IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008175|

A Study on Cybersecurity Awareness in Covid-19 Pandemic

Sonu Saw[1], Himanshu Pawar[2]

U.G. Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[1]

U.G. Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[2]

ABSTRACT: In this unusual event of covid-19 pandemic, the life of people worldwide changed their way of living. The general purpose of this research paper was to analysis the awareness of cybersecurity among the participants through survey. As cyber-attacks are increasing globally during covid and it affects every internet user. When it comes to cybercriminals, they don't look for your cast, gender, age, bank balance, student or professional, working or non-working… they just attack your system to misuse/manipulate/steal/encrypt your data in hope to increase their capital in anyway. We analysed the survey for the awareness of cybersecurity by asking some simple question to technically specific question so a general individual can also answer the questionary. We also added the cybersecurity safety tips as the solution to help the internet users.

KEYWORDS: Computer security, threats, Cybersecurity Awareness, covid-19, cyber safety.

I. INTRODUCTION

Cyber security is the practice of protecting your computers, servers, mobile devices, electronic systems, networks, and data from cybercriminals who misuse your device or data for their personal benefit. In recent years, cybercrime is a huge challenge in all areas including national security, public safety and personal privacy. In covid-19 pandemic, the frequency of cyber-attacks has increased dramatically due to increased user and usage of internet and therefore the need for cyber awareness has been increased. Thus, to prevent a user form cybercrime, internet users must know about their own security and safety measures to protect by themselves. Due to lockdown, many companies have encouraged their employees to work from home. Thus, this made these technologies closer to us and even an important part of our working and personal lives. Despite this, it is noticeable that companies or organization are not capable to provide a 'cyber-safe' remote-working environment to their employee due to lack of technology advancement and unpreparedness. Due to the lockdown, the people who are connected to the networks is increased and thus it became a major concern to everyone including government bodies, enterprises as well as remotely working employees, online lectures attending students and other internet users. Therefore, it is genuinely concerning issue on account of the emerging cyber-threats and security incidents targeting vulnerable people and systems globally.

II. RELATED WORK

The internet users seems to be under safe environment and use it on a daily basis using their mobile, tablets and computers whereas there are a large number of attacks on a daily basis [1]. The global covid pandemic, has led to huge number of employees globally are working from home. This has created drastic change in way of living and thus increased the need of cybersecurity awareness. Because Cybersecurity breaches can impact a lot by DDoS attack, manipulation/misuse of data, identity theft, fraud or even taking over control of systems [1]. In 2019, Global Endpoint Security Trend Report shows 42 per cent of endpoints are unprotected at any given time. Therefore, the employee working from home should immediately get knowledge about their privacy and cybersecurity [2]. Our society is appearing as a cyberphysical society having dependency on Information and Communication Technology (ICT) across all aspects of livelihood [1]. Ransomware is malware that encrypts your computer or prevents you from accessing you're your files using private key encryption until you pay a ransom generally in crypto currency. If the data is backed up, there is no need to pay a ransom to get your files. It can be easily recovered from the backups saved by you. Of course, the backups should not be much old. Some ransomware attempts to encrypt locally connected backup systems,

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008175|

so users are recommended to use a cloud backup or a system that is only connected while the backup is being made [3]. Checkpoint's report titled 'Cyber Attack Trends: 2021 Mid-Year Report' highlights dominance of ransomware attacks which has increased 93% in the first half of the year compared to the same period a year ago. As per global cybersecurity company Kaspersky's, recent report shows 45% of online users in India were attacked by local threats in the year 2020. The year 2020 has witnessed a great chaos due to the covid19 pandemic and therefore there are rise in number of cyberattacks in India as well as around the world. The increased activity of cybercriminal became a major concern for the government bodies, businesses as well as working from home employees, students and internet users (Kaspersky.com). This pandemic was a remarkable unusual event which changed the lives of billions of citizens worldwide. Beside the extraordinary impact, the pandemic has generated a group of unique cyber-crime related circumstances which also affected society and business [4]. Cybercriminals generally look for targeting vulnerable systems for their benefits. A Rise in COVID 19 Related Phishing and Ransomware Attacks: Authors also noticed an increase in phishing attacks, and ransomware attacks from a study released by the Cyber Intelligence Centre [6]. All different size of companies and types have minimal cybersecurity resources as compared to normal days before covid-19.

III. METHODOLOGY

To check the targeted group for cybersecurity awareness, we used non-probability sampling in this research paper i.e there is an assumption that there is an even distribution of characteristics within the population, believing that any sample would be representative. The age range of below 18 till above 60 years was taken into consideration for the purpose of the study. We received 62 responses in the survey within 4 days of timeframe. The tools used were a structured questionnaire where most questions were close-ended including gender and age was self-administered. We used Google Forms to create the layered questionary Form and link of the Form was circulated in social media platform to get responses. Our aim from this questionnaire-based survey research was to analyse evaluate the understanding and awareness of cyber security. So, we started with some basic questions to the participants like gender, age etc.

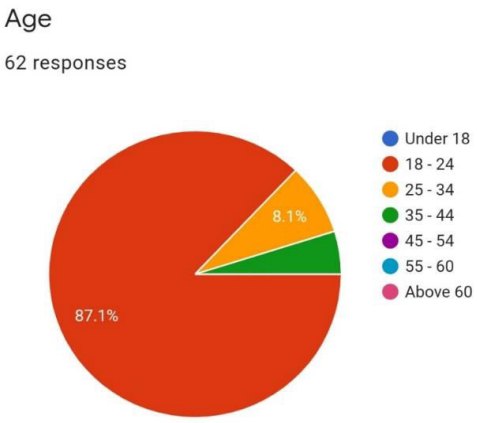

Figure 1

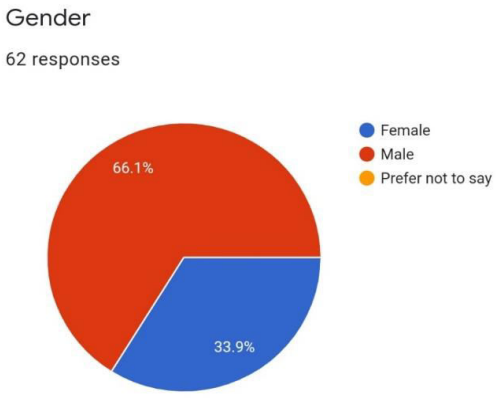

Figure1.1

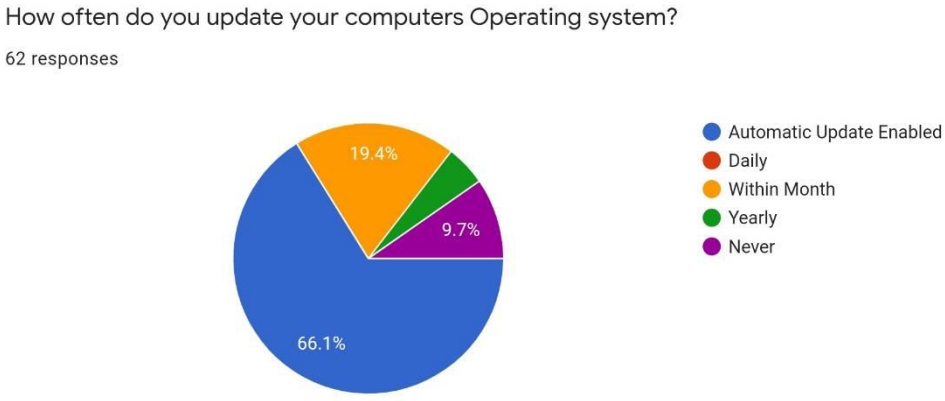

Figure 2

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008175|

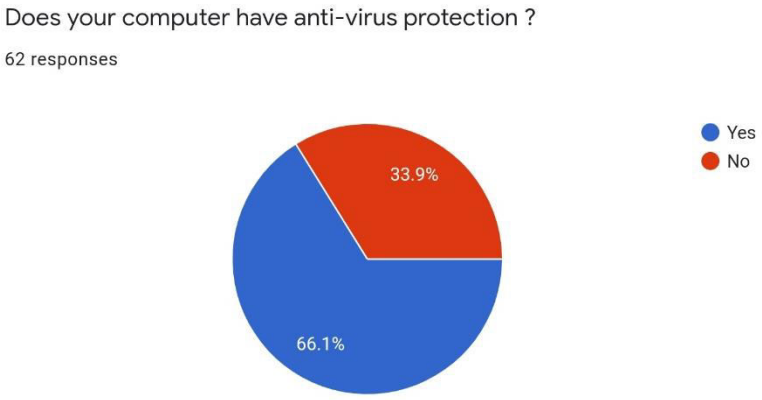

Figure 2.1

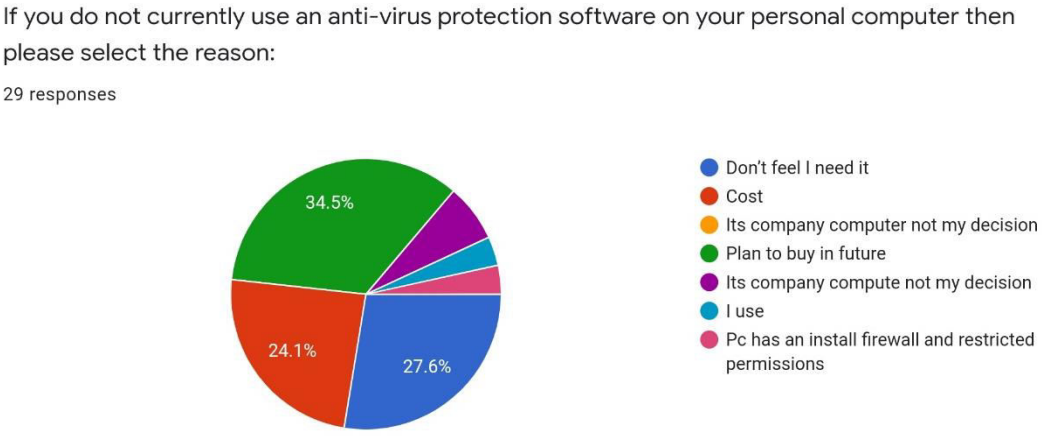

Figure 2.2

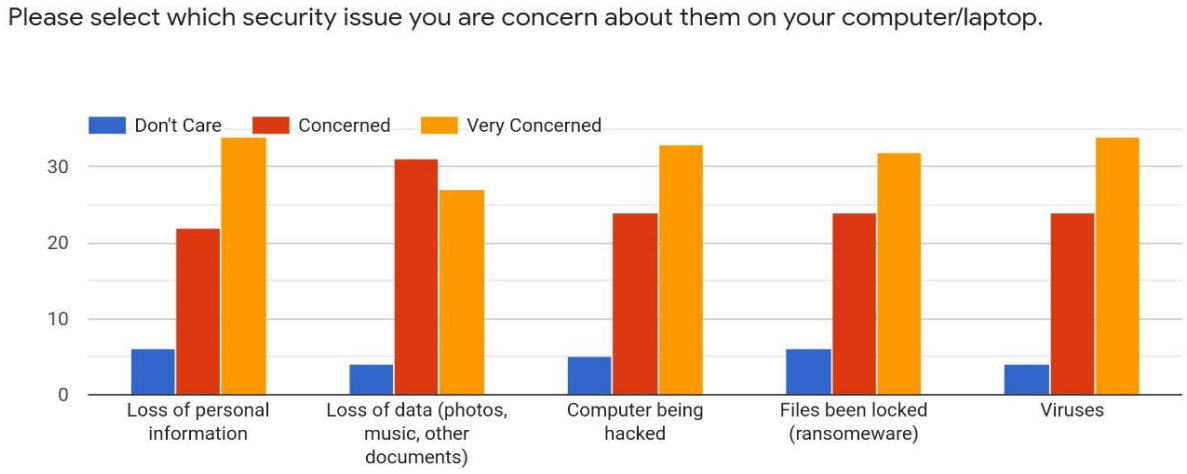

Figure 3

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008175|

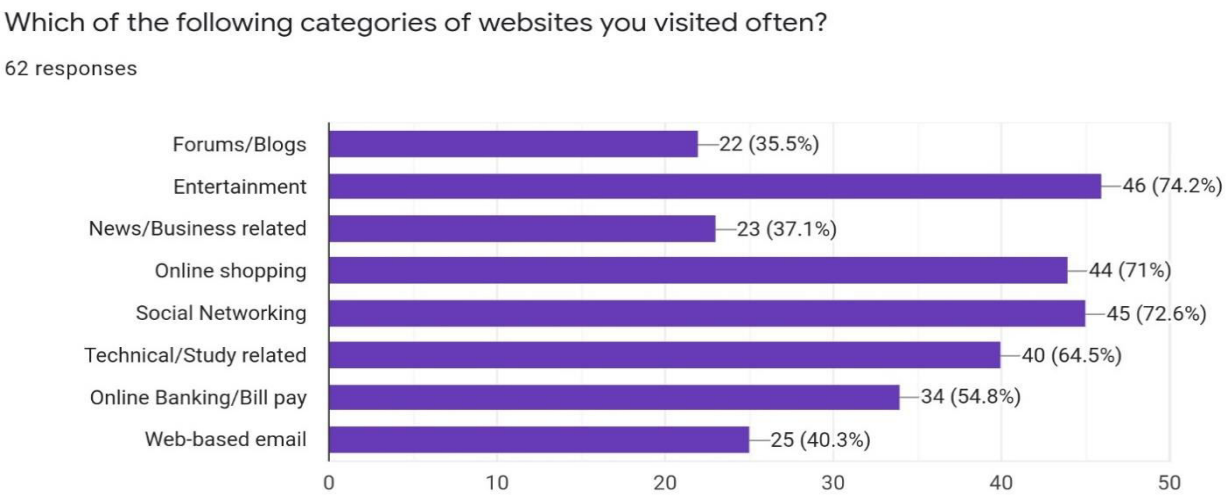

Figure 4

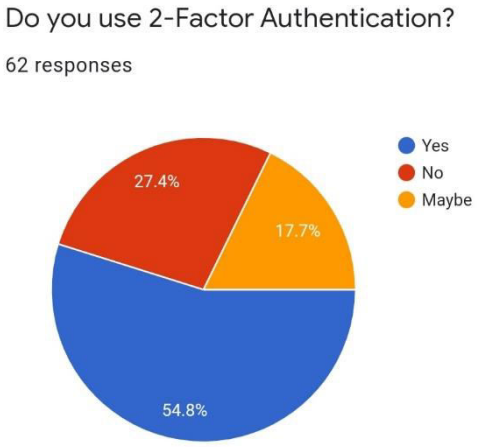

Figure5.1

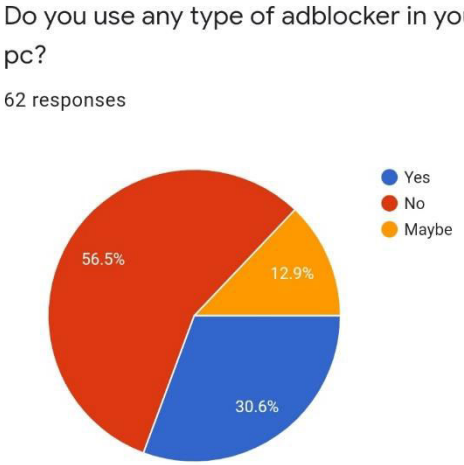

Figure5.2

IV. EXPERIMENTAL RESULTS

We got 62 responses in the survey where 66.1% were male and 33.8% were females as in figure 1.1. The major age group involved were 87.1% of 18-24 age range in figure 1.2. It is observed that nearly 66.1% of participants (figure 2) keep automatic update enable for their Operating System. Figure 2.1 shows that 66.1% of participants have installed anti-virus protection in their system while remaining 33.9% have some reasons or issue with it. For participants not using anti-virus protection on their system refer figure 2.2 show a surprised result that 34.5% participants want to buy Anti-virus software in future and 27.6% don't even feel that they need anti-virus software. The third major insight here is that 24.1% don't use antivirus protection software because of high cost and one of the reasons can be renewal of the license for the antivirus program yearly. From Figure 3, we get analytics that almost all participants are very concerned to lose their personal information from their system. Overall, we can say that participants having anti-virus protection or not they are concerned about their data being lost or stolen or hacked/misused or data locked. Very few responses were in all category that they don't care for their data. From Figure 4, we asked that which website you visit often or regularly, So, we got participants often likes to visit entertainment-based website followed by Social Networking, Online shopping, study-related website respectively. The least visited websites by the participants are Forums/blogs followed by News/Business related, web-based email respectively. Keeping Maybe option apart, figure 5.1shows that only 54.8% participants use 2-factor authentication and 27.4% says a clear no to 2-factor authentication. From Figure 5.2 we came to know that 56.5% participants don't use adblocker in their system while 30.6% uses it and remaining 12.9% responded maybe.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008175|

V. RECOMMENDED SAFETY TIPS

1. Keep your operating system and software's updated.
2. Use anti-virus software to monitor your system in real time and keep your software updated for the best level of protection.
3. Use strong passwords with two-factor-authentication wherever possible to add extra security layer.
4. Avoid using unsecure Wi-Fi networks in public places because unsecure networks leave you vulnerable to man-in-the-middle attacks.
5. Always have a backup copy of your important files in cloud storage or have a dedicated external hard disk to keep the data offline available in case of Ransomware attack.
6. Use adblocker to block unnecessary ads/ad click/popups to your system/browser.
7. Never share any OTP, CVV, Pin, Password or confidential information.
8. Only Visit sites having SSL certificate.

VI. CONCLUSION

We can conclude that more people are becoming aware of cyber threats as most user were using antivirus program though it does not mean that they are completely safe from cyberattacks. They should also consider the use of 2-factor authentication and adblocker because they are one of the effective ways to avoid the unwanted ads/popup and be safe. The overall results indicate that they need more awareness of all cyber security incidents and their consequences. Based on the weaknesses identified in this survey, we have some recommendations as suggested solutions to overcome them for a proper safeguard of their personal data or important files now and in the future.

VII. ACKNOWLEDGEMENT

I would like to express my gratitude to our Prof. Swapna Augustine Nikale, Department of Information Technology of B.K. Birla College of Arts, Commerce and Science (Autonomous) Kalyan, who guided me throughout this research. I would also like to thanks participants who responded, my friends and family members who supported me.

REFERENCES

[1] Building Cybersecurity Awareness: The need for evidence-based framing strategies, de Bruijn & Janssen - Government Information Quarterly – 2017
[2] Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity, Ahmad - SSRN Electronic Journal – 2020
[3] Ransomware: Evolution, Mitigation and Prevention, Ronny Richardson and Max North, GA USA -2017
[4] Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Lallie et al. - Computers & Security – 2021
[5] Impact of COVID-19 Pandemic: A Cybersecurity Perspective, Baz et al. - Intelligent Automation & Soft Computing – 2021
[6] McKinsey & Company, "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets." 2020
[7] COVID ‐ 19 pandemic cybersecurity issues, Pranggono & Arabo - Internet Technology Letters - 2020

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details