s/article/9177326/Sneaky_browser_tabnapping_phishing_tactic_surfaces (9 July 2010).
6. To know more about tabnapping technique, visit: http://www.exploit-db.com/papers/13950/ (9 July 2009).
7. To know more about *Security Labs Report*, visit: (January–June 2010): http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_1H2010.pdf (26 July 2010).
8. To know more about the article *There is No Free Phish: An Aanalysis of "Free" and Live Phishing Kits*, visit: http://www.usenix.org/event/woot08/tech/full_papers/cova/cova_html/ (26 July 2010).
9. Visit DIY Phishing kits introducing new features at: http://www.zdnet.com/blog/security/diy-Phishing-kits-introducing-new-features/1104 (26 July 2010).
10. To know more about Phishing attacks and countermeasures, visit: http://www.cert-in.org.in/knowledgebase/whitepapers/ciwp-200-03.pdf (26 July 2010).
11. To know more on article *How Identity Theft Works*, visit: http://www.howstuffworks.com/identity-theft.htm (8 September 2009).
12. To know more on identity theft, visit: http://www.identitytheft.org/ (8 September 2009).
13. To know more on identity theft, visit: http://www.321identitytheftnews.com/ (8 September 2009).
14. To know about article *2009 Identity Theft Statistics*, visit: http://www.spendonlife.com/guide/2009-identity-theft-statistics (8 September 2009).
15. To know more on article *Your Growing Exposure for Identity Theft Risks,* visit: http://www.idtheft101.net/articles/wiley_rein_white_paper.pdf (26 July 2010).

16. To know about article *NCUA – Guidance on Identity Theft and Pretext Calling*, visit: http://www.ffiec.gov/ffiecinfobase/resources/info_sec/frb-sr-01-identity_theft_pretext_calling.pdf (26 July 2010).
17. To know about article *Privacy and Identity Theft Conference*, visit: http://blogs.technet.com/privacyimperative/archive/2008/12/23/privacy-identity-theft-conference.aspx (27 June 2010).
18. To know about article *Identity Theft and the Internet*, visit: http://www.student.cs.uwaterloo.ca/~cs492/papers/idTheft.pdf. (27 June 2010).
19. http://money.howstuffworks.com/identity-theft4.htm (Accessed on)
20. To know about article *CID, Mumbai: Phishing Case*, visit: http://www.cybercellmumbai.com/case-studies/case-of-fishing (27 June 2010).
21. To know more about identity theft, visit: http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf (27 June 2010).
22. To know more about identity theft, visit: http://www.nacrc.org/events/annualconfpresentations2005/idtheftnacojuly05.pdf (27 June 2010).
23. To know more about the article *Identity Theft – Case Studies*, visit: http://www.id-theft-info.com/Case-Studies.html (10 June 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Ibid Chapter 29 (*Privacy – Fundamental Concepts and Principles*), Chapter 30 (*Privacy – Business Challenges*), Chapter 31 (*Privacy – Technological Challenges*) and Chapter 32 (*Web Services and Privacy*).
3. Hayward, C.L. (2004) *Identity Theft*, Nova Science Publishers Inc., USA.
4. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Articles and Research Papers

1. To read article *Who Is Fighting Phishing*, visit: http://www.markmonitor.com/download/wp/wp-fighting-phishing.pdf (8 June 2010).
2. To read article *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You*, visit: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (8 June 2010).
3. Dr. Kamlesh Bajaj's scholarly paper *The Cybersecurity Agenda Mobilizing for International Action* is available at: http://www.dsci.in/sites/default/files/cybersecurity_-_mobilizing_for_international_action_0.pdf (28 October 2010). It was presented at the EastWest Institute.
4. Proceedings of "Hack.in 2009" – the 3rd Hacker's Workshop on Computer and Internet Security, organized by IIT Kanpur, can be downloaded at: http://www.security.iitk.ac.in/hack.in/2009/repository/proceedings_hack.in.pdf (28 October 2010).
5. To know more about article *Stopping Distributed Phishing Attacks* by Alex Tsow, Markus Jakobsson and Filippo Menczer, visit http://archive.nyu.edu/bitstream/2451/15020/2/Infosec+BOOK_Tsow+Jacobson.htm (10 October 2010).

The appendices that serve as extended material for the topic addressed are: A, C, D, E, L, M, O, V. These are provided in the companion CD.