Society, Law and Ethics(SLE-1) – Cyber Safety

TEACHING TOPICS

- Cyber Safety : Safely browsing Web, Identity Protection
- Confidentiality, Social Networks, Cyber trolls and bullying
- Appropriate usage of Social Networks : Spread of rumors
- Common Social Networking Sites : Twitter, LinkedIn, Facebook
  - Specific usage rules
- Safely accessing websites : adware, malware, viruses, Trojans
- Safely communicating data : Secure connections, eavesdropping
- Phishing, Identity Verification

WHAT IS CYBER SAFETY ?

- Cyber Security refers to the safe and responsible use of Internet to ensure safety and security of personal information 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.

IDENTITY PROTECTION

- Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits.
- It is an act of stealing someone's personal credentials like Login details, Credit card number, etc.

MOST COMMON SOLUTIONS:

- Private browsing or Anonymous Browsing(Incognito Mode)

HOW WEBSITES TRACK US

IP ADDRESS – Size → 32 bytes or 4 bits

- IP Address is a unique address of our device when we connect to the Internet.
- The computer shares our IP Address with other networked device across the Network.
- Hence a computer on the Internet can be reached by its IP Address.
- The IP Address shares our geographical location along with the device details.

COOKIES

- **COOKIES :** These are small text files on our computer storing small piece of information, storing our online habits.
- **First Party Cookies :** These cookies store our login ID, Password, auto-fill information for some websites that we frequently visit.
- **Third Party Cookies :** These cookies store our recent search history, web browsing history so as to place advertisements as per our interests.

Third Party Cookies are responsible for Unwanted Advertisements on our WebPages.

HTTP REFERRER

- Some websites when clicked, take us to another website and internally information about our IP Address, Location, Machine type, etc will be sent to the linked website. This is called as HTTP Referrer.

SUPER COOKIES

- Super cookies otherwise called as Ever-cookies are persistent cookies.
- They come back even after we delete them.
- These cookies are deleted at multiple places like Flash Cookies, Silverlight Storage, browsing history, HTML5 Local storage, etc.
- So even if we delete our browsing history, these cookies get repopulated from other locations like Flash cookies.

USER AGENT

- The User agent is sent by the browser every time we connect to a website.
- This tells the website about the browser, OS, etc. by providing extra piece of information about our system.
- These informations are used to target ads while we browse the Internet.

ANONYMOUS BROWSING

- Anonymous browser allows users to view websites without revealing any personal information of the User like the IP Address, Machine Type, location, etc.
- An anonymous browser lets users access the websites anonymously.
- It can be used as a tool for Governments, Journalists where security is the main concern.

PRIVATE BROWSING

- Incognito Browsing : This opens up a version of the browser that will not track our activity. It's very useful if we are opening browsing from a shared computer.
- This minimizes the risk of saving information and cookies saving onto the computer.
- Incognito mode deletes all temporary files and cookies while closing the browser.
- Private search engines like DUCKDUCKGO are useful for searching information which can't be tracked.

PROXY

- Proxy works by acting as a middleman between our computer and the website we want to access.
- The tracking website gets the IP Address of the proxy server instead of our computer.
- So effectively we get the same information from the website through another Computer, by securing ourselves from external attacks.

VIRTUAL PRIVATE NETWORK

- VPN is a method to add security and privacy to public networks like WIFI Hotspot, Internet.
- VPNs are generally used by corporate sectors for protecting their sensitive data.
- VPNs create a virtual network where information can be kept secure from hackers.

CONFIDENTIALITY OF INFORMATION

- Internet is a public platform. So all our activities on the internet are mostly public.
- But there are some information like our banking transactions, credit card history or emails, which need to be private and confidential.
- Confidentiality of Information ensures that only authorized users get access to sensitive and protected data.

PRACTICES TO ENSURE CONFIDENTIALITY OF INFORMATION

- **Use Firewall where ever possible**
  - The firewall can be a hardware or a software that blocks suspected incoming connections instead of leaving completely open access to the internet from our machine.
- **Control Browser settings to block tracking**
  - We can setup our browser to exclude cookies, especially third-party cookies, since they can build up detailed profiles of our surfing patterns over time.
- **Browse Privately whenever possible**
  - To avoid the tracking of websites, we should try to browse privately wherever possible. This way website would not be able to store cookies on our computer.
- **Do not give sensitive information on wireless networks**
  - While using public networks like WIFI on Airports, Railway Stations or coffee shops, do not open any personal emails or any sensitive information like banking, etc. The reason is free

wireless networks are not encrypted and hence information on it can be tapped and used for fraudulent purposes.

- **Avoid using public computers**
  - Ensure not to use a public computer while dealing with crucial data. But if still we use, make sure to do the followings:
    - Browse Privately
    - Don't save login information
    - Never save passwords on public computers
    - Don't leave the computer un attended with sensitive information on the screen
    - Log out before leaving the computer
    - Erase history and traces of your work

CYBER CRIME

- Cyber crime 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.
- The term CYBER CRIME is a general term that covers crimes like phishing, credit card frauds, illegal downloading, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and distribution of viruses, spam and so on.
- **CYBER TROLLS**
  - Derogatory messages or comments posted online targeting people are called cyber trolls.
  - Toll refers to a person who purposely posts opposing, sarcastic, demeaning or insulting comments about something or someone targeting a person online.
- **CYBER BULLYING**
  - Harassing, demeaning, embarrassing, defaming or intimidating someone using modern technology like internet, cell phones, instant messengers, social networks etc. is called Cyber bullying.
- **CYBER STALKING**
  - A cyber stalker relies upon the anonymity afforded by the internet to allow them to stalk their victim without being detected.
- **SPREADING RUMORS ONLINE**
  - Through fake profiles, people sometimes indulge 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.
  - As per Information Technology Act of India, publishing/circulation of rumors, especially hurting the religious sentiments is a Cybercrime. It may invite a fine with imprisonment extendable up to 3 years.

REPORTING CYBER CRIME

- If any Cybercrime happens, it must firstly be reported to parents, school authorities and to police.
  - The local police station can be approached for filing complaints just as the cybercrime cells specially designated with jurisdiction to register complaint.
  - In addition, provisions have been made for filing e-FIR in many states.
  - Ministry of Home Affairs is also launching a website for registering crimes against women and children online including cybercrimes.
  - The Information Technology Act categorically provides that cybercrime has a global jurisdiction, meaning that the crime can be reported in the Cyber Crime Units of any city, irrespective of the place where the act was committed.

SOCIAL NETWORKING

- A Social networking site is a web application or online platform where people can setup their public profiles and make connections with other online people, called Online Friends.
- Some common social networking websites are :FACEBOOK, TWITTER, LINKEDIN, INSTAGRAM, GOOGLE+, SNAPCHAT PINTEREST, REDDIT, QUORA, etc.
- FACEBOOK
  - It is a platform where we can share we can share our ideas in the form of posts, share our photos, videos etc. Through Facebook we can connect with other Facebook users and exchange messages, posts, etc.
  - It allows you to view the posts, images and videos shared by your friends and provides options to like it or comment on it.
- TWITTER
  - It is a micro-blogging website which allows to post very small messages upto 140 Characters.
- INSTAGRAM
  - It is one of the most popular social networks for online photo sharing.
- LINKEDIN
  - It is a social networking website for professionals. It provides features to make profiles look sort of detailed resumes, with sections for Work Experience, Education, Certifications, Awards and all sort of work related informations.

APPROPRIATE USAGE OF SOCIAL NETWORKING

- DIGITAL FOOTPRINT :
  - Digital footprints are records and traces individuals leave as they use the Internet.
  - The sites we visit, online purchases, locations visited, check-ins, etc. all make up our Digital Footprints.
  - Once we post or share anything online, it stays forever and cannot be undone. Digital Footprints last forever and the leave the records of activities we've performed over the years.

PRIVACY SETTINGS

- Social media accounts can be set-up with privacy settings as:
  - Who can see your posts
  - Who can send friend request
  - What all information about you is visible to others

USAGE RULES ON SOCIAL MEDIA

- Be Authentic
- Use a Disclaimer
- Don't Pick Fights Online
- Don't Use Fake Names or Pseudonyms
- Protect your Identity
- Respect your Audience
- Respect other's Sentiments
- Monitor Comments

THREATS TO COMPUTER SECURITY

- A Threat is a potential violation of security.
- When a threat is executed, it becomes Attack.
- Those who execute such actions, or cause them to be executed are called Attackers.

COMMON THREATS

- Viruses
  - WORMS
  - TROJANS
- Spyware
- Adware
- Spamming
- PC Intrusion
  - Denial of Service (D O S)
  - Sweeping
  - Password Guessing
- Phishing

COMPUTER VIRUSES

- Computer viruses are the malicious codes that cause damage to data and files on a system. Viruses can attack any part of a computer's software such as boot-block, operating system, system areas, files and application programs.
- Two other program can cause virus like effects.
  - Worms
  - Trojan Horses
- **WORM :**
  - A worm is a self-replicating program which eats up the entire disk space and memory. A worm keeps on creating its copies until all the disk space or memory is filled.
- **TROJAN HORSES :**
  - A Trojan Horse is a program that appears harmless but actually performs malicious functions such as deleting or damaging files.

DAMAGES CAUSED BY VIRUSES

- Damage or delete files.
- Slow down your computer
- Invade your email program

SPYWARE

- Spyware is a software which is installed on your computer to track 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.
- These get installed to system without your consent, by "Piggybacking" onto a file.

DAMAGES CAUSED BY SPYWARE

- Compromise your data, computing habits and identity
- Alters PC Settings
- Slows down your PC

ADWARE

- These are the programs that deliver unwanted ads to your computer (generally in Pop-ups form).
- They consume network bandwidth.
- Adwares get installed with the user's consent. So it is very important to read the installation agreement thoroughly before installing any new software.

DAMAGES CAUSED BY ADWARE

- Adware tracks information just like spyware
- Displays arrays of annoying advertisements

- Slows down your PC by consuming resources.

SPAMMING

- Spamming refers to the sending of bulk-mail by an identified or un-identified source.
- In non malicious form, bulk-advertising mails are being sent to many accounts.
- In malicious form (e-mail bombing) the attacker keeps on sending bulk mail until the mail server runs out of disk space.

DAMAGES CAUSED BY SPAMMING

- Spam reduces productivity
- Spam eats up your time
  Spam eats up disk space

PC INTRUSION

- Every PC connected to Internet is a potential target for hackers.
- Sweeper Attack
  - This is another malicious program used by hackers. It sweeps i.e. deletes all data from the system.
- Denial of Services
  - This type of attack eats up all the resources of a system and the system or application come to a halt.
- Password Guessing
  - Most hackers crack or guess passwords for accounts and get entry to remote computer systems.

EAVESDROPPING

- Eavesdropping is a passive attack in which an attacker gains access to the communication-medium through which the communication is taking place.
- Eavesdropping can be carried out on telephone systems, emails, IMs, Mobile devices, etc.
- Eavesdropping activities do not affect normal operation of transmission or communication; thus both sender and receiver can hardly notice that their data is being stolen, intercepted or defaced.

PHISHING AND PHARMING

- In Phishing, an imposter uses an authentic looking email or web-site to trick recipients into giving out sensitive personal information. Though it appears to be genuine, it will take you to fraudulent sites where all sensitive data is obtained and used for cyber-crimes and frauds.
- Pharming is an attack in which a hacker attempts to redirect a website's traffic to another, bogus website. Through Pharming attack, the attacker points to a malicious and illegitimate website by redirecting the legitimate URL.

SOLUTIONS TO VIRUSES, ADWARE AND SPYWARE

- Active Protection:
- Use Antivirus and Anti-spyware software
  - Disconnect the infected system from the network
  - Restore files from disk backups
  - Scan the whole system for more evidence of virus
  - Download updates regularly
- Preventive Measures:
  - Keep system up-to-date
  - Download from trusted websites
  - Be careful with emails
  - Disable cookies, if possible

SOLUTIONS TO SPAM AND EAVESDROPPING

- Active Protection:
  - Use Anti-Spam software
    - Sender filtering
    - Keyword Filtering
    - Digital Signatures
- Preventive Measures:
  - Keep e-mail address private
  - Use encrypted connection
  - Install personal firewall
  - Avoid Public Networks
  - Install Internet Security Software

SOLUTIONS TO PC INTRUSION

- Active Protection:
  - Authorization
  - Authentication
  - Firewall
- Preventive Measures:
  - Proper file access permissions while sharing files on Internet
  - Disconnect from Internet when away

SOLUTIONS TO PHISHING AND PHARMING

- Active Protection:
  - Backup files regularly
  - Check for the installed keyloggers in the computer
  - Contact credit agencies to report any identity theft
- Preventive Measures:
  - Don't open emails from unknown sources
  - Instead of Clicking on link, type the link on browser
  - When in doubt, DO NOT CLICK

FIREWALL : AN IMPORTANT SOULTION FOR COMPUTER SECURITY

- Firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules.
  - Software Firewall : Eg:- Antivirus
    - Software firewall is a special type of computer software running on a system. It controls the system from outside attempts to gain access.
  - Hardware Firewall : Eg:- Router
    - It is a physical piece of equipment, designed to perform firewall duties. These are affective with minimum configuration and can protect all computers on a network.