**Aim**: Study of different laws and standards of cyber security.

**Theory:**

**Define cyber security**

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

**Importance of Cyber security**

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data much of which is sensitive or confidential the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

**Types of Cyber Attacks.**

**1. Malware Attack** This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans. The [trojan virus](https://www.simplilearn.com/what-is-a-trojan-malware-article) disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen. Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

* Use antivirus software. It can protect your computer against malware. Avast Antivirus, Norton Antivirus, and McAfee Antivirus are a few of the popular antivirus software.
* Use firewalls. Firewalls filter the traffic that may enter your device. Windows and Mac OS X have their default built-in firewalls, named Windows Firewall and Mac Firewall.

### **2. Phishing Attack**

### Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake emails. Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.

Phishing attacks can be prevented by following the below-mentioned steps:

* Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.
* Make use of an anti-phishing toolbar.

### **3. Password Attack**

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attack .Listed below are a few ways to prevent password attacks:

* Use strong alphanumeric passwords with special characters.
* Abstain from using the same password for multiple websites or accounts.

### **4. Man-in-the-Middle Attack**

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data. As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.MITM attacks can be prevented by following the below-mentioned steps:

* Be mindful of the security of the website you are using. Use encryption on your devices.
* Refrain from using public Wi-Fi networks.

### **5. SQL Injection Attack**

A Structured Query Language ([SQL](https://www.simplilearn.com/tutorials/sql-tutorial/what-is-sql)) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information. This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

To prevent a SQL injection attack: Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

### **6. Denial-of-Service Attack**

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth. When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended. It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack. Let’s now look at how to prevent a DDoS attack:

* Run a traffic analysis to identify malicious traffic.
* Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.

### **7. Cryptojacking**

The term Cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else’s computer to mine cryptocurrency. The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Cryptojacking can be prevented by following the below-mentioned steps:

* Update your software and all the security apps as cryptojacking can infect the most unprotected systems.
* Have cryptojacking awareness training for the employees; this will help them detect crypotjacking threats.

### **8.. Watering Hole Attack**

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

### **9. Spoofing**

An attacker impersonates someone or something else to access sensitive information and do malicious activities. For example, they can spoof an email address or a network address.

### **10. Code Injection Attacks**

Performed by inserting malicious code into a software application to manipulate data. For example, the attacker puts malicious code into a SQL database to steal data.

**Tools used for cyber security**

**1. Kali Linux**

Kali Linux is among the most popular penetration testing tools with over 300 features for website and server security. Suited for users with varying levels of knowledge in cybersecurity, Kali Linux can be used to monitor network systems with one click. The tool is particularly useful for securing databases from various cyber-attacks and online threats. Currently maintained by Offensive Security, Kali Linux was initially developed as BackTrack – a Linux-based distribution tool used for penetration testing.

**2.Wireshark**

Wireshark is a free and open-source cybersecurity tool that can analyze network protocols and can be used to enhance network security. Packet-sniffing in this console-based tool can monitor your network in real-time, along with network traffic at different levels. Cybersecurity professionals use this security tool to identify any network security weaknesses by capturing and analyzing data packets.

**3.Snort**

Snort is another open-source tool used for detecting and stopping attempted intrusions on computer networks. This tool supports Windows, Centos, FreeBSD, and Fedora platforms. The Snort, intrusion prevention tool, is capable of performing real-time analysis of network traffic and packet logging. Suited for small to medium-sized businesses, Snort is compatible with different types of operating systems and hardware configurations.Firewall protection for blocking malicious network requestsTimely alerts of potential intrusions to security professionals

**Standards of cyber security**

**ISO**

ISO stands for International Organisation for Standardisation. International Standards make things work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard was officially established On 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

**ISO/SAE 21434**

Standard covers the aspects of automotive cybersecurity. This standard includes a list of requirements related to cyber security risk management. It also covers a cybersecurity process framework that helps OEMs to come on a common platform and communicate risks related to security.

**ISO/IEC 20243-1**

This Information technology standard refers to the Open Trusted Technology ProviderTM Standard (O-TTPS). This particular standard helps in mitigating maliciously tainted and counterfeit products.

**ISO 27000 Series**

It is the family of information security standards which is developed by the International Organisation for Standardisation and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization faces. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

**Laws of cyber security**

**1. IT Act**

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India that deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of the United Nations. This act is also used to check misuse of cyber networks and computers in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitates electronic governance by means of reliable electronic records.IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offenses, and the remaining section 80 to 94 deal with miscellaneous of the act.

**2. Copyright Act**

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

Rights of copyright owners

Works eligible for protection

Duration of copyright

Who can claim copyright

The copyright act does not covers the following-

Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries

Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)

Familiar symbols or designs

Titles, names, short phrases, and slogans

Mere variations of typographic ornamentation, lettering, or coloring

**3. Patent Law**

Patent law is a law that deals with new inventions. Traditional patent law protects tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent laws have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

Not a natural object or process

New

Useful

Not obvious.

**4. IPR**

Intellectual property rights is a right that allows creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

**Conclusion:**

Thus we studied an overview of cybersecurity and cybercrimes, the tools that are used and the important standards and laws related to cybersecurity