Loss of Data Privacy through Hacking

Ms. Doreen Dsouza[1], Ms. Arwa Rangwala[2], Ms. Amanpreet Kaur Hora[3], Ms. Sanskriti Koli[4] and [5]Dr. Shine David

[1]Student, Institute of Management Studies, Devi Ahilya University, Indore, MP, India

[2]Student, Institute of Management Studies, Devi Ahilya University, Indore, MP, India

[3]Student, Institute of Management Studies, Devi Ahilya University, Indore, MP, India

[4]Student, Institute of Management Studies, Devi Ahilya University, Indore, MP, India

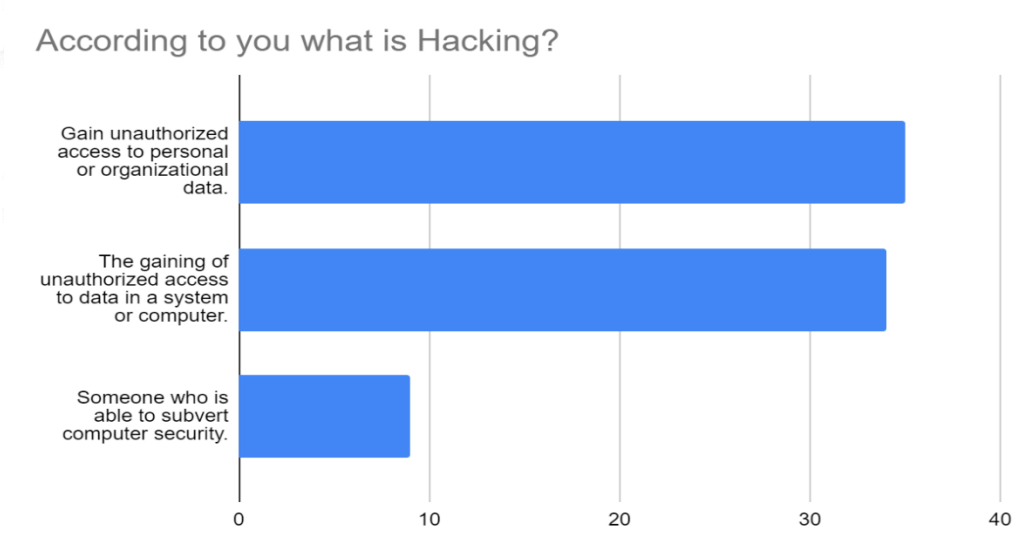
[5]Assistant Professor, Institute of Management Studies, Devi Ahilya University, Indore, MP, India

Abstract - In today's increasingly interconnected digital world, data privacy has become a critical concern for everyone. The widespread use of online services, social media platforms, and digital communication channels has led to the generation and storage of vast amounts of personal and sensitive information that stays online. This has made individuals and organizations exposed to hacking attacks, where cyber fraudsters exploit vulnerabilities to gain unauthorized access to confidential data.

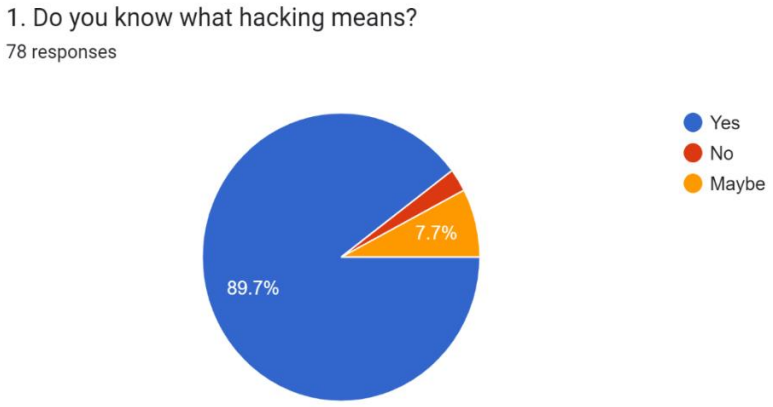
Index Term - Privacy issues, hacking, hacker, ethical hacking, cyber security.

I. INTRODUCTION

Data security is the safety given to an individual from unauthorised access from third parties and black hackers which steal our information. For controlling these issues hacking is created. Information Technology is turning towards hacking more and more each day. Hacking is not only done by criminals or any political parties or government bodies but it's also done by an organisation who wants data safety, and security as their main motive or means of earning.



Hacking is gaining unauthorised access to someone's digital devices. This is done by exploiting weakness of a computer system or network. This can be saved to some extent by using anti-virus software. Through our research we found that about 89.7% people are aware what is hacking.



Hackers are people proficient in hacking skills, have high level knowledge of computer network, computer languages and have intentions of harming others by entering their digital devices and causing harm to their devices or system or use their personal information.

There are mainly three types of hackers.

WHITE HAT HACKERS

They aim to improve security of the system or network. They do not have bd intentions. They work to spot computer system or network security flaws that ill-intentioned hackers could use to their advantage.

GREY HAT HACKERS

They hack for fun and enjoyment. They do hack private networks without permission and break the law, but do not have malicious intentions.

BLACK HAT HACKERS

These hackers cause serious damage to someone's device and steal personal information for their advantage. They are hacking experts and are great at causing cyber-attacks and cyber-crimes.

Hacking is illegal when-

* Working is illegal when a person or any hacker tries to breach someone's data without permission. It is unlawful or illegal. These are known as Black Hat Hackers. They are known for notorious ways of hacking. They do for fun.

* Cyber espionage is also termed as illegal hacking. Some hackers try to expose someone or leak personal information.

* Hackers hack for political parties which is also illegal.

* Hackers sometimes used for making higher profits in the organisation this type of hacking is known for organisation crime hacking which is illegal.

* They hack for their personal fun, for money, or because somebody tries to put pressure on them for their own motive or agenda.

* Hacking is illegal when all the above points are conducted by any hacker. Because permission is not given to hackers to access the data.

Hacking is legal when-

* Not all types of hacking are crime, some people are engaged in Cybersecurity and work as ethical hacker for earning.

* Ethical hacking is done for gaining access over the system to find weakness.

* Professional penetration also testing another type of legal hacking. Penetration hacking is done when an organisation wants to check in their system and if find any mistakes then hackers can catch them.

There are 3 types of penetration testing which are -

1) Web Application Penetration Testing: - In this type of testing, company ask hackers to test their websites and application to find any weakness in their system.

2) Big Bounty: - In this type of testing, a group of Hackers are chased by an organisation to find weaknesses and if any hacker catches the mistake and find the weakness then he/she will be paid by the organisation.

3) Mobile Device and Mobile Application: - In this hacking is done on mobile devices by the hacker to find any fault.

Legal hacking helps in preventing access to our system or network and helps in protecting our data from getting misused.

II. Measures to control hacking

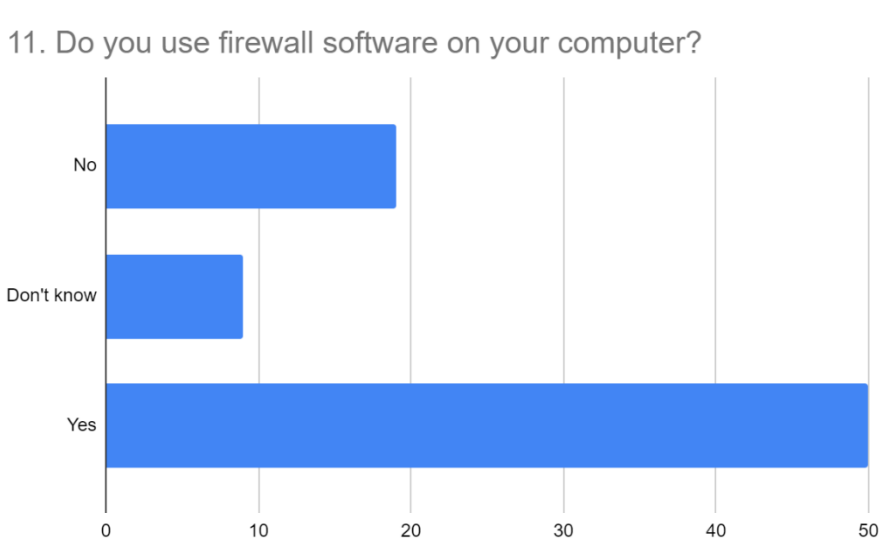
1) We can also use firewall for security of our data from hackers: -

Firewall is a network security device that check if the data is safe or not which is coming from other network systems or going outside from our system. Firewall can be of two types-

• Hardware and

• Software

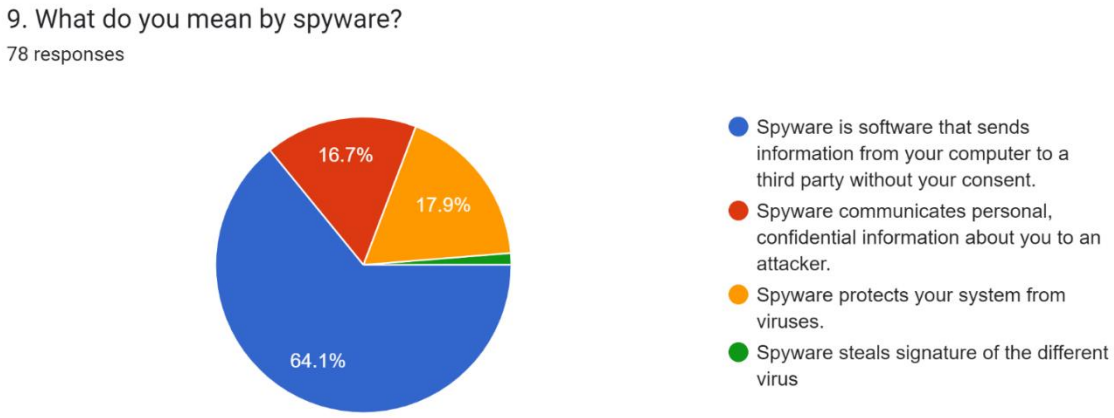
It acts as a barrier between your information and other network systems.



2) We can install anti-spyware to protect our computer: -

Spyware is a software that collect all the information of the data which is not permitted or unauthorised to used. Some spywares access each bit of the information.

Therefore, to resolve this we install anti-spyware to protect our data from getting fetched by other people.



3) Antivirus software can be installed: -

It detects any source of virus in your computer and provide safety to our data as well as it provides automatic updates so that it predicts new viruses that are emerging into your computer.

4) Have a computer back up: -

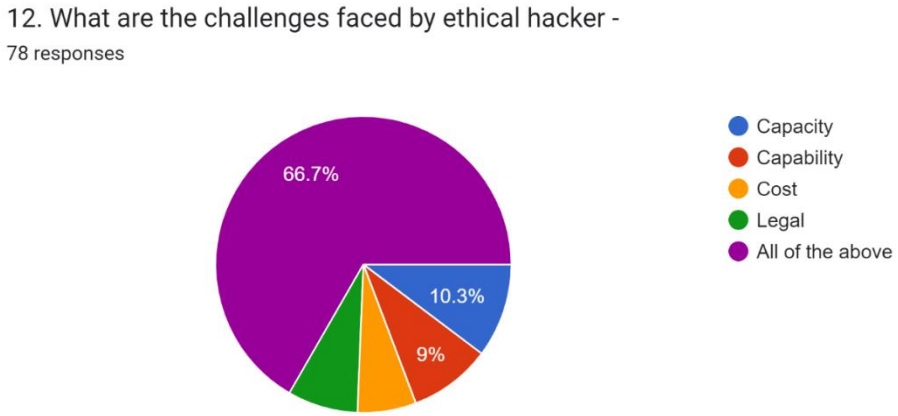
If you are known that your data can easily breached by hacker, then you should always prepare for the back up your computer and restart it.

5) We can also use double authentication: -

We can use double authentication or double password for stored data, so that it lowers the chances of getting hacked. Two layers of authentication or putting double password will increases safety as it requires long procedure to process in someone's computer or any device.

III. Ethical Hacking

Hacking is not always bad as there are hackers who work with different motives. White hat hackers also known as ethical hacker's hack with permission at defended organisation. This form of hacking is legal and known as ethical hacking or we can say that ethical hacking is based on ethical or moral values without any ill motive.



IV. Types of ethical hacking:

1) Web application hacking: It is a type of process of exploiting, vulnerability, or weaknesses in web-based applications. It is possible to perform some actions on a website without being authorised.

2) Hacking wireless network: It can access computer without authorisation, by exploiting the weak points in system's security. In this an attacker can drives around with a laptop or other device capable of picking up wireless signals, looking for poorly protected network.

3) Social Engineering: Social engineering involves making direct contact usually by phone or email to gain the confidential information. Basically, it is of three types:

1) Human based social engineering.

2) Mobile based social engineering.

3) Computer based Social Engineering.

4) System Hacking: System hacking is the sacrifice of computer software to access the targeted computer to gain the sensitive data. It aims to gain access, acquire privileges, and hide files.

5) Red teaming: red team is a group of security experts. Red teaming plays a significant role in organisations to access and improve cybersecurity defences. Red teaming allows organisation to identify vulnerability and strengthen their defences before a real attack occurs.

V. CONCLUSION

People are very serious about their own company. They see hacking as a very serious matter and to deal with it some companies pay a lump-sum amount for it, and some are not that much concerned about it as technologies are emerging in the markets and people are more focused on earning high revenue and keeping the track or checking all the trends are followed or not. But they do not understand that for growth they need safety and security of their data as well it is a factor of concerning more about rather than earning revenue. For security of the data, companies should keep a check on what information is going in and out of the company and maintain those confidential records in their personal servers. Ethical hackers play a major role here, as they are trained for the data security and help companies from data breaching. These types of hackers stored the data and kept it private only authorised people can access it. Security is everything for the companies to run effectively and efficiently and hold the high position in the markets. Ending the security issues a user or developers should employ a highly skilled professional.

VI. REFERENCES

[1] Segun, D., & Segun, D. (2022). When Is Hacking Illegal And Legal? [Honest Answer]. SecureBlitz Cybersecurity. https://secureblitz.com/when-is-hacking-illegal-and-legal/

[2] Singh, J. (2021, May 27). Hacking Legal or Illegal? (Ethical Hackers, Hacktivists). Cyber Security Kings. https://cybersecuritykings.com/2021/05/27/hacking-legal-or-illegal-ethical-hackers-hacktivists/

[3] Freedman, M. (2023). 18 Ways to Secure Your Devices From Hackers. Business News Daily. https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html

[4] Home. (n.d.). https://m.economictimes.com/definition/hacking/amp

[5] What is a Hacker. (n.d.). study.com.

[6] Naveen, & Naveen. (2023). What is Ethical Hacking? Definition, Basics, Types, & Attacks Explained. Intellipaat Blog. https://intellipaat.com/blog/what-is-ethical-hacking/

[7] Different Types of Ethical Hacking with Examples. (n.d.). https://www.knowledgehut.com/blog/security/types-of-ethical-hacking