Chapter – 9
Overview of Cyber Security

Class #31

Cyber Security- इन्टरनेट से जुड़े सिस्टम की सुरक्षा है जिसमे हार्डवेयर, सॉफ्टवेर, और डाटा शामिल है | यह दो शब्दों से मिलकर बना साइबर और सुरक्षा | साइबर उस तकनीक से सम्बंधित है जिसमे सिस्टम नेटवर्क, प्रोग्राम और डाटा शामिल है | जबकि सिक्यूरिटी से सम्बंधित सुरक्षा जिसमे नेटवर्क सुरक्षा और एप्लीकेशन एव सूचना शामिल है |

It is the security of systems connected to the Internet, which includes hardware, software, and data. It is made up of two words: cyber and security. Cyber is related to the technology which includes system network, program and data. Whereas security related security includes network security and application and information security.

Need and Goal of Cyber Security - साइबर सुरक्षा महत्वपूर्ण है क्योंकि यह व्यक्तियों और संगठनों को साइबर हमलों और संवेदनशील और गोपनीय जानकारी की चोरी या हानि से बचाती है। साइबर सुरक्षा पेशेवरों की आवश्यकता हर क्षेत्र और उद्योग में है, लेकिन यह स्पष्ट है कि वित्तीय सेवाओं, स्वास्थ्य देखभाल, सरकार, विनिर्माण और खुदरा क्षेत्र में विशेष रूप से तत्काल आवश्यकता है।

Cyber security is important because it safeguards individuals and organizations against cyber attacks and theft or loss of sensitive and confidential information.

Cyber security professionals are needed across every sector and industry, but it is clear that there is particularly urgent need in financial services, health care, government, manufacturing and retail.

Securing PC (कंप्यूटर सुरक्षा)- कंप्यूटर सिक्योरिटी को साइबर सिक्योरिटी या आईटी सिक्योरिटी के नाम से भी जाना जाता है। यह सूचना प्रौद्योगिकी की एक शाखा है जिसे विशेष रूप से कंप्यूटर की सुरक्षा के लिए बनाया गया है। इससे कंप्यूटर सिस्टम और डेटा, जिसे ये स्टोर या एक्सेस करते हैं, की सुरक्षा होती है। यह सूचना सुरक्षा के रूप में जाना जाता है, जो कंप्यूटर पर लागू होता है। कंप्यूटर सुरक्षा के उद्देश्य में सूचना की चोरी से सुरक्षा करना शामिल है।
Computer security is also known as cyber security or IT security. It is a branch of information technology specifically designed to protect computers. This protects computer systems and the data they store or access. This is known as information security, which applies to computers. The purpose of computer security includes protecting information from theft.

Cyber Attack निम्न तरह से हो सकता है (Cyber attack can happen in the following way)-

1. **Downloadable Programs:** Downloadable Files Virus का सबसे प्रमुख तथा सम्भव स्रोत है। किसी भी प्रकार की Executable File; जैसे- Games, Screen Saver इत्यादि इसके प्रमुख Source हैं। यदि आप किसी Programme को Internet से Download करना चाहते हैं। Download करने से पहले प्रत्येक Programme को Scan करना आवश्यक है।

Downloadable files are the most important and possible source of viruses. Any type of executable file; Like- Games, Screen Saver etc. are its main sources. If you want to download any program from the Internet. It is necessary to scan each program before downloading.

2. **Cracked Software:** ये Software Virus Attacks के अन्य स्रोत हैं। इस प्रकार के Software में Virus तथा bugs, के होने की सम्भावना अत्यधिक होती है। जिन्हें ढूँढकर सिस्टम से दूर करना बेहद कठिन है। इसलिए Internet से सूचना को किसी भी Reliable Source से ही Download करना चाहिए।
Cracked Software: These are other sources of Software Virus Attacks. There is a high possibility of viruses and bugs in this type of software. It is very difficult to find them and remove them from the system. Therefore, information from the Internet should be downloaded from any reliable source only.

3. **E-Mail Attachments:** ये Attachment Virus के मुख्य स्रोत होते हैं। इन E-Mail Attachments को आसानी से Handle किया जा सकता है।
E-Mail Attachments: These are the main sources of Attachment Virus. These e-mail attachments can be handled easily.

4. **Internet:** सभी कम्प्यूटर के Users, Computer Systems पर Virus Attacks से Unaware होते हैं। इंटरनेट पर उपलब्ध Click या Download इत्यादि तत्व ही Virus के फैलने के लिए उत्तरदायी होते हैं।
Internet: All computer users are unaware of virus attacks

on computer systems. Click or download etc. elements available on the internet are responsible for the spread of the virus.

5. **Booting from Unknown CD:** जब भी Computer कार्य नहीं कर रहा होता है उस समय कम्प्यूटर में पड़ी CD को निकाल लेना ही ठीक माना जाता है। यदि हम कम्प्यूटर से CD नहीं निकालते हैं तो यह स्वतः ही Disc में Boot होने लगती है, जिससे Virus Attack की सम्भावना बढ़ जाती है।
Booting from Unknown CD: Whenever the computer is not working, it is considered appropriate to remove the CD lying in the computer. If we do not remove the CD from the computer, it automatically starts booting into the disc, which increases the possibility of virus attack.

कम्प्यूटर सुरक्षा के घटक (Components of Computer Security)

Computer Security System के Basic Components इस प्रकार हैं

1. **Confidentiality:** किसी भी Information/data के अन्य Illegal person द्वारा Access न होने की घटना को सुनिश्चित करना इसके अन्तर्गत आता है।
This includes ensuring that any information/data is not accessed by any other illegal person.

2. **Non-Repudiation:** Message को भेजने वाला Original Person कहीं अपने Message को स्वयं का होने से न Ignore कर दे। इस प्रकार की सुनिश्चितता को **Non-Repudiation** कहते हैं।
The original person sending the message may ignore

his message as being his own. This type of assurance is called Non-Repudiation.

3. **Authentication:** यह computer system को इस्तेमाल करने वाले व्यक्ति के Legal अथवा Illegal होने को सुनिश्चित करता है।
It ensures that the person using the computer system is legal or illegal.

4. **Access Control:** जिस User को जिन resources का प्रयोग करने की अनुमति प्राप्त हो वह केवल उन्हीं Resources को इस्तेमाल करे। इस बात की सुनिश्चितता को **Access Control** कहा जाता है।
The user should use only those resources which he has permission to use. Ensuring this is called Access Control.

5. **Availability:** सभी Systems के कार्य करने के Process का सही होना व किसी भी Legal User को सेवाएं देने से न मना करना। इसे Availability के नाम से जाना जाता है।
The working process of all the systems should be correct and not denying services to any legal user. This is known as Availability.

6. **Cryptography:** किसी सूचना को छिपाकर या Secret तरीके से लिखने की तकनीक को **Cryptography** कहा जाता है। इसके माध्यम से Internet पर Data Transfer के दौरान Data को सुरक्षित रखा जाता है।
The technique of writing any information in a hidden or secret manner is called Cryptography. Through this, data is kept safe during data transfer over the Internet.

Cryptography में प्रयोग होने वाले तत्व

Cryptography में प्रयुक्त होने वाले तत्व निम्नलिखित है:

1. **Plain Text:** यह Input के रूप में दिया जाने वाला Original Message होता है।
   This is the original message given as input.
2. **Cypher:** यह bit-by-bit या character-by-character परिवर्तन करने की प्रक्रिया है, जिसमें सन्देश का अर्थ नहीं बदलता।
   It is the process of making bit-by-bit or character-by-character changes, in which the meaning of the message does not change.
3. **Cipher Text:** यह Coded message या encrypted data होता है जिसे User सीधे-सीधे नहीं पढ़ सकता।
   This is a coded message or encrypted data which the user cannot read directly.
4. **Encryption:** Plain Text को Cyber Text में परिवर्तित करने की प्रक्रिया को **Encryption** कहते हैं। इसके तहत एक encryption algorithm का प्रयोग होता है।
   The process of converting plain text into cyber text is called encryption. Under this an encryption algorithm is used.
5. **Decryption:** यह Encryption Process का Reverse होता है अर्थात् इसमें cyber text को Plain Text में परिवर्तित किया जाता है।
   This is the reverse of the encryption process, that is, in this the cyber text is converted into plain text.

6. **Stenography:** Message को उसके Original रूप को छुपाने की कला को **Stenography** कहते हैं। यह Data Privacy & Integration में मदद करता है।
   The art of hiding a message in its original form is called Stenography. It helps in Data Privacy & Integration.
7. **Integrity:** यह सुनिश्चित करता है कि Information को किसी Illegal User द्वारा इस प्रकार बदला तो नहीं गया कि उसे legal User भी न पहचान सके। Integration Computer Security का एक अत्यन्त महत्वपूर्ण Component हैं।
   This ensures that the information is not changed by any illegal user in such a way that even the legal user cannot recognize it. Integration is a very important component of Computer Security.

कंप्यूटर सुरक्षा के उपाय (Computer Security Threats Solutions)

Windows Firewalls: ये या तो Hardware या Software Programme होते है, Windows Firewall एक अवरोध है, जो Internet या किसी अन्य Network से आने वाली जानकारी (जिसे कई बार Traffic कहा जाता है) की जाँच करती है और आपकी Firewall Setting के आधार पर या तो उसे नकार देती है या आपके Computer पर आने की अनुमति देती है |
These are either hardware or software programs, Windows Firewall is a barrier that checks for information (sometimes called traffic) coming from the Internet or any other network and either rejects it depending on

your firewall settings. Gives or allows access to your computer.

Firewall अनधिकृत Users को किसी Network या Internet से आपके Computer तक आने से रोककर इसकी सुरक्षा करता है। Windows firewall Windows XP में अन्तर्निहित होता है और अपने आप चालू हो जाता है, जिससे आपके Computer की वायरसों अन्य सुरक्षा खतरों से रक्षा करने में मदद मिलती है।
A firewall protects your computer by preventing unauthorized users from accessing it through a network or the Internet. The Windows firewall is built into Windows XP and turns on automatically, helping to protect your computer from viruses and other security threats.

Antivirus Software: यह उन Computer Programme से बना होता है, जोकि Computer Virus को पहचानने का और उसे हटाने का कार्य करते हैं, और अन्य Malicious Software (Malware) की पहचान करते हैं। Antivirus Program Virus, Verse और Trojan Horses देखने के लिए e-mail और आपके कम्प्यूटर की अन्य फाइलों की जाँच करता है। यदि कोई Virus, Worm या Trojan Horse मिलता है, तो यह आपके Computer को नुकसान पहुँचाए उससे पहले Antivirus Programme या तो इसे रोक कर रखता है या इसे पूरी तरह से हटा देता है।
It is made up of computer programs that identify and remove computer viruses and identify other malicious software (malware). Antivirus programs check e-mail and other files on your computer for viruses, viruses and Trojan horses. If a virus, worm or Trojan horse is found,

the antivirus program either stops it or removes it completely before it can cause damage to your computer.

कई Antivirus Programme में Automatic Updates की क्षमता होती है. जब आपका Antivirus Software Update किया जाता है, तो जाँचने के लिए नए Viruses की एक List जोड़ दी जाती है, जिससे आपका Computer नए Attack से सुरक्षित हो जाता है।
Many antivirus programs have the capability of automatic updates. When your antivirus software is updated, a list of new viruses is added to check, making your computer safe from new attacks.

Example:

- ❖ K7 Total Security
- ❖ Avast Antivirus
- ❖ McAfee
- ❖ Bit defender
- ❖ Norton
- ❖ Quick Heal
- ❖ Kaspersky
- ❖ Symantec
- ❖ Norton
- ❖ MacAfee

Virus: Virus विनाशक या Misleading program होते हैं, जो Internet पर या किसी Network पर एक Computer से दूसरे Computer पर फैलते हैं। Virus अन्य फाइलों से Attached हो जाते हैं या स्वयं को सामान्य रूप से दिखाई देने वाली फाइल के रूप में

छुपा लेते हैं। वे स्वयं की Copy बना सकते हैं और आपके Computer के विभिन्न भागों जैसे Documents, Programme और आपके Operating System के भागों को Infect कर सकते हैं।
Viruses are destructive or misleading programs that spread from one computer to another on the Internet or over a network. Viruses attach to other files or disguise themselves as normally visible files. They can make copies of themselves and infect various parts of your computer such as documents, programs, and parts of your operating system.

अधिकतर Virus स्वयं को किसी फाइल या आपकी Hard Disc के किसी भाग से अनुलग्न कर लेते हैं और तब Operating System के भीतर अन्य स्थानों पर अपनी Copy बनाते हैं। कुछ Virus में कोड होता है, जो फाइलों को हटाकर या Security Settings का स्तर घटाकर, अन्य आक्रमणों को आमन्त्रित कर अधिक Destruction का कारण बनता है। Example- Creeper, Melissa, I Love You, Code Red, Trojan Horses etc.
Most viruses attach themselves to a file or part of your hard disk and then make copies of themselves in other places within the operating system. Some viruses contain code that causes more destruction by deleting files or lowering the level of security settings, inviting other attacks. Example- Creeper, Melissa, I Love You, Code Red, Trojan Horses etc.

Worms: Worms एक ऐसा Programme है, जो अपनी Copies तैयार करता है और Operating System के बाहर भी फैल सकता

है। यह E -mail या अन्य परिवहन युक्तियों का उपयोग कर भी एक Computer से दूसरे Computer पर जा सकता है.
Worms are programs that create copies of themselves and can spread outside the operating system. It can also move from one computer to another using e-mail or other transportation devices.

Worms आपके Computer Data और Security को लगभग उसी प्रकार से नुकसान कर सकता है जैसे- Virus, परन्तु ये Virus से इस प्रकार भिन्न हैं कि वे एक System से दूसरे System में स्वयं की Copy बना सकते हैं.
Worms can damage your computer data and security in almost the same way as viruses, but they are different from viruses in that they can make copies of themselves from one system to another.

Trojan Horse: Trojan Horse एक Harmless Programme है, जो इस प्रकार बनाया जाता है कि आप यह सोचने लगें कि आपको इसकी आवश्यकता है, पर जब आप इसे चलाते हैं, तो यह नुकसान पहुंचाता है। यह सामान्यतः Internet से Downloads के साथ आता है। Trojan Horse Virus और Worms की तरह अपने आप नहीं फैलते अधिकतर Virus Protection Programs केवल एक सीमित संख्या में ही Trojan Horse को ढूँढ सकते हैं। अपने Computer को Trojan Horse से सुरक्षित रखने का अच्छा तरीका है केवल भरोसेमंद Websites पर ही जाना और चीजों को तब तक Downloads करने से बचना जब तक कि आपको उनके स्रोत के बारे में भी भरोसा न हो।
Trojan Horse is a harmless program that is designed to make you think you need it, but when you run it, it

causes harm. It usually comes with downloads from the Internet. Trojan Horses do not spread on their own like viruses and worms. Most virus protection programs can only detect a limited number of Trojan Horses. A good way to keep your computer safe from Trojan horses is to only visit trusted websites and avoid downloading things unless you are confident about their source.

Hacking: Network से जुड़े Computer में घुसपैठ करने की प्रक्रिया को **Hacking** कहते हैं। Hacking DOS (Denial of Service) Attack का परिणाम भी हो सकता है। यह कम्प्यूटर के सभी Resources को Valid Users द्वारा इस्तेमाल करने से दूर रखती है। इस प्रक्रिया को अन्तिम चरण तक पहुंचाने वाले व्यक्ति को **Hacker** कहते हैं।
The process of infiltrating a computer connected to a network is called Hacking. Hacking can also result in a DOS (Denial of Service) attack. It keeps all the resources of the computer away from being used by valid users. The person who takes this process to the final stage is called a Hacker.
