Chapter – 9
Overview of Cyber Security

Class #32

Crackers: ये मुख्यतः वह होते हैं, जोकि Computer Security में डाले गए secret code को तोड़कर उसकी Security में घुसते हैं। इस प्रकार के Software या उनके Component को तोड़ने की प्रक्रिया को **Cracking** कहते है। ये secret code को तोड़कर computer और उसके Programs को सार्वजनिक भी कर देते हैं। इसमें Password, Cracker, Trojans, Viruses, War Dialer इत्यादि सम्मिलित हैं।
Crackers: These are mainly those who penetrate the security of the computer by breaking the secret code entered in it. The process of breaking this type of software or its components is called cracking. They also make the computer and its programs public by breaking the secret code. This includes Password, Cracker, Trojans, Viruses, War Dialer etc.

Phishing: कम्प्यूटर की Sensitive Information को धोखेबाजी से प्राप्त करने की कोशिश करना इत्यादि विशेषताओं को **Phishing** कहते हैं। इसके अन्तर्गत Passwords, Credit Card Details इत्यादि सम्मिलित हैं। यह एक प्रकार का Internet Fraud (धोखा) है, जिसमें User को बहकाकर उसके सभी Credentials को प्राप्त कर लिया जाता है।
Phishing: Trying to obtain sensitive computer information fraudulently is called phishing. This includes Passwords,

Credit Card Details etc. This is a type of Internet Fraud, in which the user is deceived and all his credentials are obtained.

Spam: यह एक प्रकार से Messaging Systems का दुरुपयोग है, जिसके अन्तर्गत Unwanted Messages को E-mails के रूप में भेजा जाता है।

This is a kind of misuse of messaging systems, under which unwanted messages are sent in the form of e-mails.

Spyware: स्पाइवेयर एक जासूसी वायरस होता है. जो लगभग हर उन डिवाइसेस में जा सकता है, जो इंटरनेट से जुडी होती हैं. या उन डिवाइसेस में इंटरनेट का प्रयोग किया जाता है. इसे स्पाइवेयर इसलिए कहा जाता है, क्योंकि ये बिना आपसे पूछे आपके मोबाइल, लैपटॉप जैसी डिवाइसेस से आपकी जानकारी चोरी करता है और इस जानकारी को उस जगह तक पहुंचता है, जहां से इसे कंट्रोल किया जा रहा है |Spyware is an espionage virus. Which can go to almost every device which is connected to the internet. Or internet is used in those devices. It is called spyware because it steals your information from devices like your mobile, laptop without asking you and reaches this information to the place from where it is being controlled.

स्पाइवेयर की शुरुआत कैसे हुई? (How did spyware start?)

इसकी शुरुआत 1995 के आस-पास हुई, लेकिन ये लोगों की नजरों में सबसे पहले 2006 में आया. जब इस स्पाइवेयर को Internet Explorer और माइक्रोसॉफ्ट Windows Operating System में मौजूद पाया

गया. जब इसके कारण Windows Operating System में कुछ तकनीकी गड़बड़ियां होने लगी. हालांकि बाद में microsoft कंपनी ने इसे सही कर लिया था ।

It started around 1995, but it first came into public notice in 2006. When this spyware was found present in Internet Explorer and Microsoft Windows Operating System. When due to this some technical glitches started occurring in the Windows Operating System. However, later Microsoft company corrected it.

स्पाइवेयर के प्रकार (Types of Spyware)

ये वाइरस वैसे तो कई तरह के होते हैं लेकिन मुख्य रूप से चार प्रकार के होते हैं (There are many types of these viruses but mainly there are four types) -

- एडवेयर (Adware),
- की लोगर (Key Logger)
- सिस्टम मॉनिटर्स (System monitors),
- ट्रैकिंग कुकीज़ (Tracking cookies),

Adware: यह एक ऐसा software package है, जोकि Advertisement को स्वतः ही टुकड़े-टुकड़े कर Screen पर दिखाता है। इसे अधिकांशतः Unwanted Advertisements को दिखाने के लिए इस्तेमाल किया जाता है।
This is a software package that automatically breaks the

advertisement into pieces and shows it on the screen. It is mostly used to show unwanted advertisements.

Keylogger: Keylogger एक ऐसा program होता है जो की सभी Keystrokes को record करता है एक computer में. ये ऐसा करने के लिए एक User के Input को monitor करता है और साथ में एक log में maintain करता है सभी keys का जिसे की press किया जाये. इस log को एक file में save कर दिया जाता है या फिर दुसरे machine को भेज दिया जाता है एक network के द्वारा या Internet में |
Keylogger is a program that records all the keystrokes in a computer. To do this, it monitors a user's input and also maintains a log of all the keys that are pressed. This log is saved in a file or sent to another machine through a network or over the Internet.

Keylogger programs को अक्सर कहा जाता है spyware क्यूंकि वो ज्यादातर रन कर रहे होते हैं बिना User के जानकारी के ही. मतलब की User को ये बिलकुल भी नहीं पता होता है की कोई keylogger program background में run कर रहा है या नहीं |
Keylogger programs are often called spyware because they mostly run without the user's knowledge. This means that the user does not know at all whether any keylogger program is running in the background or not.

इन्हें इसलिए गलत तरीके से install भी किया जाता है hackers के द्वारा, जिससे की वो एक user के computer को spy कर सकें, साथ में ये भी जान सकें की एक user आखिर में क्या typing कर रहा है |

These are also installed incorrectly by hackers so that they can spy on a user's computer and also know what a user is typing.

System Monitors- System Monitor एक एडवेयर प्रोग्राम है जो पॉप-अप विज्ञापन और अन्य अवांछित विज्ञापन प्रदर्शित करता है जो उन साइटों से उत्पन्न नहीं होते हैं जिन्हें आप ब्राउज़ कर रहे हैं। System Monitor is an adware program that displays pop-up ads and other unwanted advertisements not originating from the sites you are browsing

Tracking Cookies - ट्रैकिंग कुकीज़ ऐसी कुकीज़ होती हैं जो या तो उपयोगकर्ता के वेब ब्राउज़र पर उस वेबसाइट द्वारा या किसी तीसरे पक्ष द्वारा सेट की जाती हैं। ये कुकीज़ उपयोगकर्ता के ऑनलाइन व्यवहार को ट्रैक करती हैं यानी उनका डेटा एकत्र करती हैं, जैसे क्लिक, खरीदारी प्राथमिकताएं, डिवाइस विनिर्देश, स्थान और खोज इतिहास। Tracking cookies are cookies that are either set on a user's web browser by the website they are on or by a third party. These cookies track the user's online behaviour i.e. collect their data, such as clicks, shopping preferences, device specifications, location, and search history.

Rootkits: यह एक प्रकार का Malware है, जिसके द्वारा किसी Computer System में administrative level की control प्राप्त की जाती है व इसकी जानकारी किसी को भी नहीं होती है। Rootkits को निकालना बेहद मुश्किल होता है तथा कभी-कभी पूर्णतः Operating System के reinstall की भी आवश्यकता होती है।

This is a type of Malware, through which administrative level control is achieved in a computer system and no one is aware of it. Rootkits are extremely difficult to remove and sometimes require a complete reinstallation of the operating system.

कम्प्यूटर सुरक्षा सम्बन्धित जानकारियाँ (Computer Security Related Information's)

1. **Proxy Server:** Proxy Server को **"Proxy or Application-Level Gateway"** भी कहा जाता है। यह User एवं Server के मध्य कार्य करता है। यह Network के सही Address को Hide करता है और नेटवर्क में आने-जाने वाले सभी Messages को Intercept करता है।
   Proxy Server is also called "Proxy or Application-Level Gateway". It works between the user and the server. It hides the true address of the network and intercepts all incoming and outgoing messages on the network.
2. **Application Gateway:** यह कुछ Specific Applications पर Security Procedure को लागू करता है। इन Specific Applications में File Transfer Protocol तथा Telnet Services इत्यादि सम्मिलित हैं।
   It implements security procedures on some specific applications. These specific applications include File Transfer Protocol and Telnet Services etc.
3. **Time Bomb:** यह Software का हिस्सा है, जोकि किसी विशेष समय पर Active होता है।

It is a part of the software, which is active at a particular time.

4. **Logic Bomb:** यह एक Code होता है, जिसे Computer Memory में जान-बूझकर डाला जाता है। जोकि Favorable Conditions के मिलते ही हानिकारक रूप से सक्रिय हो जाते हैं। ये Code अपनी Duplicate तैयार करने में सक्षम नहीं होते हैं।
   This is a code, which is deliberately inserted into the computer memory. Which become harmfully active as soon as favorable conditions are met. These codes are not capable of creating their own duplicate.
5. **Patches:** यह Software का एक ऐसा भाग होता है जिसे उस Software में सुधार करने के लिए बनाया जाता है।
   This is a part of the software which is created to improve that software.
6. **Masquerading:** इसमें Attacker Valid User होने का Acting करता है व Illegal रूप से विशेषाधिकार प्राप्त कर लेता है।
   In this, the attacker acts as a valid user and acquires privileges illegally.

Securing Browser – जब आप इन्टनेट पर किसी वेबसाइट पर विजिट करते है तब किसी न किसी ब्राउज़र का स्तेमाल करना पड़ता है जैसे – Google Chrome, Mozilla Firefox, Microsoft Edge etc. जब हम ब्राउज़र का स्तेमाल करते है तो हमे इसकी सुरक्षा का भी ध्यान रखना चाहिए |
When you visit any website on the Internet, you have to use some browser like Google Chrome, Mozilla Firefox,

Microsoft Edge etc. When we use the browser, we should also take care of its security.

HTTP (Hyper Text Transfer Protocol) – जब भी अप किसी वेबसाइट पर विजित करते है तो ब्राउज़र एड्रेस बार में लेफ्ट साइड में आपने http या https देखा होगा | जिमसे केवल http होता है वह वेबसाइट अधिक सुरक्षित नहीं माना जाता है |

Whenever you visit any website, you must have seen http or https on the left side of the browser address bar. A website which has only http is not considered more secure.

HTTPs (Hyper Text Transfer Protocol Secure) – जिस वेबसाइट पर https भी होता है उस पर SSL (Secure Socket Layer) की सुरक्षा होती है जिसकी बजह से यूजर की जानकारियों को कोई और नहीं चुरा सकता है |

Any website that has https is protected by SSL (Secure Socket Layer) due to which no one else can steal the user's information.

Incognito Mode (Private Window)- ब्राउज़र में हमें प्राइवेट ब्राउज़िंग का भी आप्शन मिल जाता है जिसके स्तेमाल से हम प्राइवेट ब्राउज़िंग कर सकते है, इसमें ब्राउज़िंग हिस्ट्री में डाटा सेव नहीं होता है |

We also get the option of private browsing in the browser,

using which we can do private browsing, in this the data is not saved in the browsing history.

Clear History–जब भी आप ब्राउज़िंग करते है, आपका ब्राउज़र आपकी ब्राउज़िंग हिस्ट्री को सेव कर लेता है अत: आपको समय समय पर ब्राउज़िंग हिस्ट्री को डिलीट करते रहना चाहिए | Whenever you browse, your browser saves your browsing history, hence you should keep deleting the browsing history from time to time.

Cookies – Cookies वे फाइल्स होती है जो वेबसाइट वेब ब्राउज़र पर सेव करके रख लेती है | हमें अपने ब्राउज़र में Cookies को भी समय समय पर क्लियर करते रहना चाहिए | Cookies are files that a website saves on a web browser. We should also keep clearing the cookies in our browser from time to time.

Tracking Protection – ब्राउज़िंग करते समय वेबसाइट आपकी जानकारी को थर्ड पार्टी प्रोवाइडर को भेज सकती है जिससे बचने के लिए आपको ट्रैकिंग प्रोटेक्शन का फीचर दिया जाता है जिससे आप अपने ब्राउज़िंग डाटा को थर्ड पार्टी वेबसाइट के द्वारा ट्रैक होने से रोक सकते है | While using, the website may send your information to the third party provider, to avoid this, you are given the feature of tracking protection, through which you can prevent your browsing data from being tracked by the third party website.

Securing Email and Social Media Accounts (ईमेल और सोशल मीडिया अकाउंट सुरक्षित करना)

Two Step Verification (टू-स्टेप वेरिफिकेशन): अकाउंट की सेफ्टी के लिए आपको सबसे पहले तो टू-फैक्टर ऑथेंटिकेशन के जरिए सेफ्टी करना जरूरी होता है। किसी अकाउंट में साइन इन करते समय आपको टेक्स्ट मैसेज, मेल, फोन कॉल के जरिए पहचान 2 बार वेरीफाई करनी होगी। अगर आपने पहले से यह नहीं किया हुआ है तो आप सभी ऑनलाइन अकाउंट को इसके लिए इनेबल कर सकते हैं।
You must first purchase a credit card through two-factor authentication. While signing in to any account you will have to verify 2 times through text message, mail, phone call. If you haven't done so before, you can open an account online for free.

Keep mobile apps up-to-date (मोबाइल ऐप्स को अप-टू-डेट रखें): हमेशा मोबाइल ऐप्स को अपडेट रखना चाहिए। इससे आपके फोन की सुरक्षा ज्यादा बढ़ जाती है। ऐप डेवलपर हमेशा ऐप्स को नए खतरों से अपडेट और सेफ रखने के लिए कुछ न कुछ नया करते रहते हैं। ऐसे में आपको यह सुनिश्चित करना चाहिए कि आप हमेशा ऐप का लेटेस्ट वर्जन इस्तेमाल कर रहे हैं। इससे आप हैकर्स को ऐप के जरिए फोन तक पहुंचने का मौका नहीं देते हैं।
Mobile apps should always be kept updated. This increases the security of your phone. App developers are always doing something new to keep apps updated and safe from new threats. In such a situation, you should ensure that you are always using the latest version of the app. With this you do not give hackers a chance to access the phone through the app.

Pay attention to safety on public networks (पब्लिक नेटवर्क पर सेफ्टी का ध्यान दें) : हम में से अधिकतर लोगों को फ्री वाई-फाई

इस्तेमाल करना पसंद है, लेकिन आपको इसके नुकसान को भी जानना जरूरी है। जब भी ओपन नेटवर्क की बात होती है तो उसका इस्तेमाल सभी कर सकते हैं। ऐसे में खतरा होने की संभावना भी बढ़ जाती है। ऐसे में जब तक बहुत ज्यादा जरूरी न हो तब तक किसी भी ओपन नेटवर्क का इस्तेमाल नहीं करना चाहिए। या फिर जरूरत पड़े तो इस दौरान कनेक्ट होने पर निजी अकाउंट को लॉगइन नहीं करना चाहिए।

Most of us like to use free Wi-Fi, but you also need to know its disadvantages. Whenever we talk about open network, everyone can use it. In such a situation, the possibility of danger also increases. In such a situation, one should not use any open network unless it is absolutely necessary. Or if necessary, one should not login to the personal account while connected during this period.

Have a separate email for social media (सोशल मीडिया के लिए अलग से ईमेल रखें): सबसे पहले आपको यह ध्यान देना चाहिए कि आप हर अटैक से सुरक्षित नहीं रह सकते हैं। मान लें कि आपका सोशल मीडिया अकाउंट हैक हो गया और हैकर्स ने आपके ईमेल से छेड़छाड़ की है। अगर आप सोशल मीडिया के लिए अलग ईमेल इस्तेमाल करते हैं तो ऐसे में हैकर्स के पास आपकी निजी जानकारी जैसे बैंक डीटेल, पर्सनल ईमेल आदि नहीं पहुंच पाएंगी। इस प्रकार की चीजों को इस्तेमाल करके आप ऑनलाइन सेफ्टी कर सकते हैं।

First of all, you should note that you cannot be safe from every attack. Suppose your social media account got hacked and hackers compromised your email. If you use a separate email for social media, then hackers will not be able to access your personal information like bank

details, personal email etc. You can maintain online safety by using these types of things.

Changing account password from time to time (समय समय पर अकाउंट पासवर्ड बदलते रहना)- हमें ओने ई-मेल अकाउंट तथा अन्य सोशल मीडिया अकाउंट का पासवर्ड समय समय पर बदलते रहना चाहिए | कम से कम 90 दिनों अर्थ 3 माह में हमें अपना पसवर्ड बदल देना चाहिए|

We should keep changing the password of our e-mail account and other social media accounts from time to time. We should change our password at least after 90 days i.e. 3 months.

Cyber Security से महत्वपूर्ण शब्दावली-

1) Cyber Security
2) Network Security
3) Threat Security
4) SSL (Secure Socket Layer)
5) TLS (Transport Layer Security)
6) IDS (Intrusion Detection System)
7) IPS (Intrusion Prevention System)

Hacker (हैकर):

1. **Black Hat Hackers**- Black-hat Hackers को एक अनैतिक हैकर (Unethical Hacker के रूप में भी जाना जाता है। इस तरह के Hackers कंप्यूटर सिस्टम या नेटवर्क की कमजोरी का पता लगाकर आपको या आपके Organization को नुकसान पंहुचा सकते है। ये लोग अपने स्वयं के अवैध लक्ष्यों

को प्राप्त करने के लिए सिस्टम को हैक करते हैं। Black-hat hackers are also known as unethical hackers. This type of hackers can cause harm to you or your organization by finding weaknesses in computer systems or networks. Let's hack the system to get it.

वे कमजोर सुरक्षा वाले बैंकों या अन्य कंपनियों की वेबसाइट को ढूंढते हैं और पैसे या क्रेडिट कार्ड की जानकारी चुराते हैं। इस तरह के हैकर आपके Important Data को हैक करके उसके बदले पैसे मांग संशोधित या नष्ट भी कर सकते हैं। ब्लैक हैट हैकिंग अवैध है और ऐसा करना कानूनी तौर पर अपराध हैं। They find websites of banks or other companies with weak security and steal money or credit card information. Such hackers can hack your important data, modify or destroy it and demand money in exchange for it. Black hat hacking is illegal and doing so is a legal offence.

2. **White Hat Hackers**-White hat Hackers को Ethical Hackers के रूप में भी जाना जाता है। White hat Hackers से किसी व्यक्ति य किसी Organization को कोई खतरा नहीं होता है क्योकि यह हैकिंग किसी को नुकशान पहुंचाने के लिए नहीं करते |

   White hat hackers are also known as ethical hackers. White hat hackers do not pose any threat to any person or organization because they do not do this hacking to harm anyone.

White hat Hackers उसी तकनीक का इस्तेमाल करते हैं जिसका इस्तेमाल ब्लैक हैट हैकर्स करते हैं। वे सिस्टम को हैक भी करते हैं, लेकिन वे केवल उस सिस्टम को हैक कर सकते हैं जिसे सिस्टम की सुरक्षा का परीक्षण करने के लिए उन्हें उस सिस्टम या वेबसाइट को हैक करने की अनुमति मिलती है। वे सुरक्षा और आईटी प्रणाली की सुरक्षा पर ध्यान केंद्रित करते हैं। और इसीलिए White hat Hacking को कानूनी कोई अपराध नहीं माना जाता है।

White hat hackers use the same techniques as black hat hackers. They also hack the system but they can only hack the system which allows them to hack that system or website to test the security of the system. They focus on security and protection of the IT system. And that is why White hat Hacking is not considered a legal crime.

3. **Gray Hat Hacker**- Black hat Hackers और White hat hackers के बीच Gray hat Hackers भी होते है, Gray hat Hackers को Hybrid Hacker कहा जाता है I Gray hat Hackers किसी भी सिस्टम को हैक कर सकते हैं भले ही उनके पास सिस्टम की सुरक्षा का परीक्षण करने की अनुमति न हो लेकिन वे कभी भी धन की चोरी नहीं करेंगे या सिस्टम को नुकसान नहीं पहुंचाएंगे। ग्रे हैट हैकिंग को कभी-कभी कानूनी रूप से कार्य किया जाता है और कभी-कभी नहीं। There are also Gray hat Hackers between Black hat Hackers and White hat hackers, Gray hat Hackers are called Hybrid Hackers. Gray hat Hackers can

hack any system even if they do not have permission to test the security of the system but they will never steal money or harm the system. Gray hat hacking is sometimes done legally and sometimes not.