2nd National Level Students' Research Conference on
"Innovative Ideas and Invention with Sustainability in Computer Science and IT-2021"
In association with International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

An Answer to all the Wh questions of Cyber Security

Poojan Patel, Nareshkumar Borana, Rohan Khalipe, Rohan Das, Deepali Sonawane
School of computer science, Dr. Vishwanath Karad MIT-WPU, Pune, Maharashtra, India

ABSTRACT

In today's digital world where man can't even think of doing anything without the help of internet, the most important thing that comes to everyone's mind is that 'Is their data safe or not'. And from these suspicious questions arises the topic 'Cyber Security'. Every year lots and lots of money is invested into this field just to be sure that everyone's data is safe and secure. But still the crimes are increasing day by day. Every other day thousands of people suffer due to Cyber Attacks and Hacking. But is this only governments responsibility to investigate this concern? isn't this an educated citizens responsibility too? This paper mainly focuses on such Wh questions that arises to many people and besides will provide the answers to their questions.

Key points:

- When was Cyber security introduced?
- What are the biggest cybersecurity threats?
- Where do we use Cyber Security?
- Who all are responsible for Cyber-security?
- Why do we need to worry about information security?
- How to prevent and overcome Cyber-attacks?

Keywords: cyber-security, cyber-attack, hacking, cyber-crime, threats, information security, network security, recover.

I. INTRODUCTION

Before digging into the research paper, the biggest question arises to all of us is 'What is cyber security'? The answer lies into the question itself. Protection as well as recovering of network-based devices and programs from any kind of malware attacks is basically cyber security.

The data and its integrity of computing assets that belong to a certain organization are protected by cyber security. The sole purpose of it is to defend against all the threats throughout the entire cyber-attack.

With every passing second the danger of cyberattacks to common people, companies and organizations

increases. Nobody knows how a malware attack is designed to access one's data. It can destroy/steal their personal information; it can also disrupt businesses and one's financial assets. To avoid being cyberattacked we need to build strong cyber security systems along with making smart cyber defence choices.

II. WHEN WAS CYBER SECURITY INTRODUCED?

The history of Cyber security can be traced back to an era when file malwares and ransomware attacks where not much to worry about. The history can be traced back to 1970s when the topic rose to great hights just because of a research project. Bob Thomas sensed that he could send a program across certain network simultaneously leaving trails
behind it. He named this program "CREEPER". He found it entertaining and went on printing a message "I'M THE CREEPER: CATCH ME IF YOU CAN."

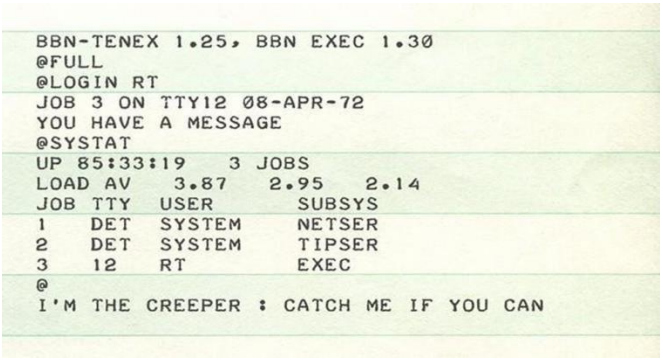

Fig 1: This is an example of the creepers taunting message.

Not soon a man named Ray Tomlinson followed this idea and by doing some changes he made his own self-replicating program also known as the very first "COMPUTER WORM". At the same time, he wrote another program that helped to detect the Creeper. He named it "REAPER" which was also the first ever Anti-virus software.

III. WHERE DO WE USE CYBER SECURITY?

Questioning about uses of IT security might sound like a fool's question, but there is lot to discuss about.

- As we talked earlier the main use of cyber security is to protect businesses and sensitive data breaches.
- Secondly comes the protection of endpoint user from unauthorized user.
- It protects the computer from certain viruses and malwares. A virus might not harm a business initially, but it can slow down the productivity carried by the employees.
- Along with the protection of public data it also needs to ensure quick recovery after a malware attack.
- To sum up a security shield also holds the reputation and trust of the people to their company.

IV. WHO ALL ARE RESPONSIBLE FOR CYBER-SECURITY?

Cybercrime is either everyone's problem or no one's. It can't be blamed on anyone. In a business or organization, people generally say that the CEO is responsible for handling such issues. But the matter should be looked after by every single employee, by every junior/senior partner, the manager and finally the CEO. Talking about the common people we are completely depended on ourselves. Timely checking of personal data, changing of password and using verified anti-virus software.

Fig 2: Who's responsibility is cyber- security.

V. WHAT ARE THE BIGGEST CYBERSECURITY THREATS?

Without any doubt whenever we talk about the threats of cyberattack the first term that comes to our mind is 'HACKING'. To elaborate we can divide those threats as follows:

- **Ransomware attacks**
  These kinds of attacks are planned intentionally. It follows a basic path of locking an organization's network and encrypt their sensitive data. The main target of such attacks are commonly big business firms.

- **Phishing scams**
  This is one of the most common online scams, targeting the consumers it effects a lot of livelihood. The cycle starts from sending an e-mail or message that seems to be sent by a well-known company, bank, insurance agency or network provider. They trick the consumer into giving their personal details and later use the information to gain access to one's mail, bank and many other accounts.

- **Malicious threats**
  Malicious attacks are done by the MCAs (Malicious cyber attackers). They generally provide viruses, exploits or other threats that carry the potential to destroy one's device, network and systems. It completely crashes the whole system with no chances of recovery.

- **Unauthorized access**
  As we all know unauthorized access means bursting into someone's else data without their knowing or consent. The main reason for such data breaches is weak passwords and firewall. Sometimes due to broken authentication mechanism invites the unauthorized parties.

Leaving all the above threats there are also many other threats such as Insider attacks, APT attacks, brute force attack etc.

Graph 1: Biggest cyber-security threats.

VI. WHY DO WE NEED TO WORRY ABOUT INFORMATION SECURITY?

The biggest asset one hold is his own information and protecting it is very vital. When it comes to protection of personal information the very first thing to strike one's mind is using a strong password for various sites and using effective anti- viruses. Apart from protecting one's personal data information security plays many other important roles in organizations and companies. Some of them are:

- Protecting the organization's sensitive and liable information along with the clients confidential information.
- Helps to protect the company system from crashing.
- Prevents the Data-breaches that may lead to financial downfall of the company in terms of revenue and stocks.
- A good firewall between the organization and hackers saves a lot of money.

- Sustains the ability of the company to keep on functioning and maintains the reputation of the company.

VII. HOW TO PREVENT AND OVERCOME CYBER-ATTACKS?

Preventing a cyber-attack might look like a headache but there are various simple and economical steps:

i. The very first step is to change your password on daily basis.
ii. Keep an eye on the latest updates of your browser and ensure your site is secure before visiting it.
iii. When someone obtains your personal data without your knowledge, identify it as soon as possible to prevent fraud in future.
iv. In an organization it is the duty of the CEO and the manager to provide the knowledge regarding cyber security.
v. Keep your anti-virus updated and always trust on the verified software' only.
vi. Backup your data after every certain period.
vii. Whenever you are suspicious about a malware or fraud you should always report it.
viii. In an organization to prevent physical fraud, limit the access of employee to the data and information.
ix. Using a secured network is also important to make sure it is hidden and private.
x. To prevent future loss of money you should purchase a Cyber insurance policy, in case you suffer a cyber-attack.

Even after following the principles to prevent cyber-attack there are chances that we still might fail. To overcome a cyber-attack, we should always be ready.

Some of the ways are:

i. Having a backup of data is always helpful. In case of a malware attack if you lose your data, you can easily regain it.
ii. Close all the unauthorized and unproductive accounts that charges your account.
iii. Leaving all the regrets apart one should think about what other information might be at risk and take necessary steps to prevent it.
iv. In case if there is a financial fraud you should file a report instantly.
v. Finally, if an organization gets hit by a data-breach they should instantly make changes to their encryption level and make sure that every employee follows the same.

Fig 3: How to overcome cyber-attack.

VIII. CONCLUSION

From the paper we would finally like to conclude our topic. After covering major topics, we can say the field of IT is spreading very fast. Whether we like it or not, but IT is the reason for the rise of cybercrime and it's our duty to fight it and overcome it. People might try to take advantage of this, but we should be prepared from our side. Campaigns on cyber security should be raised to increase the awareness. With

proper knowledge we will have more skilled workers in the field of cyber security organizations. However, looking at the evolving nature of cyber security we need to declare it as a global threat and need to find a solution to it internationally.

IX. REFERENCES

[1]. https://www.upguard.com
[2]. Cyber Security: Understanding Cyber Crimes - Sunit Belapure Nina Godbole
[3]. https://www.quora.com