# Study on Cyber Security applicable for digital life

[1] Pranali Prakash Mahadik, [2] Rama Gaikwad
[1,2] Assistant Professorr,
[1,2] Department of Computer Engineering,
[1,2] Anantrao Pawar College of Engineering & Research, Pune, Maharashtra, India

***Abstract :*** There is considerable overlap between cyber security and information security but these both concepts are totally different. Cyber security is goes beyond information security it include only protection for information resources. In information security reference to the human factor usually relates to the role of human in security process but in cyber security human is target of cyber attack.Main aim of Cyber Security is of protecting information and various information systems such as database, networks, different data centers and various applications by using suitable procedural and technological security measures.

Now a days to protect personal data only firewall, antivirus software are not sufficient. Because now a day's cyber infrastructure is speedily growing and Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be included in the educational. Security counter measure helps ensure the confidentiality, availability and integrity of information systems by preventing or serious asset losses from Cyber Security attacks.

***IndexTerms*** **- Cyber Security, Threats, Cyber safety, Cyber attack**

## I. INTRODUCTION

Cyber security is related with protecting cyberspace from cyber-threats. Cyber-Threats mean malicious use of communication technology and information as a target or a tool by a wide range of malicious actors.

Internet is one of the fasted-growing areas of technical infrastructure development today total commercial transaction are done online so this field required a high quality if security transparent and best transactions. Cyber security plays a significant role in the development of information technology and internet services. Increasing cyber security and protecting critical information infrastructure are essential for all. Society is reliant on cyber systems across the full range of human activities such as health care, entertainment, energy, national defense, commerce, finance and communications.

Cyber security mainly depends on decisions taken by people while setup and maintenance of computer and internet. Cyber-security covers provide protection for software and hardware with personal information from unauthorized.

Different Elements of cyber security

To ensure cyber security mainly requires the synchronization of efforts all over an information system, which includes:

- Application security
- Operational security
- Network security
- End-user education
- Information security
- Disaster recovery

One of the most difficult elements of cyber security is the continuously developing nature of security risks. In traditional approach focus protect against the biggest known threats and ignoring less affecting threats

Cyber security is the set of security concepts, risk management approaches, actions, training, best practices assurance, technologies, tools, security safeguards, and policies and guidelines that can be used to defend the cyber environment along with organization as well as user's assets. Organization and user's assets contain connected computing devices, infrastructure, services, applications, telecommunications systems, personnel, and the totality of transmitted and stored information in the cyber environment. Cyber security strives to make sure the maintenance and attainment of the security properties user or organization against security risks in the cyber environment.

Security objectives encompass the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

This paper focus on the fundamental nature of security.

### 1.1 Information security

Information security is also called as InfoSec, main aim is to prevent unauthorized access, modification, use, inspection, disclosure, recording, destruction and disruption of information. The information also refer to data in any form like physical or electronic. InfoSec's mainly focus on integrity, confidentiality and availability of data

It is significant to note that there is a difference between information and communication technology security and information security

### 1.2 Information and communication technology security

Information and communication technology (ICT) security related with the providing protection to the technology-based systems on which information is commonly stored and transmitted. And information security include the protection to the fundamental information resources.

ICT have additional characteristics like include non-repudiation, accountability, authenticity and reliability.

## II. Threats To Cyber Security

Computer security threats are constantly changing and are very inventive and constantly find new ways to steal and harm system. Cyber security is divided into two different parts,

- Actions that intended to damage or destroy cyber systems
- Actions that look to exploit the cyber infrastructure for harmful or unlawful purposes without damaging or compromising that infrastructure.

Some attacks may not give instant impact on cyber system first they establish itself in system and they permits actions that degrade computer capacity.

### 2.1 Examples of Online Cyber security Threats

#### 2.1.1Computer Viruses

Computer virus is most renowned threat for computer security It is a program written to modify the way by which a computer operates, without the authorization or knowledge of the user. Computer virus replicates and executes itself typically doing damage to computer.

To avoid Computer virus avoid downloading from peer-to-peer file sharing site ,evaluate free software's and emails.

#### 2.1.2 Spyware Threats

Spyware is a serious computer security threat it is a program that moinitors online acitvites and install program on system without your consent to capture your important personal information and to gain profit form it. Best way to avoid such type of thread to read terms and conditions how your activities get tracked online.

#### 2.1.3Hackers

Here People, not system or computer generate computer security threats and malware. Hackers are programmers who discriminate against others for their own gain by breaking into computer systems for the purpose of stealing or changing and destroying information.

#### 2.1.4Phishing

Masquerading as a reliable individual or any business phishers go to steal information which is sensitive or personal in financial or any important aspect thorough fraud email or messages. financial or personal information through fraudulent email or instant messages.

.

#### 2.1.5 Password Cracking

Password Cracking is a typical form of attack. This attacker will guess your password repetitively and also check it alongside a cryptographic hash of the password. Password cracking is used to enter your computer system for steal stored information. To avoid such type of attack generate a strong as well as memorable password having mixture of upper and lower case letters, symbols and numbers and most important thing is change it regularly with different patterns.

Strong password can decrease the probability of an attack. While setting password avoid following mistakes,

- Avoid family information and your name and birthdates.
- Ensure while changing password is significantly dissimilar in form of old pattern.
- Avoid same password for different applications.

#### 2.1.6 Ransomware

Ransomware attack design software to block access to a system and all data until some money is paid out as per attackers Demand.

It has the capability to affect massive disruption to the workplace.

To avoid such type of attack,

1. Take daily backup of your important files and keep it in encrypted form.
2. Always use notepad to Open JavaScript files as it will be very useful to block any Ransomware scripts.
3. Always Scan compressed files it may have infection with your anti-ransomware application.
4. Do not download suspicious attachments to the email.

## III. CYBER SECURITY TECHNIQUES

**3.1Firewalls –**

A firewall may be a program or some piece of hardware that helps find out viruses, hackers and worms that try and reach your pc over the internet. All messages coming into or leaving the internet undergo the firewall present, which examines every message and blocks those who don't meet the desired security criteria. thus firewalls play a very important role in detection the malware.

**3.2 Authentication of knowledge –**

The documents that we have a tendency to receive should always be documented be before downloading that's it ought to be checked if it's originated from a trustworthy and a reliable supply which they're not altered. Authenticating of those documents is typically done by the antivirus computer code present within the devices. therefore a good antivirus software is also essential to protect the devices from viruses.

**3.3 Malware scanners –**

this can be software that usually scans all the files and documents present within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses square measure samples of malicious software that are usually classified together and stated as malware.

## IV. NECESSITY OF CYBER SECURITY

Information is that the most valuable asset with relation to a private, cooperate sector, state and country with relation to a private the involved areas are:

1. Protective unauthorized access, disclosure, modification of the resources of the system.

2. Security throughout on-line transactions concerning shopping, banking, railway reservations and share markets.

3. Security of accounts whereas using social-networking sites against hijacking.

4. One key to improved cyber security could be a higher understanding of the threat and of the vectors utilized by the attacker to bypass cyber defenses

5. Need of separate unit handling security of the organization.

6. Totally different organizations or missions attract differing types of adversaries, with totally different goals, and so need different levels of readiness.

7. In characteristic the nature of the cyber threat an organization or mission faces, the interaction of AN adversary's capabilities, intentions and targeting activities should be considered. With relation to state and country

8. Securing the information containing varied essential surveys and their reports.

9. Securing the info basis maintaining the small print of all the rights of the organizations at state level.

## V. INTRUSION DETECTION SYSTEM (IDS)

Attacks on the computer infrastructures are getting an progressively major problem. an intrusion is outlined as any set of actions that arrange to compromise the indignity, confidentiality or availability of a resource. Intrusion Detection is so needed as a further wall for safeguarding systems. Intrusion detection is beneficial not solely in police work made intrusions, however conjointly provides vital data for timely counter measures.

There are three primary components of IDS:

- Network Intrusion Detection System (NIDS): NIDS does study for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is like to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- Host Intrusion Detection System (HIDS): HIDS consider status of whole system and file set and compare it with previous status of system and if found significant variation like if some files are missing or changed then it alert them to administrator

## VI. Cyber-Security educational System

In education system, the youngsters should be created alert to the attainable attacks and kinds of intruders. They have to even be alert to the terms like: Hardware/Desktop Security, Wi-Fi security, personal data security, Social networking attacks security and malicious software. Education must develop awareness about cyber security.

## VII. Conclusion

In this paper include Cyber Security threats related issues and challenges it also gives idea about how to avoid attacks on our system and personal data.

## References

[1] G.Nikhita Reddy, G.J.Ugander Reddy," Study Of Cyber Security Challenges And Its Emergning Trends On Latest Technologies"
[2] I.Duić, V.Cvrtila, T. Ivanjko," International cyber security challenges"
[3] Kutub Thakur, Meikang Qiu, Keke Gai, Md Liakat Ali,"An Investigation on Cyber Security Threats and Security Models"
[4] Om Pal1, Vandana Srivastava",Cyber Security Risks and Challenges in Supply Chain."
[5] Vairaprakash Gurusamy, Bhargav Hirani ,"Cyber Security for Our Digital Life."
[3] Rossouw von Solms, Johan van Niekerk,"From information security to cyber security"
[6] Klimburg A, editor.," National cyber security framework manual" ,NATO CCD COE Publications; 2012, December.
[7] Martin N, Rice J.," Cybercrime: understanding and addressing the concerns of stakeholders. Computers & Security", 2011;30:803e14.