Chapter 17

Societal Impacts-Cybercrime & cyber law,IT Act.,Ewast mgmt

Health issues - technology

New syllabus 2023-24

Informatics Practices

Class XI (As per CBSE Board)

Visit : python.mykvs.in for regular updates

Cyber Crime - Any crime that involves a computer and a network is called a “Computer Crime” or “Cyber Crime.

Or in other term ,it is a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

STEPS TO PROTECT YOURSELF AGAINST CYBER CRIME

1. Make sure your security software is current – and update it regularly.
2. Lock or log off your computer when you step away.
3. Go offline when you don’t need an internet connection.
4. Consider sharing less online.
5. Think twice about using public Wi-Fi.
6. When in doubt, don’t click.

Types of Cyber Crime

A computer is the target of the attack—for example, a data breach on a bank site

A computer is the weapon for an attack—for example, a denial of service (DoS) attack

A computer is an accessory to a criminal act—for example, digital identity theft which leads to theft of funds from a bank account

Hacking –

Hacking is the process of gaining unauthorized access into a computing device, or group of computer systems. This is done through cracking of passwords and codes which gives access to the systems.

Difference between hacker and cracker is that a cracker breaks the security of computer systems, and a hacker is a person who likes to explore computer systems and master them.

Types of Hackers

Black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious / destructive activities. Black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

White hat hackers are those individuals who use their hacking skills for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good. Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use,but with one major difference that Ethical hacking is legal.

Grey-Hat Hackers These are individuals who work both offensively and defensively at different times. Their behavior can't be predicted. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

Society, Law and Ethics 2

Hacking Process

- Foot Printing - Whois lookup,NS lookup,IP lookup
- Scanning - Port Scanning,Network Scanning
- Gaining Access-Password Attacks,Social Engineering,Viruses
- Maintaining Access - Os BackDoors,Trojans,Clears Tracks

Required Skills of an Ethical Hacker

- Microsoft: skills in operation, configuration and management.
- Linux:knowledge of Linux/Unix;security setting, configuration, services.
- Network Protocols: TCP/IP; how they function and can be manipulated.
- Firewalls: configurations, and operation of intrusion detection systems.
- Project Management: leading, planning, organizing, and controlling a penetration testing team.
- Routers: knowledge of routers, routing protocols, access control lists.
- Mainframes

What do hackers do after hacking?

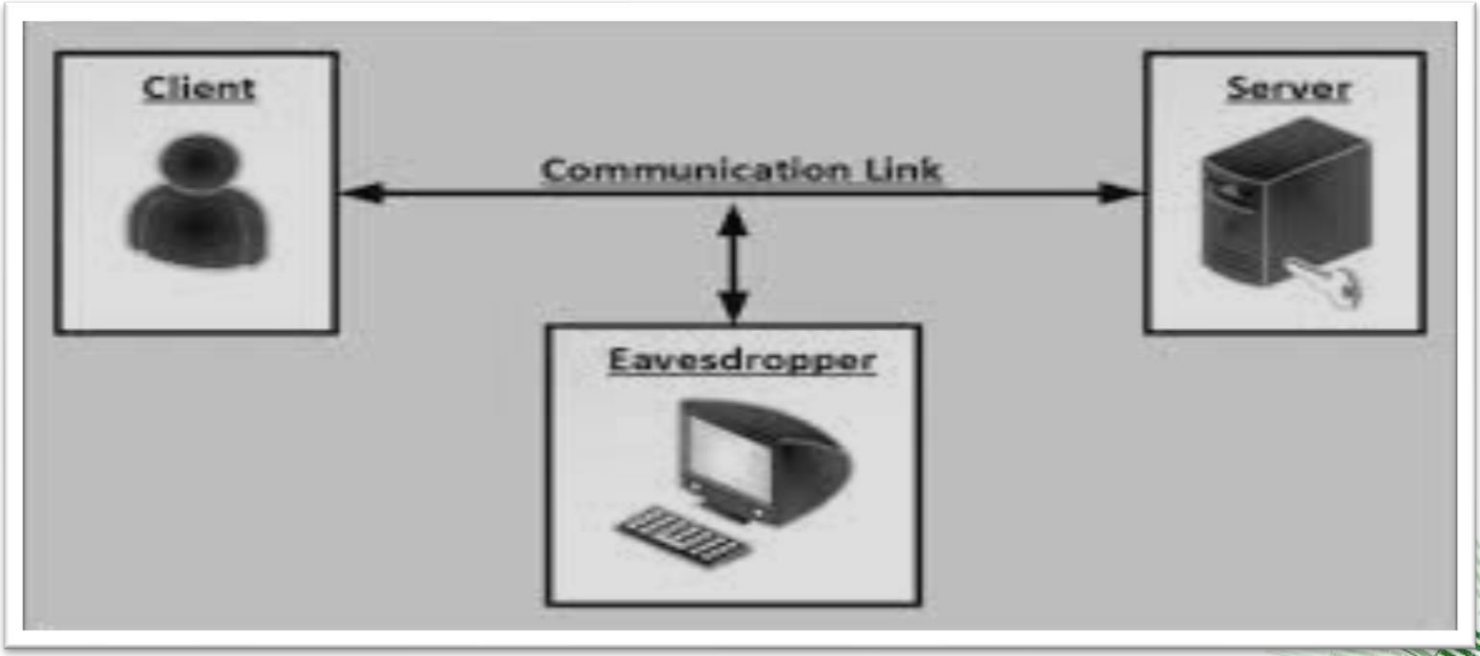
- Clear logs and hide themselves
- Install rootkit (backdoor) -The hacker who hacked the system can use the system later, It contains trojan virus, and so on
- Patch Security hole- The other hackers can't intrude
- Install irc related program - identd, irc, bitchx, eggdrop, bnc
- Install scanner program- mscan, sscan, nmap
- Install exploit program
- Install denial of service program
- Use all of installed programs silently

How to Prevent Hacking?

- Download software from authorized websites
- Scan all types of hard drives before running
- Abstain from keeping easy passwords
- Never store or share login information
- Do not click on random email attachments

Eavesdropping

It is the unauthorized real-time interception of a communication, such as a phone call, instant message, videoconference or fax transmission.



Phishing is a cyber attack that uses disguised email as a weapon.The attackers masquerade as a trusted entity of some kind, The goal is to trick the email recipient into believing that the message is something they want or need — recipient fills/send sensitive information like account no, username ,password etc. ,then attacker use these.

How to prevent phishing

- Always check the spelling of the URLs before click
- Watch out for URL redirects, that sent to a different website with identical design
- If receive an email from that seems suspicious, contact that source with a new email, rather than just hitting reply
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media

Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment.

Backup data and system and antivirus update timely may prevent from ransomware.

Preventing cyber crime

- Use strong password
- Secure your computer
- Protect your data
- Secure your mobile devices
- Secure wireless network

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.

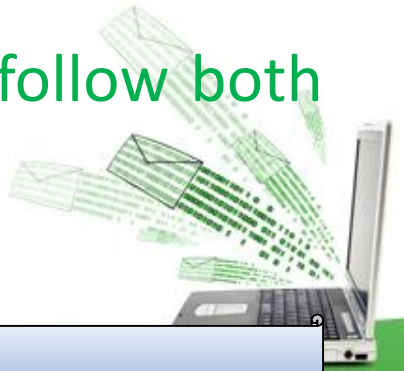
Tips to Protect Information Confidential

- **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**

Cyberbullying is the use of technology to harass, threaten or humiliate a target. Examples of cyberbullying is sending mean texts, posting false information about a person online, or sharing embarrassing photos or videos.

Cyberbullying differs from in-person bullying :

- More difficult to recognize –Bullying conducted via text or online medium can more easily go unnoticed.
- More relentless – Cyberbullying doesn't end at school, and can reach at child home.
- More enduring –It leaves a paper trail that can follow both the bully and the victim for years



Different Types of Cyber Bullying

- Doxing – publishing revealing personal information about an individual online, for purposes of defaming,humiliating, or harassing the victim
- Harassment – posting threatening,hurtful, or intimidating messages online, or sending them directly to someone, with the intention of harming that person
- Impersonation – creating fake accounts or gaining access to a person's real social media accounts and posting things to damage the victim's reputation
- Cyberstalking – tracking and monitoring a person's online activity, and using the internet to stalk or harass an individual

How to Prevent Cyber Bullying?

- Be aware of child's online activities
- Watch for the following signs of cyberbullying in children:

➢ Refusal to allow to see what they are doing online
➢ Avoidance of discussing what they are doing online
➢ Sudden, unexplained increase or decrease in online activity
➢ Deactivating social media accounts
➢ Emotional responses (including sadness, anger, happiness) linked to their device usage

Adults should also teach children to recognize and be aware of the signs of cyberbullying themselves.

Cyber Trolling has become a more common term for any kind of purposeful online abuse on social media sites like Twitter or Facebook.

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 sent through computer generated program.

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

The Information Technology Act of India, 2000 According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997"

Some key points of the Information Technology (IT) Act 2000 are as follows:

- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company

Society, Law and Ethics 2

The Information Technology Act, 2000 provides legal recognition to the transaction done via an electronic exchange of data and other electronic means of communication or electronic commerce transactions.Some of sections under it act 2000 are given below.

SECTION	OFFENCE	PENALTY
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to Rs.1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs.1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to Rs.200,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to Rs.100,000

E-Waste -Whenever an electronic device covers up its working life, or becomes non-usable due to technological advancements or becomes non-functional, it is not used anymore and comes under the category of e-waste or electronic waste. As the technology is changing day by day, more and more electronic devices are becoming non-functional and turning into e-waste. Managing such non-functional electronic devices is termed as e-waste management.

Ewaste Hazards -

On environment

- Acidification of soil
- Air pollution
- Pollution of ground water
- Landfills with lead and heavy metals

On Human Health

- Lung cancer
- DNA damage
- Asthmatic bronchitis
- Chronic damage to the brain
- Damage to heart, liver and spleen

Society, Law and Ethics 2

E-waste management can be defined as the practical and holistic approach and the founding pillar of cutting down waste from our mother earth. It is reusing and recycling of e-waste which is no longer in use and can be salved for some of its components. We are on the verge of a technological breakthrough with the introduction of AI and we need to dispose off toxic e-waste from our home before we pile up more and more e-waste. We are is dire need of introducing a customer awareness campaign because of lack of interest and knowledge regarding e-waste.

Proper disposal of used electronic gadgets

E-waste is a growing problem for us in India. As an 132cr strong economy, we produce e- waste in large quantities. It is very important to dispose off waste in a pragmatic manner.

Ways to dispose off e-waste:

1. Give Back to Your Electronic Companies and Drop Off Points
2. Visit Civic Institutions
3. Donating Your Outdated Technology
4. Sell Off Your Outdated Technology
5. Give Your Electronic Waste to a Certified E-Waste Recycler

Society, Law and Ethics 2

Awareness of Health concerns related to the usage of technology.

Physical Problems:

- Repetitive Strain Injury: the pain exists even when resting and that the lightest work becomes hard to do.
- Carpal Tunnel Syndrome: This is an illness caused by injuries that occur due to force on the median nerve found in the wrist.Its symptoms can occur as tingling in hands and fingers and the feeling of lethargy, sudden pain in wrists and arms and sometimes even in shoulders, neck and in the body
- Computer Vision Syndrome: Experts stated that people blink their eyes more frequently while using a computer than they do at other times and that they face some problems related to this situation.
- Radiation: Computer screens produce radiations of various types. There have always been doubts that Individuals will have illnesses such as headaches and inattentiveness
- Sleeping Disorders and Decrease in Productivity
- Loss of Attention and Stress

Society, Law and Ethics 2

Awareness of Health concerns related to the usage of technology.

Psychological Problems:

- Fear of technology
- Computer anxiety
- Internet addiction
  - Egosurfing: An illness of regularly searching for one's own name on the web and checking what information is available about one's own on the net.
  - Infornography: The word, derived from pornography and information, describes the state of "trying to soothe hunger for information on the net."
  - Blog streaking: A desire to spread information online that shouldn't be known by everybody.
  - Youtube-Narcissism: Constantly uploading one's own videos in order to introduce and make himself or herself known tooth ers.
  - Google-Stalking: Trying to get information about all his or her relatives or acquaintances in the web.
  - Photolurking: Looking at the photo albums of others' on the net.
  - Wikipediholism: Contributing to the internet encyclopedia, Wikipedia, sending some one's own writings, and revising the present texts.