# UPSC 2020

# Topic – Cyber Security – UPSC GS-III

The government of India is taking many initiatives to enhance cyber security. With the rapid development in information technology, it is critical to provide safety and security cyber space. The topic, ‘Cyber Security’ comes under GS-III syllabus of the IAS Exam.This article will provide you with relevant facts about cyber security.

## What is Cyber?

The term, ‘Cyber’ is used in relation with the culture of computers, information technology and virtual reality. The connection of internet ecosystems form cyberspace. The threat to cyberspace leads to an issue and gives rise to the need of cyber security

**Threats to Cyberspace:**

1. Interconnectedness of Sectors
2. Increase in the number of exposure points
3. Concentration of assets

As per NITI Aayog report, the threats to cyberspace have increased dramatically over the last 10 years. The cyber attacks lead to the exposure of:

1. Sensitive information
2. Personal information and
3. Business information

## Need of Cyber Security

Cyber Security protects the cyberspace from the the following:

1. Cyber Attacks
2. Damage to Cyberspace
3. Misuse of Cyberspace
4. Economic Espionage

### Cyber Security - Evolution

With the introduction of cyber attacks, cyber security initiatives have evolved. They are mentioned in the table below:

| Evolution of Cyber Security |
|---|

| Issues | Cyber Security Initiatives |
|---|---|
| Virus (1990s) | • Anti-Virus<br>• Firewalls |
| Worms (2000) | Intrusion Detection and Prevention |
| Botnets (2000s - Present) | DLP, Application-aware Firewalls, SIM |
| APT Insiders (Present) | Network Flow Analysis |

## Cyber Threats and Cyber Security

There are types of cyber attacks that have evolved over a period of time:

1. Virus - It is a malware that self-replicates and spreads by inserting copies of itself into other executable code or documents.
2. Hacking Websites - An unauthorized access to any website belonging in a personal or professional space
3. Malicious Codes - It is a kind of security threat where any code present in software tends to bring harmful effects, breach the security of the system or bring damage to the system.
4. Advanced Worm and Trojan - This is again a malware that camouflages as a regular software however once accessed, brings damage to the hard drive, background systems and corrupts allocation systems
5. Identity Theft and Phishing - It is a cyber attack involving fraudulent emails posing as authorized entities in order to induce people to reveal their information (personal and professional.)
6. DOS, DDOS - DOS stands for Denial-of-Service attack and DDOS stands for Distributed Denial-of-Service attack. The attackers make the machine or network unavailable by disrupting services of the host network through the flood of superfluous requests to overload systems. And when such flooding of requests comes from various ends, it is termed as DDOS.
7. Cyber Espionage - Usually when a government’s or important organisation’s privacy is posed at risk due to illegal use of computer networks to seek confidential information.
8. Cyber Warfare - Deliberately attacking the information systems through the use of computer technology to disrupt the state’s activities, especially for military purposes.

## Cyber Attacks in India

The topmost causes of cyber attacks are:

1. Phishing and Social Engineering
2. Malware
3. Spear Phishing
4. Denial of Service
5. Out of Date Software Ransomware

The table below gives the list of cyber attacks that India has witnessed in the past:

| Cyber Attacks in India | Description of the Cyber Attacks |
|---|---|
| Coronavirus Pandemic Based Cyber Attack | Microsoft has reported that cyber crookers are using Covid-19 situation in 2020 to defraud people through phishing and ransomware in India and the world |
| Phishing | Union Bank of India heist in July 2016 |
| Wannacry Ransomware | In May 2017, various computer networks in India were locked down by the ransom-seeking hackers. |
| Data Theft | In May 2017, the food tech company Zomato faced the theft of information of 17 million users. |
| Petya Ransomware | Container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected |
| Mirai Botnet | In September 2016, Mirai malware launched a DDoS attack on the website of a well-known security expert. |

## Cyber Security - Who are the Cyber Attackers?

There are kinds of cyber players who harm cyber security:

- Cyber Criminals
- Cyber Terrorists
- Cyber Espionage
- Cyber Hacktivist

As per the Niti Ayog report, the following are the sets of group behind the cyber security breaches

Outsiders
Internal Actors
State-affiliated actors
Multiple parties
Attacks in partnerships
Organised Criminal Groups

## Cyber Security - Cyber Swachhta Kendra

It is the Botnet Cleaning and Malware Analysis Centre under Indian Computer Emergency Response Team (CERT-In) under Ministry of Electronics and Information Technology (MeitY). The aim of Cyber Swachhta Kendra is to promote awareness among Indian citizens to secure their data in computers, mobile phones and other electronic devices.

## Cyber Security - Indian Laws & Government Initiatives

There are various legislations that support cyber security in India. The table below mentions these:

| Laws related to Cyber Security in India | Important Facts |
|---|---|
| Information and Technology Act, 2000 | - Came into force in October 2000<br>- Also called Indian Cyber Act<br>- Provide legal recognition to all e-transactions<br>- To protect online privacy and curb online crimes |
| Information Technology Amendment Act 2008 (ITAA) | The amendments in IT Act mentioned:<br>- ‘Data Privacy’<br>- Information Security<br>- Definition of Cyber Cafe<br>- Digital Signature<br>- Recognising the role of CERT-In<br>- To authorize inspector to investigate cyber offences against DSP who was given the charge earlier |
| National Cyber Security Strategy 2020 | Indian Government is coming up with National Cyber Security Strategy 2020 entailing the provisions to secure cyberspace in India. The cabinet’s nod is pending and it will soon be out for the public. |
| Cyber Surakshit Bharat Initiative | MeitY in collaboration with National e-Governance Division (NeGD) came up with this initiative in 2018 to build a cyber resilient IT set up |