Chapter 17 :

Computer Science

Class XI (As per CBSE Board)

New Syllabus 2019-20

Visit : python.mykvs.in for regular updates

Introduction-Cyber Safety

Cyber safety is the safe and responsible use of Internet & ICT(Information & Communication Technology). Cyber safety is about to not only keeping information safe and secure, but also being responsible with that information, being respectful of other people online. As per Cyber safety peoples are advised to use good 'netiquette' (internet etiquettes).

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 realtime 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.

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**

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.
- **Avoide using public wifi and public computer**

Cyber Safety – Social Networks

Facebook, MySpace, Twitter, LinkedIn, 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 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**

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

Cyberbulling: 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.

Appropriate Usage of 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.

Appropriate Usage of Social Network

Problems to Avoid

- Cyber trolling
- Cyberbulling
- Cyberstalking
- Cyberharrassment
- 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 footprint of such consumers.

Appropriate Usage of Social Network

Problems to Avoid

➢ Spread of rumors -

A lie can travel halfway around the world before the truth has got its boots, this phrase totally fits with rumors spread over social media. On average, it takes more than 12 hours for a false claim to be debunked online where as only 2 hours for true claim.

A standard model of rumor spreading is given by Daley and Kendall ,which is called DK model.In this model there are N people in total. Which are categorized into three groups: ignorants, spreaders and stiflers, which are denoted as S, I, and R.

$S + I \xrightarrow{\alpha} 2I$ when a spreader meet an ignorant, the ignorant will become a spreader.

$I + I \xrightarrow{\beta} I + R$ when two spreaders meet with each other, one of them will become a stifler.

$I + R \xrightarrow{\beta} 2R$ when a spreader meet a stifler, the spreader will lose the interest in spreading the rumor, so become a stifler.

So $N = I + S + R$

Appropriate Usage of Social Network

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/facebook 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

Computer Security Threats

Malware: Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious .

computer virus: It is a small piece of software that can spread from one infected computer to another. It can corrupt, steal, or delete data on your computer/hard drive.

Trojan horse: can do anything from record your passwords by logging keystrokes (known as a keylogger) to hijacking your webcam to watch and record your every move.

Computer worm: A computer worm is a software program that can copy itself from one computer to another, without human interaction.

Spam: unwanted messages in your email inbox.

Phishing: Phishing are fraudulent attempts by cybercriminals to obtain private information. For e.g.a message prompt your personal information by pretending that bank/mail service provider is updating its website.

spyware: spyware is used to spy on their victims. An e.g. is keylogger software that records a victim's every keystroke on his or her keyboard.

Adware : unwanted ads shown while surfing internet.

Eavesdropping : is the act of intercepting communications between two points.

Safely accessing web sites

➢ **How to prevent/remove Adware/malware**

- **Uninstall the malicious programs from Windows**
- **Use antivirus program for malware and unwanted programs**
- **Reset the browser settings to their original defaults**
- **Scan for malicious programs antivirus/antimalware program**

➢ **How to prevent/remove virus**

- **Beware of Fake Download Buttons**
- **Use a Secure Browser**
- **Avoid Public Torrent Sites**
- **Don’t Open Email Attachments Forwarded to You**
- **Don’t Use Your PC’s Admin Account**
- **Scan All New Files and Disks**

➢ **How to prevent/remove Trojan**

- **Never open unsolicited emails from unknown senders**
- **Avoid downloading and installing programs unless you fully trust publisher**
- **Use firewall software**
- **Use a fully updated antivirus program**

Safely Communicating data

❑ Secure Connections

A secure connection refers to the connection which is encrypted by one or more security protocols for security of data flowing between two or more nodes. When it is not encrypted, it can be easily listened by anyone with the knowledge on how to do it.

- **Secure Sockets Layer (SSL) is a computer networking protocol used for insecure network, between network application clients and servers .Due to various flaws, SSL was deprecated for use on the internet by the Internet Engineering Task Force (IETF) in 2015 by the Transport Layer Security (TLS) protocol. Both are not interoperable, TLS is backwards-compatible with SSL 3.0**

Safely Communicating data

Secure Connections

- **Transport Layer Security (TLS)** encrypts data moving over the network or Internet to ensure that any body(hacker/evesdropper) will not be able to see what is transmitting. It is useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence.

How it works

TLS uses a combination of symmetric and asymmetric cryptography both for better security.With symmetric cryptography, data is encrypted and decrypted with a secret key known to both sender and recipient; typically 128 but preferably 256 bits in length (anything less than 80 bits is now considered insecure). Symmetric cryptography uses a common secret key ,which is shared a secure manner.

Asymmetric cryptography uses 2 keys – a public key, and a private key. The public key of the recipient to be used by the sender to encrypt the data they wish to send to them, but that data can only be decrypted with the private key of the recipient.

Safely Communicating data

Secure Connections

- **Hyper Text Transfer Protocol Secure (HTTPS)** is the secure version of HTTP, the protocol over which data is sent between your browser and the website server. HTTPS pages typically use one of two secure protocols to encrypt communications - **SSL** (Secure Sockets Layer) or **TLS** (Transport Layer Security).

- **Eavesdropping**-eavesdropping in a man in middle attack and the message is passing from the client to server. The solutions to this problem are:
  - ✓ to encrypt the message
  - ✓ to encrypt the channel

  Both are appropriate in different situations. To prevent Eavesdropping in any kind of communication channel can be achieved by usage of "Secure Tunneling" of your channel data.

Safely Communicating data

- **Phishing**-Phishing are fraudulent attempts by cybercriminals to obtain private information. For e.g.a message prompt your personal information by pretending that bank/mail service provider is updating its website.

There are various phishing techniques used by attackers:

- Embedding a link in an email to redirect to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment
- Spoofing the sender's address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain information over the phone by impersonating a known company vendor.

Few steps to protect against phishing-

Deploy a SPAM filter, Keep all systems current with the latest security patches and updates, Install an antivirus solution, Develop a security policy, Deploy a web filter to block malicious websites, Encrypt all sensitive information.

Safely Communicating data

❑ Identity verification methods

- Knowledge-Based Authentication (KBA)-by asking them to answer specific security questions
- Two Factor Authentication (2FA)-not only a password and username, but also something that the user has with them
- Database Solutions-behavioral patterns to detect if an online ID is authentic, a fraudster or a bot.
- Online Identity Verification-A mix of artificial intelligence, computer vision, and verification experts to determine if a government-issued ID is authentic and belongs to the user.
- Biometric verification -by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.