Cyber Safety-

Cyber safety is the safe and responsible use of Internet to ensure safety and security of personal information and not posing threat to anyone else's information

Safely Browsing the Web

Viruses and malware spread, easily and quickly through websites/web browsing.
Through clicking over the links found on web pages or in email mistakenly our computer may be infected.

An infected computer

- **can run slow,**
- **barrage us with pop-ups,**
- **download other programs without our permission,**
- **or allow our sensitive personal information to others.**

Tips for Safe Web Browsing

- **Common sense-** never respond to spam & disclose personal information.
- **Use an antivirus & Firewall-**It provide real time malware protection.
- **Create strong passwords**

- **Mind your downloads -**Be sure to review all pre-checked boxes prompted at download & un-check any extra applications which we don't want to install.

- **Stay updated-** Update O.S. , Applications & Anti-virus.

Identity Protection

Protection against theft of personal information over Cyber Space without consent, usually for financial gain is known as Identity Protection.

Identity Theft

It is a type **of fraud** that involves using someone else's identity to steal money or gain other benefits.

Online identity refers to an **act of stealing someone's personal information** such as name, login details etc. and then posing as that person online.

Various forms of Identity theft are:

- **Financial identity theft- when someone uses the stolen identity for financial gain**
- **Criminal identity theft-when criminals use the stolen identity to avoid detection of their true identity.**

  The person whose identity is stolen is actually a victim but this identity theft poses him as a criminal.
- **Medical identity theft- when someone tries to obtain some medical drugs or treatment using a stolen identity.**

Tips to Prevent Identity Theft

- **Use strong passwords and PINs & Keep passwords and PINs safe.**
- **Create log-in passwords for all devices.**
- **Beware of phishing scams.**
- **Restore old computers to factory settings.**
- **Encrypt your hard drive**
- **Check security when shopping online-check links authenticity which are received from an unsolicited email.**
- **Take care when posting on social media-Check security settings on social media accounts, and avoid posting personal information publicly, or publicly "checking in".**
- **Secure your home Wi-Fi network& Avoid using insecure public Wi-Fi networks**

.

Many ways Websites Track you

1. IP address- is a unique address of your device when you connect to the internet.
2. Cookies and tracking scripts-
    1. first party cookies- these store your own login id , passwords, auto fill information etc.
    2. Third party cookies-these store to know about your search history as to place advertisements as per your interests.

Many ways Websites Track you

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 .

4. Super cookies-these are persistent cookies i.e. they came back even after you delete them.

Super cookies store cookie data in multiple places-
e.g in flash cookies,Silverlight storage,browsing history etc

5. User agent-this tells websites your browser and operating system, providing another piece of data that can be stored and used to target ads.

Many ways Websites Track you

All these above things leak your identity information to websites and it may be used against you .
Solution to this is private browsing and anonymous browsing

anonymous browsing

- It allows users to view websites without revealing any personal information of the user like their IP address,machine type and location etc.

- It can be used as a tool for governments , journalists and everday security –conscious surfers

Private browsing

- Incognito browsing- useful to enter sensitive data like bank details.
- Proxy – works as a middleman between your computer and the websites you are accessing
- Virtual Private Network(VPN)- used to add security and privacy to private and public networks like wifi hotspots.

In Private browsing browser does not store cookies about your online activity

Confidentiality of Information

Allows authorized users to access sensitive and secured data maintains the Confidentiality of Information.

Tips to Protect Information Confidential

- **Build strong passwords**

- **Use multifactor authentication-** a computer user is granted access only after successfully presenting 2 or more pieces of evidence.

- **Masking -**The free version of MaskMe creates an alternate e-mail address whenever a Web site asks for a user's e-mail. E-mails from that site can be accessed via a MaskMe in-box or forwarded to a user's regular e-mail account.

- **Private Browsing & Safe Browsing-**Purpose of pvt browsing is to avoid leaving a history of one's browsing in the browser history on the computer we are using.Use updated brower for safe browsing & browse privately.

- **Encryption-**Use https based sites,as HTTPS ensures data security over the network - mainly public networks like Wi-Fi. HTTP is not encrypted and is vulnerable to attackers. PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.

- **Avoid using public wifi and public computer**

Cyber Safety – Social Networks

Facebook, Myspace, Twitter, Linkedlin, Digg, Ning, Meetup etc…
the number of social networking sites and tools is exploding nowadays.These are becoming soft tool to attack & target for scam.

Tips to stay safe on social media

- Use firewall whenever possible
- Browse privately whenever possible
- Use a strong password
- Use a different password for each social media
- Password protect your devices if using social media apps
- Be selective with friend requests.
- Be careful while sharing something.
- Become familiar with the privacy policies of the social media sites.
- Install antivirus
- log off when done
- Create a smaller social network
- Avoid using public computer/network
- Don’t give sensitive information on wireless network.

Cyber Trolls & Cyber bullying

Cyber trolling is internet slang for a person who intentionally starts arguments or upsets others by posting inflammatory remarks. The sole purpose of trolling is angering people.

Purpose – to entertain, to argument, to upset victim , to get attention

Cyberbullying: Saying and/or doing mean things to the person online. It is a harm inflicted through using the Internet, ICT devices, or mobile phones.

Purpose – to get revenge, to harass & threat, to humiliate

Cyberstalking: Doing research on every aspect of the person's life.

Cyberharrassment: Continuously contacting the person online, even though they don't want you to.

Social Network

Social Network refers to web and mobile technologies or their practices to share content, thoughts, ideas, opinions, experiences etc. online. Various examples of social networks are Facebook, Twitter, YouTube, LinkedIn, and blogging sites among many others.

Problems to Avoid

- Cyber trolling
- Cyber-bullying
- Cyber-stalking
- Cyber-harrassment
- Stranger Danger-

  Children's are advised to not to interact with strangers on social networks as there are chances that many people on social media are not who they say they are.

- Digital Footprint- The history of a person's usage of digital devices, movie , search, programs watched, flight searched, websites surfed, credit card transaction, cell phone calls, social media messages sent, links clicked and Facebook pages liked etc. Such information is being used to target ads to consumers as these are digital footprints of such consumers.

Common Usage rules of Social Networking Sites(facebook,twitter,linkedIn)

- Don’t be rude or abusive
- Don’t spread rumors
- You are what you write/tweet
- Face your problems, don’t Post your problems.
- Don’t take it too seriously.
- Don’t use fake name
- Protect your identity
- Respect other’s sentiments
- Don’t fight online
- Monitor comments
- Don’t pick fight online
- Respect your Audience
- Be reliable

Online Fraud

fraud committed using the internet.

e.g.

- identity theft (stealing information)
- fraudulent payment
- Non-delivered goods
- Non-existent companies

Measures to stop Online Fraud:

- A monitoring official organization that ensures the sanctity of E-commerce company and delivery of goods/services as promised.
- Strong security mechanism by the e-commerce site and payment gateways to prevent stealing of crucial information.
- Official guidelines and safeguards on the selling of user's data to third parties.

Scams

Any fraudulent business practice that extracts money from an unsuspecting , ignorant person is called a SCAM

Measures to Avoid Online Scams:

- Never enter personal information or any financial information on unsecure websites(the sites do not employ HTTPS or padlock sign)
- Never reply to emails from any unknown or unreliable source.
- Never respond to an e-mail or advertisement claiming you have won something.
- Never click on any links that you have received in your e-mail, if you don’t know the sender.
- Check the URL before clicking on the link in the e-mail.

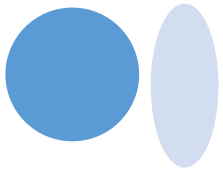
Report Cybercrime

- Approach to Local police station for filing complaints or e-FIR.
- Access a website for registering crimes against women and children online.

www.cybercelldelhi.in
cybercrime.gov.in

Computer Forensics

- Methods used for interpretation of computer media for digital evidence.
- It is a systematic process that interprets electronic data for use in a court of law.
- The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting , identifying and validating.



Data identification

Project planning

- Data processing
- Data analysis
- Data capture
- Data display
- Report Generation