1. **Introduction to Cyber Security**

**Cyber security** is the practice of protecting computer systems, networks, and data from malicious attacks, unauthorized access, damage, and theft. This involves a comprehensive set of technologies, processes, and best practices designed to safeguard information and ensure its confidentiality, integrity, and availability. Cyber security encompasses various types of threats, including malware, phishing, ransomware, and hacking, which can compromise sensitive data and disrupt operations. Effective cyber security strategies include implementing firewalls, encryption, multi-factor authentication, and regular security audits. The goal is to create a robust defence against cyber threats, ensuring that digital information and infrastructure remain secure and resilient against evolving cyber-attacks.

**Cyber Security**, also known as information technology security, focuses on protecting computer systems, networks, and data from cyber threats, attacks, and unauthorized access. This field encompasses a broad range of practices, technologies, and processes designed to safeguard digital information.

1. **History of Cyber Security in India**

* **History**

1. **1909**: The British Government included Intelligence through IPIO (Indian Political Intelligence Office) to track revolutionary activities of Indians in England.
2. **1921**: The name changed to IPI, focusing on collecting secret information securely.
3. **1930s**: IPI expanded its operations beyond Indian borders to neighbouring and foreign countries.
4. **1947**: Post-independence, IPI transformed into the Intelligence Bureau (IB), initiated by Prime Minister Jawaharlal Nehru.
5. **1962**: Sanjeev Pillai became the first Indian Director of IB, restructuring it based on British Intelligence MI5.
6. **1965**: Following the Indo-Pakistan Wars, a dedicated Foreign Intelligence agency, R&AW (Research and Analysis Wing), was established by Indira Gandhi in 1968.
7. **1968**: R.N. Kao became the first director of R&AW, starting with 250 staff and a budget of 20 million, which later expanded.
8. **1971**: The Aviation Research Canter (ARC) was established to monitor aerial spaces.
9. **2004**: The National Technical Facilities Organization (NTFO) was formed.

* **Working & Build History of IB & RA&W**
  + IB Build work under: **MHA-** Ministry of Home Affairs
    - Now Time – Amit Shah.
  + R&AW: 1968,
    - Budget of R&AW: 250 Staff,
    - 20 million Established Budget.
  + Increase “Up to 300 million, 300 Staff”.
  + **Join under R&AW:** 
    - Radio Research Center, 1970
    - Electronic & Tech Service, 1990
  + **ARC “**Aviation Research Centre” 1971 **Keep a Sharp eye on arial spaces.**
* **Key Figures in Indian Intelligence**
* **R.N. Kao**: Known as the "Father of RAW," played a crucial role in the Bangladesh Liberation War.
* **Maj. Gen. V.K. Singh**: Highlighted the weaknesses of IB during the China attacks.
* **Field Marshal Sam Manekshaw**: Chief of Army Staff during the Indo-Pakistan War of 1971.
* **Field Marshal Sam Harmusji Jamshedji Manekshaw** also known as **“Sam Bahadur.”**

1. **Fields in Cyber Security**

* **Security Analyst:** Security analysts identify and correct flaws in the company's security systems, solutions, and programs while recommending specific measures that can improve the company's overall security posture.
* **Incident Responder:** An incident responder is a professional who responds to cyber security attacks or incidents that occur within an organization. Their goal is to protect an organization's assets, ensure business continuity, and minimize damage from the incident.
* **Penetration Tester (Ethical Hacker):** A penetration tester, also known as an ethical hacker, is a paid professional who performs security assessments by simulating digital break-ins. Penetration testers use their skills and knowledge to access targeted systems and perform a systematic approach to security testing.
* **Security Engineer/Cryptographer:** Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.
* **Security Awareness Trainer:** Security awareness training helps prevent and mitigate human risk. Designed to help users understand the role they play in combatting security breaches, effective security awareness training teaches proper cyber hygiene, security risks, and how to identify cyber-attacks delivered via email and web browsing.
* **Virus & Malware Analyst:** A malware analyst works in computer and network security “to examine, identify, and understand the nature of cyber-threats such as viruses, worms, bots, rootkits, and Trojan horses,” explains the Infosec Institute.
* **Security Researcher (ISRAG):** The Information **Security Research** Association (commonly known as ISRA) is a registered non-profit organization focused on various aspects of Information.

Security researchers are skilled computer experts that use their technical knowledge to identify cybersecurity vulnerabilities within an organization or industry. A security researcher must keep up with the latest data, developments, and trends in the cybersecurity world.

* **Security Consultant:**  security consultant, also sometimes called a security analyst, pinpoints vulnerabilities in computer systems, networks, and software programs and works toward solutions to strengthen them against hackers. This consultant role is a strong example of a highly specialized IT occupation.
* **Common Cyber Threats**
* **Hackers**: Unauthorized access to systems.
* **Trojan Attacks**: Malicious software disguised as legitimate software.
* **Password Cracking**: Unauthorized access to accounts by guessing passwords.





1. **How to Join IB, Cyber Security, and R&AW:**

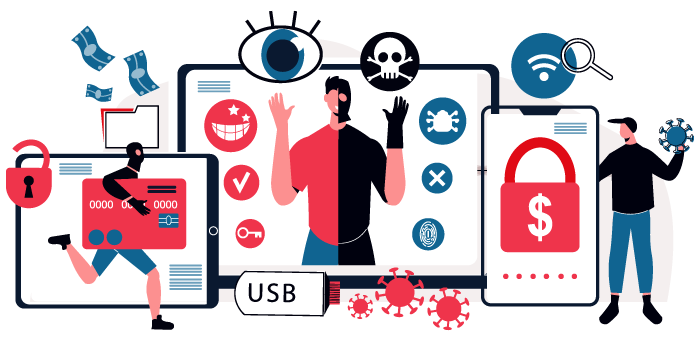
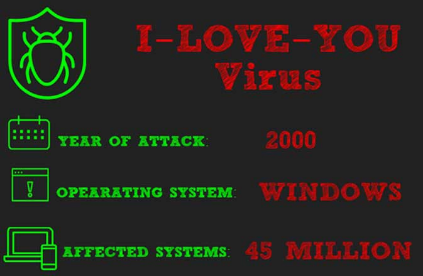
**Joining IB, Cyber Security, and R&AW**

* **Through UPSC CSE**: IFS, IPS, IAS
  + Job of an IPS officer in IB is focused on gathering and analysing intelligence related to internal security and counter-terrorism, and working closely with other law enforcement agencies and intelligence agencies to protect national security.
* **Through Indian Army**: Special Protection Group (SPG), then IB
  + The **Special Protection Group** (**SPG**) is an agency of the Government of India whose sole responsibility is protecting the **Prime Minister of India** and, in some cases, his or her family.
  + Yes …you can serve for Special Protection Group (SPG), NATIONAL SECURITY GUARD (NSG), IB, CBI, NARCOTICS CONTROL BOARD (NCB) etc on deputation basis by qualifying standard measurements and criteria set by above mentioned departments.
* **Certifications**:
  + **CEH:** Certified Ethical Hacker
    - **Certified Ethical Hacker** (**CEH**) is a qualification given by **EC-Council** and obtained by demonstrating knowledge of assessing the security of computer systems by looking for vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system.
  + **CHFI:** Certified Hacking Forensic Investigator
  + **EJPT**: eLearn Security Junior Penetration Tester
    - The Exam · INE Security's **eJPT** is for entry-level **Penetration testers** that validates that the individual has the knowledge, skills, and abilities ...
    - You have **two attempts** to pass the certification exam.
  + **OR, Learn degree in relative field as IT.**



1. **Benefits & Losses in Cyber Security**

* **Benefits**
* Protects data and information
* Prevents unauthorized access
* Controls web portals
* Safeguards against viruses and fraud
* Ensures cyber crime safety
* **Losses**
* DDoS Attacks can overload systems (e.g., HDFC, SBI, ICICI faced attacks in February 2021).
* USB Drop Attacks can compromise systems.
* First Virus is “**Creeper Virus**” developed by Bob Thomas at BBN as experimental, self-duplication program. “Purpose Security Test”
* The My doom virus was the dangerous than **ILOVEYOU virus**.

His Create One in Four Mail sent globally, Most destructive virus in history. (No body knew his developer)

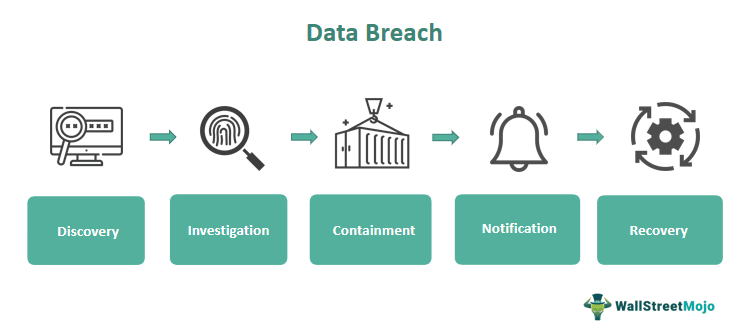
1. **Cyber Crime Laws in India**
   * The Information Technology Act (IT Act) of 2000 is a set of laws that regulate cyberspace and address cybercrimes and electronic frauds. The act defines and penalizes cybercrimes, and also covers other related topics such as:
     1. Certifying Authorities
     2. Electronic signatures and contracts
     3. Acknowledgement of receipt
     4. Acknowledgement of receipt

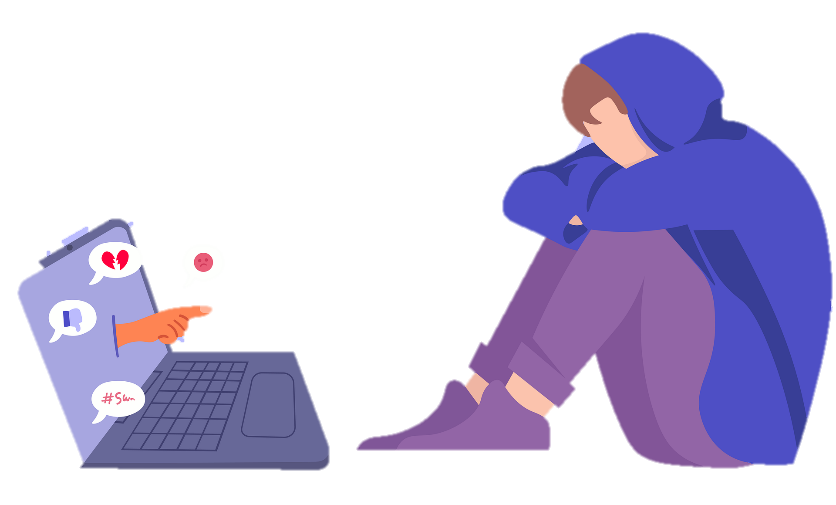
* **IT Act 2013**: Needs updates to keep pace with technological advancements.
  + The IT Act has 13 chapters and 94 sections.
* **Indian Penal Code (IPC)**: Addresses various cyber offences:
  + Section 503: Sending threatening messages
  + Section 499: Defamation
  + Section 420: Cheating through bogus websites
  + Section 383: Extortion through web jacking
  + Section 463: Forgery
  + Section 292: Obscenity (pornography)
  + Section 354D: Stalking



1. **Importance of Cyber Security Awareness**

* **Phishing Prevention**: Recognizing and avoiding phishing attempts.
* **Strong Password Security**: Using robust and unique passwords.
* **Malware Defence**: Protecting devices from malicious software.
* **Data Protection**: Safeguarding personal and organizational data.
* **Device Security**: Ensuring the security of personal and work devices.
* **Safe Online Practices**: Adopting safe practices for online transactions and activities.
* **Social Engineering Awareness**: Recognizing and defending against social engineering attacks.
* **Public Wi-Fi Awareness**: Understanding the risks of using public Wi-Fi networks.
* **Hacking & Phishing:** Hacking is using exploits to gain access to something you do not normally have access to. Phishing is masquerading as a trustworthy source in an attempt to bait a user to surrender sensitive information such as a username, password, credit card number, etc.
* **Identity Theft & Cracking:** identity theft is a crime in which an attacker uses fraud or deception to obtain personal or sensitive information from a victim and misuses it to act in the victim's name.
  + The four types of identity theft include medical, criminal, financial and child identity theft.
* **Cyber Stalking & Email Spoofing:** Sending the target threatening, controlling, or lewd messages or emails. Making a fake social media profile to follow the victim. Gaining access to the victim's online accounts. Posting or disseminating real or fictitious photos of the victim.
* **Online Scams, Cheating & Fraud:** Cyber fraud is a blanket term to describe crimes committed by cyberattacks via the internet. These crimes are committed with the intent to illegally acquire and leverage an individual's or business's sensitive information for monetary gain.
* **Cyberbullying & Child Pornography:** Cyberbullying is defined as the use of technology to harass, threaten, embarrass, stalk or target another person and often persists among young people. When explicit images of minors are disseminated online, anyone involved in posting or distributing these images may be charged with **child pornography.**
* **Malware & DDoS Attacks:** In DDoS attacks, malware such as Mirai affects vulnerable devices, turning them into bots under the control of the attacker.
* **Data Breaches & Unauthorized Access:** A data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information).
  + This intrusion can result in substantial financial loss, damage to a company's reputation, and potential legal repercussions. Additionally, in certain instances, the intruder may not only steal data but also corrupt, destroy, or encrypt it.





1. **Weakness of Privacy & Security** 
   * Hackers and cybercriminals can face criminal charges like computer fraud, identity theft, and wrongful disclosure, which may lead to jail sentences.
   * **Data Brich Illegal System Access:**
     1. Revenue Loss.
     2. Significant revenue loss as a result of a security breach is common. ...
     3. Damage to Brand Reputation.
     4. Loss of Intellectual Property. ...
   * **Illegal Interception:** A vulnerability is a weakness that can be exploited by an attacker. Thus, a weakness is an error, typically in the software code, that might lead to a vulnerability.
   * **System Interference:** An example of system interference is a denial-of-service attack (or DoS attack).
   * **Data Interference:** When committed intentionally, the damaging, deleting, deterioration, alteration, or suppression of computer data without right
   * **Misuse of Device:** Electronic Device Misuse means technology use that is unauthorized, that threatens, humiliates, harasses, or intimidates school-related individuals, disrupts the educational process, and/or violates local, state, or federal law.
   * **Fraud:** In law, **fraud** is intentional deception to secure unfair or unlawful gain
   * **Limited Resources:** Strategic resource allocation can make or break an organization's cybersecurity readiness. Operating within a limited resource framework necessitates a fine balance between coverage and precision.
   * **Old IT Act. 2013 overall 10 years:** The IT Act of 2000 also modified the Indian Penal Code. Reporting cybercrimes in India is a cumbersome process, demanding effort from complainants.
   * **Constantly Evolving Threats:** The landscape of cyber threats will include more sophisticated artificial intelligence techniques, such as advanced phishing campaigns and deepfakes, for which organizations must prepare.
   * **Legal and Compliance issues.:** Compliance in cyber security is the adherence to information security and data protection laws and mitigate legal and financial risks associated with non-compliance.
2. **How to Protect Yourself from Cyber-attacks**

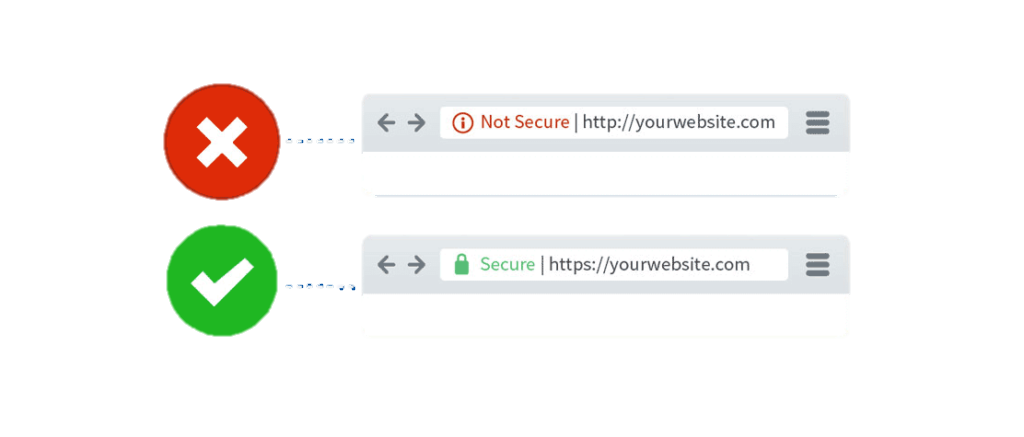
* **Use antivirus software.**: Antivirus software keeps the system secure by automatically blocking pop-ups and spam coming from malicious websites.
* **Insert Firewalls, POP UP blocker.**: A firewall offers system-wide protection while controlling in/out internet traffic and blocking pop-ups.
* **Uninstall unnecessary software.:** If you believe you already have unwanted software Uninstall software you don't need using Settings
* **Maintain system backup.**: Protect your backup data from prying eyes by encrypting it.
* **Check security setting.**: if you have Android, ISO, or Any System check it Security Setting, on your device (e.g. Password, Access Type, or Connection).
* **Use secure connection:** Secure connection refers to a connection that uses encryption protocols to protect the data being transferred.

(Ex. Always prefer Personal Wi-Fi, or https://)

* **Open attachment carefully.**: Opening unverified files attached to emails can be dangerous. These files can easily infect your computer with viruses or malware.

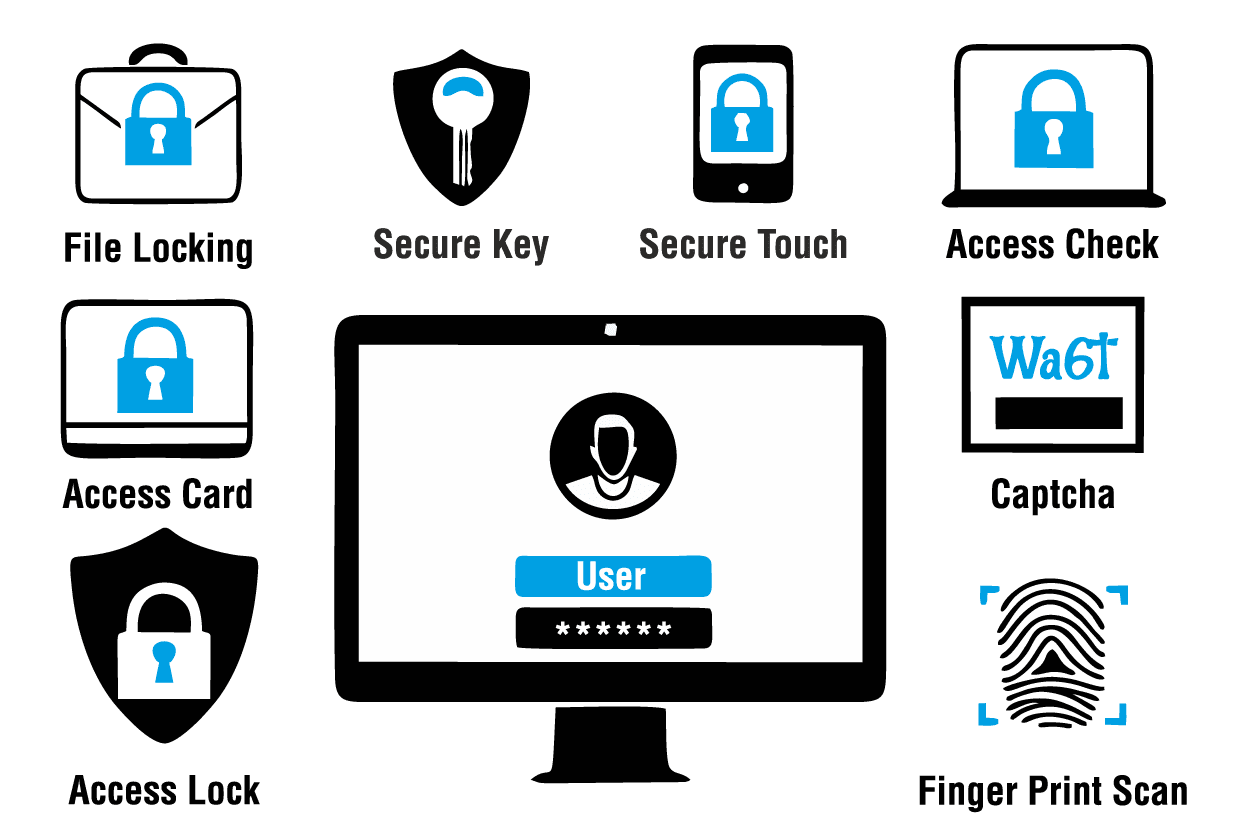
Don’t Click Unknown Links and mail attachment file etc.

* **Use strong password and (not save on email).:** Beyond a certain point, a complex password can be difficult to crack if the number of possible combinations is extremely high, but it can also be too complex to be useful to users. (USE Like: Abcd@#!1235)
* **Don’t give personal information unless required.:** Don't give out your personal information unless you are comfortable with how it is going to be used. An organisation or agency must only collect your personal information by lawful and fair means and in general must only collect information that is reasonably necessary for their functions.

****

1. **Its Safety tips** 
   * Use antivirus software
   * Implement firewalls and pop-up blockers
   * Uninstall unnecessary software
   * Maintain system backups
   * Check security settings regularly
   * Use secure connections (prefer personal Wi-Fi or https://)
   * Be cautious with email attachments and links
   * Use strong passwords and avoid saving them on emails
   * Share personal information only when necessary

**11. Advantages of Cyber Security**

* **Protect data and Information:**
* **Prevention from unauthorized access**
* **Control web portal**
* **Safeguard from viruses**
* **Safe & Secure**
* **Safe with Fraud**
* **Cyber Crime Safety**
* **Protect personal information**
* **Save govt. information**
* **Protect Nuclear Weapon, Controls**
* **Save by Threats & Hacker Attacks**

1. **Cyber Crime:**

Cybercrime encompasses a broad range of illegal activities conducted through digital devices and networks. These offenses vary from minor incidents like email scams to more severe threats such as hacking, cyberterrorism, and cyber espionage. Common types of cybercrime include phishing, malware attacks, hacking, identity theft, cyberbullying, DDoS attacks, online fraud, and cyberstalking. Combating cybercrime necessitates a holistic approach, incorporating technical solutions, legal enforcement, and user education. This entails implementing strong cybersecurity measures, enforcing relevant laws and regulations, and promoting digital literacy and awareness to mitigate risks and protect individuals and organizations from cyber threats.

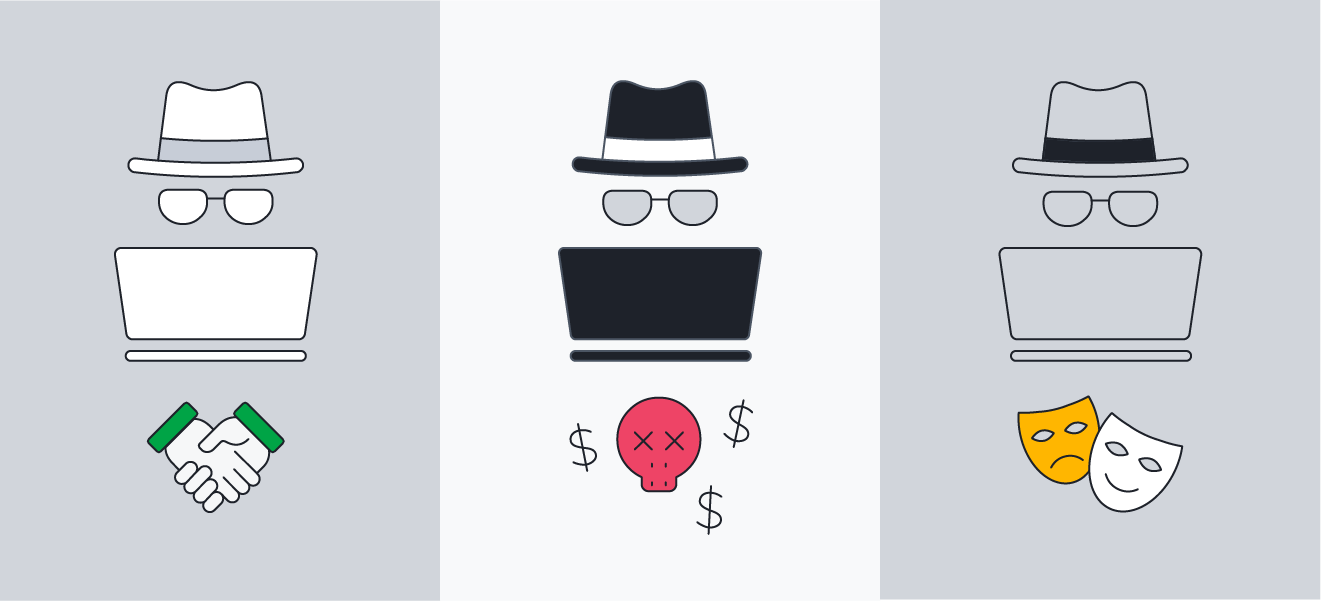
1. **Types of Cyber Crime:** 
   * **Hacking & Phishing**:
   * **Cracking & Identity Theft**:
   * **Cyber Stalking**: Persistent harassment or threatening behaviour through digital means.
   * **Email-Spoofing**: Sending emails with forged sender addresses to deceive recipients.
   * **SMS Spoofing**: Sending text messages with fake sender information to trick recipients.
   * **Online Scams, Cheating & Fraud**: Deceptive online schemes aimed at stealing money or personal information.
   * **Cyber bullying Child Pornography**: Using digital platforms to harass, intimidate, or exploit children.
   * **Transmitting Virus etc**.: Distributing malicious software designed to damage or disrupt systems.
   * **Malware & DDoS Attacks.**: employing malicious software and overwhelming servers with traffic to disrupt services.
   * **Data Breaches:** Unauthorized access to and exposure of sensitive information.
   * **Anonymous Unauthorized Access**.: aiming access to systems or data without identification or permission.
2. **Types of Hacking & Hackers:**

* **Types of Hacking**

1. **Ethical Hacking (White Hat Hacking)**
2. **Un-Ethical Hacking (Black Hat Hacking)**
3. **Gray Hat Hacking**
4. **Script Kiddie Hacking**
5. **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**
6. **Man-in-the-Middle (MITM) Attacks**

* **Types of Hackers**

1. **White Hat Hackers**
2. **Black Hat Hackers**
3. **Gray Hat Hackers**
4. **Script Kiddies**
5. **Hacktivists**
6. **Cyber Terrorists**

****

1. **Why need Cyber Security Knowledge C**ybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. As cyber-attacks volume and complexity increase, cybersecurity's importance also increases. Cybersecurity is critical because it helps to protect organizations and individuals from cyber-attacks. Cybersecurity can help to prevent data breaches, identity theft, and other types of cybercrime.

* Necessary Cyber Security Knowledge:
* Protect Against Cyber Treats
* Safeguarding Personal Information
* Securing Financial Assets
* Preserving Privacy
* Preventing Business Disruption
* National Security & Data Breach
* Maintaining Reputation
* Compliance and Legal Obligations
* Adaptation of Technological Changes
* ****Promoting Innovation

1. **Support & Resources**
   * **Supports:**
     + Help: [Government Cyber Crime Reporting Portal](https://cybercrime.gov.in/)
     + Education: [Certified Ethical Hacker](https://cert.eccouncil.org/certified-ethical-hacker.html)
       1. https://cert.eccouncil.org/certified-ethical-hacker.html
   * **Resources:**
     + **Photos:** 
       1. Googles:
       2. Picture-Gallery:
       3. Pinterest:
       4. Wikipedia
     + **Information:**
       1. <https://ia801509.us.archive.org/28/items/in.ernet.dli.2015.548410/2015.548410.Rules-For.pdf>
       2. <https://docs.google.com/document/d/16OUckGRn2K00Sjjf4gT07-ZvcQXWe8kPwh7NIMMUotU/edit?usp=sharing>
       3. <https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security>
     + **Thames:** 
       1. **Bings :** [**Click Here**](https://www.bing.com/ck/a?!&&p=962ff38d69fb716aJmltdHM9MTcxNzQ1OTIwMCZpZ3VpZD0wMTQ3NDNmYi1mYjlmLTYxNzctM2RkNy01N2QxZmE5OTYwN2QmaW5zaWQ9NTE2MQ&ptn=3&ver=2&hsh=3&fclid=014743fb-fb9f-6177-3dd7-57d1fa99607d&u=a1L2ltYWdlcy9zZWFyY2g_cT1wcHQrdGhlbWVzK2ZvcitjeWJlcitzZWN1cml0eSZxcHZ0PXBwdCt0aGVtZXMrZm9yK2N5YmVyK3NlY3VyaXR5JkZPUk09SUdSRQ&ntb=1)
       2. **Microsoft :** [**Click Here**](https://www.bing.com/ck/a?!&&p=3f123c74e497b37bJmltdHM9MTcxNzQ1OTIwMCZpZ3VpZD0wMTQ3NDNmYi1mYjlmLTYxNzctM2RkNy01N2QxZmE5OTYwN2QmaW5zaWQ9NTIzMw&ptn=3&ver=2&hsh=3&fclid=014743fb-fb9f-6177-3dd7-57d1fa99607d&psq=ppt+themes+microsoft&u=a1aHR0cHM6Ly9jcmVhdGUubWljcm9zb2Z0LmNvbS9lbi11cy9wb3dlcnBvaW50LXRlbXBsYXRlcw&ntb=1)
       3. **PPT Presentation:** <https://docs.google.com/presentation/d/15uLCx8Iu055-2ByM9eb5-KOJZl9xBrAt/edit?usp=drive_link&ouid=111962080053355257549&rtpof=true&sd=true>
     + **Icons:**
       1. **Google Icon:** <https://fonts.google.com/icons>
       2. **Google Font:** <https://fonts.google.com/specimen/Open+Sans>
2. **References & Books**

* **References:**
  + **Learn from** [www.hackthetech.org/@pratipalmaurya](http://www.hackthetech.org/@pratipalmaurya)
  + **Learn from** <https://en.wikipedia.org/wiki/B._Raman>
  + **Learn from** <https://en.wikipedia.org/wiki/R.N.Kao>
  + **Learn from** <https://cert.eccouncil.org/certified-ethical-hacker.html>
  + **Learn from** <https://en.wikipedia.org/wiki/Computer_security>
  + **Learn from** <https://en.wikipedia.org/wiki/Cybercrime>
  + **Learn from** <https://en.wikipedia.org/wiki/Research_and_Analysis_Wing>
* **Books:**
  + **Hack-the-Tech:** Writer “Grover” Security Trainer.
  + **Gentleman Spymaster:** Writer “R. N. Kao”
  + **The Kaoboys of R&AW:** Writer “B. Raman”
  + **The Down Memory Lane:** Writer “B. Raman”
  + **Research Paper:** Researcher “S. Jayshankar”, “Nitin Pandey”, “Vivek Ramchandran”. All Research of (IIT Patna, Kharagpur, Roorkee, Kanpur).
  + **Expert:** Dipanshu “Youngest Trainer”, BHU, JNU’s Professors.

1. **Conclusion:**

Cyber security is essential for protecting systems, networks, and data from digital attacks. Historical development in India's intelligence agencies, such as IB and R&AW, showcases the evolution of national security measures. The field encompasses roles like security analysts, incident responders, and ethical hackers, each addressing specific threats like malware, phishing, and DDoS attacks. Legal frameworks, like the IT Act, and continuous awareness are crucial for safeguarding against cybercrimes. With proper tools, training, and vigilant practices, individuals and organizations can significantly enhance their security posture against evolving cyber threats.

**Thank You**