Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Gap Between Cybercrime Awareness and Preventive Practices

A Survey-Based Study

Diwakar Neopaney
Cyber Forensics
Vivekananda Global University
Jaipur, India

Parikshit Vyas
Cyber Forensics
Vivekananda Global University
Jaipur, India

Gunjan Mundra
Cyber Forensics
Vivekananda Global University
Jaipur, India

Abstract: ***People use the internet for everything nowadays including communication, online shopping, and money transfers. This has made people's lives very easy but it can make people vulnerable to cybercrimes. So, it is important for people to know how to stay safe online. Even though different programs make people aware of cybercrimes, they do not follow proper precautions. The result shows that 96.17% people are aware of the risk like using public wi-fi for payment transactions, reusing the same password everywhere and clicking on unknown links yet they put themselves on risk and fall victims to cybercrimes the result shows the main reason for the gap are carelessness, lack of knowledge, time constrain. The research concludes that both awareness and behavior need improvement.***

Keyword: Digital technology advancement, Internet-based media, information dissemination, monetary transactions, communication channels, cybercrime, cyber safety awareness, public awareness programs, cyber threats, awareness vs behavior gap, risky online behavior, public Wi-Fi usage, password reuse, unknown links, cyberattack risk, human behavior in cybersecurity, carelessness, overconfidence, lack of time, behavioral factors, cybersecurity practices, behavior-oriented approach, safe online practices.)

I. INTRODUCTION

The development of digital technology has led to the modern world; the internet has become an integral part of our lives. People do their banking, business, learning and communication digitally. However, our reliance on digitalization has increased cybercrime such as financial fraud, identity theft, phishing, hacking, etc. Several awareness programs have been initiated by governments and other bodies to create awareness regarding cyber threats and appropriate behaviors in view of this growing concern. As a result, today there exists a significant proportion of the population that understands the basics of cyber threats. However, despite this awareness, the incidences of cybercrimes globally continue to rise, thereby questioning the effectiveness of awareness alone. According to studies, mere awareness does not automatically translate into actions. As most people do not put what they know into practice, human behavior plays a key role in the area of cybersecurity (Hadlington, 2017). In spite of their awareness of the threats, certain issues such as negligence, laziness, and confidence often lead to improper cyber behaviors. Moreover, consumers often have a misconception that they may be less vulnerable to cybercrime. This misconception reduces the likelihood of taking consistent preventative actions (Princely Ifined o (2012)). In this connection, the present study aims to analyze the gap between preventative actions and awareness about cybercrime. To achieve this purpose, survey data analysis will be performed to examine whether awareness impacts behavior, as well as to identify the key barriers that prevent individuals from adopting secure cybersecurity practices.

II. LITERATURE REVIEW

Cyber Security doesn't only depend on technology; it also depends on an individual's behavior while they are interacting online.

Hadlington, L. (2017), said that people who are impulsive and spend too much time online, they have poor cybersecurity habits. It shows that being aware about risk is not enough, safe cyber practices should also be followed. Abdulkader, M. (2023), in his research he found out that many people know public wi-fi can be risky but still they use it. This shows that even after being aware people don't avoid it. Mberikwazvo, W. Z. (2024), stated that cyber behavior can also be affected by age, gender and education level so just having knowledge about cybercrime is not enough. Kyaw, P. M. (2025), also found something similar while studying parents. Many parents know about cyber security risks but when it comes to monitoring their children many of them were not very active. This shows the gap between awareness and practice Mah, P. M., & Nasr, M. A. (2026), they looked at this issue in more depth. They suggested that improving online safety is not only about awareness but also about creating safe cyber environment After reviewing the above literature it becomes clear that awareness about cybercrime is not enough. People often choose convenience even after knowing that it is not safe. This is why People need to pay attention on how they actually behave online

Cyber Security doesn't only depend on technology; it also depends on an individual's behavior while they are interacting online.

Hadlington, L. (2017), said that people who are impulsive and spend too much time online, they have poor cybersecurity habits. It shows that being aware about risk is not enough, safe cyber practices should also be followed. Abdulkader, M. (2023), in his research he found out that many people know public wi-fi can be risky but still they use it. This shows that even after being aware people don't avoid it. Mberikwazvo, W. Z. (2024), stated that cyber behavior can also be affected by age, gender and education level so just having knowledge about cybercrime is not enough. Kyaw, P. M. (2025), also found something similar while studying parents. Many parents

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

know about cyber security risks but when it comes to monitoring their children many of them were not very active. this shows the gap between awareness and practice Mah, P. M., & Nasr, M. A. (2026), they looked at this issue in more depth. They suggested that improving online safety is not only about awareness but also about creating safe cyber environment.

After reviewing the above literature it becomes clear that awareness about cybercrime is not enough. People often choose convenience even after knowing that it is not safe. This is why People need to pay attention on how they actually behave online

III. METHODOLOGY

A. *Research Design*

In order to examine awareness and behavior patterns, this study uses a quantitative research methodology based on survey data.

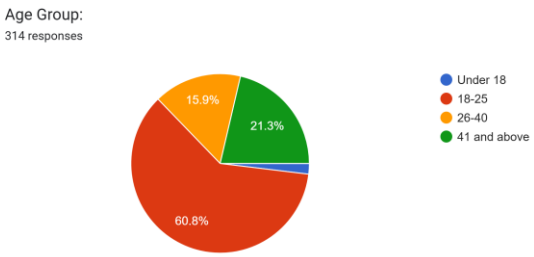
B. *Data Collection Method*

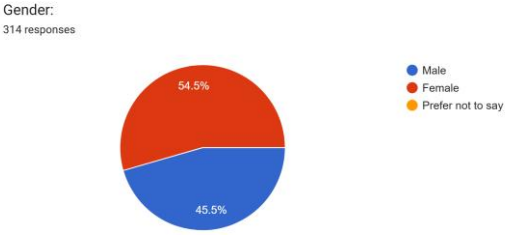
A standardized questionnaire disseminated using Google Forms was used to gather data. Multiple-choice questions on cybersecurity awareness, behavior, and attitudes were included in the questionnaire.

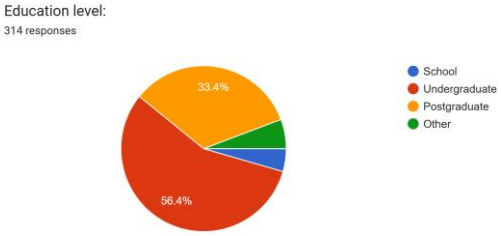
C. *Sample Size and Participants*

The survey was completed by 314 people in total. The individuals represented a variety of

- Age groups
- Backgrounds in education
- Gender classifications







D. *Variables Studied*

The following variables were the focus of the study:

- Knowledge of cybercrime
- Preventive measures (passwords, updates, etc.)
- Risky actions (using public Wi-Fi, clicking links)
- Self-perception of cybersecurity procedures
- Obstacles to implementing safe practices

E. *Ethical Considerations*

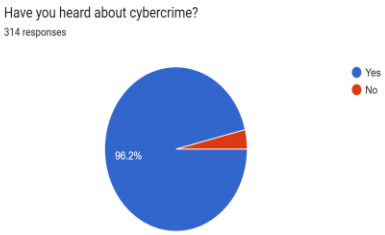
Despite being gathered, personal information like names and email addresses was not utilized in the analysis. The information was kept private and utilized only for scholarly research.

IV. RESULTS

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. *Awareness of Cybercrime*

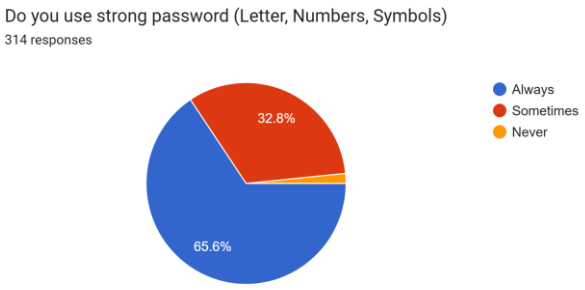
96.2% respondents reported awareness of cybercrime.



B. *Password Practices*

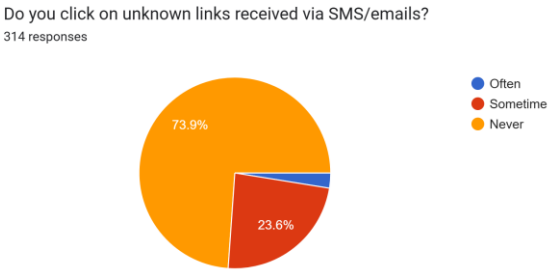
- 65.6% always use strong passwords
- 32.8% use strong passwords sometimes
- 47.1% reuse passwords across accounts

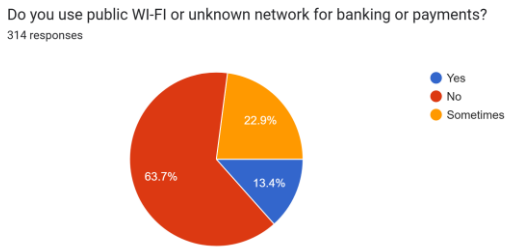
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026



C. *Risky Online Behavior*

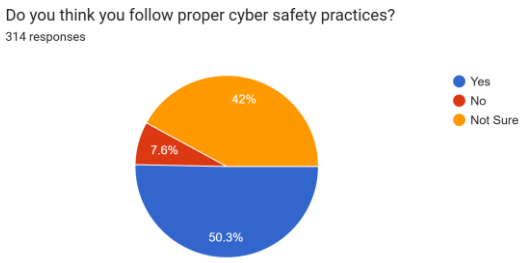
- 26% click unknown links at least occasionally
- 36% use public Wi-Fi for sensitive activities





D. *Self-Perception*

- *50.3% believe they follow proper cybersecurity practices*
- *42% are unsure*



V. DISCUSSION

The results of this research clearly show that there is an imbalance between prevention and awareness. Increased awareness notwithstanding, there are still many who are practicing behaviors that make them vulnerable on the internet.

The most significant finding in this study is the variation between what the respondents believed they did and what they did. Although the majority of them believe that they are practicing in a safe manner, their behaviors demonstrate the opposite. This is in line with the findings of Princely Ifined o (2012), who opined that knowing doesn't necessarily imply that you will act on what you know.

It is necessary to mention that behavioral aspects contribute to cybersecurity issues. The reason why people do not do their safety regulations is that they believe that they are invincible, it is easy or they do not care. This assertion is consistent with the view of Hadlington (2017), who focuses on psychological aspects that influence cybersecurity behavior.

In addition, the results are in line with those of the international study, undertaken by Verizon (2023), which reports human error as the main cause of cyber incidents.

It is agreeable that behavioral methods should be used instead of awareness strategies in improving cybersecurity.

VI. CONCLUSION

Results of this research show that people are aware of the threats of cybercrime, but they do not necessarily follow the appropriate guidelines when on the Internet.

The lack of connection between what people know and what they do is apparent. The absence of technical skills is not the cause of this conflict, but usually, common practices like negligence, convenience, time constraints and overconfidence. Humans have the choice of taking the easy or fast way out, such as reusing passwords and neglecting to follow certain basic security precautions, despite being aware of the dangers.

The other critical aspect is that individuals always believe they are taking the right security measures even when their behaviors reveal otherwise. Such a divide between knowing and doing demonstrates a fundamental issue in cybersecurity: the knowledge is not the guarantee of safety.

More than just awareness we should change our behavior online to tackle this issue. Rather than explaining what is right or wrong, people should follow safety practices like using strong passwords consisting of symbols, letters, numbers and special characters. People should also avoid clicking on unknown or suspicious links which can lead to phishing attacks.

To conclude, knowledge is not enough, we should also improve our online behavior and safety practices or else our system might become vulnerable leading to victimization.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

REFERENCES

[1] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," 2010. https://doi.org/10.2307/25750690

[2] I. Ajzen, "The theory of planned behavior: Frequently asked questions," 2010. https://doi.org/10.1002/hbe2.195

[3] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," 2012. https://doi.org/10.1016/j.cose.2011.10.007

[4] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using HAIS-Q," *Computers & Security*, vol. 42, pp. 165–176, 2014. https://doi.org/10.1016/j.cose.2013.12.003

[5] L. Hadlington, "Human factors in cybersecurity: Examining the link between internet addiction and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, 2017. https://doi.org/10.1016/j.heliyon.2017.e00346

[6] M. Abdulkader, "Why do people use public Wi-Fi? An investigation of risk-taking behaviour and factors leading to decisions," 2023. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1774094

[7] W. Z. Mberikwazvo, "The impact of demographic indicators on cybersecurity behaviour of e-commerce users in South Africa," PQDT Global, 2024.

[8] P. M. Kyaw, "A study of parental awareness and practices for online safety (Case study: South Okkalapa Township)," MERAL Portal, 2025.

[9] P. M. Mah and M. A. Nasr, "Digital trust: Online safety, identification models, ethical digital environments," Walter de Gruyter GmbH & Co KG, 2026.