I'm not a robot

Annual Membership Enjoy unlimited access on 10000+ Hand Picked Quality Video Courses. Subscribe now Tutorials Point is a leading Ed Tech company striving to provide the best learning material on technical and non-technical subjects. © Copyright 2025. All Rights Reserved. How can financial brands set themselves apart through visual storytelling? Our experts explain how.Learn MoreThe Motorsport Images Collections captures events from 1895 to today’s most recent coverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors’ Picks.Browse Editors' FavoritesHow can financial brands set themselves apart through visual storytelling? Our experts explain how.Learn MoreThe Motorsport Images Collections captures events from 1895 to today’s most recent coverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors’ Picks.Browse Editors' FavoritesHow can financial brands set themselves apart through visual storytelling? Our experts explain how.Learn MoreThe Motorsport Images Collections captures events from 1895 to today’s most recent coverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors’ Picks.Browse Editors' Favorites DSA to Development: A Complete GuideBeginner to AdvanceJAVA Backend Development - LiveIntermediate and AdvanceTech Interview 101 - From DSA to System Design for Working ProfessionalsBeginner to AdvanceFull Stack Development with React & Node JS - LiveBeginner to AdvanceJava Programming Online Course [Complete Beginner to Advanced]Beginner to AdvanceC++ Programming Course Online - Complete Beginner to AdvancedBeginner to AdvancePage 2Our website uses cookiesWe use cookies to ensure you have the best browsing experience on our website. By using our site, you acknowledge that you have read and understood our Cookie Policy & Privacy Policy Tutorials Point is a leading Ed Tech company striving to provide the best learning material on technical and non-technical subjects. © Copyright 2025. All Rights Reserved. Ask the publishers to restore access to 500,000+ books. Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. 0 ratings0% found this document useful (0 votes)863 viewsCybercrime can harm individuals, groups, governments, and private organizations. It most significantly threatens financial security by causing billions in losses each year. There are several…SaveSave Cyber Crime & Cyber Security - Tutorialspoint For Later0%0% found this document useful, undefined Cyber security is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks." It involves a range of strategies, technologies, and best practices designed to safeguard computers, networks, and data from cyber attacks.What is Cyber SecurityCyber Security involves using specialized tools to detect and remove harmful software while also learning to identify and avoid online scams. Practicing good cybersecurity habits helps keep your data private and ensures a safe online experience. It's also referred to as Information Security (INFOSEC), Information Assurance (IA), or System Security.What is Cyber Security? (Definition & Importance)Cybersecurity is all about protecting your computer, phone, or any digital device from hackers and online threats. It keeps your personal information, bank details, files, and online activity safe from being stolen, damaged, or misused. By acquiring knowledge of cyber attacks and cyber security we can secure and defend ourselves from various cyber attacks like phishing and DDoS attacks.Common Cyber Attacks You Should KnowAttack TypeWhat It MeansPhishingPhishing is a cyber attack where hackers trick users into revealing sensitive data like passwords, banking details, or session tokens through fake emails, messages, or websites. It uses social engineering to impersonate trusted sources and often includes malicious links or attachments to steal information.DDoS (Distributed Denial of Service)Hackers flood a website or server with too much traffic, so it slows down or crashes. It’s like a traffic jam that blocks real users from getting in.Every day, there are cyberattacks happening around the world. Without basic protection, anyone—individuals or companies—can become a victim. That’s why knowing about cybersecurity is just as important as locking your house.One crucial aspect of cybersecurity is Encryption, which ensures that sensitive information remains private and readable only to authorized users. This is especially important for financial transactions, personal communications, and corporate databases to prevent data theft and unauthorized accessIn short, cybersecurity keeps your online world safe and secure. It ensures that sensitive information remains confidential, intact, and accessible only to authorized users. Whether it's securing personal information, financial transactions, or corporate databases.Start your Cybersecurity journey with: Cyber Security TutorialTypes of CybersecurityThere are seven types of cyber security, each explained below in detail with uses and functions:It focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. This involves implementing technologies such as Firewalls, Intrusion detection systems (IDS), Virtual private networks (VPNs), and Network segmentation as well as deploying antivirus software Using public Wi-Fi in locations like cafes and malls poses significant security risks. Malicious actors on the same network can potentially intercept your online activity, including sensitive information. If you use payment gateways on these unsecured networks, your financial data could be compromised because these open networks don’t have proper security layers, which means anyone—even hackers—can watch what you're doing online.So, use a secure private network or VPN to protect your internal network from outside threats2. Application Security (Ensuring Secure Software and Apps)Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.Most of the Apps that we use on our cell phones are Secured and work under the rules and regulations of the Google Play Store.There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, and Amazon App Store has 483 million available for users to download. With so many choices, it’s easy to assume all apps are safe—but that’s not true.Some apps pretend to be secure, but once installed, they collect personal data and secretly share it with third-party companies.The app must be installed from a trustworthy platform, not from some 3rd party website in the form of an APK (Android Application Package).Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction. It includes Encryption, Access controls, Data classification, and Data loss prevention (DLP) measures.Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.4. Cloud Security (Defending Cloud Storage and Applications)It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance. It uses various cloud service providers such as AWS, Azure, Google Cloud, etc., to ensure security against multiple threats.Cloud-based data storage has become a popular option over the last decade. It enhances privacy if configured and managed correctly and saves data on the cloud, making it accessible from any device with proper authentication.These platforms offer free tiers for limited usage, and users must pay for additional storage or servicesIt is a cloud service provider that offers a wide range of services, including storage, computing, and security tools.5. Endpoint Security (Protecting Devices like Laptops & Phones)Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.Antivirus and Anti-malware software that scans and detects malicious software, such as Viruses, Worms, Trojans, and Ransomware. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.6. Operational Security (Managing Internal Security Protocols)Refers to the processes and policies organizations implement to protect sensitive data from internal threats and human errors. It involves access controls, risk management, employee training, and monitoring activities to prevent data leaks and security breaches.Access Controls ensure that only authorized personnel can access critical systems and sensitive information. This includes role-based access, multi-factor authentication (MFA), and least privilege principles.Risk Management involves identifying, analyzing, and mitigating security risks within an organization. It includes regular security assessments, vulnerability testing, and compliance audits.Employee Training is crucial for preventing insider threats and social engineering attacks. Organizations conduct cybersecurity awareness programs to educate employees on phishing scams, password security, and data handling best practices.Monitoring & Incident Response includes tracking user activity, detecting suspicious behavior, and responding to security incidents in real time. Security Information and Event Management (SIEM) tools help organizations analyze and mitigate threats effectively.7. Internet of Things (IoT) SecurityRefers to protecting internet-connected devices such as smart home gadgets, industrial sensors, medical equipment, and wearable technology from cyber threats. IoT security ensures that these devices do not become entry points for hackers to exploit networks and steal sensitive data.Device Authentication & Encryption ensures that only authorized devices can connect to networks. Encryption protects data transmitted between IoT devices and servers from interception.Firmware & Software Updates are crucial to patch security vulnerabilities. Regular updates help prevent exploitation by cybercriminals who target outdated IoT firmware.Network Segmentation isolates IoT devices from critical systems, reducing the risk of widespread attacks if one device is compromised. This approach limits unauthorized access and lateral movement within a network.IoT Security Standards & Compliance include implementing industry security frameworks like Zero Trust Architecture (ZTA) and following best practices such as strong password policies, secure APIs, and endpoint protection to enhance IoT device security.Why is Cybersecurity is Important?Cyber Security is important because the government, corporations, and medical organizations, collect military, financial, process, and store unprecedented amounts of data on a computer and other properties like personal information, and this private information exposure could have negative consequences. In 1972, when the internet was just starting (called ARPANET at the time), a test virus named Creeper was created—and then another program called Reaper was made to remove it. This early experiment showed why digital security was needed and helped start what we now call cybersecurity.Rising Cyber Threats: How Hackers Exploit Weak SecurityCybercriminals are constantly finding new ways to exploit vulnerabilities in systems, networks, and personal devices. Weak passwords, outdated software, and unsecured networks create easy entry points for hackers. They use sophisticated methods like phishing emails, ransomware, and social engineering to steal sensitive data, disrupt operations, and demand ransoms. With the rise of AI-driven cyber threats, even automated bots can breach security systems, making cybersecurity more critical than ever.For Example - If we shop from any online shopping website and share information like email ID, address, and credit card details as well as save on that website to enable a faster and hassle-free shopping experience, then the required information is stored on a server one day we receive an email which state that the eligibility for a special discount voucher from XXXXX (hacker use famous website Name like Flipkart, Amazon, etc.) website to receive the coupon code, and we will be asked to fill the details then we will use saved card account credentials. Then our data will be shared because we think it was just an account for the verification step, and then they can wipe a substantial amount of money from our account. Consequences of Cyber Attacks for Businesses & IndividualsA successful cyber attack can have devastating effects, both financially and reputationally. For businesses, a data breach can lead to massive financial losses, legal penalties, and loss of customer trust. Small businesses are especially vulnerable, as they often lack robust security measures. Individuals, on the other hand, face risks like identity theft, financial fraud, and personal data leaks. Cyber attacks can wipe out bank accounts, expose private information, and even lock users out of their own devices unless a ransom is paid. The consequences can be long-lasting, leading to emotional distress and financial instability.Major Cybersecurity Threats & AttacksHackers use advanced techniques to find weaknesses in systems, steal or change data, and break into networks without permission. Below are the most common cybersecurity threats that target businesses, cloud storage, and personal devices:Read complete article, here: Types of Cyber Attacks1. Malware Attacks (Viruses, Trojans, Rootkits, and Spyware)Malware is a type of harmful software created to enter, attack, and compromise systems. It includes trojans (which look like real software but are harmful), rootkits (which hide deep inside a system to take control), and spyware (which secretly steals data).Hackers use payload obfuscation (hides the malicious code making it harder for security software to identify), polymorphic techniques (changing malware code to avoid detection), and zero-day exploits (attacking unknown security flaws) to bypass intrusion detection systems (IDS) and endpoint protection platforms (EPP).2. Phishing & Spear Phishing AttacksPhishing uses tricks and manipulation to steal login details, session tokens, and financial information. Spear phishing is a more targeted version that uses open-source intelligence (OSINT) to create personalized fake messages.Hackers use domain spoofing (making fake websites look real), homograph attacks (using similar-looking characters in URLs), and malicious macros (harmful scripts hidden in email attachments) to bypass security and trick users into revealing sensitive data.3. Ransomware Attacks (Cryptographic File Encryption)Ransomware locks important system files by encrypting them using asymmetric cryptography (like RSA, ECC) or hybrid encryption (AES-RSA). It then demands a ransom, usually in cryptocurrency, to unlock the data.More advanced types, like double extortion ransomware, first steal sensitive data before encrypting it. Hackers then threaten to leak the stolen data on dark web sites if the ransom isn't paid.4. Distributed Denial-of-Service (DDoS) AttacksDDoS attacks overload a network by flooding it with massive amounts of traffic at different levels—volumetric, protocol, or application-layer—causing servers to crash and making services unavailable.Hackers use botnets (networks of infected devices), amplification techniques (like DNS reflection and NTP amplification) to increase attack size, and HTTP flood requests to overwhelm websites. These methods help attackers bypass rate-limiting defenses and take down their targets.5. SQL Injection (SQLi) & NoSQL InjectionSQL injection attacks take advantage of weak web application queries by inserting malicious SQL code to modify database records, steal login credentials, or run admin-level commands.NoSQL injection targets document-based databases like MongoDB and Firebase by altering query parameters, allowing attackers to bypass authentication and gain unauthorized access to sensitive data.6. Zero-Day Exploits & Advanced Persistent Threats (APT)Zero-day exploits take advantage of unknown software vulnerabilities before developers release security patches, making them highly dangerous.Advanced Persistent Threats (APTs) use multi-stage attack techniques to stay hidden in a system for a long time. These include lateral movement (such as pass-the-hash attacks to spread across networks), privilege escalation (gaining higher access rights), and persistence mechanisms (like rootkits and fileless malware) to maintain control over compromised networks.7. Man-in-the-Middle (MITM) AttacksMan-in-the-Middle (MITM) attacks secretly intercept and modify data exchanged between two parties by exploiting weak encryption or unsecured communication channels.Hackers use techniques like SSL stripping (removing HTTPS encryption), rogue access points (fake Wi-Fi networks), and ARP poisoning (manipulating network traffic) to steal login credentials, hijack user sessions, or inject malicious code into data transmissionsInsider threats occur when compromised or malicious employees with high-level access steal sensitive data, modify access permissions, or install backdoors to bypass security. Since insiders already have authorized access, they can easily evade traditional perimeter security measures.To detect and prevent insider threats, organizations use User and Entity Behavior Analytics (UEBA) to track suspicious activities, Privilege Access Management (PAM) to restrict sensitive access, and zero-trust architectures to ensure continuous verification.Cybersecurity tools help protect systems, networks, and data from cyber threats by detecting, preventing, and responding to attacks. These tools play a crucial role in securing infrastructure, identifying vulnerabilities, and mitigating risks. Cybersecurity Trends in 2025Cybersecurity has evolved dramatically. Before 2015, basic antivirus, firewalls, and internal IT teams were enough against simple viruses and spam. Between 2016 and 2023, cyberattacks became more serious, with new threats like ransomware, widespread phishing, DDoS attacks, and huge data breaches. Now in 2025, threats like AI-powered attacks, zero-day exploits, deepfake scams, supply chain attacks, and nation-state cyber warfare are making attacks more complex, automated, and targeted than ever.1. Rise of AI and Machine Learning: More cybersecurity tools are using artificial intelligence (AI) and machine learning to detect and respond to threats faster than humans can. AI in cybersecurity helps recognize patterns, block suspicious behavior, and even predict future threats—making it one of the most powerful tools to protect sensitive information.2. Increase in Ransomware Attacks: Ransomware, where hackers lock you out of your data until you pay a ransom, is becoming more common. Companies and individuals alike need to back up their data regularly and invest in security measures to avoid falling victim to these attacks.3. Cloud Security: As more businesses move their data to the cloud, ensuring this data is secure is a top priority. This includes using strong authentication methods and regularly updating security protocols to protect against breaches.4. Internet of Things (IoT) Vulnerabilities: With more devices connected to the internet, like smart home gadgets and wearable tech, there's an increased risk of cyberattacks. Ensuring these devices have updated security features is crucial.5. Zero Trust Security: This approach assumes that threats could come from inside or outside the network, so it constantly verifies and monitors all access requests. It's becoming a standard practice to ensure a higher level of security.6. Cybersecurity Skills Gap: There is a growing need for skilled cybersecurity professionals. As cyber threats become more sophisticated, the demand for experts who can protect against these threats is higher than ever.7. Regulatory Compliance: New regulations are being introduced worldwide to protect personal data. Companies must stay informed about these laws to ensure they comply and avoid hefty fines.Cybersecurity Best PracticesThere are several steps you can take to protect yourself from cyber threats, including:Use strong passwords: Use unique and complex passwords for all of your accounts, and consider using a password manager to store and manage your passwords.Keep your software up to date: Keep your operating system, software applications, and security software up to date with the latest security patches and updates.Enable two-factor authentication: Enable two-factor authentication on all of your accounts to add an extra layer of security.Be aware of suspicious emails: Be cautious of unsolicited emails, particularly those that ask for personal or financial information or contain suspicious links or attachments.Educate yourself: Stay informed about the latest cybersecurity threats and best practices by reading cybersecurity blogs and attending cybersecurity training programs.Challenges of CybersecurityConstantly Evolving Threat Landscape: Cyber threats are constantly evolving, and attackers are becoming increasingly sophisticated. This makes it challenging for cybersecurity professionals to keep up with the latest threats and implement effective measures to protect against them.Lack of Skilled Professionals: There is a shortage of skilled cybersecurity professionals, which makes it difficult for organizations to find and hire qualified staff to manage their cybersecurity programs.Limited Budgets: Cybersecurity can be expensive, and many organizations have limited budgets to allocate toward cybersecurity initiatives. This can result in a lack of resources and infrastructure to effectively protect against cyber threats.Insider Threats: Insider threats can be just as damaging as external threats. Employees or contractors who have access to sensitive information can intentionally or unintentionally compromise data security.Complexity of Technology: With the rise of cloud computing, IoT, and other technologies, the complexity of IT infrastructure has increased significantly. This complexity makes it challenging to identify and address vulnerabilities and implement effective cybersecurity measures.Strategies for Addressing Cybersecurity ChallengesComprehensive Risk Assessment: A comprehensive risk assessment can help organizations identify potential vulnerabilities and prioritize cybersecurity initiatives based on their impact and likelihood.Cybersecurity Training and Awareness: Cybersecurity training and awareness programs can help employees understand the risks and best practices for protecting against cyber threats.Collaboration and Information Sharing: Collaboration and information sharing between organizations, industries, and government agencies can help improve cybersecurity strategies and response to cyber threats.Cybersecurity Automation: Cybersecurity automation can help organizations identify and respond to threats in real time, reducing the risk of data breaches and other cyber attacks.Continuous Monitoring: Continuous monitoring of IT infrastructure and data can help identify potential threats and vulnerabilities, allowing for proactive measures to be taken to prevent attacks.ConclusionCybersecurity is no longer a choice—it's a must for everyone, from web browsers to corporations handling millions of sensitive information. With increasing threats such as phishing, ransomware, data breaches, and AI-driven cyber attacks, surfing online without protection can be risky.Global cybercrime losses in 2023 totaled more than $8 trillion. That figure is projected to reach approximately $9.5 trillion in 2024, and could approach $10.5 trillion in 2025. These statistics easily demonstrate the need to lock down your devices, guard your personal and financial information, and employ sound cybersecurity software and methodologies.Whether it's preventing phishing scams, securing cloud storage, or blocking malware, cybersecurity plays a key role in ensuring a safe digital environment. By staying informed, using robust security tools, and following best practices, individuals and businesses can reduce risks and enhance overall cyber protection. Cybersecurity is one of the most sought-after skills in the modern era. With such a large information pool, and an even larger network of nodes, Cybersecurity has gained a lot of importance nowadays. This cybersecurity tutorial is designed for beginners as well as professionals. In this tutorial, you will learn all essential skills, tools, and strategies regarding cybersecurity. This cybersecurity tutorial covers the topics from basic concepts to advanced techniques. Following the U.S.A. and China, India ranks third in the number of internet users. This requires resilient Cybersecurity Solutions to protect data from frequent attacks. What is Cybersecurity? Cybersecurity is the branch of Information Security that handles the protection and safeguard of networks and data from illegal access or damage. In other words, Cybersecurity is the layer of protection which protects the networks and peripheral data from cyber-attacks and/or information leakage. Nowadays, most organizations have internal and external networks established to run smoothly and transfer data and other information from one node to another. These network edges and nodes are prone to frequent attacks and data leakage from both intrinsic and extrinsic sources. Hence, many organizations fund a lot of money to protect their internal information systems. So, why should you study Cybersecurity? Cybersecurity offers many features, and its importance can be reflected in the following points − Protecting our Digital Lives − From your online banking to your social media, your personal information is valuable. Cyberattacks can steal your identity, money, or even ruin your reputation. Safeguarding Business − Companies rely on computers and networks to operate. A cyberattack can cause financial loss, damage reputation, and even put people's jobs at risk. Defending Nations − Governments and critical infrastructure like power plants, transportation, and healthcare depend on computers. Protecting these systems is crucial for national security. Exciting and Rewarding Career − Cybersecurity is a growing field with high demand for skilled professionals. You can work for big tech companies, banks, governments, or even start your own cybersecurity business. In todays digital age, everything is connected and leaves a digital trace. These information spaces are very important, and hence need protection on every step of their transfer from one point in the network to another. Challenges to Cybersecurity While Cybersecurity has a lot of features and advantages, it also has some challenges − Cost and Time − Implementing and maintaining cybersecurity systems can be expensive and time-consuming for organizations. Complexity − Cybersecurity systems can be complex to manage and maintain in the longer run. Constant Evolution − Cyber threats are constantly evolving, which require the Cybersecurity solution to be consistently adaptive to these threats. Limited Effectiveness − Despite maximum efforts, complete protection from cyberattacks is impossible to attain. Career Paths in Cybersecurity Cybersecurity experts focus on safeguarding networks, systems, and software from cyber threats. They can pursue different job roles, including − Information Security Specialist Penetration Tester Incident Response Manager Security Architect Chief Information Officer Security Consultant Application Security Specialist Forensic Scientist Security Manager Ethical Hacker Computer Forensics Analyst Malware Analyst Monitoring Software Engineer Vulnerability Assessor Threat Management Analyst Cloud Architect Security Engineer Top Companies Hiring Cybersecurity Experts Many companies hire Cybersecurity experts to handle the security perspective of the organization and protect the networks and data from security breach or data corruption. Today a Cybersecurity Expert with good skills earns about $75000 annually at entry level. Cybersecurity is one of the most demanding skill for CS graduates all over the world. A few large companies are listed below, which hire Cybersecurity experts and professional threat analyzers − Palo Alto Networks Deloitte Meta (Facebook) Rapid7 WeSecureApp Wipro Fortinet HKIT Security Solutions IBM Microsoft Roadmap to Become a Cybersecurity Expert Heres a general roadmap to become a Cybersecurity Expert − 1. Foundational Knowledge Concepts related to computer networks, operating systems, network security and cryptography are very important. Along with this, you should also be able to have command over at least one programming language (C++, Python, Java). 2. Skill to Acquire You can start learning about ethical hacking and tools like Kali Linux for testing and penetration. Also, gain practical skills like cloud management using any could service (AWS, MS Azure). 3. Certification You can also become a certified Cybersecurity Expert using a certification course. 4. Practical Experience Apart from theoretical knowledge and skill gaining, practical experience should also be acquired from Internship roles and personal projects. 5. Continuous Learning One of the most important steps to get industry experience is to follow cybersecurity news, blogs, and research. Also, one should become part of a community of experts to gain help and support. 6. Specialization You can also decide on a specialization like threat intelligence, application security, or security architecture. You must focus on specific tools, technologies, and methodologies to further enhance your career. Prerequisites to Learn Cybersecurity This tutorial is made for all levels, from beginners to advanced. The requirements of this course are given as follows − Basic knowledge of Computer Networks Any coding language with syntax Basics Data Structures and Algorithms Operating System knowledge like Linux, MS or Mac Audience This cybersecurity tutorial has been prepared for beginners to help them understand the basic concepts of cybersecurity, and then move on to more challenging topics at their own pace. On the other hand, professionals can read through and uplift their skills using this tutorial. After completing this tutorial, you will find yourself feeling confident in dealing with Cybersecurity and Threat Analysis concepts. FAQs about Cybersecurity Here is a list of the most frequently asked questions related to Cybersecurity and related fields − What are the common types of cyberattacks? Common cyberattacks include phishing, ransomware, malware, DDoS attacks, and social engineering. How can I protect my personal information online? You can use strong passwords, be cautious of phishing attempts, and avoid sharing personal information on social media. Apart from this, always try to question and be aware of what is happening in your online space. Anything that might seem suspicious to you should be investigated cautiously. What is the role of a cybersecurity professional? Cybersecurity professionals protect organizations by identifying, assessing, and mitigating cyber risks. The function of cybersecurity professionals also depends on the area of their work, and their particular specialization in the field. For example, Network engineer works on networking and file sharing, database engineer works on protection of database and denying illegal access, and so on. Which companies hire Cybersecurity experts? Top companies which hire Cybersecurity experts are Palo Alto, Wipro, Microsoft, GenAI and many more. These companies generally belong to Technical Sector, and many non-technical companies lend cybersecurity solutions from these companies, or hire a team of experts for themselves. What is MFA in cybersecurity? MFA is the acronym used for Multi-factor authentication. It is used in most systems nowadays, and it requires the user to pass via multiple security levels to gain access to a resource or asset. Which is the most popular antivirus in the world? There are several antivirus software services used around the world. Some of the most popular ones are McAfee, BitDefender, AVG and Norton. Which is the most common cybersecurity threat faced by organizations? Some of the most common cybersecurity threats include Virus, Malware and DoS attacks. How do companies implement cybersecurity solutions? Companies can implement cybersecurity solutions in one of two ways. One way is to make a dedicated team of cybersecurity experts and handle the situation on their own. Other way is to hire services and tools from other cybersecurity.