Chapter 17 – Cyber Safety

Cyber Safety

- It refers to the safe and responsible use of internet so as to ensure safety and security of personal information and not posing threat to anyone else's information.
- It involves gaining knowledge about possible threats to personal safety and security risks for the information along with measures to prevent and counter them.

Safely browsing the Web

- Safe browsing on web needs you to know many things like:

  *What are the possible dangers?

  *How to avoid these?

  *How to virtually conduct yourself while browsing web?

- There are some rules you must follow to conduct yourself online and there are things that you must know so that you can counter unknown dangers.

Identity Protection while using Internet

- When we surf the internet , we give out private data to businesses and other Internet users (such as while filling up some forms or making payments online), we trust them to use that information for legitimate purposes. This isn't always the case though and financial and personal data can be used for harmful reasons like hacking and identity fraud.
- ***Identity fraud*** is a type of fraud when personal details that have been accessed or stolen are used to commit fraudulent acts posing as someone else with stolen identity.

Ways of tracking by Websites

- **Tracking** is generally used by advertising networks to build up detailed profiles for pinpoint ad-targeting even tracking down users for special purpose such as effecting their political choices.

Various mean of tracking by websites

1. **IP Address**
   - It is a ***unique address of your device when you connect to the Internet***. From your IP address, a website can determine your rough geographical location.
2. **Cookies and Tracking Scripts**
   - Cookies are small pieces of information websites can store in your browser. They have plenty of legitimate uses- for example, when you sign into your online banking website, a cookie remembers your login information.

   Types of Cookies

   (i) **First Party Cookies:** These are the cookies that store your own login id, passwords, auto fill information etc. for some websites that you frequently visit.

   (ii) **Third Party Cookies:** These are the cookies that websites store to know about your search history and web browsing history so as to place advertisements as per your interests.
3. **HTTP Referrer**
   - When you click a link, your browser loads the web page linked to it and tells the website where you came from and also your information like IP address, location , your web browser, machine type etc. – It is known as HTTP referrer.

4. **Super Cookies**
   - These are also cookies but these are ***persistent cookies***, i.e. they come back even after you delete them.

5. **User Agent**
   - Your browser also sends a user agent every time you connect to a website. This tells websites your browser and operating system, providing another piece of data that can be stored and used to target ads.

Ways to stop Tacking by Websites

1. **Anonymous Browsing**
   - It allows users to ***view websites without revealing any personal information of the user*** like their IP address, machine type, location etc. An anonymous browser let users access websites anonymously. It can be used as a tool for government, journalists and everyday security-conscious surfers.

2. **Private Browsing**
   - **Incognito Browsing –** It opens up a version of the *browser that will not track your activity*. It's particularly useful if you're entering sensitive data like bank details into the browser.
   - **Proxy** – It works by acting as a *middleman between your computer and the website* you want to access.
   - **Virtual Private Network(VPN) –** It is a method used to *add security and privacy to private and public networks*, like WiFi hotspots and the Internet. VPNs are most often used by corporations to protect sensitive data.

Confidentiality of Information

- Confidentiality of information ensures that only authorized users get access to sensitive and protected data.

Practices to ensure Confidentiality of Information

1. **Use firewall wherever possible**
   - A firewall is a program that can monitor both incoming and outgoing communication and traps the illicit one.

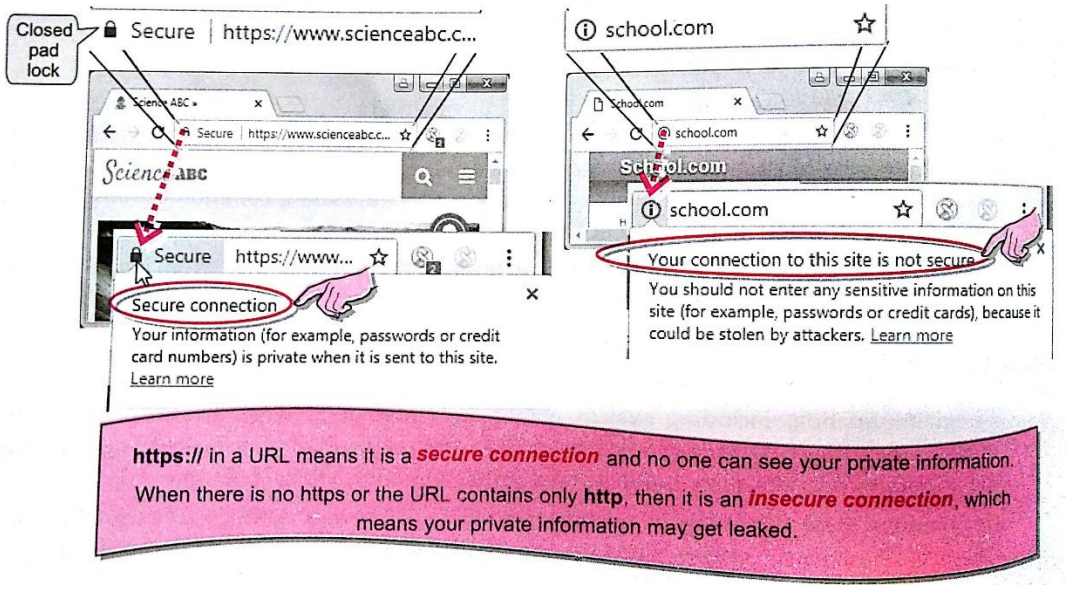
2. **Control browser settings to block tracking**
   - The default browser settings can be changed to prevent the tracking by websites.

3. **Browse privately wherever possible**
   - To avoid the tracking by websites, you should try to browse Internet privately wherever possible.

4. **Be careful while posting on Internet**
   - Ensure that you never post your crucial information like your personal details such as address, mobile number, bank details, credit card details etc. on public Internet sites.

5. **Ensure Safe sites while entering crucial information**
   - When you provide your personal details or bank details on a website, then ensure following things:

   - Type the URL of the website in the address bar of the browser on your own. Do not click on a link that takes to this website; or do not cut/copy the link of this website and paste it. Type the URL on your own in the address bar of the web browser.
   - **Ensure that the address contains HTTP and a pad lock sign.** A safe site's URL starts with https:// and not with http://. Also, it shows a closed pad lock.



6. **Carefully handle emails**
   - While opening an email, make sure that you know the sender. Even if you open the email message by accident, make sure not to open attachment or any link in an email from unrecognized source.
7. Do not give sensitive information on Open Wireless networks.
8. Avoid using Public computers.

Cybercrime

- It is any criminal offense that is facilitated by, or involves the use of, electronic communications or information systems, including any electronic device, computer, or the Internet.

Common Cybercrimes

1. **Cyber troll**
   - It refers to a person who **purposely posts opposing, sarcastic, demeaning or insulting comments** about something or someone with an aim of targeting a person online.
   - **Troll** can refer to a person also who is doing it and it may refers to the derogatory comments posted by a troll.
2. **Cyber Bullying**
   - It occurs when ***someone uses the Internet***, a cell phone, email, instant messaging, chat rooms or social networks, such as Facebook, Twitter etc., ***to harass , demean, embarrass or intimidate someone else***.
3. **Cyber Stalking**
   - This is a kind of online harassment wherein the ***victim is subjected to a barrage of online messages and emails***. A cyber stalker afforded by the Internet to allow them to stalk their victim without being detected.

   Cyber stalkers often do this to trouble their victims:
   - They collect all personal information about the victim such as name, daily routing, place of work, date of birth etc.
   - Some stalkers subscribe the email account of the victim to innumerable obscene or illegal sites because of which victim starts receiving such kind of unsolicited e-mails.
   - Some stalkers keep on sending repeated emails asking for various kinds of favors or threaten the victims.
4. **Spreading Rumors Online**
   - Through fake profiles, some people get indulged in posting false information on social media, or comments that could hurt others or spread rumors that may trigger panic or hurt religious sentiments of other people resulting into clashes and even riots etc.
   - Spreading rumours online is a cybercrime and is a punishable offence. ***As per Information Technology Act of India,*** Publishing/circulation of Rumours, especially hurting religious sentiments is a cybercrime and it may invite a **fine with imprisonment extendable up to three years**.

Reporting Cybercrime

- If any cybercrime happens, one must report it firstly to parents, school authorities and then to police.
  To report a cybercrime:
  - The local police can be approached for filing complaints just as the cybercrime cells specially designated with the jurisdiction to register complaint.
  - In addition, provisions have now been made for filing of **'E-FIR'** in most of the states.
  - In addition, the Ministry of Home Affairs is also launching a website for **registering crimes against women and children online including cybercrimes.**

Common Social Networking Sites

Facebook, Twitter, LinkedIn, Instagram etc.

Appropriate Usage of Social Networks

1. While using social networking sites, ***you should know about what the right online behavior are and what is considered a cybercrime.***
2. If one thinks that by making some anonymous profile and using fake information, he/she can do such activities without getting caught, he/she is certainly mistaken.

Digital Footprint

- Digital footprints are ***the records and traces individuals leave behind as they use the Internet.***
- Your interactions on social media, your friend circle on social media sites, sites you visit, online purchases, locations visited through Facebook check-ins etc. all make up your digital footprints.
- Digital Footprints last forever, and colleges and jobs will look back at them to see if you are what you portray and how you conduct yourself actually.

Usage Rule applicable on the use of Social media

1. **Be Authentic**
   Be honest about your identity.
2. **Use a disclaimer**
   If you are associated with an institution or organization in some form(student or faculty or staff etc.) and you are sharing your personal views about something, do make it clear that these are your personal views and you do not represent any institution or organization here.
3. **Don't Pick Fights Online**
   Convey your unhappiness over a post/comment through constructive posts/message while carefully choosing the right words.
4. **Don't use fake names or pseudonyms**
   Never pretend to be someone else.
5. **Protect Your Identity**
   Never list your full name, parents' details, home address or telephone number online. It is a good idea to create a separate e-mail address that is used only with social media sites. Also, you should never share about your location online; thieves are always ready and love such opportunities.
6. **Respect Your Audience**
   Don't use slang, personal insults, obscenity, or engage in any conduct that would not be acceptable in your connected world.
7. **Respect other's Sentiments**
   You should always respect others' privacy and be considerate for topics that may be considered sensitive- such as politics and religion.
8. **Monitor Comments**
   You should prefer to review and approve comments before posting them on your site. This way you will ensure the quality of comments.

Chapter 18 – Online Access and Computer Security

THREATS TO COMPUTER SECURITY

A threat is a potential violation of security. When a threat is actually executed, it becomes attack.

Various threats to computer security are:

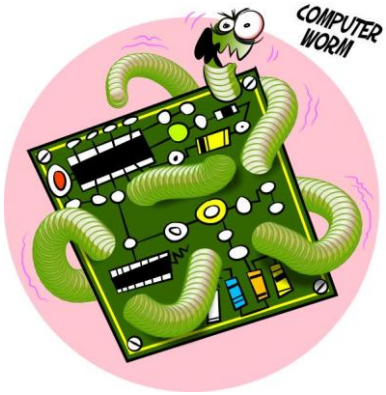
1. Viruses
   - Worms
   - Trojans
2. Spyware
3. Adware
4. Spamming
5. PC Intrusion
   - Denial of Service
   - Sweeping
   - Password Guessing
6. Phishing

VIRUSES

- Virus are malicious codes/programs that cause damage to data and files on a system.
- It can attack any part of computer's software such as operating system, application programs and system files.
- **Two common type of viruses are : WORMS & TROJAN**

WORMS

- It is a **self-replicating program** which eats up the entire disk space or memory. A worm keeps on creating its copies until all the disk space or memory is filled.



TROJAN HORSES

- It is a program that appears harmless (such as a text editor or a utility program) but actually performs malicious functions such as deleting or damaging files.

DAMAGES CAUSED BY SYPWARE

1. Damage or delete files – damage or delete random documents or specific files that are crucial to Operating System.
2. Slow down your computer
3. Invade your email program

SPYWARE

- It is software which is installed on your computer to **spy on your activities** and report this data to people willing to pay for it. It tracks the user's behavior and reports information back to a central source.

- It gets **installed on your PC without your consent**. It gets downloaded from the internet when you visit a particular website.

DAMAGES CAUSED BY SYPWARE

1. Compromises your data, computing habits and identity.
2. Alter PC Setting
3. Slows down your PC.

ADWARE

These are the programs that **deliver unwanted ads to your computer**. They consume your network bandwidth.

DAMAGES CAUSED BY ADWARE

1. Adware tracks information just like spyware.
2. Displays arrays of annoying advertising.
3. Slows down your PC.

SPAMMING

- It refers to the **sending of bulk mail by an identified or unidentified source**.

- In non-malicious form, bulk-advertising mail is sent to many accounts. In malicious form, the attacker keeps on sending bulk mail until the mail-server runs out of disk space.

DAMAGES CAUSED BY SPAMMING

1. Spam reduced productivity
   Billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance and reduce overall productivity.
2. Spam eats up your time
3. Spam can lead to worse things.

PC INTRUSION

Every PC connected to the internet is a potential target for hackers. Unauthorized access to data present in PC is known as PC intrusion.

TYPES OF PC INTRUSION:

1. **SWEEPER ATTACK:** this attack deletes all the data from the system.
2. **DENIAL OF SERVICE:** It prevents the legitimate users of a website to use the website, by flooding website with lots of messages.
3. **PASSWORD GUESSING:** Most hackers crack or guess passwords of system accounts and gain entry into remote computer systems.

EAVESDROPPING

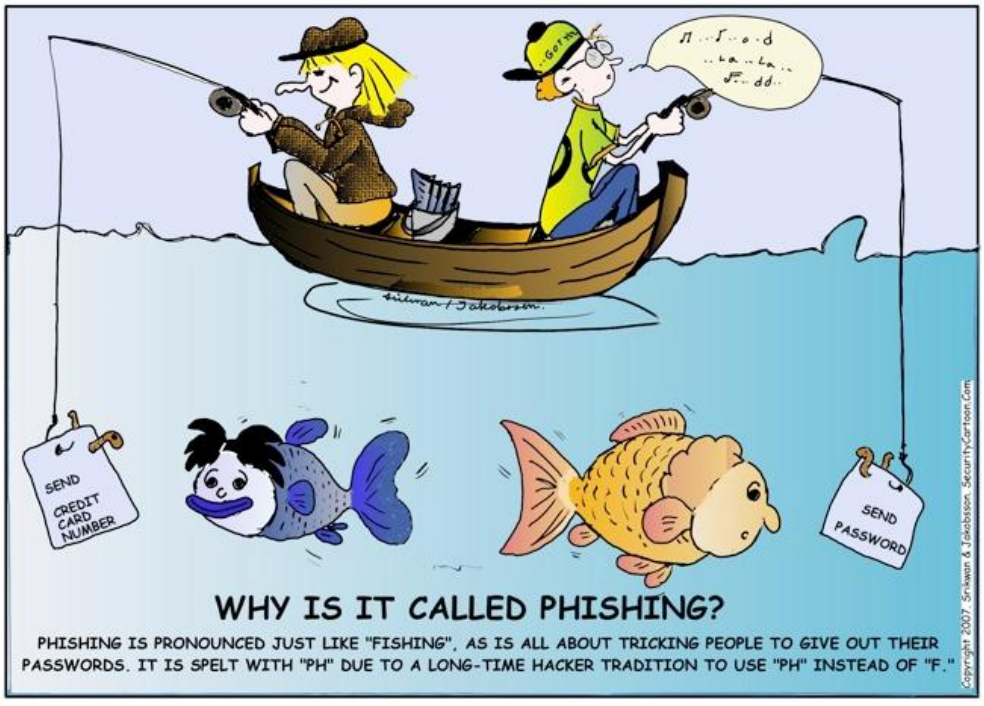
- It is a passive attack in which an attacker gains access to the communication-medium through which some communication is taking place and then listens to the communication and gets information about the content of the message.

- Eavesdropping activities do not affect normal operation of transmission and communication; thus both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced.

PHISHING

- It is the fraudulent **process of attempting to acquire sensitive information such as usernames, passwords, credit card information, account data** etc.

- In phishing, an imposter uses an authentic looking email or website to trick recipients into giving out sensitive personal information.



PHARMING

- It is an attack in which a hacker attempts to redirect a website's traffic to another, bogus website. Through pharming attack, the attacker points you to a malicious and illegitimate website by redirecting the legitimate URL.
- In this the attacker convinces you that the site is real and legitimate by spoofing or looking almost identical to the actual site down to the smallest details.

COOKIES

- Also **known as web cookie or browser cookie.**
- It is a **small piece of data sent from a website and stored in a user's web browser** while a user is browsing a website.
- Some cookies disappear after user closes his browser while others, known as **tracking cookies**, remain saved and load the next time user visits the same websites.

SOLUTIONS TO COMUTER SECURITY THREATS

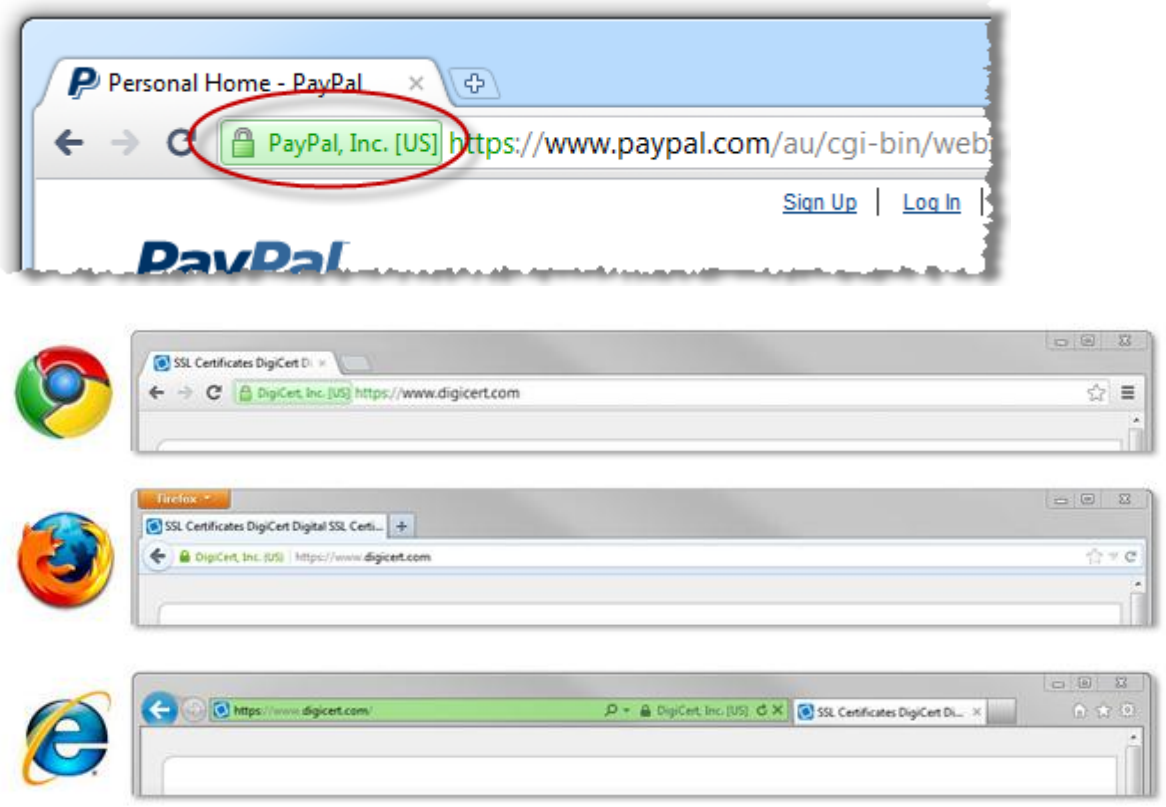
Two solutions against threats are: **1. Active Protection** **2. Preventive Measures.**

ACTIVE PROTECTION

1. **Use anti-virus and anti-spyware software**, to detect and eliminate any threat that sneaks its way onto your PC.
2. New viruses and malware emerge every day, and your **security software must be updated** in order to provide full protection.
3. **Run Frequent full system scans** at least once in a month.

PREVENTIVE MEASURES

1. **Only download files from reputable websites** by looking full contact information and **SSL encryption** of sensitive information, typically indicated by a padlock in the lower right corner of your web browser.



2. Be careful with email, **don't download or open doubtful email attachments**. And disconnect from the internet when you're away.
3. **Disable cookie** – If you are particular about the safety of your personal information, then you may disable cookies on your browser.

PREVENTION AGAINST SPAM

1. **Sender Filtering** – This method allows only messages from your approved sender list to reach your inbox. This is done on basis of **digital certificates and digital signatures.**

Digital certificates are specially formatted digital information issued to websites, are used to verify the identity of the message from sender to recipient by generating a digital signature that can be used to sign the message.

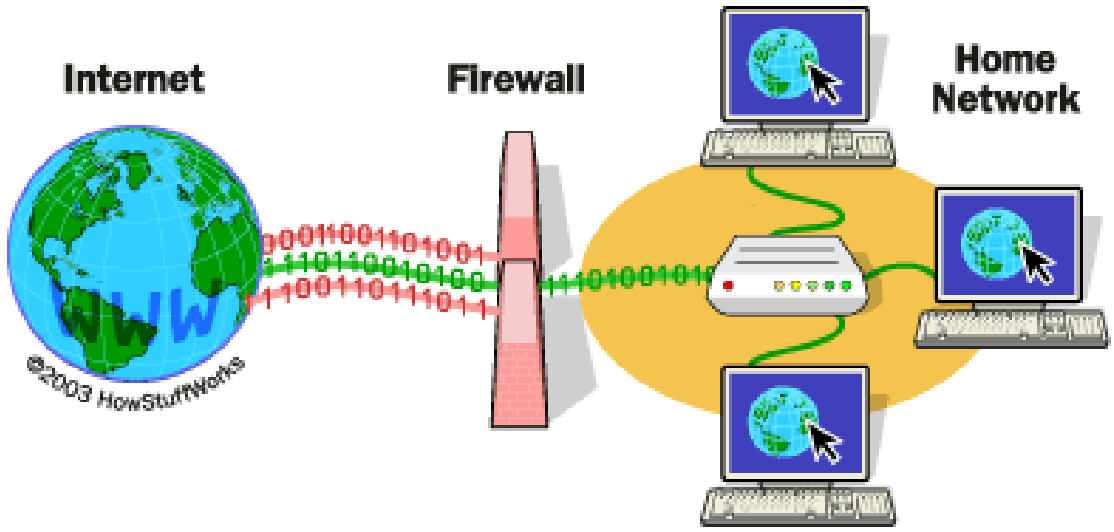
2. **Keep email address private.**
3. Install protection software such as Internet security software.
4. Avoid conducting online transactions or using online banking services on public Internet facilities.

PREVENTION AGAINST PC INTRUSION

1. **Authorization** – Asking the user a legal login –id performs authorization.

2. **Authentication** – It is also termed as **password protection** as the authorized user is asked to provide a valid password, and if/she is able to do this, he/she is considered to be an authentic user.

3. **Firewall** – A system designed to prevent unauthorized access to or from a private network is called Firewall. Firewall are a mechanism to prevent unauthorized Internet users from accessing private networks connected to the Internet.



SOLUTIONS TO PHISHING AND PHARMING

1. Don't open emails from unknown sources or click on links embedded in suspect messages.
2. Check the security guidelines of websites, so that you can distinguish between legitimate and bogus emails.
3. The best way to handle these threats is through vigilance, as these attacks rely on tricking users than advanced technology.

****