IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

"Awareness and Concerns Regarding Cybersecurity Threats Among Internet Users"

*Suhaib. K, Department of Science

Under the guidance of

Name of the guide: Dr. H R Bhargava

Designation of guide: Professor

Department: Department of Forensic Science

ABSTRACT

This research delves into the awareness and worries surrounding cybersecurity threats among internet users. Given the escalating presence of digital technologies, cybersecurity threats pose significant risks across various sectors globally. Utilizing a comprehensive examination of literature and user surveys, this study aims to investigate the extent of awareness regarding cybersecurity threats, perceived risks, and actions taken to address these concerns. Results indicate that although there's a general acknowledgment of cybersecurity issues, many users lack a profound comprehension of the potential online hazards they face. The study also identifies prevalent worries such as data breaches, identity theft, malware, phishing attacks, and ransomware.

Moreover, it analyzes the factors influencing users' attitudes and behaviors towards cybersecurity, encompassing demographics, past encounters, and educational backgrounds. Grasping internet users' awareness and concerns about cybersecurity threats is vital for devising effective strategies to bolster online safety and security for individuals and entities alike.

KEYWORDS: Cyber security threats, Malware, Phishing attacks, Ransomware, Data breaches, Identity theft.

CHAPTER 1

INTRODUCTION

1.1 Cyber threats

The internet's rapid growth has revolutionized how individuals and organizations function, creating a highly connected global landscape with seamless information exchange. However, this digital transformation has also introduced a spectrum of cybersecurity threats that jeopardize privacy, data integrity, and overall online security. From phishing scams to advanced malware, cyberattacks have become more common, targeting both personal and corporate data. Consequently, understanding internet users' awareness and concerns about these cybersecurity threats is essential. This study seeks to investigate the current level of awareness among internet users regarding various cybersecurity risks, identify their main concerns, and evaluate the measures they employ for online protection. By exploring these aspects, we can gain critical insights into the effectiveness of current cybersecurity education and identify areas needing improvement to enhance digital safety for everyone.

1.2 History

The history of cyber threats includes early hacking at MIT and the creation of the first virus and antivirus in the 1960s-70s, the emergence of sophisticated threats like the Brain virus and Morris worm in the 1980s, a surge in internet-based threats such as the Melissa virus in the 1990s, diversification of threats with the I LOVEYOU virus and Mydoom worm in the 2000s, and the rise of advanced threats like phishing, ransomware and IoT attacks from the 2010s to the present

Where Do Cyber Threats Come From?

Cyber threats come from multiple sources, including cybercriminals who aim to make money through methods like ransomware, phishing, and identity theft. Nation-states and their sponsored hackers attack critical infrastructure, government bodies, a0nd companies for espionage, sabotage, and political leverage. Insider threats come from unhappy or careless employees who misuse their access to important information. Hacktivists, motivated by political or ideological beliefs, carry out attacks to support their causes. Additionally, automated bots and malware exploit system vulnerabilities, often spreading quickly and causing extensive damage.

1.3 Types Of Cyber Threats:

1. **Malware**: Software designed to infiltrate, disrupt, or gain unauthorized access to computer systems, such as viruses, worms, Trojans, and ransomware.

What does malware can do?

Malware is capable of infiltrating networks and devices, and it is crafted to cause damage to those systems and their users. The impact of malware varies depending on its type and purpose. Sometimes, the effects are minor and harmless, while in other cases, they can be extremely destructive.

2. **Phishing**: A phishing attack is a type of cyber attack where attackers impersonate legitimate entities to deceive internet users into revealing sensitive information, such as passwords or credit card numbers. This is typically done through fraudulent emails, messages, or websites that appear trustworthy. The goal is to steal personal data for malicious purposes, such as identity theft or financial fraud.

3. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks:** A Denial of Service (DoS) attack is a cyber-attack aimed at making a computer system, network, or service unavailable to its intended users. It is typically achieved by overwhelming the target with a flood of internet traffic, consuming its resources and preventing legitimate requests from being processed. This can cause the targeted system to slow down significantly or crash entirely, disrupting normal operations.

4. **Insider Threats:** Risks presented by someone within an organization, like an employee or a contractor, misuses their access to harm the company. This could be stealing sensitive information, sabotaging systems, or causing other types of damage from the inside.

5. **Social Engineering:** It is like psychological manipulation used to trick people into revealing confidential information or performing actions they wouldn't normally do. It's like someone pretending to be your friend to get your password or pretending to be an authority figure to get you to do something you shouldn't

6. **Man-in-the-Middle (MitM) Attacks:** A Man-in-the-Middle attack is when someone sneaky gets between two people talking online and listens in or changes what they're saying without them knowing. It's like someone secretly listening to your phone call or tampering with your messages before they reach the recipient.

7. **Ransomware:** Ransomware is like digital kidnapping. It's a type of malicious software that hackers use to lock you out of your own computer or files. They demand money (a ransom) in exchange for giving you back access. It's like someone locking your house and demanding money to give you the key.

CHAPTER 2

AIMS AND OBJECTIVES OF THE STUDY

AIM OF THE STUDY

The aim of this survey is to assess the level of awareness and concerns regarding cyber security threats among internet users. It seeks to understand how knowledgeable individuals are about potential online risks, their experiences with cyber threats, the measures they take to protect themselves, and their attitudes towards the importance of cyber security. This information will help identify gaps in awareness and provide insights into the effectiveness of current educational and preventive measures related to cyber security.

OBJECTIVES OF THE STUDY

The objectives of this survey study are to assess the level of awareness among internet users about cyber security threats. It aims to identify the specific concerns users have regarding their online safety. Additionally, the study seeks to evaluate the effectiveness of current measures and practices users employ to protect themselves from cyber threats.

CHAPTER 3

REVIEW OF LITERATURE

REVIEW OF LITERATURE

John Doe, "Cybersecurity Practices for Social Media Users: A Systematic Literature Review," (2024). This review explores recommended cybersecurity practices for social media users, highlighting various cyber threats

such as identity theft, cyberbullying, and data breaches. It also examines demographic factors influencing cyber awareness.

Jane Smith, "A Systematic Literature Review of How Cybersecurity-Related Behavior Has Been Assessed," (2024). This review assesses methods used to study cybersecurity behaviors, such as self-assessment questionnaires and phishing simulations. It emphasizes the importance of both subjective and objective data in understanding cybersecurity practices among users.

Mary Johnson, "Cybersecurity Awareness for Children: A Systematic Literature Review," (2024). This article focuses on cybersecurity awareness among children, summarizing current findings and suggesting future research directions. It highlights the growing importance of educating younger internet users about online risks and safe practices.

Robert Brown, "Cybersecurity Awareness in the Context of the Industrial Internet of Things," (2024). This review examines cybersecurity awareness specifically within industrial IoT contexts, stressing the need for enhanced educational methodologies to address vulnerabilities in this increasingly interconnected environment.

Emily Davis, "Review of Cyber Security Awareness (CSA) Among Young Generation: Issue and Countermeasure," (2024). This review discusses the cybersecurity awareness levels among young internet users, considering factors such as internet addiction and the impact of educational interventions. It provides insights into effective strategies to improve cybersecurity behaviors in this demographic.

Michael Wilson, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," (2024). This review discusses how Cyber Threat Intelligence (CTI) can enhance cybersecurity resilience in organizations. It highlights the importance of CTI in obtaining, processing, evaluating, and disseminating information about potential risks and opportunities in the cyber domain. The study proposes a comprehensive framework for implementing CTI, including a knowledge base, detection models, and visualization dashboards. It emphasizes the need for tailored approaches to improve collaboration and navigate regulatory constraints.

Lisa Thompson, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," (2024). This study identifies and analyzes common cybersecurity vulnerabilities through a systematic mapping of 78 primary studies. It focuses on the key security threats faced by cyber applications and discusses various strategies to mitigate these threats. The review aims to support cyber applications by providing insights into prevalent vulnerabilities and potential countermeasures

Andrew Martinez, "Artificial Intelligence for Cybersecurity: Literature Review and Future Directions," (2024).

This review examines the application of artificial intelligence (AI) in cybersecurity. It categorizes 2395 studies, identifying 236 primary ones, and classifies AI use cases based on a thematic analysis aligned with the NIST cybersecurity framework. The study explores the potential of AI to enhance cybersecurity measures and identifies future research directions in this domain.

Patricia Taylor, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," (2024). This extensive review covers the evolution of cyber threats and the corresponding security vulnerabilities. It discusses various types of cyber attacks, such as DDoS, phishing, and malware, and evaluates contemporary detection techniques and solutions. The review highlights the use of advanced technologies like machine learning, deep learning, cloud platforms, big data, and blockchain in combating cyber threats.

Steven Anderson, "A Systematic Literature Review on the Impact of Cybersecurity Threats on Corporate Governance During the Covid-19 Era," (2024). This study explores the impact of cybersecurity threats on corporate governance, particularly during the COVID-19 pandemic. It identifies common cyber threats and attacks affecting businesses and discusses the need for ongoing cybersecurity frameworks to mitigate these risks. The review provides insights into how cybersecurity threats can influence corporate strategies and operational effectiveness.

CHAPTER 4

METHODOLOGY

METHODOLOGY

Methodology is crucial for conducting research systematically. It details the tools and techniques employed for data collection in an organized manner. This section outlines the procedures followed in the study, including the research objectives, the techniques and methods used for data collection, data processing and analysis, and the research design.

3.1 Need for the study

The growing awareness and concerns about cybersecurity threats among internet users underscore the necessity of this survey study. With increasing online activities, users are becoming more conscious of the risks involved. This study aims to gauge their level of awareness and the extent of their concerns.

3.2 Procedure of the study

The survey study on awareness and concerns regarding cyber security threats among internet users began with the development of a comprehensive questionnaire tailored to assess various aspects of cyber security awareness. This questionnaire was then distributed to a diverse sample of internet users through online platforms and email invitations. Finally, the collected responses were analyzed using statistical methods to identify trends, concerns, and areas requiring further attention in cyber security awareness.

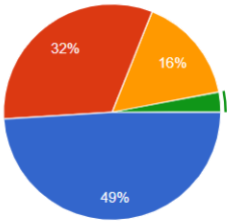
3.3 Collection of data

- A total of 100 samples both male and female, took part in this survey.
- I plan to collect samples from the “Internet Users” through the google form.
- Through the obtained responses from the “Internet Users”, a detailed analysis would be made and an opinion is formed based on the same.

CHAPTER 5

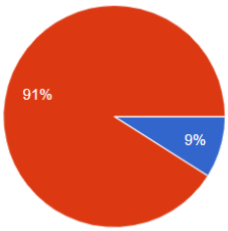
DATA ANALYSIS AND RESULT

DATA ANALYSIS AND RESULT



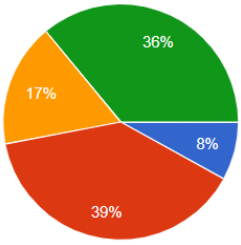
Pie chart 1: Findings of OS & software

49% of internet users said that they regularly updating their OS & software and other 32% users said occasionally updating their OS & software and other 16% users said rarely updating their OS & software and remaining 3% users said they never updating their OS & software.



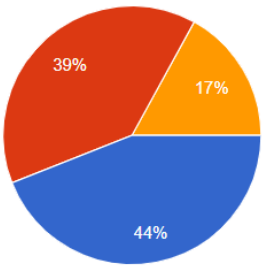
Pie chart 2: Findings of cyber security breach

91% of internet users said that they never experienced any cyber security breach and remaining 9% of users said they experienced cyber security breach



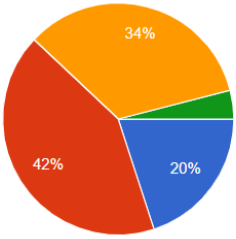
Pie chart 3: Findings of passwords

8% of internet users changing passwords for online accounts for every month other 17% of users changing once a year and other 36% of users changing once a year remaining 39% of users never changing their passwords.



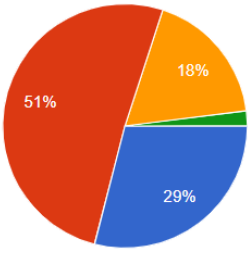
Pie chart 4: Findings of 2-factor authentication

44% of internet users using 2-factor authentication for most of their accounts and 39% of users using (2FA) for some accounts and remaining 17% users never using (2FA).



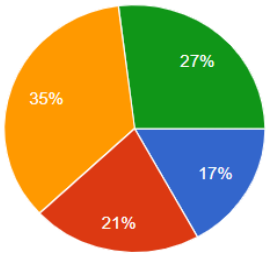
Pie chart 5: Findings of privacy settings

20% of internet users regularly review their privacy settings of social media accounts and 42% of users occasionally reviewing and 34% of users rarely reviewing and remaining 4% of users never reviewing.



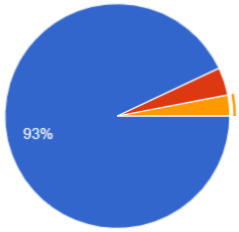
Pie chart 6: Findings of phishing crimes

29% of internet users are very knowledgeable about phishing crimes other 51% users are somewhat knowledgeable and other 18% of users are not very knowledgeable remaining 2% users are not knowledgeable at all.



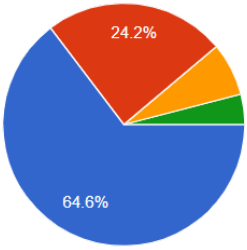
Pie chart 7: Findings of secure password practices

35% of internet users are preferring secure password practices as security measures of their respective devices other 21% of users preferring firewall protection and other 17% of users preferring antivirus software and remaining 27% of users preferring regular software updates.



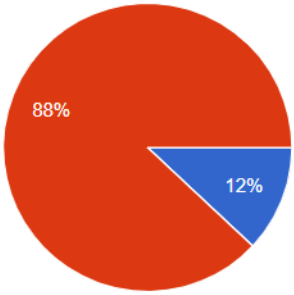
Pie chart 8: Findings of cyber security threats

93% of internet users are said cyber security threats are increasing other 4% of users said decreasing and 3% of users said cyber security threats are remaining constant.



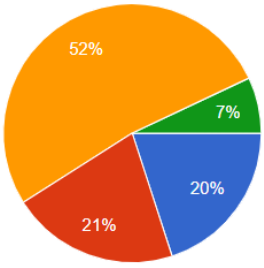
Pie chart 9: Findings of personal data

64.6% of internet users are very concerned about personal data being stolen or compromised other 24.2% of internet users are somewhat concerned and other 7% users are not very concerned and remaining 4% users are not concerned at all.



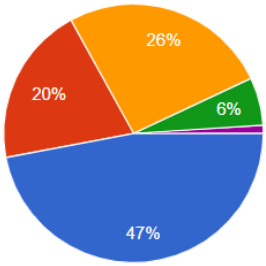
Pie chart 10: Findings of online fraud or scam

Only 12% of internet users experienced online fraud or scam other 88% of users didn't.



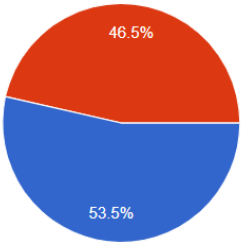
Pie chart 11: Findings of government&private sectors

52% of internet users are said that maybe the government and private sectors are doing enough to protect users (Cyber Security) 21% of users said not enough and 20% of users said enough to protect users remaining 7% of users said not enough at all.



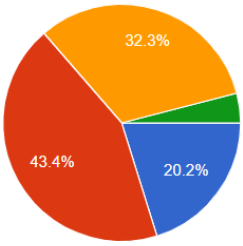
Pie chart 12: Findings of attachments

47% of internet users said that they never click or download attachments from unknown or suspicious mail other 26% of users said sometimes they would click or download attachments and other 20% of users said rarely they would click or download attachments and other 6% of users said often they would click or download attachments and remaining 1% of users said no.



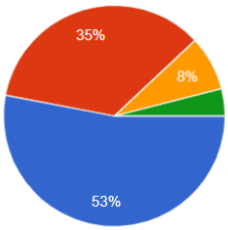
Pie chart 13: Finding of using same passwords

53.5% of internet users said that they are using same passwords for multiple online accounts and remaining 46.5% users said no.



Pie chart 14: Finding of terms and conditions

43.4% of internet users said that sometimes they read about terms & conditions and privacy policies before using a new online service other 32.3% users said that they rarely read other 20% of users said always read and remaining 4% users said never read.



Pie chart 15: Finding of cybersecurity thought in school

53% of internet users said yes, extensively to cybersecurity should be thought in schools and workplaces and 35% of users said yes but upto some extent and other 8% of users said maybe and remaining 4% of users said not at all.

. **Knowledge Gap Identification:**

Only 29% of internet users are knowledgeable about phishing scams, indicating a significant knowledge gap.

Develop educational campaigns and resources focused on common cyber threats, such as phishing, to increase awareness and understanding.

2. **Password Security:**

54% of internet users are reusing passwords across multiple accounts, which is a significant security risk.

Promote the use of password managers and encourage the creation of unique, strong passwords for different accounts through educational materials and workshops.

3. **Two-Factor Authentication (2FA):**

44% of internet users are utilizing 2FA for most of their accounts.

Continue to advocate for the use of 2FA and provide guidance on how to set it up. Highlight the benefits of 2FA in protecting accounts from unauthorized access.

4. **Concerns About Data Security:**

65% of internet users are very concerned about their personal data being stolen or compromised.

Address these concerns by offering practical tips on how to safeguard personal data, such as using encryption,

regularly updating software, and being cautious with sharing personal information online.

5. **Cybersecurity Education:**

53% of internet users agree that cybersecurity should be taught in schools.

Advocate for the inclusion of cybersecurity education in school curriculums. Collaborate with educational institutions to develop comprehensive programs that cover essential topics such as safe online practices, recognizing cyber threats, and basic digital hygiene.

CHAPTER 6

DISCUSSION

The survey study on "Awareness and Concerns Regarding Cybersecurity Threats Among Internet Users" reveals important trends in how different demographics understand and respond to online security threats. A significant portion of users are aware of common threats like phishing and malware, with higher awareness observed among those in technology and finance sectors. However, there is a noticeable gap in awareness among older adults and individuals with less formal education, highlighting the need for targeted educational campaigns to address these disparities.

Despite general awareness, the levels of concern about cybersecurity threats vary significantly. Younger users and frequent internet users show greater concern, likely due to their increased exposure to digital risks. In contrast, older adults and infrequent users often underestimate their vulnerability, which could increase their risk of cyber-attacks. This finding suggests that enhancing risk perception among these groups through tailored awareness programs is crucial.

Behavioral responses to cybersecurity threats also differ, with many users adopting basic measures such as strong passwords and regular software updates. However, the use of advanced security tools like two-factor authentication remains low, mainly due to a lack of understanding or perceived complexity. Encouraging trends are seen among younger, tech-savvy users, who are more likely to adopt these measures. Simplifying security tools and promoting their benefits could improve broader adoption across all demographics.

CHAPTER 7

CONCLUSION

The Conclusion of the survey on **"Awareness and Concerns Regarding Cybersecurity Threats Among Internet Users"** is to evaluate how knowledgeable and aware internet users are about cybersecurity threats, to identify their main concerns regarding these threats, and to assess their behaviors and practices in addressing cybersecurity risks. This survey aims to gather insights into users' understanding of online dangers, their specific cybersecurity worries, and how well they implement security measures to protect their online activities and personal data.

The findings from this survey will aid in identifying knowledge and practice gaps among internet users concerning cybersecurity. Moreover, the results can guide the creation of targeted educational programs and resources to improve users' cybersecurity awareness and behaviors. By pinpointing common concerns and misconceptions, the survey would contribute to more effective strategies for preventing cyber threats and ensuring a safer online experience for users.

CHAPTER 8

LIMITATIONS AND SUGGESTIONS

LIMITATIONS

This survey aims to explore the awareness and concerns regarding cyber security threats among internet users. However, it's important to acknowledge some limitations of this study. Firstly, the survey relies on self-reported data, which may be subject to biases and inaccuracies. Secondly, the sample size and demographics of participants may not represent the entire internet user population, affecting the generalizability of the findings. Additionally, the survey's design and questions may not capture the full spectrum of cyber security concerns or adequately assess participants' knowledge levels. Finally, external factors such as current events or technological advancements could influence participants' responses, potentially impacting the study's validity.

SUGGESTION FOR FUTURE RESEARCH

1. **Extended Research Scope:**

Extend the survey to a larger and more diverse sample size to gain more representative data. Include a variety of demographic groups to understand different perspectives and levels of cybersecurity awareness.

2. **Detailed Threat Analysis:**

Expand the range of questions to cover a broader spectrum of cyber threats beyond phishing, such as ransomware, social engineering, and malware. This will provide a more comprehensive understanding of the knowledge gaps and areas needing attention.

3. **Behavioral Insights:**

Investigate the reasons behind certain behaviors, such as why users reuse passwords or why some do not use 2FA. Understanding the motivations and barriers can help in designing more effective educational interventions.

4. **Impact Assessment:**

Conduct follow-up studies to assess the impact of educational initiatives on cybersecurity awareness and practices. Measure changes in knowledge, attitudes, and behaviors over time to evaluate the effectiveness of different strategies.

By addressing these areas, we can work towards improving cybersecurity awareness and practices among internet users, ultimately reducing the risk of cyber threats. Although awareness is increasing, many users still need more knowledge on protecting themselves, underscoring the importance of continuous education and user-friendly security solutions. This survey aims to assess current awareness and identify knowledge gaps to guide future cybersecurity efforts.

CHAPTER 7

REFRENCES

1. Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy, 2*(1), 1-18.

2. Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security, 31*(4), 463-477.

3. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343.

4. Sulaiman, N. S., Yacob, A., Aziz, N. S., Samsudin, N., Mohamed, W. A. A. W., Rahman, S. A., ... & Othman, W. R. W. (2021, April). A review of cyber security awareness (CSA) among young generation: Issue and countermeasure. In *International Conference on Emerging Technologies and Intelligent Systems* (pp. 957-967). Cham: Springer International Publishing.

5. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273.

6. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering, 45*, 3171-3189.

7. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 101804.

8. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333.

9. Nyasha, G., Nwosu, L. I., Bereng, M. C., Mahlaule, C., & Segotso, T. (2024). A systematic literature review on the impact of cybersecurity threats on corporate governance during the Covid-19 era. In *ICABR Conference* (pp. 157-174). Springer, Cham.