Chapter 18
Societal Impacts-
Cybercrime,Ewast mgmt
Gender and disability
issues

Computer Science

Class XI (As per CBSE Board)

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.

fppt.com

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.

fppt.com

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

fppt.com

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

fppt.com

Eavesdropping- Interception of communication between two parties by a malicious third party.

Methods of Eavesdropping

- Hackers convert Voice-over-IP calls into audio files and analyze them.
- Data sniffing-Used in LAN.As data reach to every port and can be used for eavesdropping. Wireless networking data can be similarly manipulated if it broadcasts unsecured information to all the network ports.

Preventing Digital Eavesdropping

- Encryption
- Building More Secure Networks
- Contributing to Digital Literacy

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

fppt.c...

Fraud Emails- is intentional deception used for either personal gain / damage another individual through email. Usually naive individuals are targeted to put their confidential information for schemes to get rich quickly.

How to avoid fraud emails

- Check that the email address and the sender name match.
- Check if the email is authenticated.
- Hover over any links before you click on them. ...
- Check the message headers to make sure the "from" header isn't showing an incorrect name.

Ransomware - A type of malware that prevents users from accessing their system / personal files and demands ransom payment in order to access again. Today, ransomware developer order payment to be sent via cryptocurrency or credit card.

Protection against ransomware

- Never click on unsafe links
- Avoid disclosing personal information
- Do not open suspicious email attachments
- Never use unknown USB sticks
- Keep your programs and operating system up to date
- Use only known download sources
- Use VPN services on public Wi-Fi networks

fppt.com

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).

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.

Visit : python.mykvs.in for regular updates

fppt.com

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.

fppt.com

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**

fppt.com

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.

fppt.c

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

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

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

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

Gender and disability issues while teaching/using computers

Gender Issues

1. Preconceived notions – Notions like "boys are better at technical and girls are good at humanities.
2. Lack of interest
3. Lack of motivation
4. Lack of role models
5. Lack of encouragement in class
6. Not girl friendly work culture

Issues list above are not intentionally created , hence need a different type of handling

1.There should be more initiative program for girls to take computer subject.

2. Film and tv censor board should ensure fair representation of female role models in tv or cinema

3. In practical room they should be more helped and assisted

Gender and disability issues while teaching/using computers

Disability Issues

1. Unavailability of teaching materials/aids
2. Lack of special needs teachers
3. Lack of supporting curriculum

Possible Solution

- Enough teaching aids must be prepared for specially abled students
- Must employ special needs teachers
- Curriculum should be designed with students with specially abled students in mind.

fppt.com