WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Security Awareness: Educating Users for A Safer Online Experience

Sunidhi Swamy[1], Dr. Vishal Shrivastava[2], Dr. Akhil Pandey[3], Ms. Megha Rathore[4]

[1]B.TECH. Scholar, [2,3]Professor, [4]Assistant Professor
Computer Science & Engineering, Arya College of Engineering & I.T. India, Jaipur
[1]vaishnavsunidhi@gmail.com , [2]vishalshrivastava.cs@aryacollege.in,[3]akhil@aryacollege.in, [4]rathore.megha@gmail.com

ABSTRACT

It is important to know what cyber security is and how it can be used in real life effectively. If there is no protection , then there is risk on system files, digital data and other virtual files also. As the cyber security technology enhances , attackers also evolves new measures for attacking or hacking. Hackers are always one step above and have very good catch on various technologies. Cyber Security is essential for almost all sectors because all sector contains large amount of data of their sectors. Data can be of any types like sensitive data, property data, personal information etc. On these types of data illegal access of information is not allowed. Government and Private sector both are facing the problems of cyber attacks. The challenging issue is to protect data from cyber attacks. Cyber attacks are done for money or sometimes for revenge from someone by leaking their data. Research is done by researchers to overcome cyber attacks.[1]

Keywords: Cyber Security, Protection, Risk Management, Digital Data, Virtual Files, Attackers, Hacking, Sensitive Data, Illegal Access, Cyber Attacks, Research

Introduction

From more than 200 years ago, Internet has played a very important role in all over world communication. Advancement and cheap rate in this area have abundantly improved the availability and performance of Internet. The Internet has global network with 3 billion users worldwide. Cyber space involves sensitive information. Most important and sensitive information are contained in this space. Media data also involved in this space. Financial activities are also done through this space. A major part of capital is spent on this space by every country. Cyber space have some challenges also. Sometimes virus that comes through attacks damage financial and economic data. One more example is of a incorrect message,if an incorrect message is send the hacked message is able to stop and fail a country' s power plant. It also has a power to discontinue air traffic control system. One should always know what cyber attack is and what are its characteristics. Detailed study is important to know about cyber security and cyber attack clearly. A citizen does not know how securely his/her data ,audio/video files are transmitted. A person never wants that their information is leaked. All over world 60 percent transactions are done online , so this sector requires high security for no loss of finance. Cloud computing , E-commerce etc. also need cyber security in a large level. Law enforcement agencies should be involved in investigating cyber crimes. Today laws are imposed for cyber security. Everyone should know about cyber crimes because the cyber crimes are increasing because of very less awareness about this matter.[2]

Technology

Technology is important to provide security tools to people and organizations to protect themselves from cyber attacks. Important objects are PC, Cloud and Routers. Cyber is the collection of workstations and network. Security means to protect something. When security breaks then cyber and security takes place. Using cyber security any person or organizations can protect their data from hackers. Ethical hacking is used in cyber security.[2]

Fundamental Concepts

Some important concepts in cyber space:

Cyber Space: Cyber space is a digital network. Here interconnection of network exist where two persons communicate with each other by sending electronic messages.

Cyber Capital: It contains important data of a country in large amount and the information about the individuals residing in that country.

Cyber Threats: Cyber threat is the harm that occurs to a system.

Cyber Warfare: This is the most harmful type of cyber attack that are mentioned in national cyber crimes and have most dangerous effects.

Virus: A virus is a program that replicates itself and spreads to many documents in a system.

Hacker: A person who access a computer or program without permission and access the functionalities and browse, modify or delete the programs.

Cyber Weapon: A cyber weapon is a program to harm other cybers.[3]

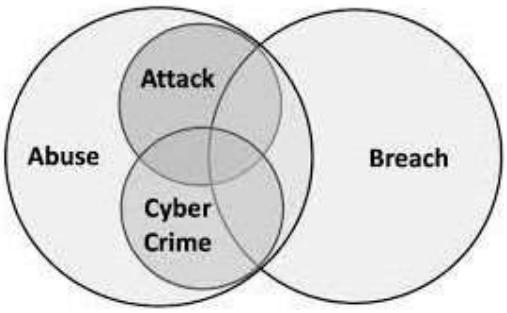

Figure: Relation between cyber attack and cyber crime

Cyber Crime

Cyber crime is an auspicious activity that uses computer as a means to commit hacking. Cyber crime is also used to store evidence in computer as per U.S. Department of Justice . Mainly all cyber crimes are done through computers. Major problems to people are identity theft, bullying and stalking. Cyber crime uses internet to steal any person' s identity. Since technology advancement is increasing ,cyber crimes are also increasing with technological advancement and hackers have a very proficient knowledge of technology.[3]

Cyber Security

It refers to providing security to users data that are connected to internet ,browse something or communicate with each other. There are various techniques to destroy virus. By cyber security only we use internet without any worry about data. People sometimes suffer a lot by loss of their money due to unawareness about crime.[1]

Types of Cyber Security

Phishing: Phishing occurs through email . The email which looks normal but actually it contains harmful program that is a form of cyber attack and is used to get data about credit card or user login details.

Ransomware: It is a harmful software. It occurs while some transaction is in processing or any person is paying something. It blocks the system until the transaction is done.

Malware: It is illegal use of a software or system that can harm system.[4]

Cyber Security Techniques

Password Security and Access Control: Most useful and basic technique for cyber security is by authentication of user which can be checked by user name and password. If the user name is valid and password is correct then only it the user can access the system, website or application. This is the first method used for cyber security.

Authentication of Data: Whenever we receive a document digitally we should check that the document is authenticated or not. Authentication of document can be checked by checking that the document is originated from a trusted source. In source we cross check that the document is not altered. Authentication is automatically done by anti virus software present in the system. So a good anti virus software is essential for a system.

Malware scanners: A software used to scan documents which are in the system that contains harmful programs. Some examples of malware are virus, worm and trojan horses. These examples are referred to as malware.

Firewall: Firewall is a software used to keep stay away hackers and virus from system that come from Internet. All the documents or messages that downloaded or shared through internet first passed through firewall to check authentication. Firewall is also used to examine messages . In detection of malware, firewall plays a signficant role.

Anti-Virus Software: This software is used to detect and then remove harmful programs,applications and viruses. Anti virus software do it functionality automatically. Anti virus software contains information about different viruses .Whenever a new virus come it stores all information about this and remove that virus. An anti virus software is also a very important part of a network and computer.[5]

Cyber Security Tools

Case Study of WannaCry ransomware attack in 2017

In 2017, a major attack occurs which influences all over world which is Ransomware attack. Ransomware mainly targets operating system which contains Microsoft Windows by demanding ransom payments in the form of cryptocurrency Bitcoin. This effect affected various sectors like hospitals, government institutions etc.

Wanna cry easily attacks software that are not updated with latest features. It increases rapidly because it replicate itself. It also infects computers connected with the infected computers.

This attack spread awareness to regularly update applications and systems. After this attack robust cyber security measures starts to implement. It includes updating of data and data backup. These measures are implemented to overcome the effects of ransom ware attacks.[3]

Methodology

Research Design: This step involves about the first step to start research . What to research and from where to research. We should made our research paper like that the person who reads research paper should understand why this topic is important.

Data Collection Methods: This step involves how to collect data for research paper. One should always while writing a research paper that how data is collected.

Data analysis techniques: This step involves the classification of data which is required for our research paper. Classification is necessary because only relevant data we should add to our research paper. We should also explain how data is classified.

Ethical Considerations: One should also discuss the issues that arise during research. Explain how you resolve these issues.

Validation and Reliability: Discuss the steps taken to check validation and reliability of a system.

Scope for Future Research : Discuss about the future scope of the research paper topic.[2]

Future of Cyber Security

Future of cyber security is challenging and complex but it has very much abundant scope and opportunities . As technological advancement increases in cyber security ,in parallel cyber threats are also increasing. But innovative ways are researched by researchers to protect people from such cyber threats.[2]

Future of cyber securities such as:

Artificial Intelligence and Machine Learning: AI tools can faster response to cyber threats to virus .So it is more effective. But right now it is not implemented. Researchers search about this and tell that it is possible to protect from cyber threats using AI tool.

Quantum Computing: Quantum Computing is used to do advancement in cyber security. Quantum computers are more efficient than traditional computers so that the encryption is done in less time. Quantum Computing is also is not implemented . It is under development stage to threat cyber crimes.[4]

The Internet of Things (IOT): IoT is he combination of both hardware and software. Today's scenario is that right now 30 billion IoT devices are available in world. These devices not help in cyber security as these devices are like a challenge to protect these devices from cyber threats.

Cloud: Cloud is a virtual network that provides software, hardware platforms on demand. This network is also vulnerable to cyber threats. So development of cyber security should also be eyed upon this sector.

So for better future of Cyber Security following points should be followed:

1. Investment upon AI and ML tools.
2. Strategy for Quantum Computing.
3. IoT devices security.
4. Training and employment of cyber security developers[5]

Conclusion:

Cyber security is a topic that is unlimited information. So advancement in this field should be done because everything is on internet today from our email, transactional details etc. All important sources are on internet. Cyber space and technologies plays a very major role in this. A hacker can be anyone .A hacker can harm anyone .It can harm not only to a single person. Sometimes it influenced on a large scale. For example… If a terrorist is a hacker than it is harmful for whole country if it gets any confidential data. National security is not only in terms of Military providing security. Cyber Security is also important on a same level. The upcoming cyber security is hard to understand and it can also be understandable to only that persons who developed that security. Before 2010 ,no one knows what is cyber security. In pandemic of covid-19 ,cyber crimes rate is doubles because everything comes digital that time. So it's a very good opportunity for hackers to threat the persons who are unaware about cyber crimes. The cyber security techniques that will come in next years need for intelligence to work upon. The humans that have good digital skills are able to understand that level of cyber security techniques. The situation of cyber crime is increasing day by day that it is necessary to fasten the cyber security techniques. The research in this domain is necessary for better exposure into this.

This research paper shows perspectives from different angles for cyber war also. Cyber Security is a very vast topic. Cyber security is also plays a role in earning of money. Cyber security also effects technological control. This research paper also provides knowledge about the cyber security goals. We

should see cyber security impacts from both angles i.e. Good or Bad. Government policies are also implemented against cyber crime. People should also know how cyber security is addressed by government.

Cyber Security also improves our decision making process. These are in the basic levels of abstraction. Complexity issues for cyber security should be resolved. The policy makers face issues while making policies for cyber security. The policy makers should also focus on that the policy does not result in undesirable consequences. Security is also a major issue in online transaction. The current security system is not so secure as sometimes scammers enters in transactional environments and users loss their money. The online payment system are not able to detect scammers. Anyone can gain that confidentiality information when the scammers or hackers enters into the payment system. Single factor authentication is not very secure that's why two factor authentication is implemented now a days for online payment system, electronic mails, etc. Financial institutions should focus on reducing risk factors and implements security techniques. This technique is very useful to reduce fraud for financial institutions. So conclusion is that cyber security implementation is necessary. [5].

References

[1] Mrs. Ashwini Seth (2021). Research Paper on Cyber Security https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security

[2] Nikhita Reddy Gate (2014). A study of cyber security challenges and its emerging trend on latest technologies. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[3] Yuchong Li (2021). A comprehensive study of cyber security and cyber attacks

:Emerging trends and recent development. https://www.sciencedirect.com/science/article/pii/S2352484721007289

[4] Kutub Thakur (2015). An Investigation on Cyber Security Threats and Security Models. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing

[5] Rossouw von Solms (2013). From information security to cyber security.https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801