Cyber attacks in India

In computers and computer networks an **attack** is any attempt to expose, alter, disable, destroy, steal or gain information through unauthorized access to or make unauthorized use of an asset. A **cyberattack** is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities.

A **cyber attack** is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A **cyber attack** can maliciously disable computers, steal data, or use a breached computer as a launch point for other **attacks**. Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. Net crime is criminal exploitation of the Internet. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

A cyberattack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

Type of Cyber attacks

1. **Indiscriminate attacks** - These attacks are wide-ranging, global and do not seem to discriminate among governments and companies.
2. **Destructive attacks** - These attacks relate to inflicting damage on specific organizations.

3. **Cyberwarfare** - These are politically motivated destructive attacks aimed at sabotage and espionage.
4. **Government espionage** - These attacks relate to stealing information from/about government organizations.
5. **Corporate espionage** - These attacks relate to stealing data of corporations related to proprietary methods or emerging products/services.
6. Stolen e-mail addresses and login credentials - These attacks relate to stealing login information for specific web resources.
7. Stolen credit card and financial data

Cyberattacks in India

India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%. In a recent study, it was revealed that out of 15 Indian cities, Mumbai, New Delhi, and Bengaluru have faced the maximum number of cyber attacks. As per NITI Aayog there are major Cyber attacks enumerated as below;

1. **JULY 2016 - "UNION BANK OF INDIA HEIST"** - Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171

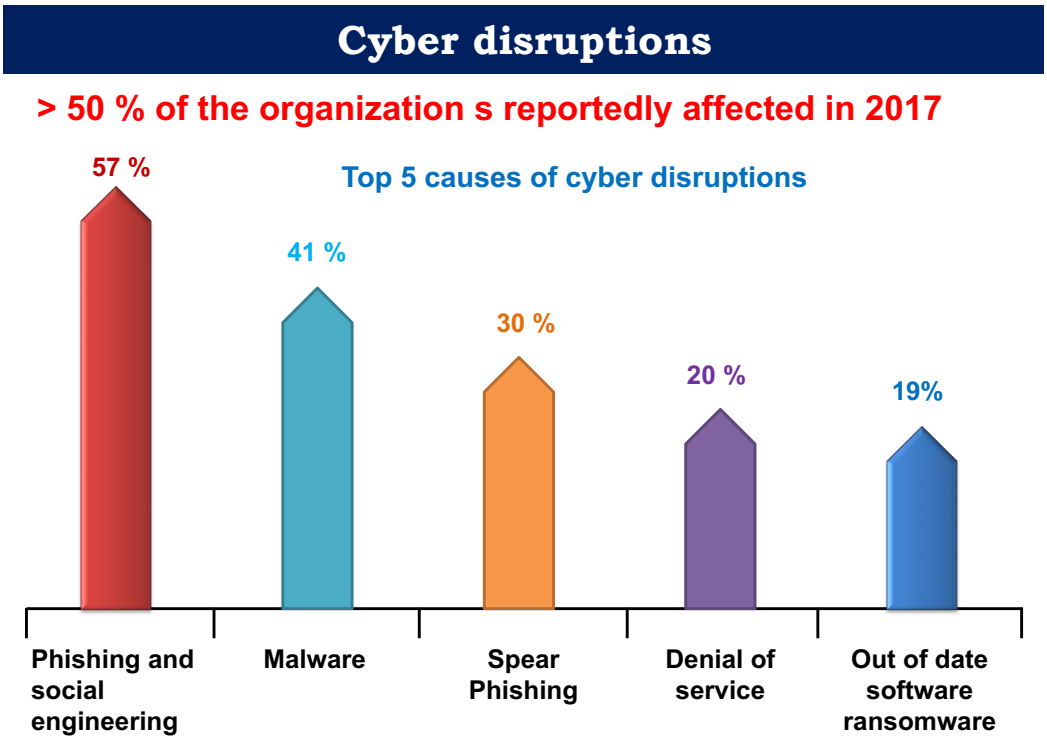
million, Prompt action helped the bank recover almost the entire money.

2. **MAY 2017 - "WANNACRY RANSOMWARE"** - The global ransomware attack took its toll in India with several thousands computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal
3. **MAY 2017 - "DATA THEFT AT ZOMATO "** - The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web.
4. **JUNE 2017 - "PETYA RANSOMWARE "** - The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected.

The Biggest Cyber Attacks in India

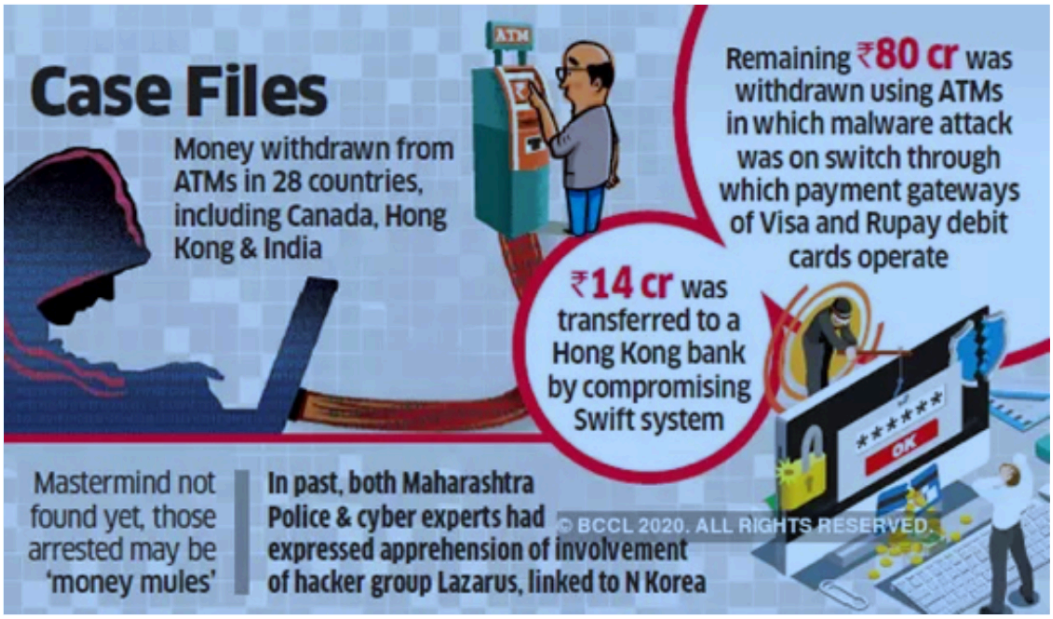
In the Annual Cyber Security Report by CISCO, 53% of cyber attacks caused more than $500K of financial loss to organizations in 2018. Cyber attacks in India have risen up to such an extent that our country ranks fourth out of the

top 10 targeted countries in the world. In a report by India Today, Chennai experienced the highest percentile of cyber attacks with a stat of 48% in the first quarter of 2019. Cyber criminals have adapted advanced cyber attack techniques for their targeted end-users. Various business sectors and geographical locations have faced recent cyber attack in India.



1. Cosmos Bank Cyber Attack in Pune

A recent cyber attack in India 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crore from Cosmos Cooperative Bank Ltd. in Pune.



Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

Prevention: Hardening of the security systems by limiting its functions and performance only to authorized people can be the way forward.

Any unauthorized access to the network should immediately set an alarm to block all the access to the bank's network. Also, to minimize risk, enabling a two-factor authentication might help.

Through testing, potential vulnerabilities can be fished out and can make the entire digital part of the banking system safe.

2. Canara bank's ATM System Hacked

Around mid-2018, Canara bank ATM servers were targeted in a cyber attack. Almost 20 lakh rupees were wiped off from various bank accounts. Count of 50 victims was estimated and according to the sources, cyber attackers held ATM details of more than 300 users. Hackers used skimming devices to steal information from debit cardholders. Transactions made from stolen details amounted from Rs. 10,000 to the maximum amount of Rs. 40,000.

Prevention: Enhancement of the security features in ATM and ATM monitoring systems can prevent any misuse of data.

Another way to prevent fraudulent activity is to minimize the risk of skimming by using lockbox services to receive and transfer money safely.

3. UIDAI Aadhaar Software Hacked

UIDAI revealed that around 210 Indian Government websites had leaked Aadhaar details of people online.

Data leaked included Aadhaar, PAN and mobile numbers, bank account numbers, IFSC codes and mostly every personal information of all individual cardholders. If it wasn't enough shocking, anonymous sellers were selling Aadhaar information of any person for Rs. 500 over Whatsapp. Also, one could get any person's Aadhaar car printout by paying an extra amount of Rs.300.

4. Hack Attack on Indian Healthcare Websites

Indian-based healthcare websites became a victim of cyber attack recently in 2019. As stated by US-based cyber security firms, hackers broke in and invaded a leading India-based healthcare website. The hacker stole 68 lakh records of patients as well as doctors.

5. SIM Swap Scam

Two hackers from Navi Mumbai were arrested for transferring 4 crore rupees from numerous bank accounts in August 2018. The illegally transferred money from bank accounts of many individuals. By fraudulently gaining SIM card information, both attackers blocked individuals' SIM cards and by the help of fake document posts, they carried out transactions via online banking. They also tried to hack accounts of various targeted companies.

6. Websites Hacked: 2017 - 2018

Over 22,000 websites were hacked between the months of April 2017 and January 2018. As per the information presented by the Indian Computer Emergency Response Team, over 493 websites were affected by malware propagation including 114 websites run by the government. The attacks were intended to gather information about the services and details of the users in their network.

Prevention: Using a more secure firewall for network and server which can block any unauthorized access from outside the network is perhaps the best idea.

Personal information of individuals is critical for users and cannot be allowed to be taped into by criminals. Thus, monitoring and introducing a proper network including a firewall and security system may help in minimizing the risk of getting hacked.

7. Indian journalists, activists spied on by Israeli spyware Pegasus

2019 saw another big cyber attack when Israeli spyware Pegasus was used to spy on academicians, lawyers, activists, and journalists in India.

WhatsApp confirmed that NSO Group used Israeli spyware, called Pegasus to get access to the passwords, text messages on messaging apps like WhatsApp. Pegasus took advantage of loopholes in the servers. It allowed the government spies to hack the details of about 1,400 users. Pegasus allowed to hack and get access to everything on the phones of the user (victims) remotely. Even, WhatsApp announced renovating its security features.

Cyber Attacks on India or any other part of this world is an attempt to destroy or infect computer networks in order to extract or extort money or for other malicious intentions such as procuring necessary information.

NITI Aayog has suggested 10 steps to Cyber Security

Cyber attacks alter computer code, data, or logic via malicious code resulting in troublesome consequences that can compromise the information or data of the organizations to make it available to cybercriminals.

Cyber attacks consist of various attacks which are hacking, D.O.S, Virus Dissemination, Credit Card Fraud, Phishing or Cyber Stalking.

High-profile cyber attacks on companies such as Target and Sears have raised awareness of the growing threat of cyber crime.

1. **Network Security** - Protect your networks against external and internal attack. Manage the network primer. Filter out unauthorised access and malicious contents. Monitor and test security controls

2. **Malware Protection** - Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the Orgn.

3. **Monitoring** - Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT system and networks. Analyse logs for unusual activity that could indicate an attack.

4. **Incident Management** - Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

5. **User Education and Awareness** - Produce user policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

6. **Home and Mobile Working** - Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline to all devices. Protect data both in transit and at rest

7. **Secure Configuration** - Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a base line build for all ICT devices.

8. **Removable Media Controls** - Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before imported on the corporate system.

9. **Managing User Privileges** - Establish account management processes and limit the number of privileged accounts. Limit

user privileges and monitor user activity. Control access to activity and audit logs.

10. **Information Risk Management Regime** - Establish and effective governance structure and determine your risk appetite. Maintain boards engagement with cyber risk. Produce supporting information risk management policies.

Other major Prevention to secure computer system ;

A cyber attack is a deliberate exploitation of your systems and/or network. Cyber attacks use malicious code to compromise your computer, logic or data and steal, leak or hold your data hostage. Cyber attack prevention is essential for every business and organisation.

- Train your staff
- Keep your software and systems fully up to date
- Ensure Endpoint Protection
- Install a Firewall
- Backup your data
- Control access to your systems
- Wifi Security
- Access Management
- Passwords Protections
- Maintain Up-to-Date Software
- Protect the Gateway Layer

- Provide Extra Layer of Protection for Business-Critical Transactions
- Protect the Endpoint, the Computer

How to avoid Phishing attacks?

Phishing links can impersonate as authentic links with some minor changes that might not be visible at a single glance.

- Make sure that you have read the complete link before clicking it.
- Install measures that can effectively prevent such attacks
- Make sure that the websites you are accessing are secure. Usually, a secure website will have a security certificate to safeguard all the customer information. Make sure that that website begins with https and has a lock symbol on the extreme left of the address bar.
- Check your online account on a regular basis and make sure that there are no suspicious activities. Change the password frequently. Update your browsers regularly as updates often will have security patches for existing loopholes.
- Keep your personal details secret

How to prevent Social Media Profile Hacking?

Social media is infested with third-party applications.

- Make sure that you are using legitimate authorized applications
- Use strong credentials and change it often
- Install proper antivirus

- Enable two-factor authentication

How to Prevent Database Hacking?

- Make sure that proper web application firewall is installed
- Strengthen network security by login expiration, changing password, Make sure that the admin level of your website is not exposed with a simple password
- Change the database prefix from wp6 to something random which can’t be guessed
- Stay updated regarding the latest hacking threats

How to make your API secure?

- Validate all the incoming data
- Use the essential method for authentication verification Monitor and manage using automated scripts
- Encrypt data

Conclusion ; -

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. But, with the broad range of opportunities that Internet has also opened risk of cyber attacks for us. Cyber attacks and threats can be prevented by being aware of the various types of protocols, exploits, tools, and resources used by malicious actors. It can be difficult to know where to begin when it comes to protecting your business from

cyber crime and cyber attacks. It is very essential for organizations to implement cyber security measures and follow the above-mentioned security guidelines. Therefore, I would suggest you apply above mentioned preventions to protect and prevent your yourself; money, property, social life, business and much more for easy and secure life.

Sanjay Sarraf

10/03/2021