Box 2.5 Ports and Ports . . . (*Continued*)

Open ports present two vulnerabilities of which administrators must be wary:

1. Vulnerabilities associated with the program that is delivering the service.
2. Vulnerabilities associated with the OS that is running on the host.

Closed ports present only the latter of the two vulnerabilities that open ports do. Blocked ports do not present any reasonable vulnerabilities. There is also the possibility that there are no known vulnerabilities in either the software (program) or the OS at the given time.[2]

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

Most of the tools listed in Table 2.2 are used for computer network scanning as well.

Usually, most of the attackers consume 90% of the time in scanning, scrutinizing and gathering information on a target and 10% of the time in launching the attack.

2.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password (we will address it in Chapter 4);
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

2.3 Social Engineering

Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action. Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes. It is generally agreed that people are the weak link in security and this principle makes social engineering possible. A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behavior so that

Box 2.6 Social Engineering Example

Mr. Joshi: Hello?

The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

Mr. Joshi: Ohh ... okay. I will be at my home by then, anyway.

Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?

Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?

Mr. Joshi: My password is "ABCD1965," all characters in upper case.

Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.

Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting in trouble. The sign of truly successful social engineers is that they receive information without any suspicion. A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on (see Box 2.6).

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

Human-based social engineering refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.

1. **Impersonating an employee or valid user:** "Impersonation" (e.g., posing oneself as an employee of the same organization) is perhaps the greatest technique used by social engineers to deceive people. Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to help someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.
2. **Posing as an important user:** The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system. The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.
3. **Using a third person:** An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
4. **Calling technical support:** Calling the technical support for assistance is a classic social engineering example. Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

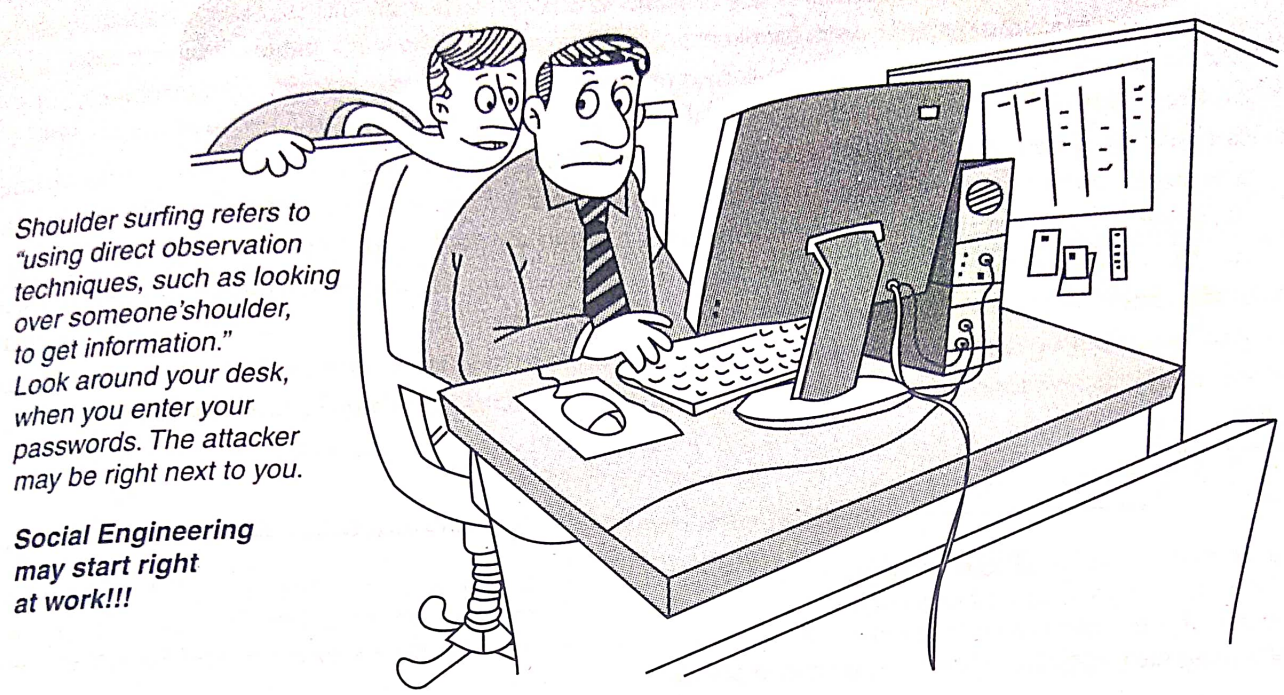

Figure 2.3 | Social engineering – shoulder surfing.

5. **Shoulder surfing:** It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system (Fig. 2.3).
6. **Dumpster diving:** It involves looking in the trash for information written on pieces of paper or computer printouts. This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded. It is also called dumpstering, binning, trashing, garbing or garbage gleaning. "Scavenging" is another term to describe these habits. In the UK, the practice is referred to as "binning" or "skipping" and the person doing it is a "binner" or a "skipper."

In practice, *dumpstering* is more like fishing around than diving in. Usually, people dumpster dive to search the items, to reclaim those, which have been disposed of but can still be put to further use, for example, E-Waste, furniture, clothes, etc. The term "dumpster diving" may have originated from the notional image of someone leaping into large rubbish bins, the best known of which are produced under the name "dumpster." "Scavenging" is equivalent of "dumpster diving," in the digital world. It is a form in which discarded articles and information are scavenged in an attempt to obtain/recover advantageous data, if it is possible to do so. Consider, for example, going through someone's trash to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN number in India, credit card identity (ID) numbers, etc.]. According to a definition in the glossary of terms for the convoluted terminology of information warfare, "scavenging" means "searching through object residue (e.g., discarded disks, tapes, or paper) to acquire sensitive data without authorization."

Computer-Based Social Engineering

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet. For example, sending a fake E-Mail to the user and asking him/her to re-enter a password in a webpage to confirm it.

1. **Fake E-Mails:** The attacker sends fake E-Mails (see Box 2.7) to numerous users in such that the user finds it as a legitimate mail. This activity is also called "Phishing" (we shall address it in Chapter 5). It is an attempt to entice the Internet users (netizens) to reveal their sensitive personal information, such as user names, passwords and credit card details by impersonating as a trustworthy and legitimate organization and/or an individual. Banks, financial institutes and payment gateways are the common targets. Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website. This Phishing is also an example of social engineering techniques used to fool netizens. The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails lures to *fish* for passwords and financial data from the sea of Internet users (i.e., netizens). The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users. As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

Box 2.7 Fake E-Mails

Free websites are available to send fake E-Mails. From Fig. 2.4, one can notice that "To" in the text box is a blank space. Hence, anyone can fill any E-Mail address with the intention of fooling the receiver of the E-Mail. In such a case when the receiver will read the mail, he/she would think that the E-Mail has been received from a legitimate sender.

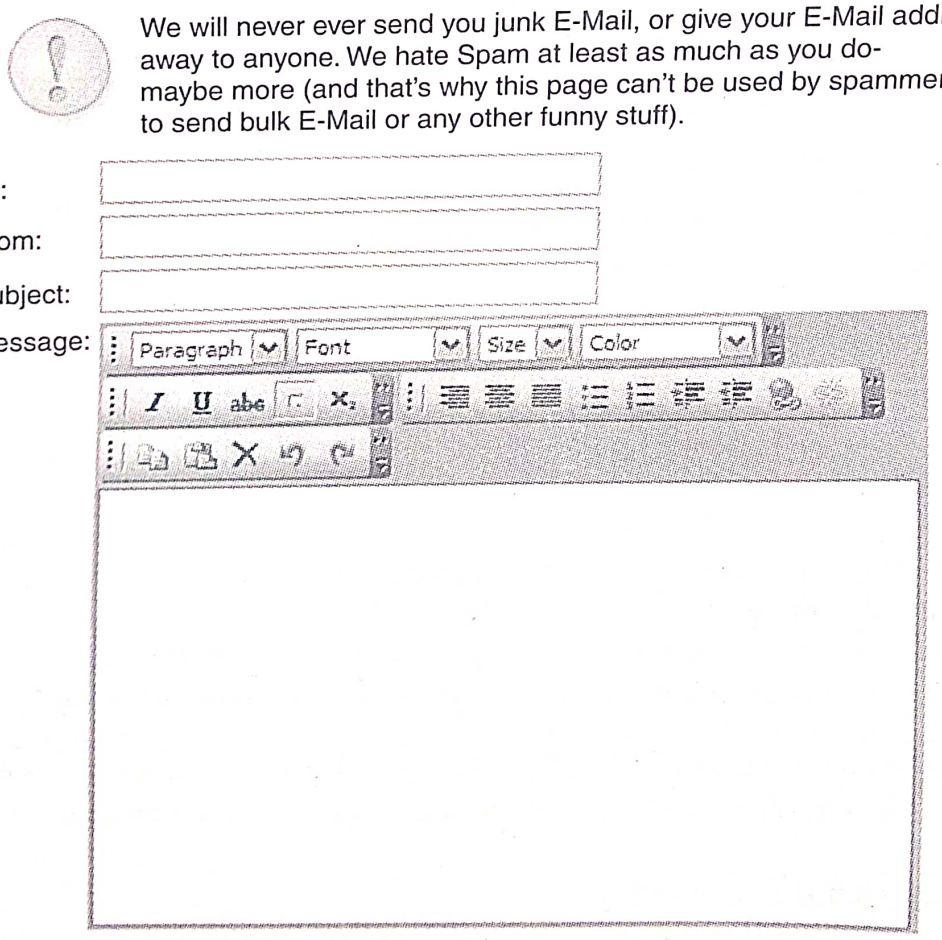

Figure 2.4 | Sending fake E-Mails.
Source: http://deadfake.com/Send.aspx (2 April 2009).

2. **E-Mail attachments:** E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment. We will address keylogger, viruses, Trojans, and worms in Chapter 4.
3. **Pop-up windows:** Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Social engineering indeed is a serious concern as revealed by the following past statistics on numbers:

1. As per Microsoft Corporation recent (October 2007) research, there is an increase in the number of security attacks designed to steal personal information (PI) or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was US$ 1.8 million.
2. The Federal Trade Commission (FTC) report of 2005 shows that "more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations" (2005, Consumer Fraud and Identity Theft section, para 1; we will discuss ID Theft in Chapter 5).
3. According to a 2003 survey [released on 2 April 2006 by the United States Department of Justice (Identity Theft Hits Three Percent, para 1)], "An estimated 3.6 million – or 3.1% – of American households became victims of ID theft in 2004." This means that now, more than ever, individuals are at a high risk of having their PI stolen and used by criminals for their own personal gain.

Typically, many organizations have information valuable enough to justify expensive protection mechanisms/security mechanisms. Critical information may include patient records in the medical and healthcare domain [known as protected health information (PHI)], corporate financial data, electronic funds transfers, access to financial assets in the financial services domain, and PI about clients or employees. Compromising critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and collapse of the organization. To respond to the threats, organizations implement InfoSec plans to establish control of information assets. However, "social engineers" try to device a way to work their way around this to obtain the valuable information, an illicit act on ethical grounds.

Social engineering succeeds by exploiting the trust of the victim. Hence, continuous training/awareness sessions about such attacks are one of the effective countermeasures. Strict policies about service desk staff never asking for personally identifying information, such as username and passwords, over the phone or in person can also educate potential victims and recognize a social engineering attempt.

Social engineering and dumpster diving are also considered passive information-gathering methods.

2.4 Cyberstalking

The dictionary meaning of "stalking" is an "*act or process of following prey stealthily – trying to approach somebody or something.*" Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group

of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threat ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.[3]

Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. **Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
2. **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet (see Table 2.1). The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyberstalking

The majority of cyberstalkers are men and the majority of their victims are women. Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking. In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor. However, there also have been many instances of cyberstalking by strangers.

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

Box 2.8 Cyberbullying

The National Crime Prevention Council defines *Cyberbullying* as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.[4]

Source: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails (refer to Chapter 5).

2.4.4 Real-Life Incident of Cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi[5] – the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved, we have changed their names.

Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad. The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.

A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. This person was chatting on the Internet, using her name and giving her address, talking in obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

This was the first time when a case of cyberstalking was registered. Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

2.5 Cybercafe and Cybercrimes

In February 2009, Nielsen survey[6] on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication. Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people.

Public computers, usually referred to the systems, available in cybercafes, hold two types of risks. First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as *keyloggers* or *Spyware*, (we will discuss it in Chapter 4) which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior. Second, over-the-shoulder peeping (i.e., shoulder surfing) can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

Indian Information Technology Act (ITA) 2000[7] (it is discussed in great detail in Chapter 6) does not define cybercafes and interprets cybercafes as "network service providers" referred to under the erstwhile Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. The concept of "due diligence" was interpreted from the various provisions in cybercafe regulations where available or normal responsibilities were expected from network service providers.

Cybercriminals prefer cybercafes to carry out their activities. The criminals tend to identify one particular personal computer (PC) to prepare it for their use. Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target – techniques used for this are discussed in Chapter 4. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

A recent survey conducted in one of the metropolitan cities in India reveals the following facts (this is an eye-opener after going through the following observations:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cybercriminals hoodwink the investigating agencies. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button.[8] Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack (Phishing attacks are explained in Chapter 5) was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security.

There are thousands of cybercafes across India. In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.

There is an expectation that the Indian Computer Emergency Team referred to under Section 70B of ITA 2008 may itself be designated as the agency of the Central Government with a national jurisdiction and (Computer Emergency Response Team) CERT, and may itself be stepping into the shoes of the Indian Computer Emergency Team.[7,8]

Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or "sign out" before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options before logon.
2. **Stay with the computer:** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.
3. **Clear history and temporary files:** Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. Therefore, before you begin browsing, do the following in case of the browser Internet Explorer:
   - Go to *Tools* → *Internet options* → click the *Content* tab → click *AutoComplete*. If the checkboxes for passwords are selected, deselect them. Click *OK* twice.
   - After you have finished browsing, you should clear the history and temporary Internet files folders. For this, go to *Tools* → *Internet options* again → click the *General* tab → go to *Temporary Internet Files* → click *Delete Files* and then click *Delete Cookies*.
   - Then, under history, click clear history. Wait for the process to finish before leaving the computer.
4. **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.
5. **Avoid online financial transactions:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.
6. **Change passwords:** The screenshot displayed in Fig. 2.5 by ICICI Bank about changing the bank account/transaction passwords is the best practice to be followed.[9]
7. **Virtual keyboard:** Nowadays almost every bank has provided the virtual keyboard on their website. The advantages of utilizing virtual keyboard and its functions are displayed in the screenshot shown in Fig. 2.6.[10]
8. **Security warnings:** One should take utmost care while accessing the websites of any banks/financial institution. The screenshot in Fig. 2.7 displays security warnings very clearly (marked in bold rectangle), and should be followed while accessing these financial accounts from cybercafe.

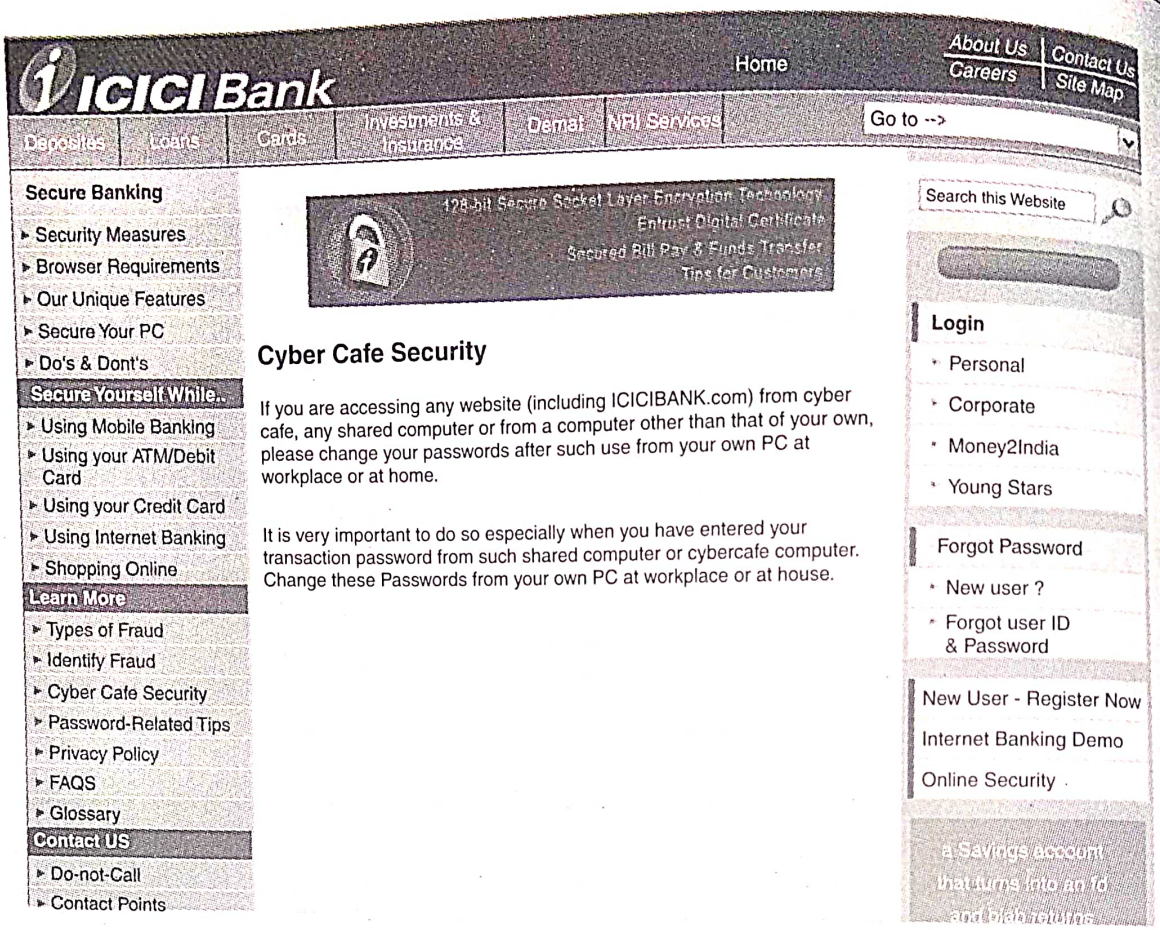

Figure 2.5 | Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).

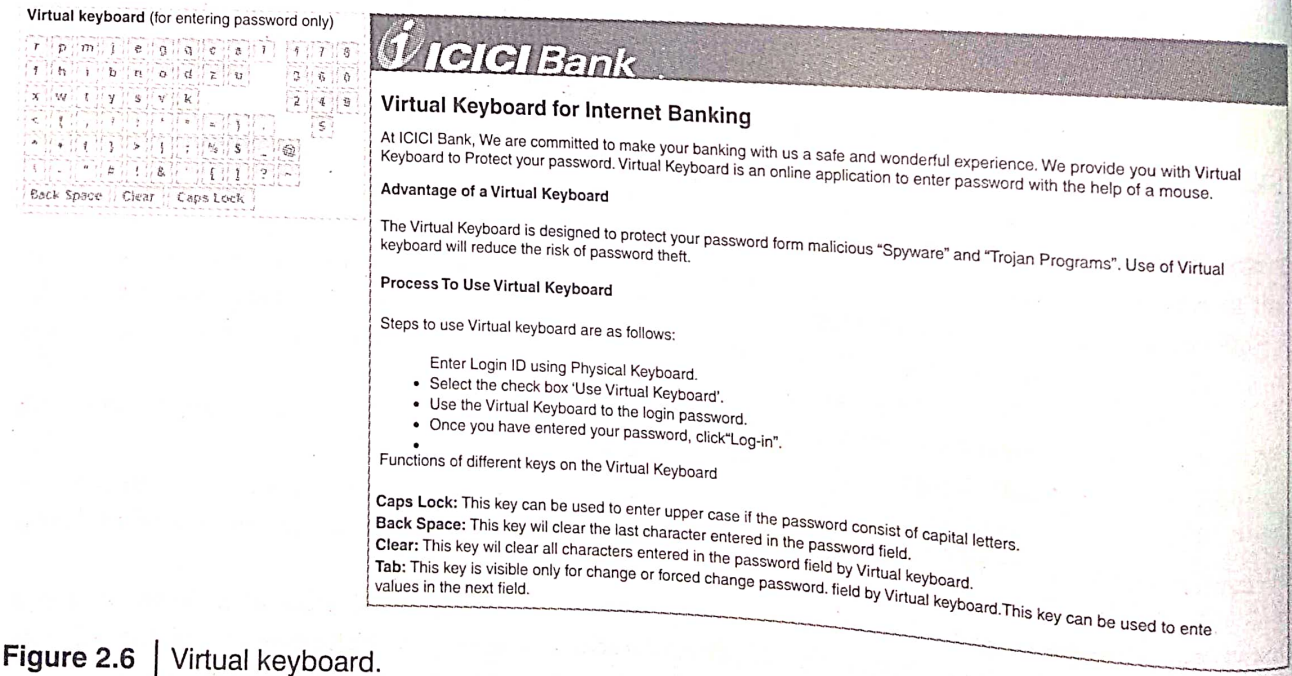

Figure 2.6 | Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

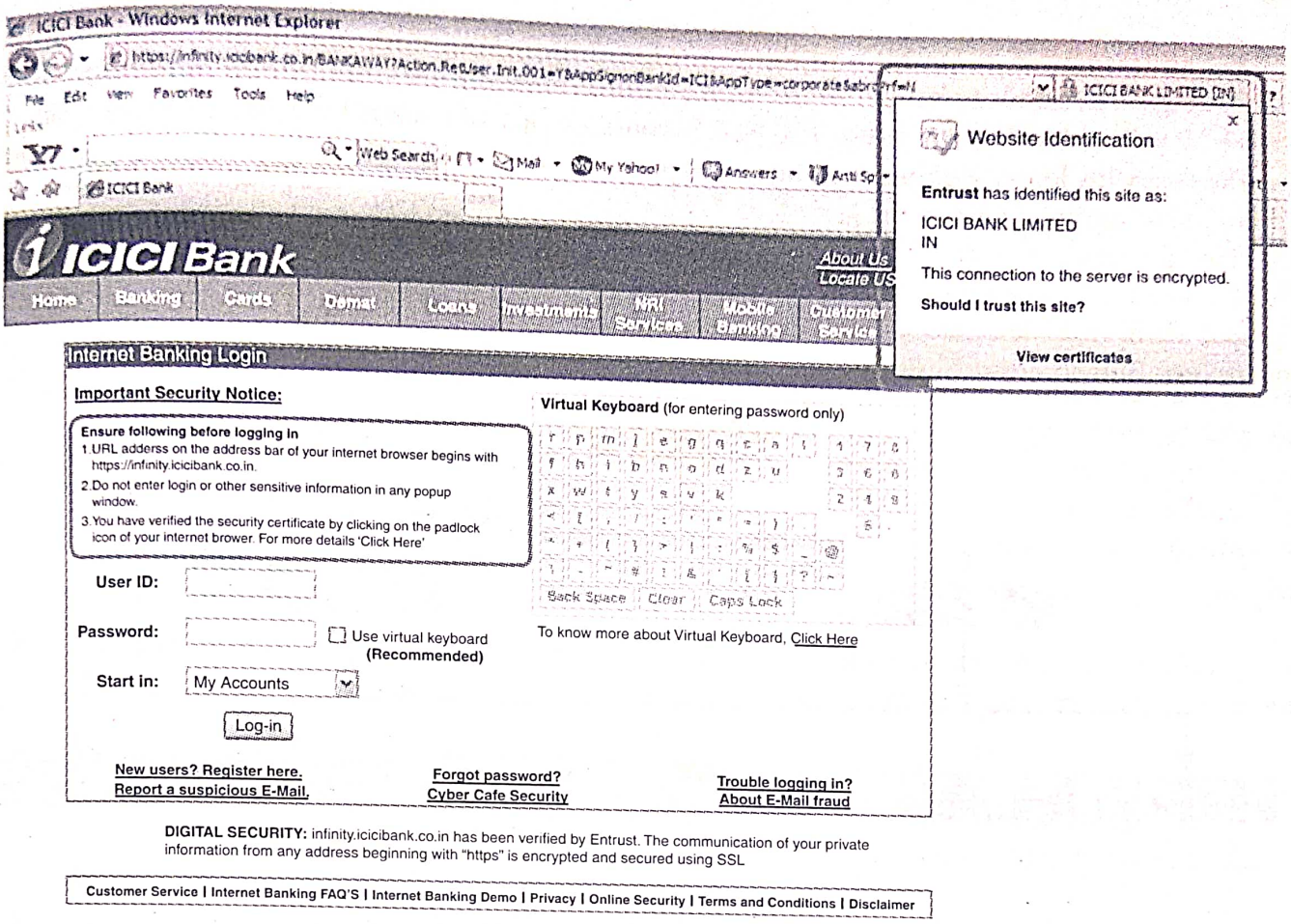

Figure 2.7 | Security warnings.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Individual should take care while accessing computers in public places, that is, accessing the Internet in public places such as hotels, libraries and holiday resorts. Moreover, one should not forget that whatever is applicable for cybercafes (i.e., from information security perspective) is also true in the case of all other public places where the Internet is made available (refer to Appendix J in CD). Hence, one should follow all tips about safety and security while operating the systems from these facilities.

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

The dictionary meaning of Bot is "(*computing*) *an automated program for doing some particular task, often over a network.*"

Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically. The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.[11]

In simple terms, a Bot is simply an automated computer program (explained in Box 1.2, Chapter 1). One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access. Your computer system maybe a part of a Botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks (the term is discussed in detail in Chapter 4).

A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge. "*Zombie networks*" (explained in Chapter 1, Fig. 1.3) have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools. Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.

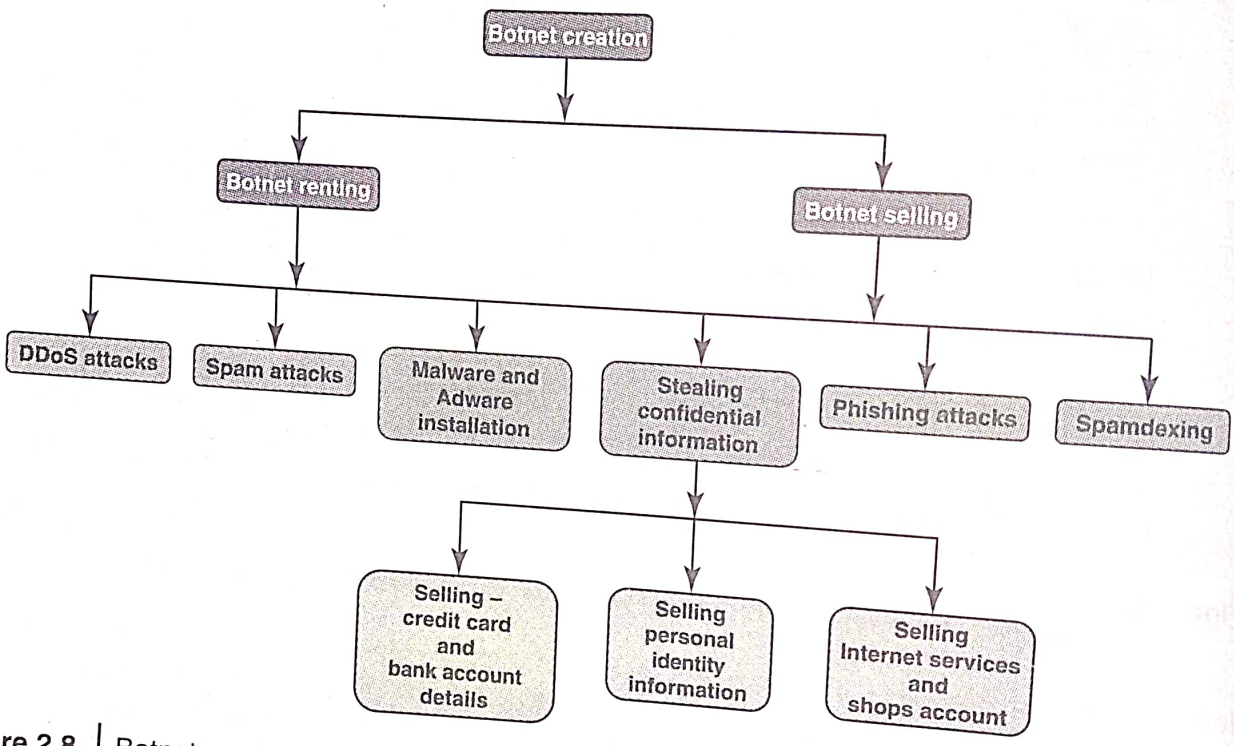

Figure 2.8 | Botnets are used for gainful purposes.

Box 2.9 Explanation for Technical Terms used in Fig. 2.8

Malware: It is malicious *software*, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.

Adware: It is *advertising-supported software*, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.

Spam: It means unsolicited or undesired E-Mail messages (this is discussed in detail in Chapter 5).

Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.

DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods (this is discussed in details in Chapter 4).

A Botnet (also called as zombie network) is a network of computers infected with a malicious progra that allows cybercriminals to control the infected machines remotely without the users' knowledge. "Zomb *networks*" (explained in Chapter 1, Fig. 1.3) have become a source of income for entire groups of cybercrim nals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge requir to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same wa to protect them from detection by antivirus tools. Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.

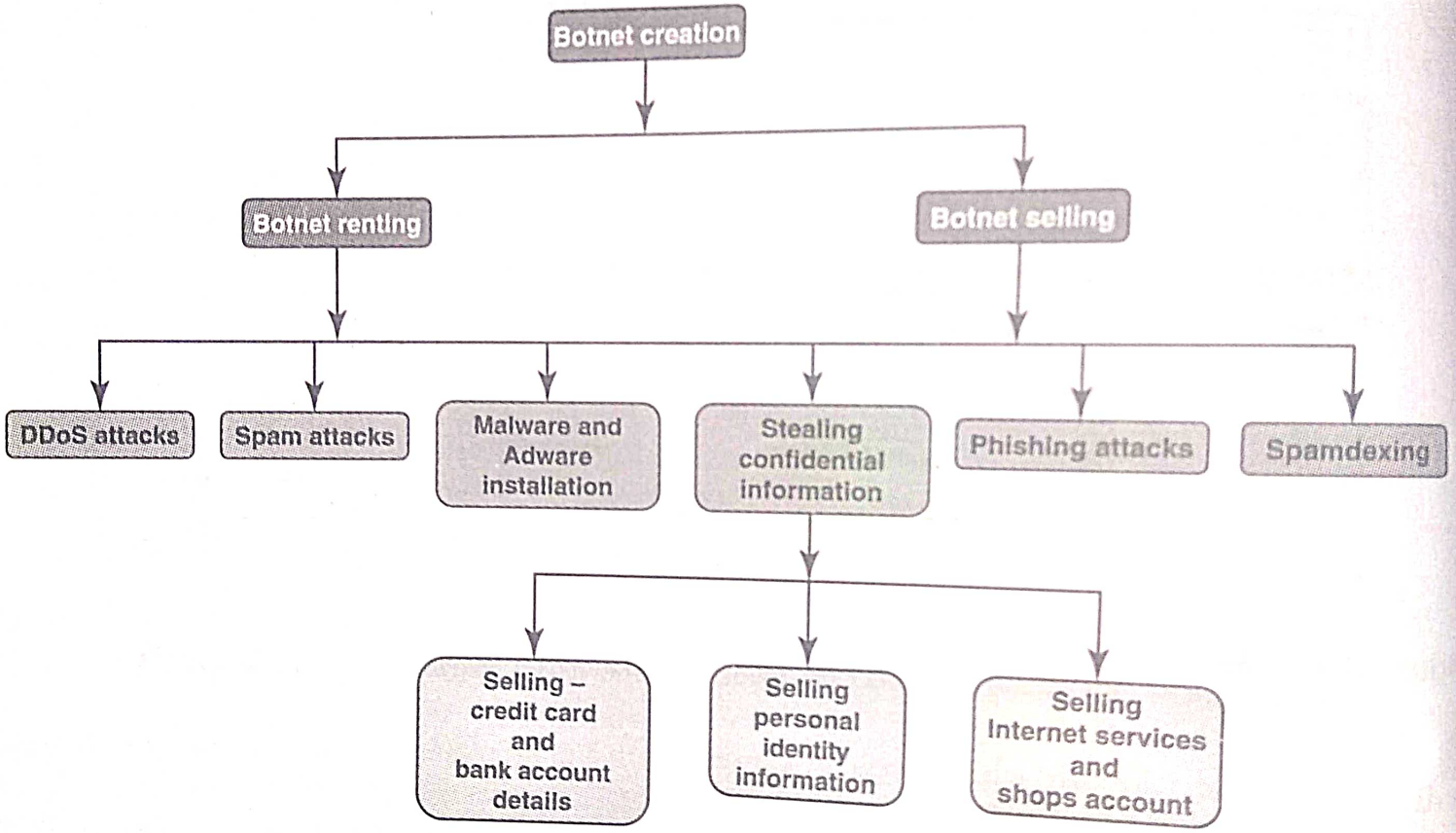

Figure 2.8 | Botnets are used for gainful purposes.

Box 2.9 Explanation for Technical Terms used in Fig. 2.8

Malware: It is malicious *software*, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.

Adware: It is *advertising-supported software*, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.

Spam: It means unsolicited or undesired E-Mail messages (this is discussed in detail in Chapter 5).

Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of meth ods, such as repeating unrelated phrases, to manipulate the relevancy or prom indexed by a search engine in a manner inconsistent with the purp

DDoS: Distributed denial-of-service attack (DDoS) a

One can reduce the chances of becoming part of a Bot by limiting access into the system. Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open. One can ensure following to secure the system: [12,13]

1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
3. **Use a firewall to protect the system from hacking attacks while it is connected on the Internet:** A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-à-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.
5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.
7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

2.7 Attack Vector

An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.[14]

To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof. A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.

Box 2.10 Zero-Day Attack

A zero-day (or zero-hour) attack[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package.

Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also visit the weblink http://www.isotf.org/zert to get more information about it.

Source: http://en.wikipedia.org/wiki/Zero_day_attack (9 October 2009).

The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware (refer to Chapter 4). If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

In the technical terms, *payload* is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs. From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end-user at the destination.[15,16]

The attack vectors described here are how most of them are launched.[16,18]

1. **Attack by E-Mail:** The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, hoaxes, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering and hoaxes are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics,

and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

5. **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses. Next they begin scanning the Internet from the computer they have just infected, and start looking for other computers to infect. If the worm is successful, it propagates rapidly. The worm owner soon has thousands of "zombie" computers to use for more mischief.
7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart (IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.
8. **Foistware (sneakware):** Foistware is the software that adds hidden components to the system on the sly. Spyware is the most common form of foistware. Foistware is quasi-legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.
9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

2.8 Cloud Computing

The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals. Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet ("cloud")-based development and use of computer technology ("computing").[19] The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks. Cloud computing is a term used for hosted services delivered over the Internet. A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand – typically by the minute or the hour;
2. it is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
3. the service is fully managed by the provider – a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.