# *CYBER SECURITY –*

*A knowledge for safer tomorrow*

cscoe.itewb.gov.in

## Cyber Security Centre of Excellence

**Department of IT & Electronics | Government of West Bengal**


*"Security is always seen as too much until the day it is not enough"*

William Hedgcock Webster

# CYBER SECURITY –

## A Knowledge For Safer Tomorrow

**CYBER SECURITY CENTRE OF EXCELLENCE**

**Department of IT & Electronics**
**Government of West Bengal**

First Published October 2021

Published By

**Cyber Security Centre of Excellence**

Webel Bhavan, Ground Floor

Block - EP & GP, Sector - V

Bidhannagar, Salt Lake

Kolkata - 700 091

Phone No. : 033 2357-5218

Email : cscoe@wb.gov.in

Edited by

**Sanjay Kumar Das**

Collected, collated and scripted by

**Janhabee Ray**

Cover and designs by

**Tarak Nath Mandal**

Printing

**Saraswaty Press Ltd.**

## PREFACE

Security is a sense that allows every other feeling or emotion to manifest. While, insecurity has overpowering effect as it suppresses them. With the start of the present millennia, physical security paved way for digital security as society progresses from 'going digital' to 'being digital.' Cyber-security talks about the sense that prevails when one feels safe and secured while accessing digital content over a network-connected environment. Often the term cyber-security, is constricted to World Wide Web or Internet. While in reality, security within a Local or Limited Area Network poses a great challenge. Exponential rise in connected devices creates vulnerabilities as various applications running on them, talk to each other. Ease-of-Use and Security are two sides of the same coin - they don't see eye-to-eye. In public service delivery sphere, plethora of software run from secured Data Centre and use connectivity highway spread across the State. Now, responsibility of protecting these critical IT infrastructures has befallen on the State. In a nutshell, with passage of time, governance has gone to the door-steps via secured digital transactions. A physical security guard has thus become a cyber-security guard.

Cyber-security is a moving train. One who starts today by boarding from the rear can easily reach the engine with time and perseverance. Hope, this book helps all new boarders.

**Sanjay Kumar Das**
Joint Secretary, Department of IT & Electronics and
Member Secretary, Cyber Security Centre of Excellence
Government of West Bengal, INDIA

## ACKNOWLEDGEMENT

Acknowledgement of deep gratitude is due for the State Government of West Bengal; Dr. Partha Chatterjee, Hon'ble Minister-in-Charge and Shri Rajeev Kumar, IPS, Principal Secretary of the Department of Information Technology & Electronics along with all the officers and employees. Heartfelt gratitude also goes toward the Managing Director of Webel and all her officials, the authorities of West Bengal Police, Kolkata Police and CID West Bengal. Without their support and co-operation, this book would not have seen the light of the day. Special gratitude is reserved for Shri H. Kusumakar, IPS, Chief Information Security Officer, West Bengal - whose guidance has been paramount to conceive, ideate and fructify this book. Due credit for this book also goes to the officials of Cyber Security Centre of Excellence, West Bengal where various employees from the IT&E Department, Webel, West Bengal Police, Society for Natural Language Technology Research and Institute of Open Technology Applications congregate to work in addition to their normal duties. Their invaluable co-operation and support have made this book a reality. Last but not the least, Ms. Janhabee Ray of Webel has painstakingly collected, collated and aggregated materials from all corners to put together this anthology on Cyber Security. Acknowledgement of her toils is also due.

Member Secretary
Cyber Security Centre of Excellence

# Table of Contents

## 1. What is cybercrime?

Cybercrime or computer-oriented crime is a criminal activity that either targets or involves a computer, a computer network or a networked device to attain illegal ends such as committing a financial fraud, trafficking in child pornography, intellectual property, stealing identities, or violating privacy.

## 2. Defining cybercrime

Evolution and wide spread use of new technologies have created new opportunities for criminals. What distinguishes cybercrime from traditional crime is the use of digital devices, computers and internet. Almost all these crimes existed earlier also, but cyber crime is a modified way to commit those existing traditional crimes involving digital devices and internet.

In the digital age, we all have our virtual identities where we are bundle of numbers and identifiers in various computer databases owned by the governments and corporations. Our identifiers include Aadhaar number, PAN card, Bank account number, Credit card number, User Ids for different accounts, email ids, Health card number and such.

Most cybercriminals attack on these information of individuals, corporations, or governments. Although the attacks do not take place physically, but they do a lot of harm to the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet.

Where exactly does cybercrime take place? Contrary to traditional crimes, a cybercrime is non-local in character. A cyber criminal can physically be present miles and miles away from the victim and still commit the crime and the extent of damage is often much higher than that in traditional crimes.

Since cyber crime can occur in jurisdictions separated by vast distances, and that evokes severe problems for law enforcement. Many cyber crimes require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal?

As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals also leave clues as to their identity and location despite their best efforts to cover their tracks.

## 3. What is cyber security?

All types of organizations, such as medical, financial or education institutions utilize the network for collecting, processing, storing, and sharing vast amounts of digital information. The protection of this information is vital for national security and economic stability of any country.

Computer security, cyber security or information technology security (IT security) is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from unauthorized use or harm as well as from the disruption or misdirection of the services they provide.

Cyber security can be described as the collective methods, technologies, and processes to protect the confidentiality, integrity, and availability of computer systems, networks and data from both external and internal threats, cyber-attacks or unauthorized access as well as from disruptions caused due to natural disasters.

On a personal level, you need to safeguard your identity, your data, and your computing devices. At the corporate level, it is everyone's responsibility to protect the organization's reputation, data, and customers. At the state level, it is to ensure national security and the safety and well-being of the citizens.

## 4. The need for cyber security

Anything, once posted online, can live forever in the cyber space, even if you were able to erase all the copies in your possession. All those personal information can be made public and be used in malicious ways to spoil your social image.

If a hacker (or hacking group) can gain access to any company's website, they can vandalize it by posting untrue information and ruin the company's reputation that took years to build. If the website is down frequently for longer time, the company may appear unreliable and lose credibility leading to loss of revenue.

## 5. What is your data?

Your online identity is who you are in cyberspace. Any information which can uniquely identify you as an individual is your data such as your name, date and place of birth, medical, educational, financial, and employment information. This data includes the pictures and messages that you exchange with anybody online.

But do you know where your data is?

## 6. Data Storage

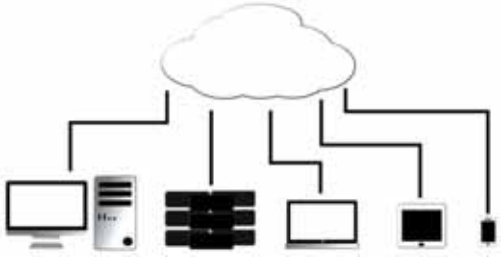
Data storage essentially means that files and documents are recorded digitally and saved in a storage system for future use. Broadly there are 3 types of data storage.

### 6.1 Direct Attached Storage (DAS)

Direct attached storage (DAS) includes types of data storage that are physically connected to your computer. This storage is generally accessible to only a single machine.

### 6.2 Network Attached Storage (NAS)

Network attached storage (NAS) allows multiple machines to share storage over a network. The key benefit of NAS is to keep the data in a centralized location and improve collaboration among connected machines.



### 6.3 Cloud Storage

Complete cloud-based or online storage solutions offer virtual data storage and convenient access to your materials from anywhere and not just a local computer or external hard disk.

### 6.4 Data Centre - Physical & Cloud based

**Definition:** A data centre is a facility composed of networked computers and storage that businesses and other organizations use to organize, process, store and disseminate large amounts of data and applications. Every organization requires a Data Centre irrespective of their size or industry.

As information technology (IT) operations started becoming complex, organizations felt the need of controlling their IT resources. With the availability of inexpensive networking equipment it became possible to use a hierarchical design that put the servers in a specific room inside the company. The term "data centre" became popular as applied to specially designed computer rooms.

A physical Data Centre is traditionally a set of highly controlled computing infrastructure, where a dedicated space within a building, or a group of buildings are used to store the organisation's information as well as other applications which are integral to their functioning. To keep all the hardware and software updated and running, a Data Centre requires a significant amount of associated infrastructure including ventilation and cooling systems, uninterruptible power supplies, backup generators, and more.

Most modern data centre infrastructures have evolved from on-premises physical servers to virtualized infrastructure that support multi-cloud environments, except where regulatory restrictions require an on-premises data centre without internet connections.


A cloud Data Centre is significantly different from a traditional Data Centre. There is nothing similar between these two computing systems other than the fact that they both store data. A cloud Data Centre is **not** physically located in a particular organization's office - it's all online! When your data is stored on cloud servers, it automatically gets fragmented and duplicated across various locations for secure storage. In case there are any failures, your cloud services provider will make sure that there is a backup of your backup as well.

A traditional Data Centre involves various purchases, including the server hardware and networking hardware and also needs replacement of these hardware as they get outdated. Additionally it needs staff to oversee its operations. While in cloud servers, you are essentially using someone else's hardware and infrastructure which saves a lot of money. In addition, you don't have to take care of miscellaneous factors relating to maintenance. But a traditional Data Centre allows you flexibility in terms of the equipment you choose, so you know exactly what software and hardware you are using. This facilitates later customizations since there is nobody else in the equation and you can make changes as you require.

With cloud server, accessibility may become an issue sometimes. If at any point of time you don't have an Internet connection, then your remote data will become inaccessible. However, realistically such instances of no Internet connectivity may be very few.

In cloud data centre, anyone with an internet connection can make inroads into your repository. The advantage of traditional data centre is that you have total control over your data and equipment, which makes it safer to an extent. However, in reality most cloud service providers leave no stone unturned to ensure the safety of your data.

Physical data centre is usually underutilized because of a lack of planning on Server Capacity and Network Capacity. Provisioning based on overestimated demand leads to underutilisation of costly resources. In a traditional data centre, each server is devoted to a specific function. For instance, an e-mail server deals only with e-mail and a payroll server handles only payroll. The average utilization ratio of many hardware devices installed in data centres is around 30% or even below thus wasting costly resources.

Virtualization technology allows users to free up idle server capacity quickly without costly expansion, relocation, or new construction. It provides different solutions by offering an opportunity to consolidate multiple underutilized volume servers onto fewer physical servers.

On the other hand cloud service providers have many flexible plans to suit your requirements, and you can buy more storage as and when you need it. You can also reduce the amount of storage you have, if that's no longer required by you.

Large Cloud data centres comprise of many thousands of servers and most of the time these servers are underutilized. For cloud data centres, resource allocation and utilisation is managed using Dynamic Resource Management Algorithm (DRMA).

Ministry of Electronics and Information Technology, Government of India (MeitY) has empanelled the Cloud Service Providers (CSPs) who offer the "Basic Cloud Services" under at least one of the Cloud Deployment Models defined by MeitY. The details of empanelled CSPs are available here:

https://www.meity.gov.in/writereaddata/files/Contact%20CSP%20_Final%20updated_05.04.2021.pdf

## 7. The CIA Triad


Confidentiality, Integrity and Availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

### 7.1 Confidentiality

Confidentiality or privacy ensures the privacy of data by restricting access through authentication encryption. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data.

### 7.2 Integrity

Integrity assures that the information is accurate, consistent and trustworthy during its entire life cycle. Data must be unaltered during transit and not changed by unauthorized entities. File permissions and user access control can prevent unauthorized access. Version control can be used to prevent accidental changes by authorized users. Backups must be available to restore any corrupted data.

### 7.3 Availability

Availability ensures that the information is accessible to authorized people. Maintaining equipment, performing hardware repairs, keeping operating systems and software up

to date, and creating backups ensure the availability of the network and data to the authorized users.

## 8. Levels of cyber crimes

### 8.1 Cybercrime

Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

### 8.2 Cyber-attack

Often involves politically motivated information gathering.

### 8.3 Cyber-terrorism

A widely acceptable definition of cyber terrorism is "a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda."

### 8.4 Cyber-warfare

Cyber-warfare is an Internet-based conflict conducted in and from computers and the networks connecting them, waged by nations or their proxies against other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against government and military networks of other nations in order to cause damage or disrupt services, such as shutting down a power grid. Cyber-warfare can destabilize a nation, disrupt commerce, and citizens may lose confidence in the government's ability to protect them.

## 9. Types of Attackers

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. They are interested in everything, from credit cards to product designs and anything with value. Attackers attempt to access data, functions, or other restricted areas of the system to expose, alter, disable, destroy, steal or gain information through unauthorized access or make unauthorized use of an asset.

## 9.1 Script Kiddies

They are usually unskilled attackers, often using existing scripts or instructions such as a web shell, found on the Internet, to launch attacks mostly out of curiosity. Script kiddies usually don't understand the inner workings of software and computer networking. They rely on software or scripts written by others and don't possess the knowledge or know-how to modify or produce their own software. They may be using basic tools, but the results can still be devastating.

## 9.2 Hackers

A computer hacker is a computer expert who uses his/ her technical knowledge to gain access to a system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more. Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed. Depending on their intention, these attackers are classified as white, gray, or black hats.

- **9.2.1 White Hat Hackers:** These are ethical hackers who use their programming skills for good ethical and legal purposes. The white hat attackers break into networks or computer systems to discover weaknesses so that the security of these systems can be improved. These break-ins are done with prior permission and any results are reported back to the owner.
- **9.2.2 Black Hat Hackers**: These are unethical criminals who exploits vulnerabilities to compromise computer and network systems for illegal personal, financial or political gain, or for other malicious reasons.
- **9.2.3 Grey Hat Hackers:** Grey hat attackers are somewhere between white and black hat attackers. They do unethical things, but not for personal gain or to cause damage. A grey hat hacker may disclose a vulnerability to the affected organisation after having compromised their network. This allows the organisation to fix the problem.

## 9.3 Organized Hackers

These hackers include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused

on control, power, and wealth. The criminals are highly sophisticated and organized, and they may even provide cybercrime as a service to other criminals. Hacktivists make political statements to create awareness to issues that are important to them. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

### 9.4 Legal aspect of ethical hacking

Ethical hacking is a pre-emptive action for hacking and the person who performs it is called an ethical hacker. Theoretically, both are the same because the underlying principle in both is to intrude upon the computer data of another but the difference lies in the intention and permission. The term "Ethical hacking" has always been controversial as the two words "ethical" and "hacking" are themselves contradictory.

Hacking is a wrongful act under Indian legal system. But before going into the legality of ethical hacking, we have to keep in mind that hacking and ethical hacking are different. Ethical hacking is an authorized simulated cyber-attack on a computer system, performed to evaluate the security of the system. That is why the activity may better be referred as Anti-hacking.

Before conducting any ethical hacking / anti hacking activity to check about the strength of the computer system and/ or network to withstand any hacking / intrusive effort, a prior written agreement has to be signed by the entity to be tested and the ethical/ anti hacker. The written agreement is a proof that the ethical / anti hacker has a legal right to exploit the organisation's security vulnerabilities and gain access to the system and thereby advice the organisation to make their IT assets cyber safe.

## 10. Sub-domains of cyber security

Various types of systems are connected in the network. An effective and efficient cyber security posture requires coordinated efforts across all its information systems. Cyber security can be classified in the following sub-domains:

### 10.1 Application Security

Application security (short AppSec) includes all tasks that introduce a secure software development life cycle. It involves implementing various defences within all software and services used within an organization against a wide range of threats. It means designing secure application architectures, writing secure code, implementing strong data input validation, threat modelling, etc.

### 10.2 Internet security

Internet security encompasses the Internet, browser security, web site security, and email security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures against attacks over the Internet.

### 10.3 Cloud Security

Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from theft, leakage and deletion. It refers to designing secure cloud architectures and applications for cloud service providers such as AWS, Google, Azure, etc.

### 10.4 Mobile Security

Mobile security, or more specifically mobile device security, is the protection of both organisational and personal information stored on mobile devices like cell phones, tablets and laptops from threats associated with wireless computing such as unauthorised access, malware etc.

### 10.5 Network Security

Network security involves implementing both hardware and software mechanisms to protect the network and infrastructure from unauthorized access, disruptions, and misuse. In simple terms it is a set of rules and configurations designed to protect the confidentiality, integrity and accessibility of computer networks and data using both software and hardware technologies. Network security is used to prevent unauthorized or malicious users from getting inside your network.

### 10.6 Identity Management and Data Security

Identity management and access control is the discipline of managing access to enterprise resources to keep systems and data secure. Identity management includes frameworks, processes, and activities that enables authentication and authorization of legitimate individuals to access information systems within an organization. Data security involves implementing strong information storage mechanisms that ensure security of data at rest and in transit.

### 10.7 Endpoint security

The connection of laptops, tablets, mobile phones, Internet-of-things devices, and other wireless devices to corporate networks creates attack paths for security threats. Endpoint security is the practice of safeguarding endpoints or entry points of end-user devices such as desktops, laptops, and other remotely bridged devices from being exploited by malicious actors and campaigns. Endpoint protection platforms (EPP) work by examining files as they enter the network.

### 10.8 Disaster recovery and business continuity planning (DR&BC)

DR&BC deals with monitoring, alerts and plans that ensures continuity of operations with minimal downtime during and after any kind of a disaster as well as resuming lost operations and systems after an incident. Business continuity focuses on keeping the business operational during a disaster, while disaster recovery focuses on restoring data access and IT infrastructure after a disaster.

### 10.9 User education

Formally training individuals regarding cyber threats and computer security is essential for raising awareness about industry best practices, organizational procedures and policies as well as monitoring and identifying malicious activities.

## 11. The vulnerability landscape

Security vulnerabilities are all kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it. An exploit is the term used to

describe a program written to take advantage of a known vulnerability. The act of using an exploit against a vulnerability is referred to as an attack. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

## 11.1 Hardware vulnerabilities

Hardware vulnerabilities are often introduced by hardware design flaws. They are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and a physical security are sufficient protection for the everyday user.

## 11.2 Software vulnerabilities

Software vulnerabilities are usually errors in the operating system or application code. Unfortunately, testing and manual code reviews cannot always find every vulnerability. The operating system producers release patches and updates almost every day. Updates for applications like web browsers, mobile apps and web servers are also very common. The goal of software updates is to stay current and avoid exploitation of vulnerabilities. Most software security vulnerabilities may be classified into the following categories:

- **11.2.1 Race conditions :** A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or proper timing and a computing system that's designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously such as two threads access a shared variable at the same time.
- **11.2.2 Buffer overflow :** Buffers are memory areas allocated to an application. Buffer overflow occurs when data is written beyond the limits of a buffer and the application accesses memory allocated to other processes. This can lead to a system crash.
- **11.2.3 Non-validated input :** Programs often work with data input. This data coming into the program could have malicious content, designed to force the program to behave in an unintended way.
- **11.2.4 Weaknesses in security practices :** Systems and sensitive data are often protected through techniques such as authentication, authorization, and encryption.

Developers are advised to use security libraries that have already created, tested, and verified. Attempts to create new security algorithms may lead to introduce vulnerabilities.

- **11.2.5 Access-control problems :** Access control is the process of controlling who does what, who can access which resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

Nearly all access controls and security practices can be breached if the attacker has physical access to target equipment. To protect the machine and the data it contains, physical access must be restricted and encryption techniques must be used to protect data from being stolen or corrupted.

## 12. The weapons of cyber criminals

So, how do malicious actors gain control of computer systems? Here are some common techniques used to threaten the cyber world.

### 12.1 Social Engineering

Social engineering, in the context of information security, is the psychological manipulation of people to perform actions or divulge confidential information. The aim is to gather as much as possible information about the potential victim and then use that information for executing various kinds of phishing attacks.

- **12.1.1 Pretexting** is a type of social engineering attack that involves an imaginary situation, or pretext, invented by an attacker in order to convince a victim to divulge private information which the victim would typically not give outside that pretext.
- **12.1.2 Quid-pro-quo** or Something for Something attack is when an attacker requests personal information from a party in exchange for a benefit, like a free gift.
- **12.1.3 Tailgating attack** is a social engineering attempt by cyber threat actors in which they trick employees into helping them gain unauthorized access into a restricted area where access is controlled by software-based electronic devices.

## 12.2 Malware

Malware is short for malicious software. One of the most common cyber threats, malware is a code that a cybercriminal or hacker has created to steal data, bypass access controls, or compromise a system of a legitimate user. Malware is often spread via unsolicited email attachments or legitimate-looking downloads. Below are a few common types of malware:

- **12.2.1 Spyware :** This malware secretly track and records information about a person or organisation and send it to another entity. Spyware includes activity trackers, keystroke collection, and data capture. Spyware often modifies security settings.
- **12.2.2 Adware :** Advertising supported software is designed to automatically display unwanted advertisements. Some adware is designed to deliver advertisements only but it is also common for adware to come with malware.
- **12.2.3 Bot :** Derived from the word robot, a bot is a malware designed to automatically perform action much faster than human. Several computers are infected with bots which are programmed to quietly wait for commands provided by the attacker.
- **12.2.4 Rootkit :** This malware is designed to modify the operating system to create a backdoor through which attackers access the computer remotely.
- **12.2.5 Ransomware :** This malware encrypts victim's files and sometimes lock the computer. Then demands a ransom from the victim to restore access to the data. Users are shown instructions for how to pay a fee to get the decryption key.
- **12.2.6 Scareware :** is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying and downloading unnecessary potentially dangerous software, such as fake antivirus etc. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation. If the user agrees his or her system will be infected with malware.

- **12.2.7 Virus :** A self-replicating executable code that attaches itself to other clean files and spreads throughout a computer system, infecting files with malicious code. Most viruses require end-user activation and can activate at a specific time or date.
- **12.2.8 Worms :** Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation.
- **12.2.9 Trojan horse :** A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. Often, Trojans are found in image files, audio files or games. A Trojan horse differs from a virus because it binds itself to non-executable files. Unlike viruses, Trojan horses do not replicate themselves.

## 12.3 Phishing

Phishing is when cybercriminals sends fraudulent email to victims that appear to be from a legitimate trusted source asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information. There are many forms of phishing.

- **12.3.1 Spear phishing :** Spear phishing is attacking well-researched targets where emails are customised for a specific person. The attackers often gather personal data and research on the target's interests before sending the email. The aim is to either infect devices with malware or convince victims to hand over information or money.
- **12.3.2 Whaling :** Whaling refers to spear-phishing attacks aimed particularly at senior executives and other high-profile targets. Whaling attack emails are highly customized and personalized, and they often incorporate the target's name, job title or other relevant information obtained from a variety of sources.
- **12.3.3 Voice phishing :** Voice phishing or 'vishing' is a form of phone fraud, using social engineering over the telephone claiming to be from banks or other reputed institution. After gaining the trust, they ultimately seek personal and financial information for the purpose of financial gain.

Example: Sometimes attackers send messages that claimed to be from a bank telling users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a voice over IP service) is dialled, the attacker prompts the caller to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

- **12.3.4 Clone phishing :** Clone phishing is a type of phishing attack where the content and recipient address(es) of a legitimate, and previously delivered email, containing an attachment or link is used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original.
- **12.3.5 Link manipulation :**

  i. Disguise emails as coming from some reputed and trustworthy organization.

  ii. Misspelled URLs.

  iii. Use of subdomains.

  Example: http://www.yourbank.loan.com/. It appears the URL will take you to the loan section of the "yourbank" website. Actually this URL points to the "yourbank" (i.e. phishing) section of the "loan" website.

  iv. The displayed text for a link suggest a reliable destination, while the link actually goes to the phishers' site. Many desktop email clients and web browsers will show a link's target URL in the status bar while hovering the mouse over it, which can be overridden by the phisher.

  v. Internationalized domain names (IDN) can be exploited via IDN spoofing or homograph attacks, to create web addresses visually identical to a legitimate site.

- **12.3.6 Filter evasion :** In this method, attackers use images instead of text to make it difficult for anti-phishing filters to detect the text commonly used in phishing emails. Highly sophisticated anti-phishing filters are able to recover hidden text in images using OCR (optical character recognition).

- **12.3.7 Tabnagging :** Tabnabbing is a phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine.
- **12.3.8 Website forgery :** Here JavaScript commands are used to modify the URL address bar of a website. This is achieved either by placing a portrait of a legitimate URL over the address bar or by blocking the original bar and opening up a new one.

### 12.4 Wi-Fi Password Cracking

This is the process of discovering the password used to protect a wireless network.

- **12.4.1 Brute-force attacks :** The attacker tries several possible passwords with the hope to guess the combination correctly. Because brute-force attacks take time, complex passwords take much longer to guess. Password brute-force tools include Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
- **12.4.2 Network sniffing :** packet analyser is a computer program that can intercept and log network traffic by listening and capturing packets sent over the network. It is easy for the attacker to discover the password if the password is being sent unencrypted (in plain text). If the password is encrypted, the attacker may still be able to reveal it by using a password cracking tool.

### 12.5 Man-In-The-Middle (MitM)

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between a user and an application in order to capture user information before relaying it to its intended destination.

### 12.6 Man-In-The-Mobile (MitMo)

A variation of man-in-middle, MitMo is a type of attack used to take control over a mobile device. For example an exploit with MitMo capabilities, allows attackers quietly capture 2-step verification SMS messages sent to users.

## 12.7 SQL injection

An SQL (Structured Query Language) injection is a type of cyber-attack used to take control and steal data from a database. SQL injection usually occurs when you ask a user for input, like their username/user-id, and instead of a name/id, the user gives you a malicious SQL statement that you will unknowingly run on your database.

## 12.8 Cross-site scripting (XSS)

Cross-site scripting is a type of injection attack which is typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users.

## 12.9 SEO Poisoning

Also known as search engine poisoning, is a method that involves creating malicious web pages packed with trending keywords in an effort to trick search engines to get a higher ranking in search results. The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or perform social engineering.

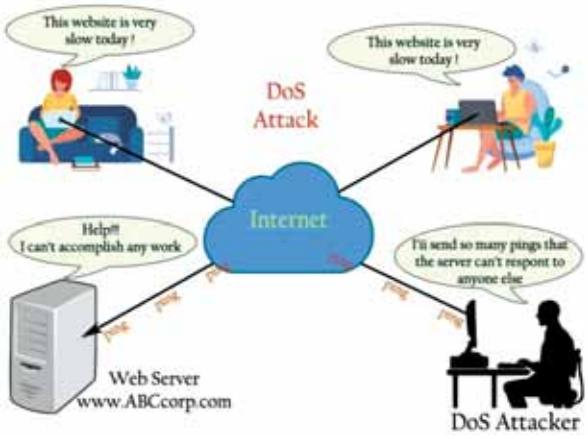
## 12.10 Vulnerability Exploitation

Exploiting vulnerabilities is another common method of infiltration. Attackers will scan targeted computers to gain information about their operating system, version and a list of services running on it, and then look for any known vulnerabilities specific to that version of OS. When a vulnerability is found, the attacker exploit that. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

## 12.11 Piggyback attack

A Piggyback Attack is specifically where an attacker gains access to a system using intervals of inactivity in another user's legitimate connection when said user is not using the account. The attacker exploits weaknesses of a network connection and force entry into a system using a registered users connection. It is also called a "between the line attack" or "piggyback-entry wiretapping".

## 12.12 Denial-of-service attack (DoS)




A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. Following are the 2 methods of DoS attack.

- **12.12.1 Overwhelming Quantity of Traffic :** when a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or a crash of a device or service.
- **12.12.2 Maliciously Formatted Packets :** when a maliciously formatted packet is sent to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.

## 12.13 Distributed Denial-of-Service (DDoS)

A Distributed DoS Attack (DDoS) is similar to a DoS attack but originates from multiple, coordinated sources. This type of attack takes advantage of the specific capacity limits that apply to any network resources. In DDoS attack an attacker builds a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems. The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs handler systems to make the botnet of zombies carry out a DDoS attack.

## 12.14 Remote code execution

Remote code execution is an attacker's ability to execute arbitrary commands or code on a target machine or in a target process. An arbitrary code execution vulnerability is a security flaw with system level privileges on a server that possesses the appropriate weakness.

## 12.15 Side-Channel Attack (SCAs)

A side-channel vulnerability bypasses a computer's account permissions, virtualization boundaries and protected memory regions and extract sensitive device information from a chip or a system, through measurement and analysis of physical parameters. Timing information, power consumption, electromagnetic emission, execution time or even sound can provide an extra source of information, which can be exploited. Side channel intrusion can also happens in end-to-end encrypted and secured communication channels viz. WhatsApp, Facebook messenger etc.

## 12.16 Keyloggers

Keyloggers are a type of monitoring software designed to capture keystrokes made by a user typically covertly so that the person using the keyboard is unaware that their actions are being monitored. A keylogger can be installed from email attachment or via a web page script which exploits a browser vulnerability. The keystroke loggers record the information you type into a website or application and send it to the person who is operating the logging program.

Hardware keyloggers are a device plugged inline between a computer keyboard and a computer. They are often installed in the back of a computer, or in other places which are normally not examined. Hardware keyloggers cannot be detected through any kind of anti-virus software or other software investigation. They are physically detectable, though no one usually thinks to check for them.

## 12.17 Blended Attack

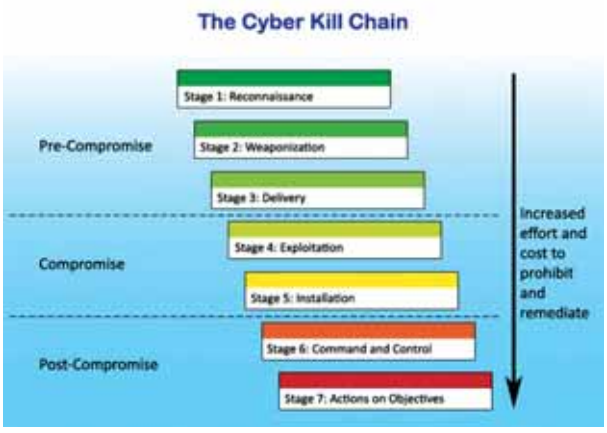
Most sophisticated cyber attacks are blended attacks in which attackers use a mix of several different attack techniques at once. Malware that are a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes are used.

## 13. The Cyber Kill Chain

Developed by Lockheed Martin Corporation (an American aerospace, defense, information security, and technology company), as a security framework for incident detection and response, the "cyber kill chain is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. Each stage demonstrates a specific goal. The Cyber Kill Chain consists of 7 following stages:

### Stage 1: Reconnaissance

In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.




### Stage 2: Weaponization

In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or it can focus on a combination of different vulnerabilities.

### Stage 3: Delivery

This step involves transmitting the weapon to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

### Stage 4: Exploitation

In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

### Stage 5: Installation

Malware and backdoors are installed on the target as an access point for the intruder / attacker.

### Stage 6: Command and Control

Remote control of the target is gained through a command and control channel or server. The malware gives the intruder / attacker access in the network/system.

### Stage 7: Actions on objectives

The attacker performs malicious actions like encryption for ransom, information theft, or executes additional attacks on other devices from within the network by working through the Kill Chain stages again.

According to Lockheed Martin, understanding the stages of Kill Chain allowed them to put up defensive obstacles, slow down the attack, and ultimately prevent the loss of data.

## 14. Infrastructure Security Assessment

IT infrastructure and network is of vital importance for any company to run the operation successfully. An infrastructure penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. Infrastructure security audit helps the process of protecting the underlying networking infrastructure by installing preventative measures to deny unauthorized access, modification, deletion, and theft of resources and data.

## 15. Web Application Security Assessment

In today's world websites play a big role for any business in attracting clients. It is the responsibility of the website owner to make the customers feel safe while browsing or buying anything online from his site. Thus website security check is very important.

The purpose of web application audit is to review an application's codebase to determine whether the code is doing something it shouldn't. Audits may also evaluate whether code can be manipulated to do something inappropriate and whether the apps are communicating sensitive data.

The application security audit is a simulated, realistic hacker attack on an application and its associated front- and back-end systems to find out all security vulnerabilities during the testing time. A superior web application audit should identify whether developers have implemented appropriate security precautions or not.

Open Web Application Security Project (OWASP) is an international non-profit organization that educates software development teams on how to conceive, develop, acquire, operate, and maintain secure applications. According to the OWASP, the top 10 Most Common Software Vulnerabilities are as below:

### 15.1 Insufficient Logging and Monitoring

Insufficient logging and monitoring processes are dangerous. This leaves your data vulnerable to tampering, extraction, or even destruction.

### 15.2 Injection Flaws

Injection flaws occur when untrusted data is sent as part of a command or query. The attack can then trick the targeted system into executing unintended commands. An attack can also provide untrustworthy agents access to protected data.

### 15.3 Sensitive Data Exposure

Sensitive data - such as addresses, passwords, and account numbers - must be properly protected. If it isn't, untrustworthy agents take advantage of the vulnerabilities to gain access.

### 15.4 Cross-Site Scripting (XSS) Flaws

Untrustworthy agents can take advantage of cross-site scripting flaws to execute their own scripts in the targeted system. In general, cross-site scripting flaws happen in one-of-two ways:

- Whenever an application includes untrusted data in a new web page without proper validation.
- Whenever an existing webpage is updated with user-supplied data using a browser API that can create HTML or JavaScript.

### 15.5 Using Components with Known Vulnerabilities

Components are made up of libraries, frameworks, and other software modules. Often, the components run on the same privileges as your application. If a component is vulnerable, it can be exploited by an untrustworthy agent.

### 15.6 Broken Authentication

Authentication and session management application functions need to be implemented correctly. If they aren't, it creates a software vulnerability that can be exploited by untrustworthy agents to gain access to personal information.

### 15.7 Broken Access Control

User restrictions must be properly enforced. If they are broken, it can create a software vulnerability. Untrustworthy agents can exploit that vulnerability.

### 15.8 XML External Entities (XXE)

XML is a popular data format that is used in web services, documents, and image files. You need an XML parser to understand XML data. But if it's poorly configured and the XML input that contains a reference to an external entity, it's dangerous. An untrustworthy agent can cause a DoS.

### 15.9 Security Misconfiguration

Security misconfigurations are often the result of:

- Insecure default configurations.
- Incomplete or impromptu configurations.
- Open Cloud storage.
- Misconfigured HTTP headers.
- Wordy error messages that contain sensitive information.

### 15.10 Insecure Deserialization

Deserialization flaws often result in remote code execution. This enables untrustworthy agents to perform replay, injection, and privilege escalation attacks.

## 16 Security operations

Security operations refers to the entire function of investigating, detecting, preventing and responding to cyber threats around the clock.

### 16.1 Critical information Infrastructure (CII)

Critical Information Infrastructure (CII) is defined as those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy, public health and social well-being of a nation. These include sectors like Defence, Banking, Aviation, Power, Telecomm and Network, Data Centres etc.

### 16.2 Incident

A security incident is a warning that there may be a threat to information or computer security. The warning could also be that a threat has already occurred. Examples of computer security incidents include attacks such as denial of service attacks and malicious code, which includes worms and viruses. Unauthorized access by someone who is not allowed to access a computer system is also considered a potentially threatening computer security incident.

### 16.3 Threat Intelligence

Threat intelligence, or cyber threat intelligence, is the information that an organization uses to understand the threats that have, will, or are currently targeting the organization. This information is used to prepare, prevent, and identify cyber threats attempting to take advantage of valuable resources.

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cyber security threats. ATT&CK is a structured list of known attacker behaviours that have been compiled into tactics and techniques and expressed in a handful of matrices.

### 16.4 Mitigation techniques

Cyber security threat mitigation refers to policies and processes put in place by companies to help prevent security incidents and data breaches as well as limit the extent of damage when security attacks happen.

### 16.5 Security Operations Centre

A security operations centre (SOC) is a centralized unit within an organization employing people, processes, and technology to continuously monitor its entire IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside and improve the organization's security posture while preventing, detecting, analysing, and responding to cyber security incidents. SOC teams are charged with monitoring and protecting the organization's assets including intellectual property, personnel data, business systems, and brand integrity.

## 17. Security best practices

The technological landscape is evolving rapidly and as a result adoption of software is increasing in almost all sectors. More and more information is becoming digital and accessible through the omnipresent internet. All these information are highly valuable to criminals and evil doers. But their effort to gain unauthorised access to the information can be mitigated by implementing right security measures and by practicing cyber hygiene.

Here are the cyber security best practices to prevent a breach:

### 17.1 For organisations

1. **Security awareness:** Security breach can happen if the employees make malicious actions intentionally or even unintentionally. A strong cyber security strategy and the best technical defences may fail if the employees are not educated on cyber security and incidence reporting. Educating employees and raising awareness on security best practices through seminars, classes, online courses is the best way to reduce negligence and the potential of a security violation.

2. **Perform risk assessments:** Organizations should perform a formal risk assessment periodically to identify security defects and vulnerabilities. Carrying out a risk assessment allows an organization to implement security control tools and prevent security breach.

3. **Ensure software patch management/updates:** It is crucial for organizational IT teams to perform identification, classification, remediation, and mitigation of vulnerabilities within all software and networks that it uses, to reduce threats against their IT systems. Software vendors periodically release updates which patch and mitigate these vulnerabilities. Therefore, keeping IT systems up-to-date helps protect organizational assets.

4. **Use the principle of least privilege (PoLP):** The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access or permissions to perform his/her job functions. The principle of least privilege is a fundamental step in protecting privileged access to high-value data and assets. Also, two-factor authentication should be used for all high-level user accounts that have unrestricted permissions.

5. **Enforce secured password policies:** Organizations should enforce the use of strong passwords that adhere to industry recommended standards for all employees. The passwords must also be changed periodically. Furthermore, password storage should follow industry best practices of using strong hashing algorithms.

6. **Implement a robust business continuity and incidence response (BC-IR) plan:** Business continuity plan outlines how a business will remain operational during or after an unplanned disruption in service. An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents like cybercrime, data loss, and service outages that threaten daily work. Having a good BC-IR plans and policies in place will help an organization effectively respond to cyber-attacks and security breaches while ensuring critical business systems remain online.

7. **Backup data :** Backing up all data on regular basis will make sure all sensitive data is not lost after a security breach. Attacks such as injections and ransomware, compromise the integrity and availability of data. Backups can help protect the data in such cases.

8. **Use encryption for data at rest and in transit :** All sensitive information should be stored and transferred using strong encryption algorithms. Encrypting data ensures confidentiality. Effective key management and rotation policies should also be put in place. All web applications/software should employ the use of SSL/TLS.

9. **Implement strong input validation :** Software and applications are designed to accept user input. Strong input validation can mitigate the chance of malicious input being entered and various types of injection attacks.

10. **Detecting Attacks in Real Time :** When a hacker exploits a flaw in a piece of software before the creator can fix it, it is known as a zero-day attack. A successful defence against zero-day attack can be achieved by performing real time scan from edge to endpoint.

11. **Protecting Against Malware :** Network administrators must constantly monitor the network for signs of malware or behaviours that reveal the presence of an advanced persistent threats (APT).

    The common malware symptoms are as below:

    - There is an increase in CPU usage.
    - There is a decrease in computer speed.
    - The computer freezes or crashes often.
    - There is a decrease in Web browsing speed.
    - There are unexplainable problems with network connections.
    - Files are modified.
    - Files are deleted.

- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.


## 17.2 Password management

A password is typically a secret string of characters, usually used to confirm a user's identity. By verifying the password a system can differentiate between authorized and unauthorized user before giving access to a resource. Your password is your first line of defense against hackers and unauthorized access to your accounts. The strength of your passwords directly impacts your online security. The following are the best practices for your password management:

1. Create strong password with a minimum length of 10 characters using the combination of letters, numbers and special characters such as ! @ # $ % ^ & * ( ). Remember weak passwords are a gift to criminals.

2. Never use common pattern of alphabets and numbers such as abc123, 12345678, 777, 654321 etc.
3. Don't use common easy-to-guess passwords such as nick names of self, friends, family members, pets name, favourite player name, birthday of anyone, birth year, etc.
4. Do not use computer names or account names.
5. Do not use dictionary words like sunshine, monkey, or football or names in any languages. Try combining two or more unrelated words.
6. Switching a letter for a symbol such as p@ssword is an obvious trick hackers know well.
7. Avoid common or famous statements, for example, lyrics from a popular song.
8. Using the same password for all your online accounts is like using the same key for all your locked doors. Don't use the same password for multiple accounts, especially for the most sensitive ones, such as bank accounts, credit cards, tax records etc. Even if one password gets hacked, your other accounts will not be compromised.


9. Since we all have more than one online account, and each account having a unique password, there will be a lot of passwords to remember. The best solution is to use a password manager. A password manager stores and encrypts all of your different and complex passwords and help you to log into your online accounts automatically. You only need to remember your master password to access the password manager.
10. Don't reuse old passwords. Re-used passwords are easier to crack through observing key-log patterns or through social engineering.

11. Use Passphrase Rather Than a Password. Choose a meaningful statement rather than a word. The longer length makes passphrases less vulnerable to brute force attacks.

12. Be very careful while entering passwords in front of others. Improve typing accuracy so that you can enter password quickly before anybody can follow the keystrokes.

13. Never select the "Save password" option prompted by your web browser. There are many websites that prompts you to save your login credentials or payment detail for future use. Decline to them.


14. Don't store the passwords in readable form in computers, notebook, notice board etc.

15. Never disclose any password with anyone. Change your password immediately if you suspect that it has been compromised.

You can check the strength of your password and how long it would take to crack your password at https://howsecureismypassword.net or at other similar sites like https://password.kaspersky.com or https://www.my1login.com/resources/password-strength-test

## PASSWORD DO'S AND DON'TS

| Do | Don't |
|---|---|
| Do combine two or more unrelated words. Change letters to numbers or special characters. | Don't use the word "password," or any combination of it. "P@ssword!" is easy for hackers to guess. |
| Do make your passwords at least 8 characters long. Aim for 12-15 characters. | Don't use short, one-word passwords, like sunshine, monkey, or football. |
| Do use a combination of upper- and lower-case letters, numbers, and symbols. | Don't place special characters (@, !, 0, etc.) only at the beginning or at the end. |
| Do include unusual words only you would know. It should seem nonsensical to other people. | Don't include personal information like your birthdate, address, or family members' names. |
| Do keep your passwords protected and safe, like encrypted in a password manager. | Don't share your passwords. Don't put them on a piece of paper stuck to your computer. |
| Do spread various numbers and characters throughout your password. | Don't use common patterns like 111111, abc123, or 654321. |
| Do create unique and complex passwords for every site. | Don't use the same password everywhere. |

### 17.3 Best practices for emails, messages, attachments and links

Phishing attacks is "a technological medium to exploit human weaknesses" and that technology cannot fully compensate for human weaknesses.

Every day, millions of emails and messages are sent to communicate with friends and conduct business. Criminals also send fraudulent emails containing malicious links and attachments, pretending to be from a legitimate sender and with a valid important reason.

However there are different techniques to identify phishing attempts and you can follow the best practices to prevent the phishing attacks.

1. Many companies, services, apps, and websites ask for your email. But it's not always required. For example, many online shopping portals allow you to check out as a guest. Don't create an account if it's not required.
2. If a website requires an email address, use services like 10minutemail or getnada, which allow you to create a temporary one.
3. Create a different email to sign up for promotions and newsletters.
4. Don't include personal information that could be used to identify you in that email address, like your name or birthday.
5. One of the top techniques used by hackers is to create an email with a familiar name. Check the sender's name. Are there unusual initials, spaces or misspellings in the person's name?
6. Always double check the e-mail sender's address. Even if you know the name of the person, verify if it is the correct e-mail address.
7. Fake or scam emails are always sent from a random private email address which do not belong to the official domain of any reputed organisation, bank or business. Check the domain of the email.
8. Look for the manipulated domains. Check for the spelling of the domain, like email@domian.com
9. Do not open emails from unknown sender which do not seem relevant to any ongoing official communication.
10. Doubt all unexpected emails.
11. Because they want to target a big audience, criminals send phishing emails which are often not personalised to the recipient and rarely use your name. Check the greeting phrase.

12. Review email content. While scammers are getting better at making their messages look more professional, but lack of consistency is very common in their emails, like odd spacing, different font styles or sizes, poor spelling and grammar or mismatching logos. Interestingly enough, the poor grammar is used purposefully to filter out the more cautious prey.
13. Emails from banks and credit card companies often include partial account numbers (usually last 4 digits). If you are contacted for verification or renew your credentials of your account through email or messages, it is sensible to contact the company directly before giving account detail.
14. Criminals often exploit specific festival times of the year or ongoing big events in their scams. Be particularly careful with any emails referencing the corona virus, as these may be phishing attempts or scams.
15. If you see an attachment that doesn't make sense, be cautious. Attachments may contain viruses including ransomware.
16. Do not click on any attachment if the e-mail sender appears suspicious or untrustworthy. Never open attachments unless you are absolutely sure they are coming from a validated sender.
17. Do not click on any link provided on the emails (or download files) from unknown people.
18. Don't allow your e-mail programs to "auto open" attachments.
19. If you have to open pdfs/docs/Excel-sheets from unknown senders, it is much better to upload them to a cloud service like Google Drive, and open via Web tools.
20. Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header). Block the attachments of file types: "exe | pif | tmp | url | vb | vbe | scr | reg | cer | pst | cmd | com | bat | dll | dat | hlp | hta | js | wsf".

21. Never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.

22. Beware of clicking on phishing URLs providing special offers like big discounts, winning prize, rewards, cash-back offers or ask you to fill up customer review form. Lucrative offers and eye-catching statements are often used to attract people's focus.

23. Avoid phone calls/ emails/ sms regarding unknown inheritance, foreign lottery, fund transfer requests from foreign country, etc.

24. A popular tactic amongst cyber-criminals is to urge you to act quickly by using various pretexts like super deals that shall last only for a short period of time. Instilling this sense of urgency is meant to make you take a decision in haste, rather than after weighing its pros and cons. Avoid.

25. Be sceptical, if you receive a mail or SMS from a delivery company claiming that you have missed a courier delivery and ask you to reschedule the delivery by clicking on a link and paying a little delivery charge. All online shopping / delivery service providers post the delivery information on their websites. Go to the shipper's actual website to see if the tracking number is real.

26. A phishing email is not like a standard email. The cybercriminal simply wants your click, and nothing else. The Unsubscribe button won't stop the email. So don't click on the Unsubscribe button. The best solution in these cases is for you to simply mark the email as spam, this will remove the mail from your inbox and block the sender from sending more spam.

27. Update spam filters with latest spam mail contents. Use specialized spam filters to reduce the number of phishing emails that reach their addressees' inboxes. These filters use a number of techniques to classify phishing emails, and reject email with forged addresses.

28. While using public/ multi-user systems, make sure that you always log out before leaving the system.

## 17.4 Safety tips for safe browsing

1. Always use pre-installed, trusted and updated web browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, etc. for web-browsing.
2. Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
3. Anyone with physical access to your computer, or your router, can view which websites you have visited using web browser history, cache, and possibly log files. This problem can be minimized by enabling the in-private browsing mode on the web browser. With private mode enabled, cookies are disabled, and temporary Internet files and browsing history are removed after closing the window or program. Most of the popular web browsers have their own name for private browser mode:
    - Microsoft Internet Explorer: InPrivate
    - Google Chrome: Incognito
    - Mozilla Firefox: Private tab / private window
    - Safari: Private: Private browsing
4. Always check for genuine https and green/grey padlock symbol to ensure that you are not being re-directed to a fake website. Yellow or red https means the website is insecure.


5. You may see the yellow warning triangle and the lock icon in the address bar while visiting a webpage that's secured with SSL. This means that the website use non-secured third-party resources, like scripts or images.

For Google Chrome, it is an indication that the browser had found insecure content on that page, either because the page contains both HTTPS and HTTP content, or because the browser detected that the website is using an obsolete encryption mechanism, such as SHA-1.

For Firefox, A gray padlock with a yellow warning triangle indicates that the connection between Firefox and the website is only partially encrypted and doesn't prevent eavesdropping. By default, Firefox does not block insecure passive content such as images; you will simply see a warning that the page isn't fully secure.

Sometimes Firefox shows a gray padlock with a red strike-through line over it, when the user reaches an HTTP page that contains a username + password log-on combination. A padlock with a red strike over it indicates that the connection between Firefox and the website is either delivered using an insecure protocol (HTTP or FTP) or that it is only partially encrypted because you've manually deactivated mixed content blocking. The site doesn't prevent against eavesdropping or man-in-the-middle attacks. Do not send any sensitive information to sites where the Site Identity button is a gray padlock with a red strike over it.

6. Check the integrity of URLs before providing login credentials or clicking a link.
7. Do not submit personal information to unknown and unfamiliar websites.
8. If there is any known Web address in any e-mail, instead of clicking them, type them in the browser and open the site. Remember, criminals can easily fool you by faking URLs.
9. Verify shortened URL. Never click on a link without knowing where the link will finally redirect you. Rather use shortened URL expander websites www.expandurl.net. The website helps users in taking an informed decision by providing the title, description and key-words of the destination web page.


10. Check for errors. Phishing websites for malicious purposes are often made hastily, therefore likely to have grammatical, punctuation, spelling or other errors.
11. While browsing, always turn ON the popup blocker in the browsers.
12. Avoid downloading unnecessary programs from anywhere, even from legitimate trusted sources.
13. Do not use torrents or download illegal content - it is a criminal offence.
14. Do not visit any illegal web-sites.
15. Always think twice before downloading audio or video content from links looking too tempting and too good to be true.
16. While you are travelling, avoid using online services which require accessing your location information.
17. Always avoid Public Wi-Fi for web-browsing.
18. Don't do office works on Public Computers or Cyber Cafes'.
19. Don't conduct financial transactions by using public computers or public Wi-Fi connections.

20. Beware of Shoulder-surfing. Don't let others watch over your shoulder while logging in or doing online transactions.
21. In Cyber Cafe, always use virtual keyboard while typing password or anything important.
22. All documents downloaded on public computers for any reason should be permanently deleted with [Shift + Delete].
23. Always ensure that you close and delete your browsing content when using public computers.
24. While working in public computers, never forget to close all browsers and logging out from all sessions before leaving.


25. For video chatting, it is always better to use Web clients inside of your browser. If you have to download and install any software, make sure that you are downloading from a legitimate website. Criminals often spoof websites and stack them with malware, which may spy into your work.
26. Note that many of the well-known video-chatting services are not end-to-end encrypted. Do not share any password or authentication details over it. There is a chance that attackers can access that information.
27. Remember to close all software that are not required during the web-meeting.
28. Connect to the internet via secure networks. Avoid open/free networks. Most Wi-Fi systems at home these days are correctly secured, but some older installations might not be.
29. Stay informed. The Anti-Phishing Working Group produces regular report on trends in phishing attacks. Also there are anti-phishing websites which publish exact messages that have been recently circulating the internet. Follow them regularly.

## 17.5 Safe use of Social Media

These days social media plays a crucial role in connecting people, developing relationships, sharing ideas, thoughts and information through virtual networks and communities. Regardless of age and gender, people are making their online presence for connecting with each other in the virtual world. Some have thousands of friends and followers spread across multiple profiles.

At the same time, cyber criminals are also active in the social media platforms creating fake profiles, posting inappropriate or illegal contents, spreading fake news, and causing harassment to legitimate users. Various undesirable incidents of "public outrage" and "mob lynching" have happened due to the viral propagation of fake news through WhatsApp and Facebook.

But ultimately, it is your responsibility to safeguard your data, your identity, and your reputation. A few simple precautions may save your big problems later.

1. Always use only one social media account for each platform i.e. WhatsApp, Facebook, Twitter, Instagram, Google Plus, etc.
2. Your username or alias is your online identity and how you present yourself to others in the virtual world. The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.
3. Share as little information as possible. You should not share information like your birth date, email address, or your phone number on your profile. The more personal information you share online, the easier it is for someone to create a fake profile in your name and take advantage of your identity.

4. Do not fill out your social media profile completely, only provide the minimum required information.
5. Do not share your login credentials with anyone.
6. Set your social media privacy settings to allow only your friends to see your activities or engage in your conversations.
7. Sometimes we set security questions like "What is your mother's maiden name?" or "In what city were you born?" which help you to retrieve you account in case you have forgotten the username or password of an online account. Better to answer these questions with false information, as long as you can remember the false answers. If you have a problem remembering them, you can use password manager to manage them for you.

Be cautious that social media profiles can actually be fake or honey-traps created to extract information through social engineering. Attackers often pose as genuine person and make a data theft attempt like a fair communication.

8. Attractive profiles of the opposite sex may be created specifically to lure you into divulging personal information. Do not add and communicate with such profiles without verification.
9. Avoid making friends with someone whom you do not know from other sources. In social media platforms only add and communicate with real persons whom you know outside of social media.
10. Do not share or post any sensitive personal private information, photo or video of yourself and others in social media or through their messenger services. Once they are published on the internet they can be downloaded and used for malicious purposes by other people without your knowledge.
11. Never disclose your travel plan, itinerary in social media. Criminal can stalk you and follow you with malicious intensions.

12. If your vacation status updates are publicly viewable, the potential burglars can also discover how long you are going to be away and get the opportunity to rob your empty house.
13. Don't share virtual meeting URLs, or screenshots from your video calls on the social media. You may accidentally be leaking information (meeting ID or other confidential information).
14. All employees, contractual staff and consultants, engaged with Government offices or on Government projects should practice extra caution to maintain confidentiality of official information on social media or at any other place.
15. Do not accept any image/ video or news received from social media to be true unless the genuineness has been verified by other sources.
16. Do not post and forward materials which appear as a statement of some event, incident, news item, statement of fact, etc, unless there has been corroboration from trusted source.
17. Do not forward any controversial communal image/video/news without verifying its genuineness or you may be criminally liable.
18. Erase your digital footprints. Close all sessions and delete all your browsing history before leaving.
19. If it appears that the matter in hand is serious, and may lead to some undesirable event, report to nearest police station.

## 17.6 Safety in Online market place

Online Shopping is easy, convenient, hassle free and comfortable. It takes just a few clicks to order a product and get it delivered to your door step. But where there's money to be found, malicious hackers will roam too.

Hackers often set up their own fake shopping websites which infect you the moment you arrive on them. But the most dangerous aspect is when you try to buy something. Completing a checkout process will give cybercriminals your most important information: credit/ debit card data (including security number), name and address. This opens you to identity theft, credit card fraud or social engineering attacks.

Here is how to be safe at online market places.

1. Do a little research to make sure you're buying from a legitimate online shop. Indications of fake shopping sites are as below:

   - **Strange URL's :** such as "the-bestonlineshopping.com" or "awesome-price.com".
   - **A strange selection of brands :** For instance, the website claims to be specialized in clothes but also sells car parts or construction materials.
   - **Prices are ridiculously low :** An online shop that has an iPhone at Rs.8000/- is most likely trying to scam you.
   - **Broken language :** Fake shopping sites will never come up with beautiful product descriptions. Spelling error or other grammatical errors are common in fake sites.

   - **Strange contact information :** If the email for customer service is "ebaysupport@gmail.com" instead of "support@ebay.com" then you can bet that online shop is fake.

2. Check that the shopping site starts with https://and notice the green/grey lock symbol, which is in the address bar at the top.
3. A phishing email with a fake offer for a desirable product is a hard thing to resist for many shoppers, so they make an impulsive decision and click on the "Order product" or "Buy now", and that's when the malware attack starts. Do not purchase from spam or phishing emails.
4. While shopping online you need to provide only two types of information: one related to payment, such as credit cards data, and second delivery address, which is usually your home or work address. Don't give internet shops more private information than they need. Be suspicious of online shops that ask for information such as: date of birth, social security number or other similar information. They don't need it to sell you things.
5. If you are a frequent online shopper, it may be difficult to remember from which site you bought a certain product. Keep a record of your purchases. Check your transaction details with the banking records.
6. Go for Cash on Delivery (COD). The safest way to pay is to give your money directly to the delivery agent instead of paying by credit card. This way, the online website won't get to have your payment information in their database, meaning a malicious hacker won't get his hands on your data if they break into the seller's website.


**For more advisories please visit: https://cscoe.itewb.gov.in/advisories**

You can also be cheated while trying to sell something in online marketplace like Olx and Quikr and instead of receiving money for selling the product you lose money from your account.

The lack of understanding of new app-based payment services and UPI is helping fraudsters to cheat the sellers and make a quick buck. Here is how to identify the fraudsters on websites like Olx, Quikr and other online market places.

7. While selling something, you may get number of calls from different numbers. But if you receive multiple calls at short intervals from several "prospective buyers" who show excessive eagerness to pay double or triple the price you quoted, it's time to practice caution.
8. Bargaining is a common practice when someone buys through Olx or Quikr. But a cheater will never bargain and will agree to pay whatever price you quote for the product you are selling. Get alert immediately.
9. Never share OTP. Always remember that you need to provide OTP or scan QR codes only when making any payments. If you are receiving payments from someone you need not provide OTP or scan QR codes.

## 17.7 Security tips for online banking transactions& Debit/Credit cards

1. Never share your net-banking credentials, passwords, Credit/ Debit card numbers, PINs, CVV/CVV2 with anyone over telephone, email or any other means even if someone claims to be from bank call centres. Your bank will never call you requesting your account numbers, PINs or passwords. They already have this information.
2. Do not share any image of your card with anyone. Do not store anywhere, as well. Never write them down on paper, in an email or in a text message. These can all be easily intercepted.
3. Do not set common PIN for mobile banking/Debit cards/Credit cards which can be easily guessed and always try to change it every 3 months.
4. Use a strong password for online banking and change passwords periodically.

5. Always make use of virtual key-pad for logging into your net-banking account.
6. When visiting your bank's website or conducting an online transaction, check your browser to verify that the green padlock and "https" symbols are active and valid. Do not enter card details in any unverified website/ application or portal.
7. Do not use public computers/ cyber café for online banking. This is never a good idea. Even if you're careful to make sure no one sees your screen and you remember to log out completely, an expert scam artist can find ways to record your activity.
8. You should avoid conducting financial transactions using public Wi-Fi.
9. For mobile banking make sure you download only verified mobile banking application of your bank.
10. Don't click links embedded in emails that claims to be from your bank. Instead, type the bank's web address in your browser and navigate from there. It is easy for scammers to rig convincing emails.
11. Never share OTP. Remember banks never ask for OTP.
12. Always read and follow your banks' guidelines on using debit or credit cards.
13. Never entertain phone calls that induce you to update your KYC over phone or else your card will be blocked. These are all fraudulent calls.
14. All banks send a transaction alert SMS on your registered mobile number every time you swipe your card or use it for an online transaction. Check the messages sincerely. In case you find these transactions have not been done by you, call the bank and report the disputed transactions immediately.
15. Keep your existing mobile number updated in Banks records so you continue to receive transactions alerts.
16. Check your account activity regularly to make sure there are no unexpected transactions. In case of discrepancies inform your Bank and ask them to freeze the card immediately.

17. Add an extra layer of security with two-factor authentication (2FA) or multi-factor authentication (MFA). Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication for account logins. On top of your username and password, 2FA requires another piece of information to verify your login credential. When you have 2FA enabled, the site will text you a code (OTP) to enter after your password. The stolen password cannot be reused on its own unless supported by other factor.

18. Always ensure that your card is swiped in your presence. Pay at the terminal instead of giving your card to a waiter for payment processing, after dining at restaurants. Do not handover your Card to anyone including company representatives.

19. Use your hand or body to cover your keypad while typing your PIN in ATM or on a payment processing machine. This will prevent shoulder surfers and pinhole cameras from observing your PIN number.

20. Watch out for skimmers. Skimmers are interesting little devices that can be placed over ATM card slots in order to steal your account information. Installing and uninstalling a skimmer is a matter of seconds. If the card slot looks peculiar, don't use it.

21. Prefer using ATM kiosks which have security guards. If there is anything at all suspicious, quit your transaction and inform the security person.

22. At the ATM, wait for your receipt to print and take it with you. Do not toss it in a trashcan. The information could be used to access your accounts.

23. Close your transaction completely before walking away from the machine.

24. Remember to collect your card after the transaction.

25. Report lost cards immediately as soon as you realize your card is missing. Call the bank and block the card and file a complaint to police as early as possible.

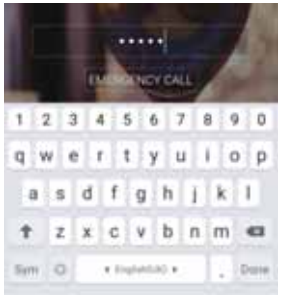
## 17.8 Safety tips for Mobile phones

Smartphones have become an essential part of everyday life. Cyber criminals are also active with a wide range of threat techniques to violate your privacy. They attack your mobile device to access your private information such as bank login credentials, saved passwords and any other information stored on your phone. You have to be very careful to protect your smartphone always.

1. Only keep the minimum necessary information in your mobile devices. Remember, if any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage such as iCloud or Google drive.
2. Always use genuine operating system.
3. Do not download any App from an untrusted sources/link.
4. Do not install and keep Any App or software which you do not require regularly.
5. Do not give unnecessary permissions to apps that you install on your smart phones.
6. Regularly install latest updates for all the app/software you are using in your smart phone. Turn on automatic updates.
7. Always use licensed anti-virus software for your smart phone and scan your device at a regular interval.
8. Secure your data by enabling "Encrypt your device" option.
9. Give a Strong password for your Wifi/Hotspot.
10. Choose a separate name/ID for your smart phone while sharing your Hotspot with others.
11. Do not disclose Device ID (which is set by mobile company at the time of purchase) with anyone.

12. Always keep your mobile data and location off when they are not required.
13. Adjust your smartphone's settings so it does not automatically connect to nearby Wi-Fi networks. This gives you more control over where and when you connect.
14. Use Bluetooth in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding your Bluetooth connection.

Always keep your Bluetooth off when not in use.



15. Turn off NFC (Near Field Communication) if you are not using it. NFC is a short-range wireless technology that allows the exchange of data between devices.
16. Always use password protection or pattern lock for your mobile device and keep your password /pattern invisible.

## 17.9 Wireless Networks Safety

1. To prevent intruders from entering your wireless network, the pre-set SSID (Service Set Identifier) and default password for the browser-based administrative interface should be changed.


2. Configure the wireless router to not broadcast the SSID, which adds an additional barrier to discovering the network.

3. You should encrypt wireless communication by enabling wireless security and the WPA2 or higher encryption feature on the wireless router.


4. Activate MAC id filter in your wireless router to avoid unauthorized access. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Set your wireless network to accept connections only from devices with MAC addresses that the router will recognize.

5. Use a Virtual Private Network (VPN), which lets you use public Wi-Fi securely and keeps your online behaviour private. A VPN routes your connection through a secure server that encrypts your data before you land on a web page.

6. Update all wireless routers and wireless capable devices, such as laptops and mobile devices, as soon as security patches become available.

7. Use anti-virus and anti-spyware software on your computer, and use similar apps on your devices that access your wireless network.

8. When transmitting sensitive information, use your cellphone data plan instead of Wi-Fi.

9. Turn off your wireless router when it will not be in use for any extended period of time.

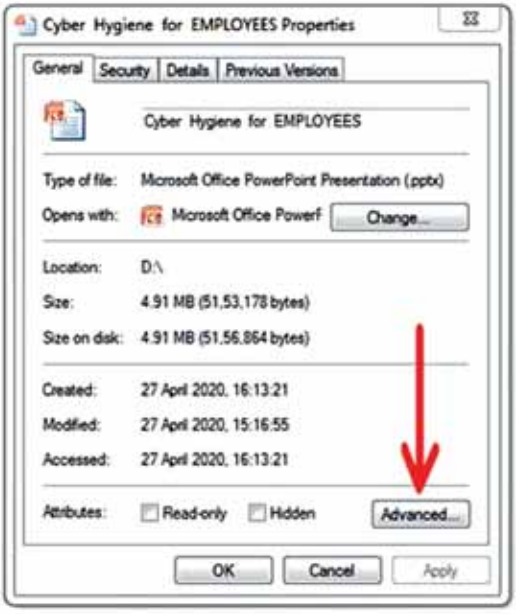
10. Disable remote management feature in routers to protect against unauthorized access.
11. IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. IoT devices are often designed to access to the customer's local network and data. The best way is to have IoT devices using an isolated network, sharing it only with other IoT devices.

## 17.10 Protecting your data and device

1. Always use genuine software and operating system. Do not download and install pirated software or anything else from random sites off the Internet. Many of them are malware ridden.
2. Do not keep any applications or software which you do not require regularly.
3. Always use device specific licensed Anti-virus and run virus scan on regular basis. Never go for installing free Anti-virus software available in the internet.
4. Keep the Firewall On. All operating systems come with default firewalls and you should not disable them. They are essential to defend against many known attacks. Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your data.
5. As and when companies find bugs in their software and OS, they also fix them by releasing regular updates. Run software and app updates as soon as they're available. These updates fix software vulnerabilities, and security problems. Turn on automatic updates.
6. Don't leave computer unattended with sensitive information on screen. Make sure to always lock your computer screen when leaving it unattended with "windows + L" or "Ctrl + Alt + Del"


7. Your computing devices, whether they are PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access.

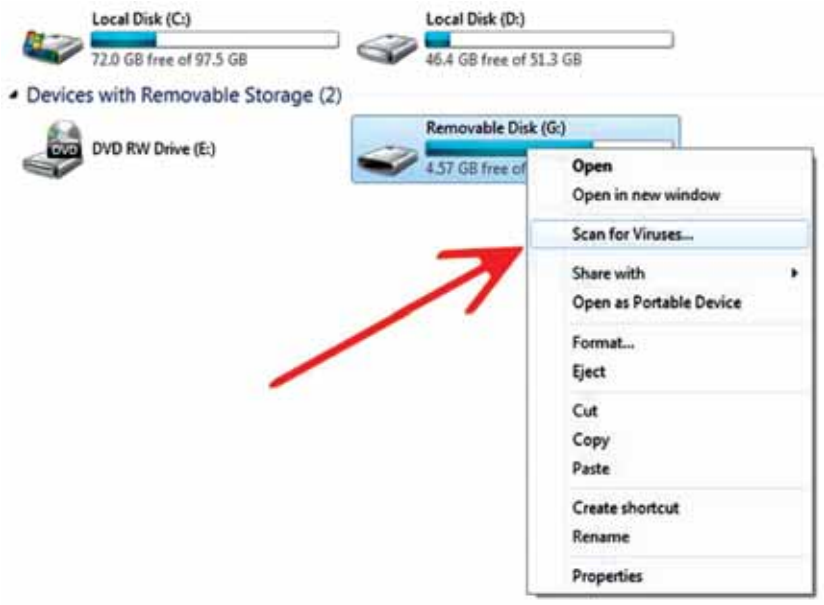
8. A very good idea to use Screensavers with timeout period of maximum 2 minutes.
9. Erase/remove the contents of removable storage media after use.
10. Protect your sensitive documents by enabling password protection on them.
11. Do not give your phone/ laptop for use to anyone, especially untrusted people.
12. The stored information should be encrypted, especially for sensitive or confidential data. Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form.





13. If you are not in a meeting, make sure that your webcam is either taped or blocked. The microphone should always be mute. In times when private topics may be discussed, having the microphone on mute will help prevent any leaks or unnecessary sharing of embarrassing information.

14. Always scan all removable media with antivirus




15. Delete your data permanently. When you move a file to the recycle bin or delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools can still recover the file.

    In order to erase data so that it is no longer recoverable, the data must be overwritten with ones and zeroes multiple times. To prevent the recovery of deleted files, you may need to use tools specifically designed to do just that. The program SDelete from Microsoft (for Vista and higher), claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OSX are some tools that claim to provide a similar service.

16. If you decide to sell your computer or mobile, reset it to Factory Setting and format repeatedly to ensure that all data have been erased permanently.

## 18. DOs and Don'ts for System & Network Administrators

1. Administrator login should be restricted through account management.
2. Update software patches regularly on all systems.
3. DON'T use the built-in Windows Administrator account for administrator functions/ activities.
4. DON'T use generic/normal user accounts as service accounts.
5. DON'T reboot a system if you don't know who's logged onto it.
6. Take regular backups of all critical systems.
7. Regularly check your log files for any errors and warnings, so they can alert you on problems before they become a threat.
8. Power supply should be controlled through UPS or Surge Protector.
9. Do not install computer systems in dusty environments.
10. Implement strong security protocols and policies.
11. Always enable the option in computers with "Show hidden file and folders".
12. Implement a workflow process with proper documentation.
13. All system changes should be only on the basis of documented approval.
14. Do not take up tasks which may not be completed on time. Beware the Late Friday Afternoon Task.
15. Do Perform Regular Security Audits and Tests.
16. Do Consistently Update and Patch Your Network and Devices.
17. Disable the Auto run/Auto play feature for insecure/downloaded software applications.

18. Create and Implement Policies and Procedures:
    - A Mobile Device Security Policy
    - A Computer Use Policy
    - A Social Media Policy
    - A Password Policy
    - An Email Policy
    - A Least Privilege Security Policy
    - A Business Continuity (BC), Data Backup and Disaster Recovery (BDR) Plan.
19. Don't use Your Admin Account for non-admin purposes.
20. Don't leave Your Network at the Mercy of Password Protection.
21. Ensure that regular cyber-security updates are received by all employees.
22. Keep the anti-virus updated.

## 19. Dos and Don'ts for Approvers and mid-level officers

1. All classified works should be done on standalone computers.
2. Take backup of all important information and files.
3. Do not enable remote access or file sharing from remote accounts.
4. Use secure deletion software for safe file purging.
5. Use private browsing mode on public computers.
6. Don't store the information on private cloud services like Google drive, Dropbox, icloud etc.
7. Store information only on organization allocated removable storage media.
8. Always reboot when required to use public computers.
9. Clean up cache files after use.
10. Regularly update the firmware of wireless device.

## 20. What to do after a cyber attack

### Read the details about the breach.

- When did the breach happen? You may receive the notice months or even years after the data breach occurred.
- Fine out what personal data of yours was included?

### Change your password IMMEDIATELY

- Lock down your account with a new password.
- If you can't log in, contact the website to ask how you can recover or shut down the account.
- See an account you don't recognize? The site may have changed names or someone may have created an account for you.
- If you've used that password for other accounts, change those too. Hackers may try to reuse your exposed password to get into other accounts. Create a different password for each of your financial accounts, email account, and other websites where you save personal information.

### Take extra steps if your financial data was breached

- If your bank account or credit card numbers were included in a breach, alert your bank to possible fraud. Monitor statements for charges you don't recognize.
- Check your credit reports for suspicious activity.
- Ensure that no new accounts, loans, or cards have been opened in your name.

### Lodge a compliant

- Contact your local police for registering your cyber crime complaint.
- You can report cyber crime complaints at National Cyber Crime Reporting Portal https://www.cybercrime.gov.in

## 21. Cyber Security Acronyms

There are too many cyber security acronyms to remember. A few prominent and widely used acronyms are compiled here.

| # | Acronym | Explication |
|---|---|---|
| 01 | APT | **Advanced Persistent Threat:** A cyber-attack that continuously uses advanced techniques to conduct cyber espionage or crime. |
| 02 | APWG | **Anti-Phishing Working Group:** An international consortium that brings together businesses affected by phishing attacks with security companies, law enforcement, government, trade associations, and others. |
| 03 | AV | **Antivirus:** A computer program used to prevent, detect, and remove malware. |
| 04 | AVIEN | **Anti-Virus Information Exchange Network:** A group of Antivirus and security specialists who share information regarding AV companies, products, malware and other threats. |
| 05 | CAPTCHA | **Completely Automated Public Turing Test to Tell Computers and Humans Apart:** A response test used in computing, especially on websites, to confirm that a user is human instead of a bot. |
| 06 | CARO | **Computer Antivirus Research Organization:** An organization established in 1990 to study malware. |
| 07 | CAVP | **Cryptographic Algorithm Validation Program:** This program provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and individual components. |
| 08 | CBC | **Cipher Block Chaining:** Operation for a block cipher using an initialization vector and a chaining mechanism. This will cause the decryption of a block of cipher text to depend on preceding cipher text blocks. |

| # | Acronym | Explication |
|---|---|---|
| 09 | CBC-MAC | **Cipher Block Chaining Message Authentication Code:** This constructs a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode. This creates a chain of blocks with each block depending on the correct encryption of the previous block. |
| 10 | CERIAS | **Centre for Education and Research in Information Assurance and Security:** A part of Purdue University dedicated to research and education in information security. |
| 11 | CERT | **Computer Emergency Response Team:** In this case, an expert group that handles computer security incidents and alerts organizations about them. |
| 12 | CHAP | **Challenge-Handshake Authentication Protocol:** A protocol for authentication that provides protection against replay attacks through the use of a changing identifier and a variable challenge-value. |
| 13 | CIRT | **Computer Incident Response Team:** A group that handles events involving computer security and data breaches. |
| 14 | CIS | **Centre for Internet Security:** A 501 nonprofit organization with a mission to "Identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace." |
| 15 | CISA | **Certified Information Systems Auditor:** Professionals who monitor, audit, control, and assess information systems. |
| 16 | CISM | **Certified Information Systems Security Manager:** A certification offered by ISACA which "Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives." |

| # | Acronym | Explication |
|---|---|---|
| 17 | CISO | **Chief Information Security Officer:** The CISO is the executive responsible for an organization's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. |
| 18 | CISSP | **Certified Information Systems Security Professional:** The CISSP is a security certification for security analysts, offered by ISC(2). It was designed to indicate a person has learned certain standardized knowledge in cyber security. |
| 19 | CNAP | **Cybersecurity National Action Plan:** A U.S. plan to enhance cybersecurity awareness and protections, protect privacy, maintain public safety, and economic and national security. |
| 20 | CNCI | **Comprehensive National Cybersecurity Initiative:** A U.S. government initiative designed to establish a front line of defense against network intrusion, defend the U.S. against the threats through counterintelligence, and strengthen the cybersecurity environment. |
| 21 | CND | **Computer Network Defense:** CND is defined by the U.S. military as defined by the US Department of Defense (DoD) as, "Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks." This style of defense applies to the private sector as well. |
| 22 | COBIT | **Control Objectives for Information and Related Technologies:** An IT management including practices, tools and models for risk management and compliance. |
| 23 | CSEC | **Cyber Security Education Consortium:** The CSEC, also known as the CEC, partners with educators and the broader cybersecurity community to ensure students are prepared to lead and be changemakers in the cybersecurity workforce. |

| # | Acronym | Explication |
|---|---|---|
| 24 | CSA | **Cloud Security Alliance:** The Cloud Security Alliance is the world's leading organization for defining best practices in cloud cybersecurity. It also provides a cloud security provider certification program, among other things. |
| 25 | CSO | **Chief Security Officer:** In some cases, the Chief Security Officer is in charge of an organization's entire security posture or strategy. This includes both physical security and cybersecurity. In other cases, this title belongs to the senior most role in charge of cybersecurity. |
| 26 | CSSIA | **Center for Systems Security and Information Assurance:** The CSSIA is a U.S. leader in training cybersecurity educators. It provides these teachers and professors with real-world learning experiences in information assurance and network security. |
| 27 | CVE | **Common Vulnerabilities and Exposures:** CVE® is a list of entries, each containing an identification number, a description, and at least one public reference – for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD). |
| 28 | CVSS | **Common Vulnerability Scoring System:** An industry standard for rating the severity of security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. |
| 29 | DDoS | **Distributed Denial of Service:** A distributed denial-of-service (DDoS) attack attempts to disrupt normal traffic of a targeted server, service or network to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets). |

| # | Acronym | Explication |
|---|---|---|
| 30 | DLP | **Data Loss Prevention:** An information security strategy to protect corporate data. DLP is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users, either inside or outside of an organization. |
| 31 | DNS Attack | **Domain Name Server Attack:** DNS uses the name of a website to redirect traffic to its owned IP address. Amazon.com should take you to Amazon's website, for example. During this type of attack, which is complex and appears in several ways, cybercriminals can redirect you to another site for their own purposes. This attack takes advantage of the communication back and forth between clients and servers. |
| 32 | EDR | **Endpoint Detection & Response:** Endpoint Detection & Response solutions are designed to detect and respond to endpoint anomalies. EDR solutions are not designed to replace IDPS solutions or firewalls but extend their functionality by providing in-depth endpoint visibility and analysis. EDR uses different datasets, which facilitates advanced correlations and detection. |
| 33 | FISMA | **Federal Information Security Management Act:** FISMA is United States legislation which requires each federal agency to develop, document, and implement an agency-wide program to provide information security for its information systems and data. The act recognized the importance of information security to the economic and national security interests of the United States. |
| 34 | FISMA | **Federal Information Security Modernization Act (2014):** Laws that assigns responsibilities within the U.S. federal government for setting and complying with policies to secure agencies' information systems. For example, Department of Homeland Security administers cybersecurity policies and the Office of Management and Budget provides oversight. |

| # | Acronym | Explication |
|---|---|---|
| 35 | FISSEA | **Federal Information Systems Security Educators' Association:** An organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, and education responsibilities. |
| 36 | GRC | **Governance, Risk Management, and Compliance:** Three parts of a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Cybersecurity people, practices and tools play a key part in GRC for many organizations. |
| 37 | HTTPS | **Secure Hypertext Transfer Protocol:** An extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network by encrypting the information you send from your computer to another website. |
| 38 | IA | **Information Assurance:** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. |
| 39 | IAM | **Identity and access management:** IAM is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. |
| 40 | IBE | **Identity-Based Encryption:** A type of public-key encryption in which the public key of a user is some unique information about the identity of the user, like a user's email address, for example. |
| 41 | IDS/IDP | **Intrusion Detection/ Intrusion Detection and Prevention:** Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyze packets as well, but can also stop the packet from being delivered based on what kind of attacks it detects, helping to stop the attack. |

| # | Acronym | Explication |
|---|---|---|
| 42 | ISACA | **Information Systems Audit and Control Association:** ISACA provides certifications for IT security, audit and risk management professionals. ISACA also maintains the COBIT framework for IT management and governance. ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. |
| 43 | ISAKMP | **Internet Security Association and Key Management Protocol:** A protocol for establishing Security Associations and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent. |
| 44 | ISAP | **Information Security Automation Program:** ISAP is a U.S. government agency initiative to enable automation and standardization of technical security operations. |
| 45 | $(ISC)^2$ | **International Information Systems Security Certification Consortium:** A non-profit organization which specializes in training and certification for cybersecurity professionals. Certifications include the CISSP. |
| 46 | ISO | **International Organization for Standardization:** An organization that develops international standards of many types, including two major information security management standards, ISO 27001 and ISO 27002. |
| 47 | ISSA | **Information Systems Security Association:** ISSA is a not-for-profit, international organization of information security professionals and practitioners. |
| 48 | ISSO | **Information Systems Security Officer:** Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. |

| # | Acronym | Explication |
|---|---|---|
| 49 | ISSPM | **Information Systems Security Program Manager:** The ISSPM, sometimes called an IT Security Manager, coordinates and executes security policies and controls, as well as assesses vulnerabilities within a company. |
| 50 | JSM | **Java Security Manager:** To use Java security to protect a Java application from performing potentially unsafe actions, you can enable a security manager for the JVM in which the application runs. The security manager enforces a security policy, which is a set of permissions (system access privileges) that are assigned to code sources. |
| 51 | MS-ISAC | **Multi-State Information Sharing and Analysis Centre:** The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. |
| 52 | MSSP | **Managed Security Services Provider:** Provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. |
| 53 | NCS | **National Cryptologic School:** A school within the National Security Agency. The NCS provides the NSA workforce and its Intelligence Community and Department of Defense partners highly-specialized cryptologic training, as well as courses in leadership, professional development, and over 40 foreign languages. |
| 54 | NCSA | **National Cyber Security Alliance:** A non-profit partnership working with the Department of Homeland Security, private sector sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education. |

| # | Acronym | Explication |
|---|---|---|
| 55 | NCSAM | **National Cyber Security Awareness Month:** NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity. It occurs each year in October. The security awareness month started with a joint effort by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance. |
| 56 | NCSD | **National Cyber Security Division:** A division of the Office of Cyber Security & Communications with the mission of collaborating with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructures. |
| 57 | NICCS | **National Initiative for Cybersecurity Careers and Studies:** An online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the United States. |
| 58 | NICE | **National Initiative for Cybersecurity Education:** The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. |
| 59 | NISPOM | **National Industrial Security Program Operating Manual:** The National Industrial Security Program Operating Manual establishes the standard procedures and requirements for all government contractors, with regards to classified information. It covers the entire field of government-industrial security related matters. |

| # | Acronym | Explication |
|---|---|---|
| 60 | NIST | **National Institute of Standards and Technology:** In cybersecurity circles, NIST is extremely well known for the NIST Cybersecurity Framework, as well the NIST Risk Management Framework (RMF), NIST 800-53 control guidance, NIST Digital Identity Guidelines and others. The overall NIST mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST is part of the U.S. Department of Commerce. |
| 61 | OPSEC | **Operational Security:** OPSEC is a term derived from the U.S. military and is an analytical process used to deny an adversary information that could compromise the secrecy and/or the operational security of a mission. OPSEC related techniques can play a significant role in both offensive and defensive cybersecurity strategies. |
| 62 | OSINT | **Open Source Intelligence:** OSINT is information drawn from publicly available data that is collected, exploited, and reported to address a specific intelligence requirement. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). |
| 63 | PCI-DSS | **Payment Card Industry Data Security Standard:** The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. |
| 64 | SANS | **System Administration, Networking, and Security Institute:** A private company that specializes in information security training and security certification. |

| # | Acronym | Explication |
|---|---|---|
| 65 | SIEM | **Security Information and Event Management:** Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual sources. |
| 66 | SOC | **Security Operations Center:** A central location or team within an organization that is responsible for monitoring, assessing and defending security issues. |
| 67 | SSO | **Single Sign-On:** A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials. |
| 68 | TTP | **Tactics, Techniques, and Procedures:** The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. |
| 69 | UBA / UEBA | **User Behaviour Analytics:** UBA tracks a system's users, looking for unusual patterns of behaviour. In cybersecurity, the process helps detect insider threats, and other targeted attacks including financial fraud. User behaviour analytics solutions look at patterns of human behaviour, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns. This guides efforts to correct unintentional behaviour that puts business at risk and risky and intentional deceit. |
| 70 | VPN | **Virtual Private Network:** By connecting through a VPN, all the data you send and receive travels through an encrypted "tunnel" so that no one can see what you are transmitting or decipher it if they do get a hold of it. VPNs also allow you to hide your physical location and IP address, often displaying the IP address of the VPN service, instead. |

## References:


https://www.britannica.com/topic/cybercrime
https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime
https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
https://en.wikipedia.org/wiki/Cybercrime
https://en.wikipedia.org/wiki/Computer_security
https://www.synopsys.com/glossary/what-is-cyber-security.html
https://www.cdw.com/content/cdw/en/articles/datacenter/2019/03/18/what-is-data-storage.html
https://www.cisco.com/c/en/us/products/security/index.html
https://www.perforce.com/blog/kw/common-software-vulnerabilities
https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/
https://www.perforce.com/blog/kw/what-is-OWASP
https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-centre
https://www.sifytechnologies.com/blog/cloud-datacentres-differ-traditional-datacentres/
https://scialert.net/fulltext/?doi=ajsr.2012.45.57
https://www.mcafee.com/enterprise/en-in/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
https://blog.ipleaders.in/ethical-hacking/
https://www.techopedia.com/definition/15957/security-incident
https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer/
https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful
https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html
https://www.secureworld.io/industry-news/67-top-cybersecurity-acronyms
https://pixabay.com/
https://pixabay.com/illustrations/binary-code-globe-africa-asia-1695475/


# Cyber Security Centre of Excellence

**Department of IT & Electronics | Govt. of West Bengal**

*Helping to make your cyber presence safe*


**Webel Bhavan, Ground Floor**
**Block – EP & GP, Sector – V**
**Salt Lake**
**Kolkata – 700 091**

**Phone No.: 033 2357 5218**
**Email : cscoe[at]wb[dot]gov[dot]in**
**https://cscoe.itewb.gov.in/**