International Journal of Research and Review
Vol.7; Issue: 5; May 2020
Website: www.ijrrjournal.com
Review Article *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Tremendous Increment of Cyber Crime due to Flaws in Cyber Security

Vidit Kumar [1], Goutam Kumar[1], Deepak Chahal[2]

[1]MCA Student, [2]Professor,
Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India

Corresponding Author: Deepak Chahal

ABSTRACT

Our world nowadays relies on computers for the smallest work processing in day to day life. We in terms of users of services always interact with computers for tasks like communication data sharing information gathering social activities and many more over the network. So it can be easily visualized that this network established between multiple devices around the world in any form such as servers, computers laptops mobile phones, etc. acts as the prime piece of technology used for all these kinds of tasks. But this continuous working system introduces a great threat that is known as cybercrime. Although cyber security has been implemented all over the network, there are flaws and impediment that disrupt the security and leads to these crimes. We can picturize the cybercrime and cyber security as a ratio in these two variables in which the higher value is of cybercrime variable. This variable is being increasing with greater difference to the cyber security.

Keywords: Cybercrime, Cyber security, Phishing, Malware.

INTRODUCTION

Data is being transferred in any form such as audio, video, emails, textual form, etc. But it is never thought that the data that involved is secure or is it traveling from a secured path.

In accordance, the people or the user using these network services may or may not have knowledge regarding this contiguous aspect. Nowadays the maximum number of transactions is being held on the network. Not only transactions around 60% to 80% of the population are always online.

So considering all these situations or conditions there is a need for better security or simply cyber security implementation to fulfil the loopholes that can result in the occurrence of cybercrime.

As technology is becoming advanced day by day like Data Analytics, data science, AI, cloud computing, electronic commerce, etc. contains highly important information that requires a great level of cyber security.

But with the high in the information and technology field, there is an incremental growth of cybercrimes as well. It is nearly impossible to pinpoint the accurate cause of these cybercrimes. So there is the need for a simple and broad-point paradigm or technique to reduce the occurrence of such kind of scenario that is not healthy in any aspect for each and every field or organization or institution or industries being involved.

This technique or paradigm should be dynamic so that we can rely on it for a healthier environment.

Cybercrime

Cybercrime is an integral work that is done by involving computers or networks or an electronic device with an intention to disrupt or destroy the growth of an individual or a group of individual growth, reputation, economy physicality or mentality. The person who commits these kinds of illegal activities is known as a

cybercriminal cyber offender. Security is looked in terms of how data is stored, coded, transmitted, encrypted and deleted. Various statistics has shown that companies take security of the data of an individual with very high priority. [1]

Cybercrime can also be referred to as computer crime.

The activities that are considered as cybercrime are information stealing, e-commerce frauds, illegal transactions both monetary and non-monetary, hacking, copyright infringement, information leaking and many more.

Cybercrime can be classified in two ways.

They are as follows:

1. Crimes generated by the computer system.
2. Existing crime evolution using computers.

Crimes generated by computer system involve network system disruption, invasion or unauthorized recordings etc.

Existing crime evolution using computers involves stealing personal information, cyber threat, child abuse, impersonation, stalking etc.

The major involvement of technology in a person's life has exponentially increased cybercrime. So there should be preventive measures taken place for these cybercrimes. This leads us to the term cyber security.

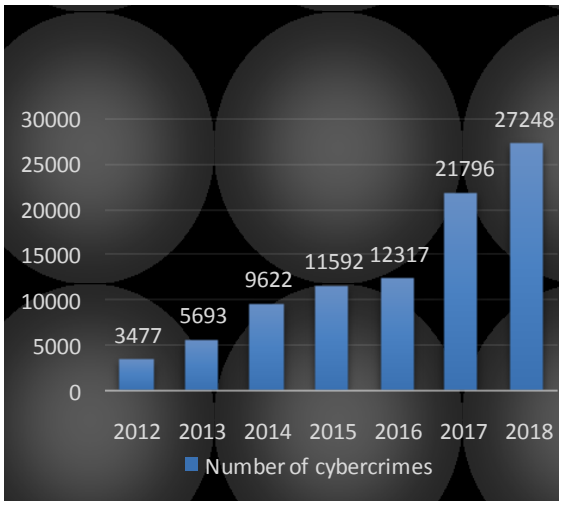

Fig:1 Following Chart Shows Number Of Cybercrimes Reported In India Only.

Top Cybercrimes or attacks

1. Compromised business emails

This kind of attack is responsible for unauthorized access to a trusted business person's email account to be accused of their identity such as making a request for fraud payments.

2. Phishing

It appears just like an authorized source but actually they are not. It tricks the person to provide his/her personal information by using any kind of Form submission or getting access to this information by making the person click on a link.

3. Malwares

Malicious Software's that enters your system by an infected link or a click-on image in an email or a web application. These software automatically runs at the background of a system and harms your system and you will never get the knowledge about its existence and processing.

4. Social engineering

Social engineering refers to social websites that let you interact with this system or other person but actually some of these social websites are used for manipulation for getting or accessing your personal information, contact information and data and even your money and much more.

5. Frauds that includes Credit and debit cards

On contrary in the last few years, millions of credit card information have been stolen and been used by unauthorized personalities.

6. Hacking

By performing hacking a hacker can get full access to the computer system that is being hacked. It has some time been proven the most dangerous situation for an organization.

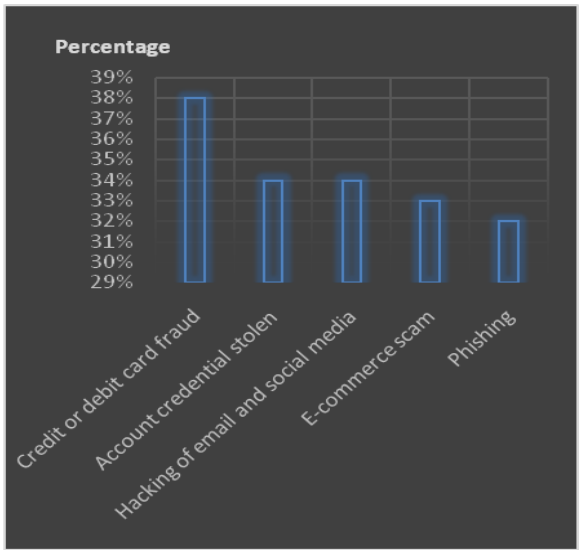

Fig: 2 Following Chart Show Different Cyber Threats With Their Occurrence In Percentage

Cyber Security

The measures are taken in against of cybercrime to enhance its security e and to deplete illegal activities performed over the network by using a computer system or any electronic device that has communication capabilities

These measures are the only thing that has result in the survival of the internet up to the date. Every organization whether small or big dealing on the internet requires some kind of security from any kind of fraud, threats, stealing, invasion, etc.

It can be considered that cyber security is a post measure taken by institutions after they interact with any kind of newly generated cybercrime or attack.

We can say that cyber security implementation is a precaution used by technical societies or organizations. Implementation of cyber security by an organization should be in a top-notch manner. As cyber security acts as a shield of protection from any kind of Cyberattacks or cybercrimes.

Cyber security can be implemented by two manners which are as follows:-

1. by an individual on a small scale.
2. by an organization at larger scale.

At individual level

At an individual level, a person using application either offline or online must create a unique authentication user ID and password that cannot be decrypted easily. He or she must take care that from and how the services are the network services are being accessed by him/her. He/she should also log out through the system after his work is the task it's finished.

At An Organization Level

As being a larger body an organization must study all kinds of aspects in the form of cyber attacks or Cybercrimes while the implementation of cyber security is being done. The organization must also make their system much more profound so it can tackle the future cyber threats that may occur at any moment of time.

Organizations Ways To Approach Cyber Security

As the information is being kept in digital form by the organization, the data privacy and security is their concern. By the implementation of cyber security, the organization wants to create a secure workspace that should also be user-friendly so they work or the task can be performed in a secure and efficient manner.

Almost every company and organization is increasing, managing and updating cyber security on contrary to their other tasks such as increment in resources and services. It has been seen that without analyzing the current situations and scenarios in terms of data implementation of cyber security is an obnoxious approach.

Techniques That Are Used For Cyber Security Are As Follows:

1. Security Of Passwords And Access Control

This implies the use of unique user identification and password for protection from unauthorized access.

It is considered to be the initial line of defense for cyber security.

2. Antiviruses

These are the software systems that are used to monitor the computer system for detecting, protecting, preventing computer viruses and malicious software programs.

They also provide protection from worms, Trojans and many more cyber threats.

3. Firewall

A firewall is a software system or hardware system that is developed to act as a security shield between the network and your computer system. It tense to protect your system from any kind of breaches, hackers, viruses, worms and don't allow them to pass through it to enter the system.

4. Scanners to locate Malware

As Malware as a security threat, the scanners are used to scan all the data in any form that documents files, etc. for locating the malware.

5. Data authentication

The data is transferred and received must be checked and authenticated that it belongs to a trusted and authorized source that is reliable too as well as while transmission of data it must not be manipulated or altered. It can be performed by data authentication tools search as a proper antivirus.

Morals For Internet Usage In Context Of Cybercrime And Cyber Security

1. The use of secure servers and networks should be in practice.
2. Not letting a server to act like a zombie server that is a server that has not been updated or used for a long period of time
3. The web is considered to be the largest collection of information it should be used in a subjective and ethical manner
4. Always avoid sharing personal information so as it may cause a good chance of being misused and traumatize your web image.
5. Never impersonate over the internet as it is a criminal offense if impersonation being used for illegal activities.
6. Avoid plagiarism whenever uploading any kind of data that you say it's yours.
7. Never use the internet with any kind of negative and destructive thinking that may cause problems in society.

CONCLUSION

Integrity of data refers to protecting information from falsely being modified by an unauthorized party. Information is valuable only if it is correct, tampered information could prove costly to both the sender and the receiver party [2]. Cybercrime can always be considered one step ahead of cyber security as even after the implementation and the usage of best of the best security patches and the services cybercrimes occurs and when it occur it sometimes results in great destruction that can be termed as cyber warfare.

We as the technology and services users and provider should never think that our security system is well and good enough for any kind of cyber attack. As somehow the offenders or the cybercriminals come with even a new way to find flaws in the system being established for the security.

In our language there is no technology present till the date without any loophole.

So we as an individual and an organization should be prepared for any kind of threats and attack over the internet at I may cause loss in many form whether physically, mutually, socially, mentally, economically in all aspect ratio.

REFERENCES

1. Chahal D. et al. Data privacy and security issues in India: An empirical study, International Journal of Research in Engineering, Volume 1; Issue 4; October 2019; Page No. 15-17.
2. Varyani Y. et al. A Survey on Cryptography, Encryption and Compression Techniques, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 11 | Nov 2019.

How to cite this article: Kumar V, Kumar G, Chahal D. Tremendous increment of cyber crime due to flaws in cyber security. International Journal of Research and Review. 2020; 7(5): 25-28.

******