RV College of Engineering®

Go, change the world

22EM106-Introduction to Cyber Security

UNIT- II

Chapter-2:Cyber Offenses How Criminals Plan Them

Text Book:

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011,Reprint 2022, ISBN:978-81-265-2179-1.

Course Incharge: Dr.Mohana
Department of Computer Science & Engineering (Cyber Security)
RV College of Engineering, Bangalore-560059

Unit - II Syllabus

Unit – II	8 Hrs
Cyber Offenses How Criminals Plan Them: Introduction, how criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercaafe & cybercrimes, Botnets: The fuel for cybercrime, Attack Vector. **Attacker Techniques and Motivations:** How Hackers Cover Their Tracks (Anti-forensics), How and Why Attackers Use Proxies, Tunnelling Techniques, Fraud Techniques.	

Learning objectives

- Understand different types of cyberattacks
- Get an overview of the steps involved in planning cybercrime
- Understand tools used for gathering information about the target.

Introduction

- Technology is a double-edged sword
- Target of offense and false sense of anonymity
- Misuse of information
- Agencies collect information about the individuals
- Cyber criminals use WWW and internet for all illegal activities
- Lack of awareness and about cybercrime and cyber laws.
- People who commit cybercrimes are known as **crackers.**

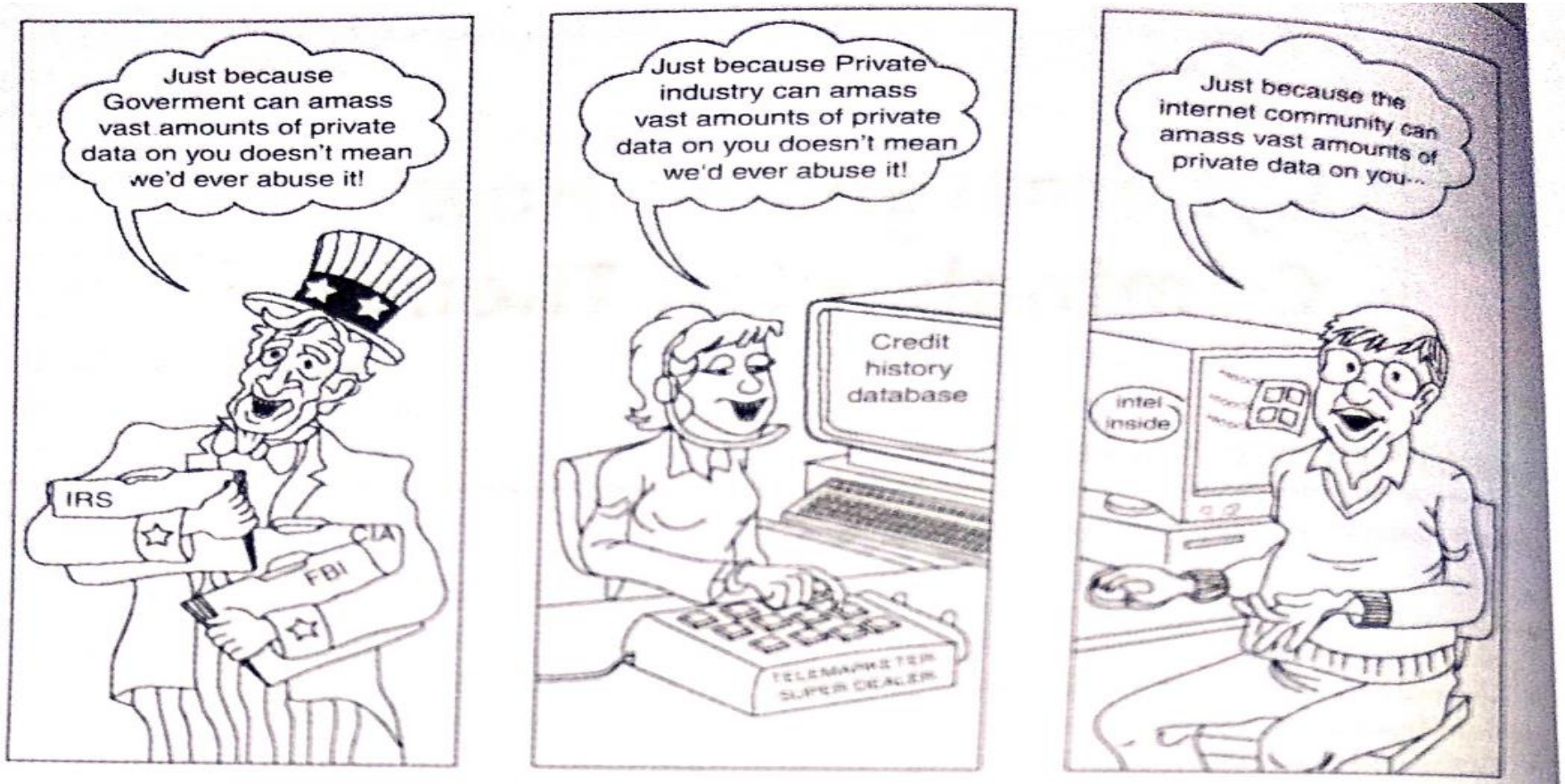
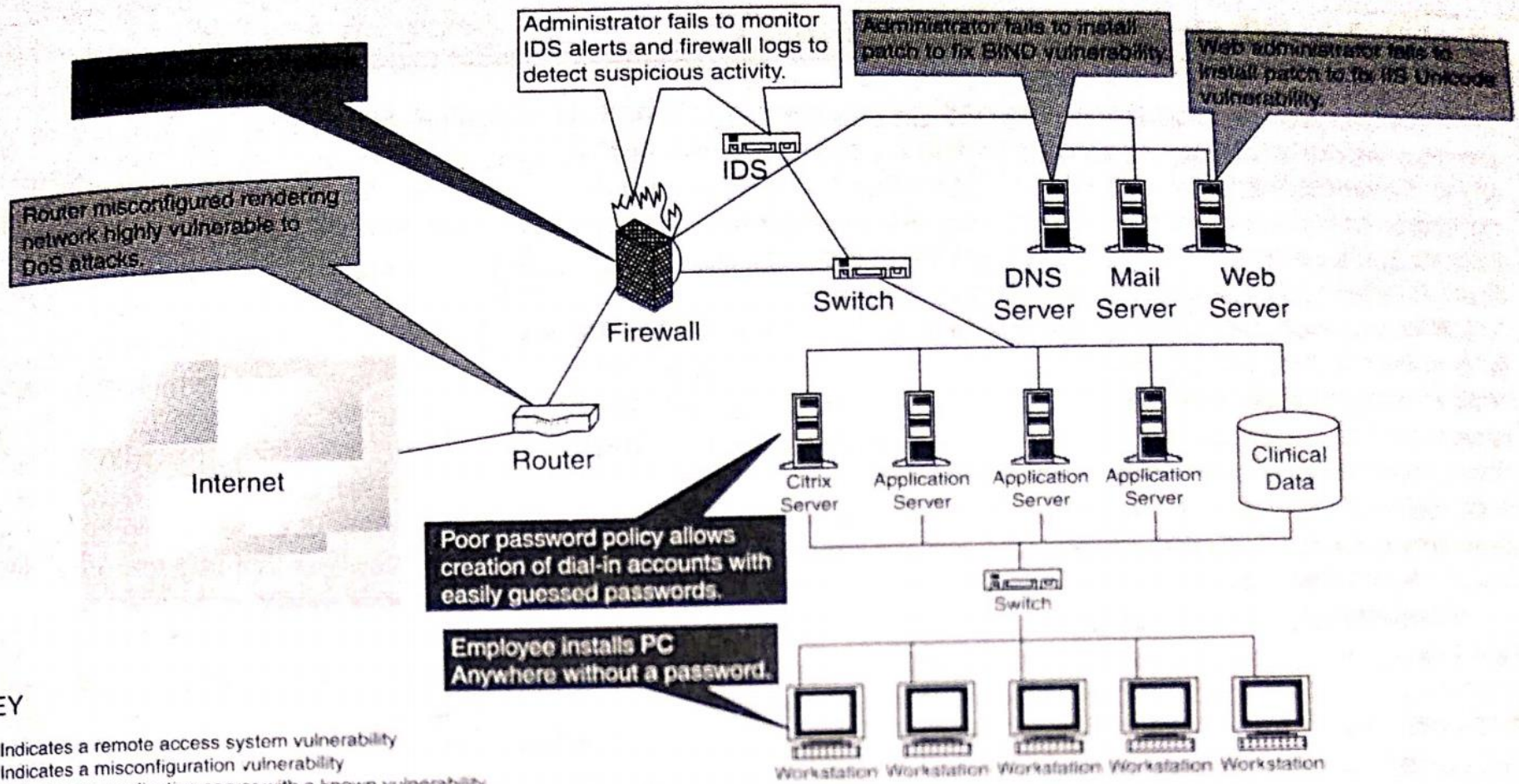


Figure 2.1 | We all vouche for keeping your personal information secret!
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

- An attacker would look to exploit the vulnerabilities in the network.
- **Categories of vulnerabilities**

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.


Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Clinical Data
Poor password policy allows creation of dial-in accounts with easily guessed passwords.
Switch
Employee installs PC Anywhere without a password.
Workstation
Workstation
Workstation
Workstation
Workstation
KEY
Indicates a remote access system vulnerability
Indicates a misconfiguration vulnerability
Indicates an application server with a known vulnerability
Indicates a vulnerability resulting from inadequate monitoring of security systems

Hackers and crackers

Hackers:

- Person with strong interest in computers and enjoys learning and experimenting
- Very talented and smart people

Crackers:

- Person who breaks into computer
- Crimes include vandalisms, theft and snooping in unauthorized areas

Types Of Hackers

White Hat Hackers:

- Ethical hackers or security researchers,
- use their skills to identify and fix security vulnerabilities in computer systems.
- They work legally and with permission to help organizations improve their security.

Black Hat Hackers:

- hacking activities with malicious intent.
- They may break into computer systems or networks to steal sensitive information, cause damage, or exploit vulnerabilities for personal gain.

Grey Hat Hackers:

- hackers fall somewhere between white hat and black hat hackers.
- They may hack into systems without permission but with no malicious intent.
- They often disclose vulnerabilities to the affected organization after the hack.

Script Kiddies:

- Script kiddies are individuals with limited technical skills who use pre-written scripts or tools developed by others to carry out attacks.
- They usually lack in-depth knowledge and understanding of hacking techniques.

State-Sponsored Hackers:

- Also known as Advanced Persistent Threat (APT) groups, state-sponsored hackers are employed or supported by governments.
- They conduct cyber espionage, sabotage, or other cyber activities to gain strategic or political advantages.

Malware Authors:

- These hackers specialize in creating malicious software, such as viruses, worms, Trojans, ransomware, and spyware.
- They design and distribute malware to compromise computer systems and steal information.

Phreakers:

- Phreakers manipulate and exploit telecommunication systems, including phone networks and voicemail systems.
- They seek unauthorized access to make free calls, disrupt services, or intercept communications.

Social Engineers:

- Social engineers focus on manipulating human psychology rather than technical vulnerabilities.
- They use deception and social skills to trick people into revealing sensitive information or providing unauthorized access.

Cybercriminals:

- Cybercriminals are individuals or groups involved in various illegal activities on the internet, such as identity theft, credit card fraud, online scams, phishing, and distribution of illegal content.

Categories of cybercrime

Cybercrime can be categorized based on

- The target of the crime
- Whether the crime occurs as a single event or as a series of events

1. Crimes targeted at individuals
2. Crimes targeted at property
3. Crimes targeted at organizations
4. Single event of cybercrime
5. Series of events

1. Crimes targeted at individuals

- Human weakness
- Financial frauds
- Child pornography
- Copy right violations
- Harassment

2. Crimes targeted at property

- Stealing devices
- Transmitting harmful programs to destroy the devices

3. Crimes targeted at organizations

- Cyberterrorism
- Attackers (individual / group)
- Usage of computer tools and usage

4. Single event of cybercrime

- It is the single event from the perspective of victim
- Unknowingly opening attachments contain virus
- This is hacking or fraud

5. Series of events

- Attacker interacting with the victims repetitively
- Series of events / demanding
- Cyberstalking

How criminals plan the attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target
- Target can be individual or / and organizations
- Active attack and passive attack
- Inside attack and outside attack

Inside attack: originating or attempted **within the security perimeter** of an organization.

- Attempted by insider
- Gains access to **more resources** than expected

Outside attack: attempted outside the security perimeter of an organization.

- Attempted through internet or remote access connection.

Phases involved in planning cybercrime

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

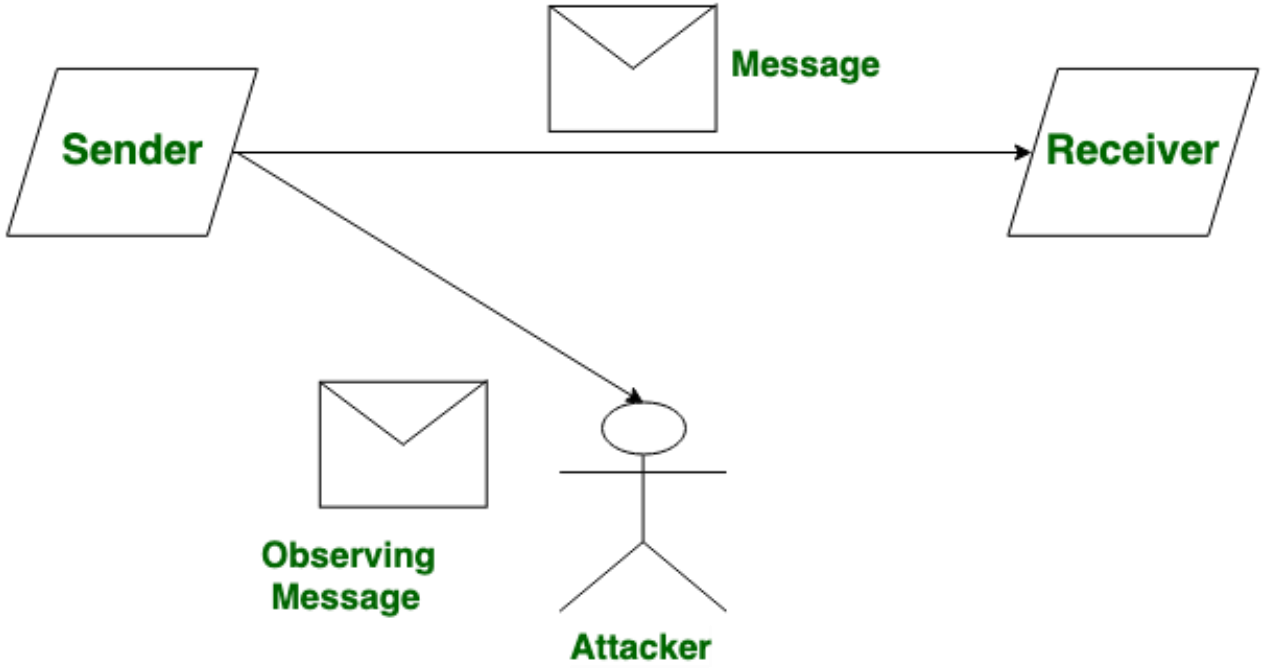
- Is an act of reconnoitering – explore, often with the goal of finding something or somebody.
- Gain information about an enemy or potential enemy.
- Foot printing- gives an overview about the system vulnerability
- Attackers gather the information in two phases
- Passive and active attacks

Passive attacks

- Gathering information about a target without his/her knowledge
- **Internet searches** or by googling.

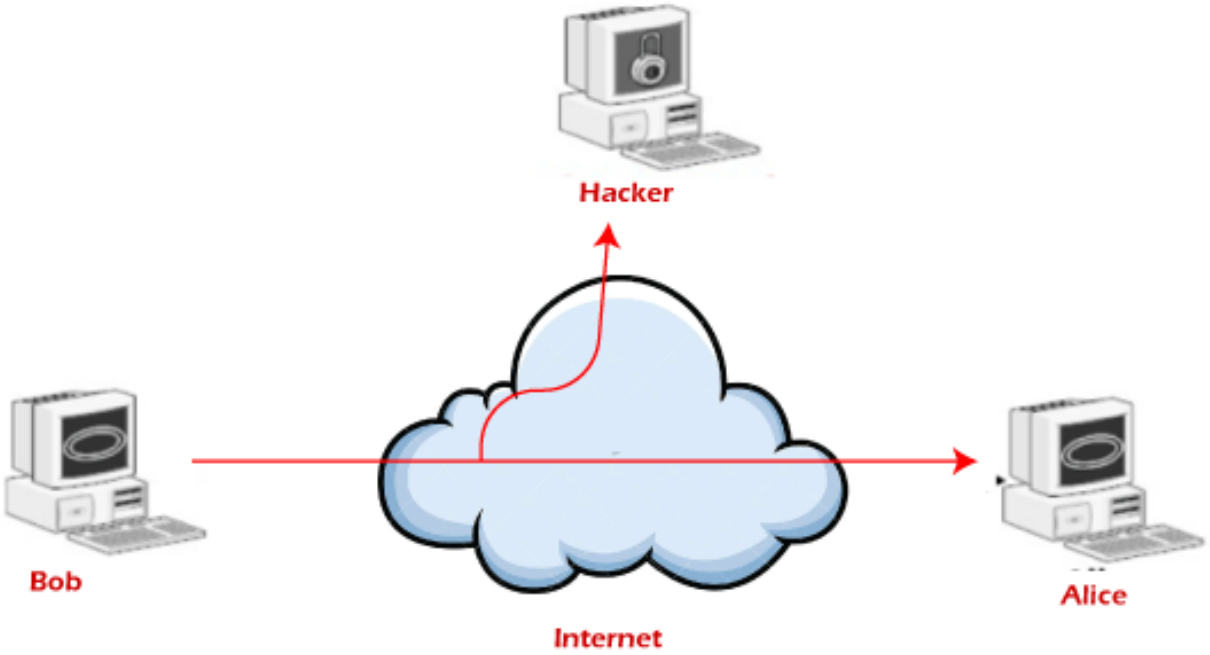
information with the help

1. Google or Yahoo search: People search to locate information about employees (see
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on it network.



Passive Attack

Passive Attacks (Traffic analysis)



Tools used during passive attack

Name of the Tool	*Brief Description*	*Remarks*
Google Earth	Google Earth is a virtual globe, map, and geographic information program. It maps the Earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe. It is available under three different licenses: Google Earth, a free version with limited functionality; Google Earth Plus (discontinued), with additional features; and Google Earth Pro intended for commercial use.	For more details on this tool, visit: http://earth.google.com/ Like "Google Earth," similar details can be obtained from http://www.wikimapia.org/ Indian Space Research Organization (ISRO) unveiled its beta version of Bhuvan (meaning Earth in Sanskrit), a Web-based tool like Google Earth, that promises better 3-D satellite imagery of India than is currently being offered by Google Earth and that too with India-specific features such as weather information and even administrative boundaries of all states and districts, visit: http://bhuvan.nrsc.gov.in/
Internet Archive	The Internet Archive is an Internet library, with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format. It includes texts, audio, moving images, and software as well as archived webpages in our collections.	An attacker gets the information about latest update made to the target's website as well as can dig the information which maybe available in the history (e.g., contact list of executives and higher management officials are always updated). For more details on this tool, visit: http://www.archive.org/index.php

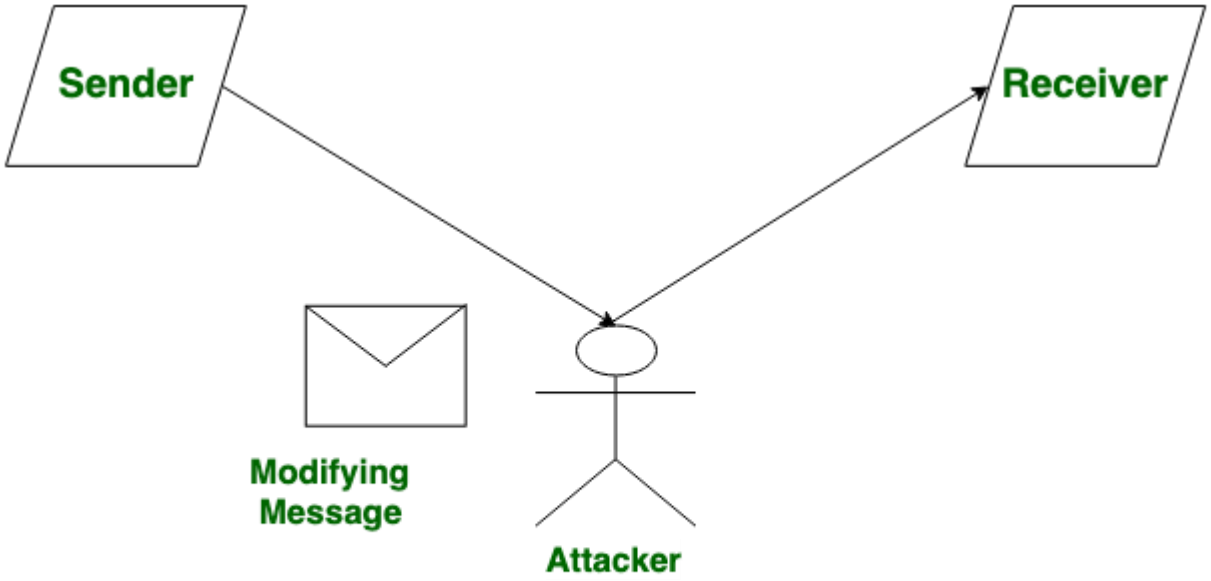
index.php

Professional Community	LinkedIn is an interconnected network of experienced professionals from around the world, representing 170 industries and 200 countries.	One can find details about qualified professionals. For more details on this tool, visit: http://www.linkedin.com/
People Search	People Search provides details about personal information: date of birth, residential address, contact number, etc.	To name a few, visit: • http://www.whitepagesinc.com • http://www.intelius.com/ • http://www.whitepages.com/
Domain Name Confirmation	To perform searches for domain names (e.g., website names) using multiple keywords. This helps to enable to find every registered domain name in "com," "net," "org," "edu," "biz," etc.	For more details on this tool, visit: • http://www.namedroppers.com/ • http://www.binarypool.com/bytes.html

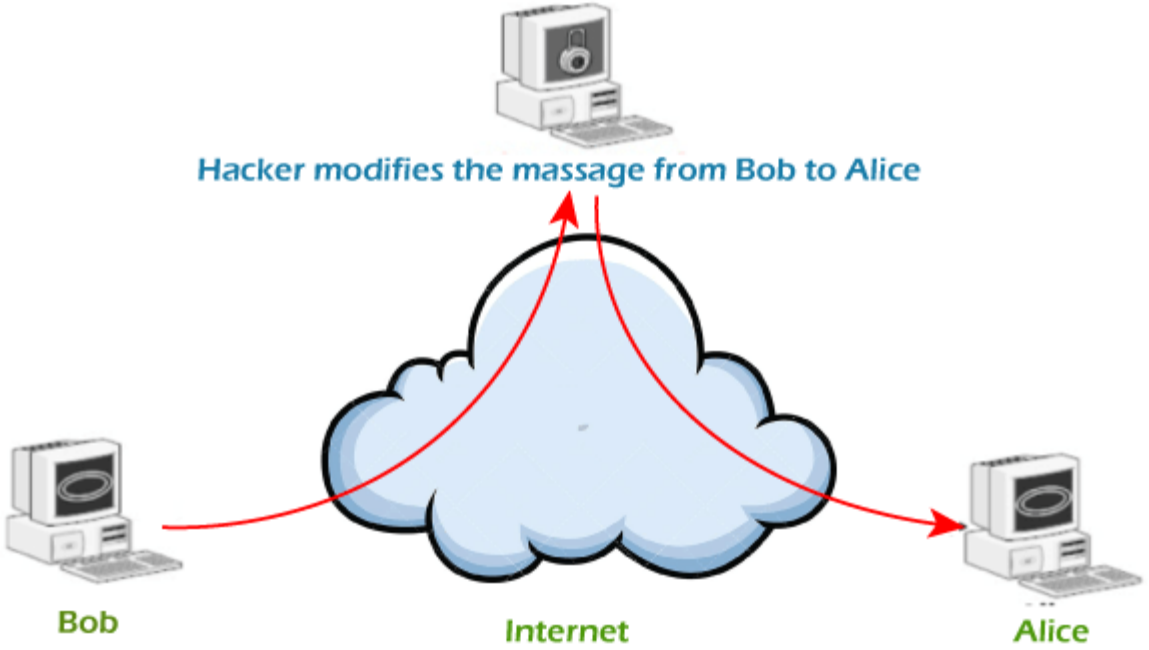
Name of the Tool	*Brief Description*	*Remarks*
WHOIS	This is a domain registration lookup tool. This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information. WHOIS supports IP address queries and automatically selects the appropriate WHOIS server for IP addresses. This tool will lookup information on a domain, IP address, or a domain registration information. You can select a specific WHOIS server, or you can use the "Default" option which will select a server for you.	For more details on this tool, visit: • http://whois.domaintools.com/ • http://www.whois.net/ • http://www.samspade.org/ For further details of this lookup utility, visit: • http://resellers.tucows.com/opensrs/whois/ • http://www.nsauditor.com/docs/html/tools/Whois.htm
Nslookup	The name nslookup means "name server lookup." The tool is used on Windows and Unix to query domain name system (DNS) servers to find DNS details, including IP addresses of a particular computer and other technical details such as mail exchanger (MX) records for a domain and name server (NS) servers of a domain.	For more details on this tool, visit: • http://www.kloth.net/services/nslookup.php • http://nslookup.downloadsoftware4free.com/
Dnsstuff	Using this tool, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups, etc.	For more details on this tool, visit: http://www.dnsstuff.com/
Traceroute	This is the best tool to find the route (i.e., computer network path) to a target system. It determines the route taken by packets across an IP network.	For more details on this tool, visit: http://www.rjsmith.com/tracerte.html
VisualRoute Trace	This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.	For more details on this tool, visit: http://www.visualware.com/
eMailTrackerPro	eMailTrackerPro analyzes the E-Mail header and provides the IP address of the system that sent the mail.	For more details on this tool, visit: http://www.emailtrackerpro.com/
HTTrack	This tool acts like an offline browser. It can mirror the entire website to a desktop. One can analyze the entire website by being offline.	For more details on this tool, visit: http://www.httrack.com/
Website Watcher	The tool can be used to keep the track of favorite websites for an update. When the website undergoes an update/change, this tool automatically detects it and saves the last two versions onto the desktop.	For more details on this tool, visit: http://www.aignes.com/
Competitive Intelligence	Competitive intelligence can provide information related to almost any product, information on recent industry trends, or information about geopolitical indications. Effective use of competitive intelligence can reveal attack against the website or an industrial espionage.	To name a few, visit: • http://bigital.com/ • http://www.amity.edu/aici/

Active attacks

- It involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase
- **Risk of detection** and is also called rattling the doorknobs or active reconnaissance
- The attacker efforts to change or modify the content of messages.
- Active Attack is danger for **Integrity as well as availability**.
- Due to active attack system is always damaged and System resources can be changed.
- The most important thing is that, In active attack, Victim gets informed about the attack.



Active Attack



Active Attacks (Modifications of messages)

Tools used during active attack

Table 2.2 | Tools used during active attacks

Name of the Tool	*Brief Description*	*Remarks*
Arphound	This is a tool that listens to all traffic on an Ethernet network interface. It reports IP/media access control (MAC) address pairs as well as events, such as IP conflicts, IP changes and IP addresses with no reverse DNS, various Address Resolution Protocol (ARP) Spoofing and packets not using the expected gateway.	This is open-source software. For more details on this tool and download, visit: http://www.nottale.net/index.php?project=arphound
Arping	This is a network tool that broadcasts ARP packets and receives replies similar to "ping." It is good for mapping a local network and finding used IP space. It broadcasts a "who-has ARP packet" on the network and prints answers. It is very useful when trying to pick an unused IP for a Net to which routing does not exist as yet.	This is open-source software. For more details on this tool and download,visit: http://www.habets.pp.se/synscan/programs.php?prog=arping
Bing	This is used for Bandwidth Ping. It is a point-to-point bandwidth measurement tool based on ping. It can measure raw throughput between any two network links. Bing determines the real (raw as opposed to available or average) throughput on a link by measuring Internet Control Message Protocol (ICMP) echo requests roundtrip times for different packet sizes for each end of the link.	This is open-source software. For installation and usage information, visit: http://ai3.asti.dost.gov.ph/sat/bing.html
Bugtraq	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources.	This software is for free usage. Visit the following site for more details: http://www.securityfocus.com/bid

	each end of the link.	
Bugtraq	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources.	This software is for free usage. Visit the following site for more details: http://www.securityfocus.com/bid
Dig	This is used to perform detailed queries about DNS records and zones, extracting configuration, and administrative information about a network or domain.	This is open-source software. For additional technical details, visit: http://www.isc.org/index.pl?/sw/bind/
DNStracer	This is a tool to determine the data source for a given DNS server and follow the chain of DNS servers back to the authoritative sources.	This is also open-source software. For additional technical details, visit: http://www.mavetju.org/unix/dnstracer.php

Table 2.2 | (Continued)

Name of the Tool	Brief Description	Remarks
Dsniff	This is a network auditing tool to capture username, password, and authentication information on a local subnet.	This is open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
Filesnarf	This is a network auditing tool to capture file transfers and file sharing traffic on a local subnet.	This is also open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
FindSMB	This is used to find and describe server message block (SMB) servers on the local network.	It is open-source software; visit the following site for downloads: http://us3.samba.org/samba/
Fping	This is a utility similar to ping used to perform parallel network discovery.	For this open-source software, visit: http://www.fping.com/
Fragroute	This intercepts, modifies and rewrites egress traffic destined for a specified host, implementing several intrusion detection system (IDS) evasion techniques.	This is another open-source material; visit: http://www.monkey.org/~dugsong/fragroute/
Fragtest	This tests the IP fragment reassembly behavior of the Transmission Control Protocol (TCP) stack on a target. It intercepts, modifies and rewrites egress traffic destined for a specified host, implementing most of the attacks.	For more details on this open-source software, visit: http://www.monkey.org/~dugsong/fragroute/
Hackbot	This is a host exploration tool, simple vulnerability scanner and banner logger.	Another open-source software, whose details can be found at: http://freshmeat.net/projects/hackbot/
Hmap	This is used to obtain detailed fingerprinting of web servers to identify vendor, version, patch level, including modules and much more. *Hmap* is a web server fingerprinting tool.	Details of this open-source software can be found at: http://ujeni.murkyroc.com/hmap/
Hping	This is a TCP/IP packet assembler and analyzer. It can perform firewall ruleset testing, port scanning, network type of service/quality-of-service (TOS/QOS) testing, maximum transmission unit (MTU) discovery, alternate-protocol traceroute, TCP stack auditing, and much more. Using *hping* you can do the following: • Firewall testing; • advanced port scanning; • network testing, using different protocols, TOS, fragmentation; • manual path MTU discovery; • advanced traceroute, under all the supported protocols; • remote OS fingerprinting; • remote uptime guessing; • TCP/IP stacks auditing;	This is open-source software. For additional technical details, visit: http://www.hping.org/
	Hping works on the following Unix-like systems: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.	
Httping	This is similar to "ping," that is, hping, but for HTTP requests. It shows how long a URL will take to connect, send a request, and receive a reply.	This is open-source software. For additional technical details, visit: http://www.vanheusden.com/httping/
Hunt	This is a tool for exploiting well-known weaknesses in the TCP/IP protocol suite.	This is also open-source software. For additional technical details, visit: http://lin.fsid.cvut.cz/~kra/index.html
Libwhisker	This is an application library designed to assist in scannabilities.	Details of this open-source software can be found at: http://www.wiretrip.net/rfp/lw.asp
Mailsnarf	This is a network auditing tool to capture SMTing for CGI/web vulnerP and POP3 E-Mail traffic (including message headers, bodies, and attachments) on a local subnet.	For this open-source software, you can visit: http://monkey.org/~dugsong/dsniff/
Msgsnarf	This is a network auditing tool to capture instant message (Yahoo, MSN, ICQ, iChat, AIM, and many more) traffic on a local subnet.	Same as above
NBTScan	This is a utility for scanning networks for NetBIOS information. It reports IP address, NetBIOS name, logged-in username, and MAC address.	Details of this open-source material can be found at: http://www.inetcat.org/software/nbtscan.html
Nessus	This is a powerful, fast, and modular security scanner that tests for many thousands of vulnerabilities. ControlScans' system can also be used to create custom Nessus reports.	To know more about this open-source utility, visit: http://www.nessus.org/
Netcat	This is a utility to read and write custom TCP/User Datagram Protocol (UDP) data packets across a network connection for network debugging or exploration.	Explore more details of this open-source utility at: http://www.atstake.com/research/tools/network_utilities/
Nikto	This is a web server vulnerability scanner that tests over 2,600 potentially dangerous files/CGIs on over 625 types of servers. This tool also performs comprehensive tests against web servers for multiple items and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).	Nikto is an open-source web server scanner; visit the following site for more detail: http://www.cirt.net/code/nikto.shtml
Nmap	This is a port scanner, operating system fingerprinter, service/version identifier, and much more. Nmap is designed to rapidly scan large networks.	For details of this open-source software, visit: http://insecure.org/nmap/

Table 2.2 | (Continued)

Name of the Tool	Brief Description	Remarks
Pathchar	This is a network tool for inferring the characteristics of Internet paths, including Layer 3 hops, bandwidth capacity, and autonomous system information.	For further details, visit: http://ee.lbl.gov/
Ping	This is a standard network utility to send ICMP packets to a target host.	For further details, visit: http://www.controlscan.com/auditingtools.html#
ScanSSH	This supports scanning a list of addresses and networks for open proxies, SSH Protocol servers, and Web and SMTP servers. Where possible, it displays the version number of the running services. ScanSSH supports the following features: • Variable scanning speed: per default, ScanSSH sends out 100 probes per second; • open proxy detection; • random sampling: it is possible to randomly sample hosts on the Internet.	The first version of the ScanSSH Protocol scanner was released in September 2000. For further details and downloading the current version, visit: http://www.monkey.org/~provos/scanssh/
SMBclient	This helps a client to talk to an SMB (Samba, Windows File Sharing) server. Operations include getting files from the server, putting files on the server, retrieving directory information, and much more. It is an open-source/free software suite that has, since 1992, provided file and print services to all types of SMB/common Internet file system (CIFS) clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License.	
SMTPscan	This is a tool to determine the type and version of a remote Simple Mail Transfer Protocol (SMTP) mail server based on active probing and analyzing error codes of the target SMTP server.	For further details, visit: http://www.greyhats.org/outils/smtpscan/
TCPdump	It is a network tool for the protocol packet capture and dumper program.	For further details, visit: http://ee.lbl.gov/
TCPreplay	This is a utility to read captured TCPdump/pcap data and "replay" it back onto the network at arbitrary speeds. TCPreplay is a suite of licensed tools written by Aaron Turner for Unix operating systems. It gives you the ability to use previously captured traffic to test a variety of network devices. It allows you to classify traffic as client or server; rewrite open system interconnection (OSI) Layers 2, 3 and 4 headers; and finally replay the traffic back onto the network and through other devices such as switches, routers, firewalls, network-based intrusion detection system (NIDS), and intrusion prevention system (IPS). TCPreplay supports both single and dual NIC modes for testing both sniffing and inline devices. TCPreplay is used by numerous firewalls, IDS, IPS, and other networking vendors, enterprises, universities, laboratories, and open-source projects.	TCPreplay suite includes the following tools: • TCPprep: It is a multi-pass packet capture (pcap) file preprocessor which determines packets as client or server and creates cache files used by TCPreplay and TCPrewrite. • TCPrewrite: It is a pcap file editor which rewrites TCP/IP and Layer 2 packet headers. • TCPreplay: It replays pcap files at arbitrary speeds onto the network. • TCPreplay-edit: It replays and edits pcap files at arbitrary speeds onto the network. • TCPbridge: It bridges two network segments with the power of TCPrewrite. For further details, visit: http://tcpreplay.synfin.net/trac/
THC-Amap	This is a scanner to remotely fingerprint and identify network applications and services.	For further details, visit: http://freeworld.thc.org/releases.php
Traceroute	This is a standard network utility to trace the logical path to a target host by sending ICMP or UDP packets with incrementing tunneled transport layer security (TTLs).	For further details, visit: http://ee.lbl.gov/
URLsnarf	This is a network auditing tool to capture HTTP traffic on a local subnet.	For further details, visit: http://monkey.org/~dugsong/dsniff/
XProbe2	This is a tool employing several techniques to actively fingerprint the operating system of a target host.	For further details, visit: http://www.sys-security.com/html/projects/X.html

Note: IP is Internet Protocol here.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Table 3
Wiley India.

Difference between Active attack and Passive attack

Based on	Active attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to **modify the message's content.**	In passive attacks, the attacker **observes the messages, then copy and save** them and can use it for malicious purposes.
Modification	In an active attack, the attacker **modifies the actual information.**	In passive attacks, **information remains unchanged**.
Victim	In active attacks, the **victim gets notified** about the attack.	Unlike active attacks, in passive attacks, **victims do not get informed** about the attack.
System's impact	The damage done with active attacks can be **harmful to the system and its resources**.	The passive attacks **do not harm the system**.
System resources	In active attacks, the **system resources can be changed.**	In passive attacks, the **system resources remain unchanged.**
Dangerous for	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Emphasis on	In active attacks, **attention is on detection.**	In active attacks, **attention is on prevention**.
Types	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.
Prevention	Active attacks are **tough to restrict from entering systems or networks**.	Unlike active attacks, **passive attacks are easy to prohibit.**

Scanning: key step to examine intelligently while gathering the information.

Objectives of scanning are

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer netwo systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

Scrutinizing phase: called enumeration in the hacking world.

The main objective 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.

Attack(gaining and maintaining the system access)

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

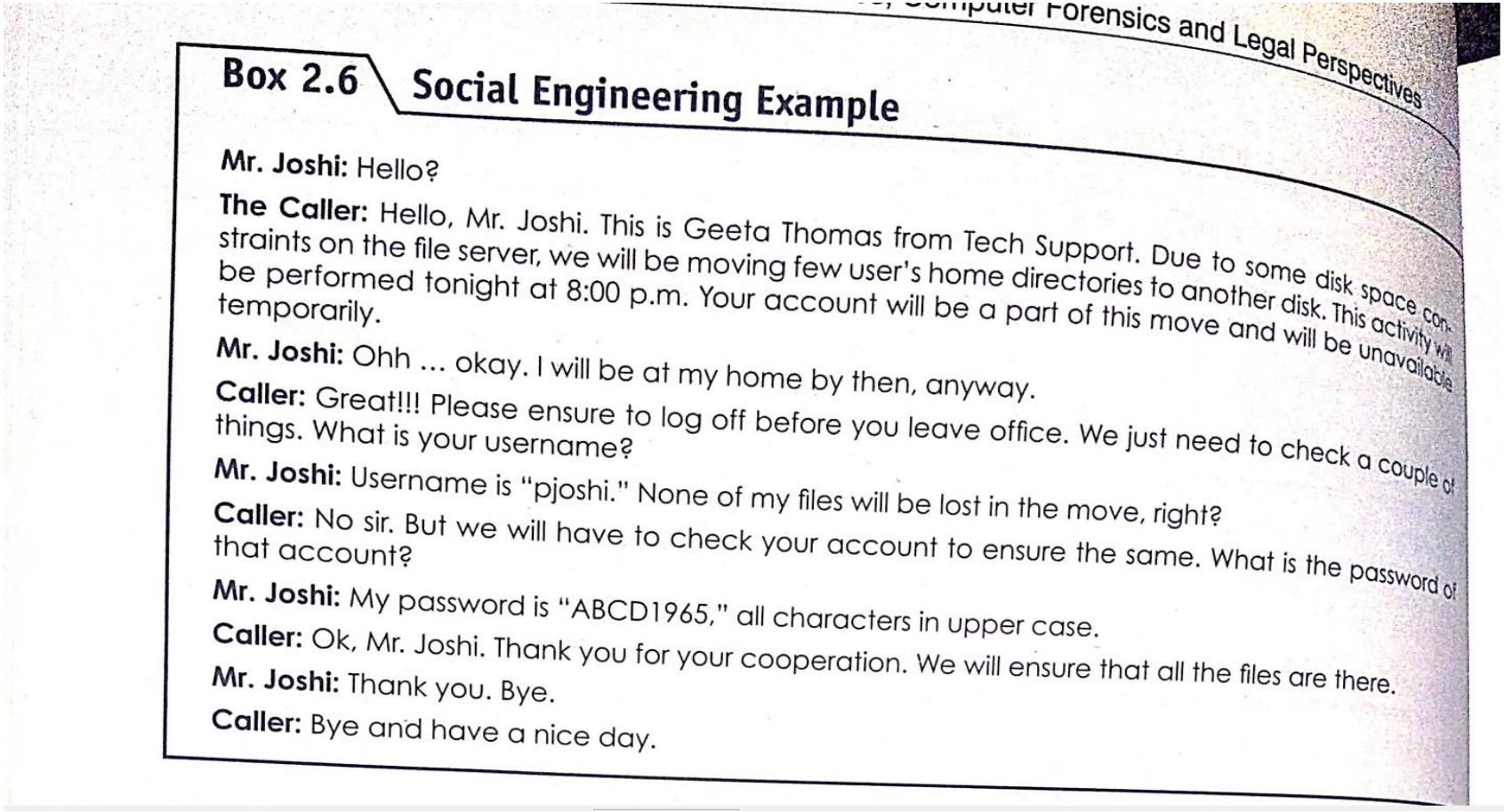
1. Crack the password (we will address it in Chapter 4);
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Social Engineering

- Technique to influence or persuasion to deceive
- It is the tactic of **manipulating, influencing, or deceiving a victim in order to gain control over a computer system**, or to steal personal and financial information.
- Uses telecommunication / internet against the security policy 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

Example



Computer Forensics and Legal Perspectives

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.

Classification of social Engineering

1. **Human based social engineering:**

- Person to person interaction
- Ex. Calling to get information

2. **Computer based social engineering:**

- Getting required information by using computer software / internet
- Ex. Fake E-mail

1. Human based social engineering:

- **Impersonating an employee or valid user**
- Posing as an important user – Ex.CEO
- Using a third person
- Calling technical support
- Shoulder suffering
- Dumpster driving

Shoulder suffering

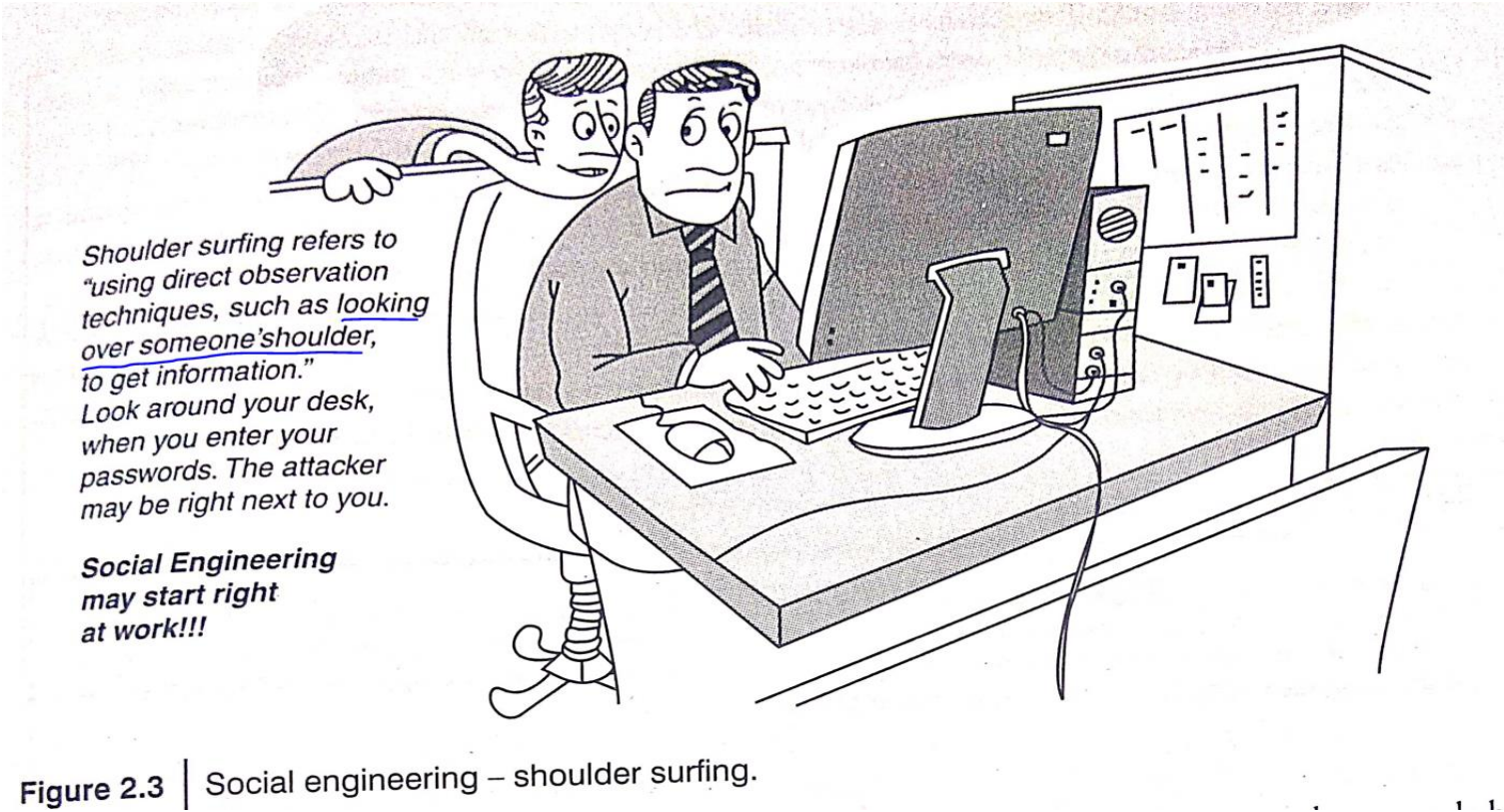


Figure 2.3 | Social engineering – shoulder surfing.

Dumpster driving: looking or getting information

- Trash
- Pieces of paper or computer printouts
- Garbage
- E-waste etc..

2. Computer based social engineering:

- Fake E-mails
- E-mail attachments
- Pop-up windows

Fake E-mails:

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.

We will never ever send you junk E-Mail, or give your E-Mail address away to anyone. We hate Spam at least as much as you do- maybe more (and that's why this page can't be used by spammers to send bulk E-Mail or any other funny stuff).

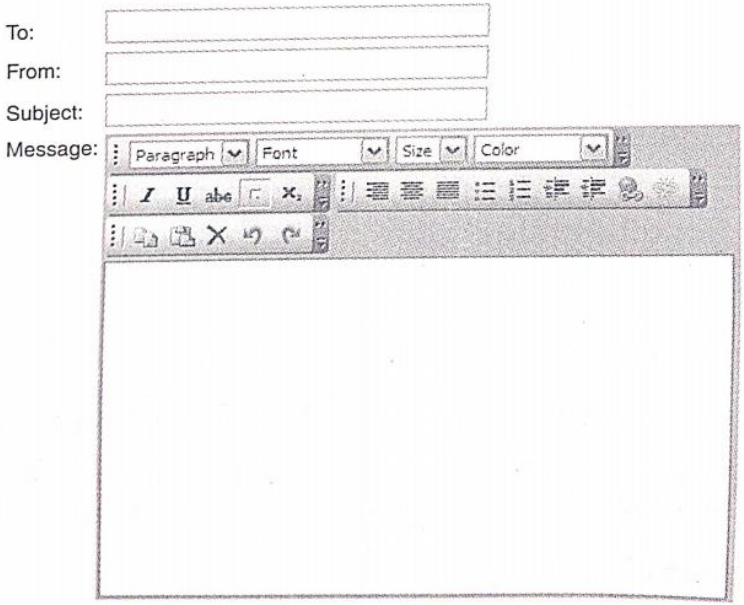


Figure 2.4 Sending fake E-Mails.
Source: http://deadfake.com/Send.aspx (2 April 2009).

E-mail attachments and Pop-up windows:

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.

Past statistics

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.

Social engineering statistics 2023

- 75% of security professionals say social engineering is the "most dangerous" threat. – CS Hub
- 2,249 social engineering incidents were reported. – Verizon.
- A hacker used social engineering attack on Twilio and gained access to the company's internal systems and the data of 125 customers. – Venturebeat

https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Social%20engineering%20statistics%202023,-75%25%20of%20security&text=2%2C249%20social%20engineering%20incidents%20were%20reported.

firewalltimes.com/social-engineering-statistics/

Firewall Times

21 Social Engineering Statistics – 2022

By Catherine Reed
May 16, 2022 — Attacks

Social engineering attacks rely not on hacking computer systems, but on manipulating people. Yet social engineering methods play a part in million of cyberattacks. In this article, we'll dig into 21 key social engineering statistics. Read on.

1. 98% of Cyber Attacks Involve Some Form of Social Engineering

In the broad world of cyber attacks, 98% involve social engineering on some level. It could involve masquerading as a trusted contact to encourage an employee to click a malicious link or email, pretending to be a reliable banking institution to capture login credentials, or similar activities designed to gain entry into target systems.

Once trust is established – which is the social engineering part of the equation – other attacks can occur. Whether it be the distribution of malware, identity theft, or anything else, social engineering was essentially the gateway.

[Source: Purplesec]

https://firewalltimes.com/social-engineering-statistics/

Cyberstalking

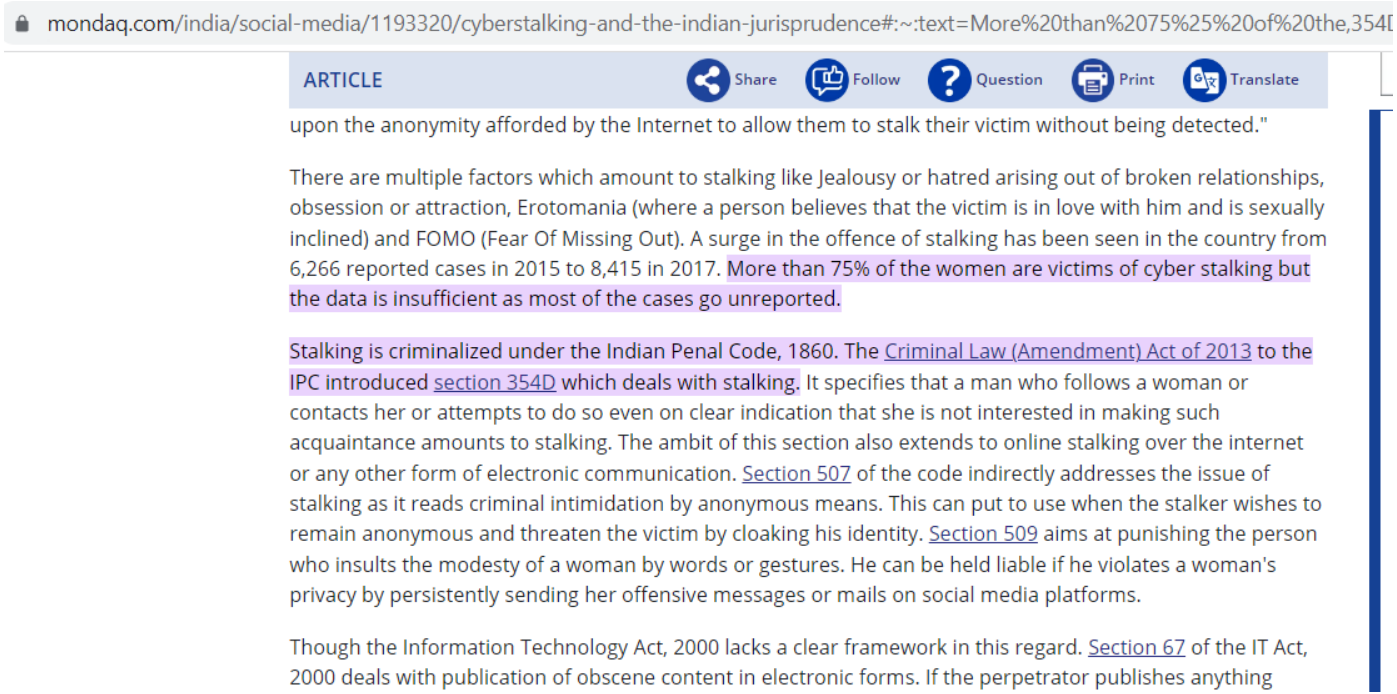
- Cyberstalkers **take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected**. The terms cyberstalking and cyberbullying are often used interchangeably.
- Trying to approach some-body or something.
- Refers to use of internet / ICT/ electronic communications devices to stalk another person
- Individual or group of individual to harass another individual, group of individual or organization.
- Behaviour includes false accusation, monitoring, transmission of threats, ID theft, damage to data or equipment, and gathering information for harassment purposes.

Types of Cyber 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.

Cases reported on cyber stalking

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.



mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian-jurisprudence#:~:text=More%20than%2075%25%20of%20the,354D

ARTICLE Share Follow Question Print Translate

upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected."

There are multiple factors which amount to stalking like Jealousy or hatred arising out of broken relationships, obsession or attraction, Erotomania (where a person believes that the victim is in love with him and is sexually inclined) and FOMO (Fear Of Missing Out). A surge in the offence of stalking has been seen in the country from 6,266 reported cases in 2015 to 8,415 in 2017. More than 75% of the women are victims of cyber stalking but the data is insufficient as most of the cases go unreported.

Stalking is criminalized under the Indian Penal Code, 1860. The Criminal Law (Amendment) Act of 2013 to the IPC introduced section 354D which deals with stalking. It specifies that a man who follows a woman or contacts her or attempts to do so even on clear indication that she is not interested in making such acquaintance amounts to stalking. The ambit of this section also extends to online stalking over the internet or any other form of electronic communication. Section 507 of the code indirectly addresses the issue of stalking as it reads criminal intimidation by anonymous means. This can put to use when the stalker wishes to remain anonymous and threaten the victim by cloaking his identity. Section 509 aims at punishing the person who insults the modesty of a woman by words or gestures. He can be held liable if he violates a woman's privacy by persistently sending her offensive messages or mails on social media platforms.

Though the Information Technology Act, 2000 lacks a clear framework in this regard. Section 67 of the IT Act, 2000 deals with publication of obscene content in electronic forms. If the perpetrator publishes anything

https://www.mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian jurisprudence#:~:text=More%20than%2075%25%20of%20the,354D%20which%20deals%20with%20stalking.

How stalking works

[illegible] 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.

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).

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.

Cybercafe and cybercrimes

- A cybercafe is **a business which allows people to pay for access to the Internet**. Another name for a cybercafe is an Internet cafe. Such places often look just like cafes or coffee shops, with the addition of computer terminals.

- 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.

As per survey in india:

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.

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.

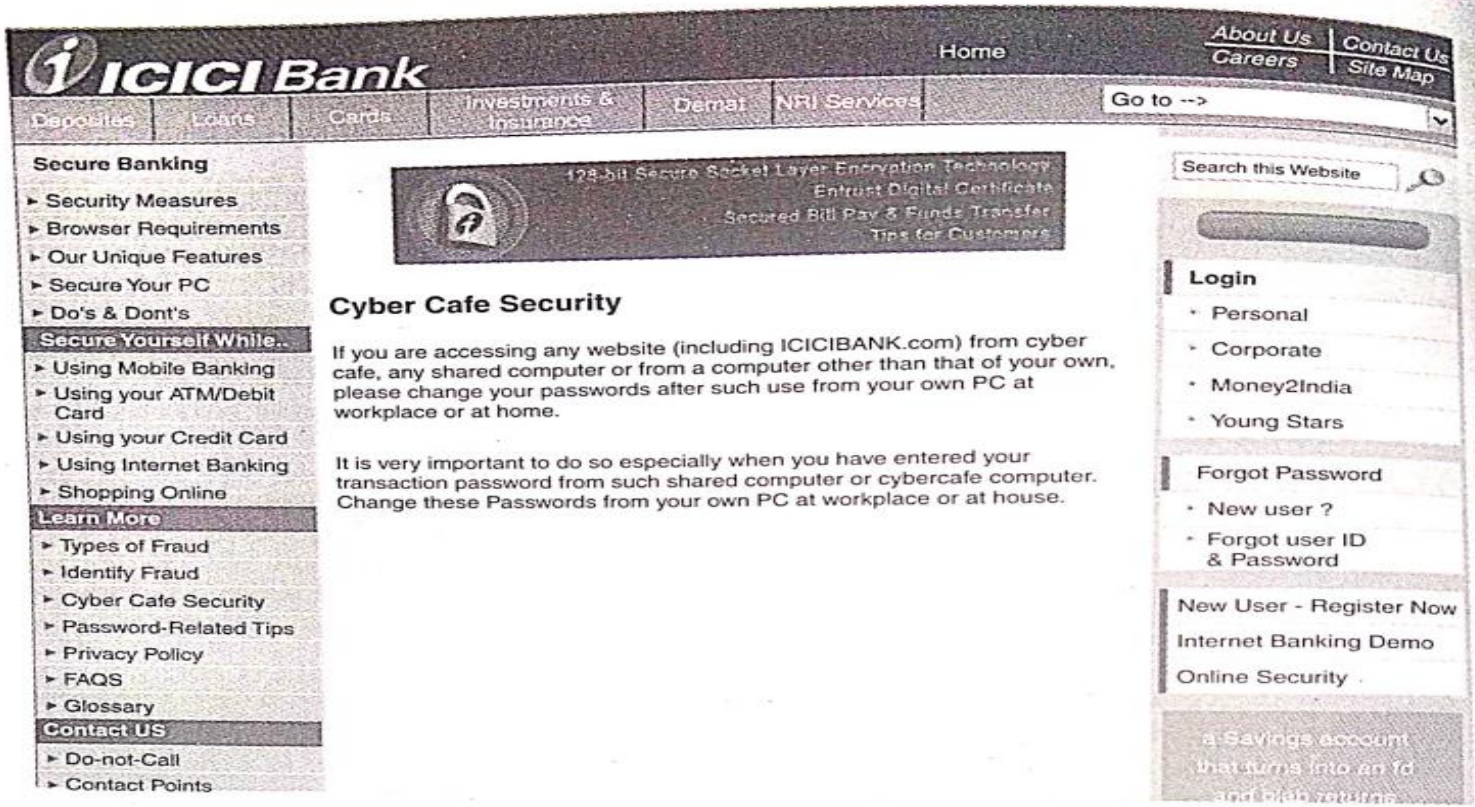
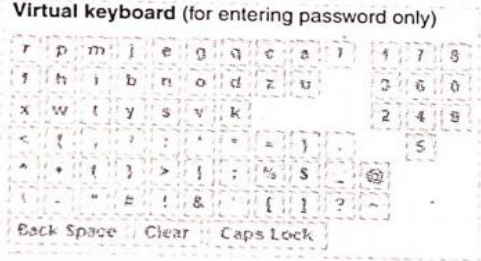


Figure 2.5 | Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).



ICICI Bank

Virtual Keyboard for Internet Banking

At ICICI Bank, We are committed to make your banking with us a safe and wonderful experience. We provide you with Virtual Keyboard to Protect your password. Virtual Keyboard is an online application to enter password with the help of a mouse.

Advantage of a Virtual Keyboard

The Virtual Keyboard is designed to protect your password form malicious "Spyware" and "Trojan Programs". Use of Virtual keyboard will reduce the risk of password theft.

Process To Use Virtual Keyboard

Steps to use Virtual keyboard are as follows:

Enter Login ID using Physical Keyboard.

- Select the check box 'Use Virtual Keyboard'.
- Use the Virtual Keyboard to the login password.
- Once you have entered your password, click"Log-in".
-

Functions of different keys on the Virtual Keyboard

Caps Lock: This key can be used to enter upper case if the password consist of capital letters.
Back Space: This key wil clear the last character entered in the password field.
Clear: This key wil clear all characters entered in the password field by Virtual keyboard.
Tab: This key is visible only for change or forced change password. field by Virtual keyboard.This key can be used to ente values in the next field.

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

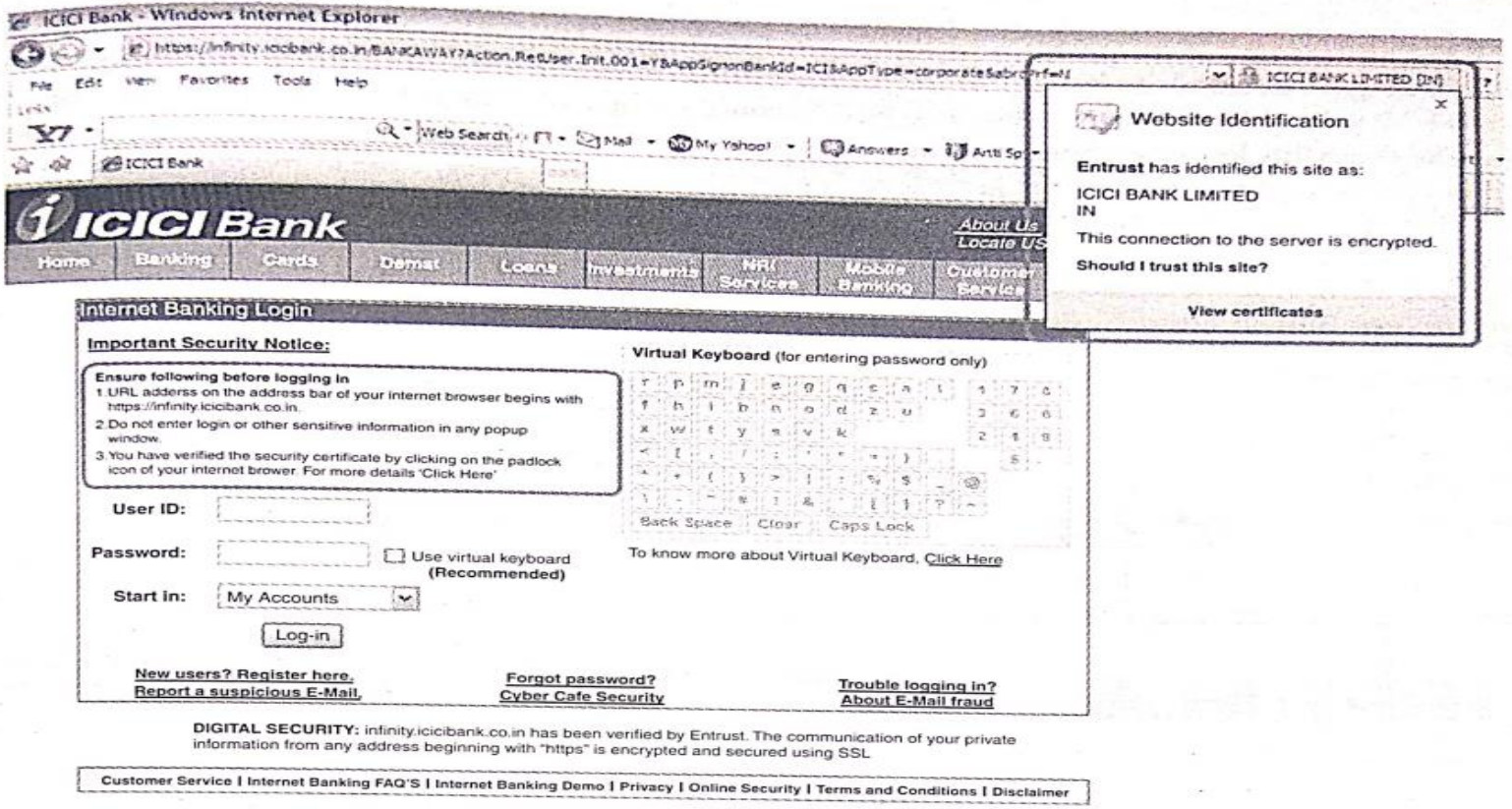


Figure 2.7 | Security warnings.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Botnets: The fuel of cyber crime

- Bot- computing
- A botnet (short for “robot network”) is **a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.”**
- Each individual machine under the control of the bot-herder is known as a bot.
- Automated program for doing some particular task

Botnet

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 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.
explains how Botnets create business.

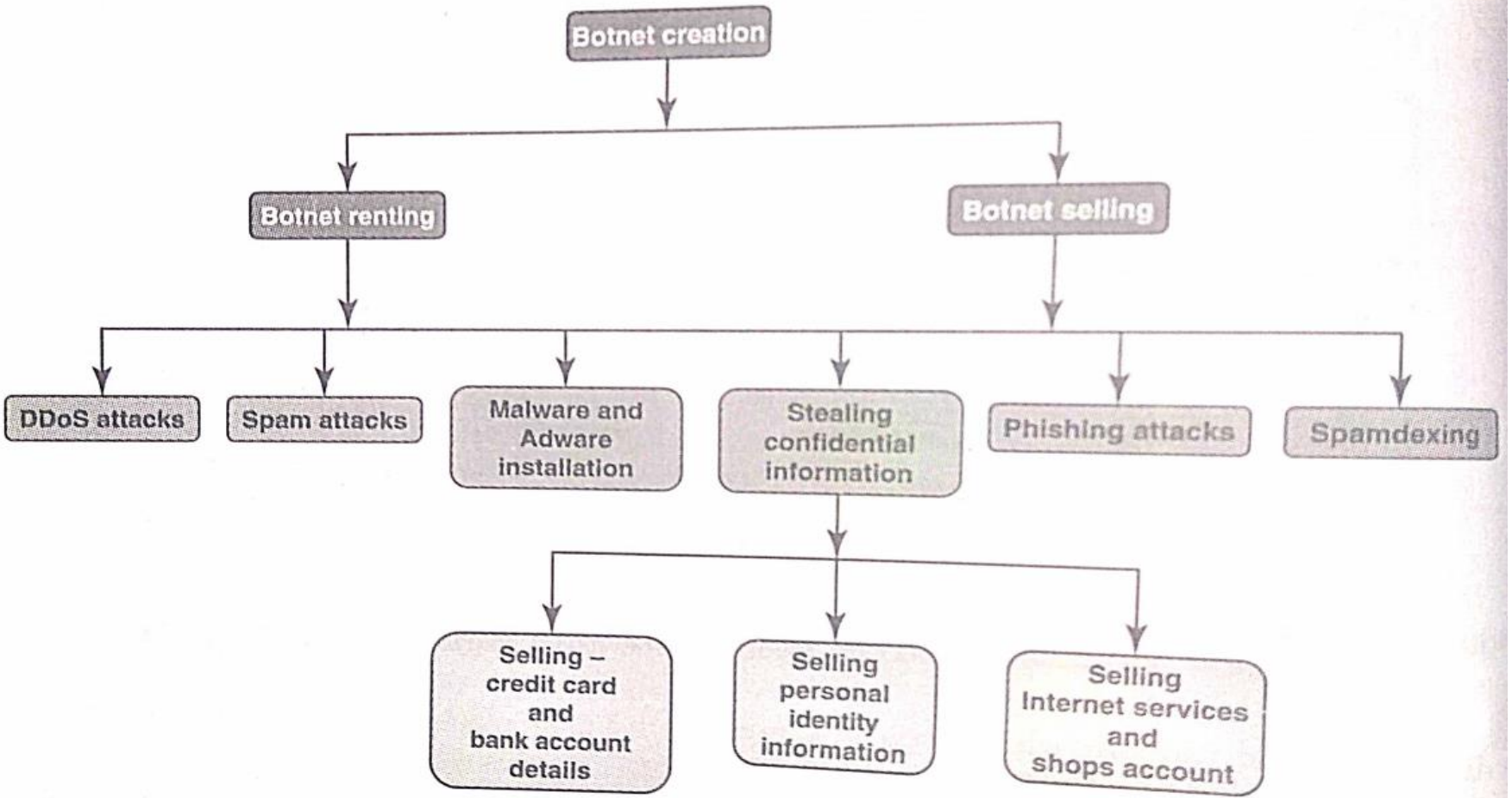


Figure 2.8 | Botnets are used for gainful purposes.

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 compromi... by attackers using a variety of methods (this is discussed in details in Chapter 4)

One can ensure the following to secure the system

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.

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.

are now 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.

Thank you