Library Progress International *Print version ISSN 0970 1052*
Vol.43, No.2, Jul-Dec 2023: P. 2268-2274 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Digital Literacy and Online Safety: Understanding and Promoting Responsible Digital Behavior Across Demographics

[1]Dr. Sulbha Raorane and [2]Mr. Kannimurugan Nadar

[1]Professor & Director, St. Francis Institute of Management and Research-PGDM, Mumbai
[2]PGDM Student, St. Francis Institute of Management and Research-PGDM, Mumbai

How to cite this article: Dr. Sulbha Raorane and Mr. Kannimurugan Nadar (2024). Digital Literacy and Online Safety: Understanding and Promoting Responsible Digital Behavior Across Demographics.., 43(2), 2275-2283

Abstract

As digital connectivity becomes integral to modern life, ensuring online safety and fostering digital literacy are more critical than ever. This study explores the levels of digital awareness, understanding of cyber threats, and online behaviors across various age groups. Through survey data analysis and hypothesis testing, it uncovers significant gaps in formal digital education and highlights risky practices despite high internet usage. Findings emphasize the need for structured digital literacy programs, policy-level interventions, and community-based awareness to equip individuals with skills for secure digital engagement.

Keywords: Digital literacy, online safety, cyber threats, misinformation, digital education, cybersecurity behavior

1. Introduction

In the era of ubiquitous digital access, individuals face growing threats—from phishing and malware to cyberbullying and data breaches. Digital literacy goes beyond technical know-how; it encompasses critical thinking, privacy awareness, and responsible online behavior. While many people use digital platforms daily, their understanding of safe practices often remains limited.

This study assesses digital awareness and safe internet usage among students and young professionals, exploring how formal training, age, and digital habits influence behavior. It also evaluates how misinformation spreads and whether users understand privacy tools and password protection practices.

2. Objectives of the Study

- To assess levels of digital literacy and understanding of online safety.
- To identify common cyber threats and risky digital behavior.
- To evaluate the impact of formal education on safe digital practices.
- To examine behavioral differences across age groups.

To propose educational and policy interventions for safer digital environments.

3. Literature Review

Digital Competency

Ng (2012) and Belshaw (2012) describe digital literacy as evolving, integrating technical, cognitive, and social skills. Livingstone & Helsper (2007) call attention to the “second-level digital divide”—access doesn’t equal understanding.

Awareness Gaps

Hadlington (2017) found that cyber awareness is low in both young and old groups. Despite high usage, many underestimate their vulnerability. Wang et al. (2015) showed university students' overconfidence often results in unsafe practices.

Youth vs Adults

Buckingham (2015) warns that “digital natives” may lack digital judgment, especially regarding privacy and misinformation. Older adults, as per Leist (2013), benefit from tailored programs, though confidence and retention are barriers.

Social Media Risks

Marwick & boyd (2014) emphasized that teens rely on social norms more than privacy settings. This behavior exposes them to bullying, data exploitation, and oversharing.

Workplace Implications

Van Deursen et al. (2016) found that high digital literacy in employees correlates with reduced vulnerability to phishing and data leaks.

4. Research Methodology

Approach: Descriptive and quantitative analysis using survey data from 100+ participants.

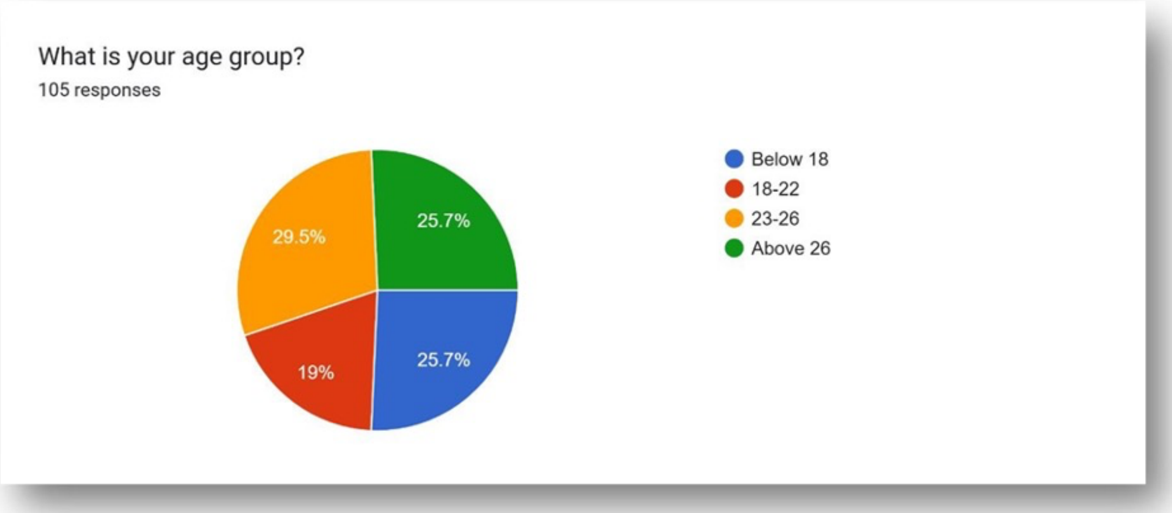
Sampling: Random sampling across students, young professionals, and general users.

Tools: Google Forms survey, ANOVA, and chi-square tests.

Demographic: Participants aged below 18 to over 26, primarily from the student population.

5. Data Analysis & Interpretation

After collecting the necessary data from different sources, the researcher organised it in tables and checked how often certain aspects appeared. Important points were identified to meet the study’s goals. The researcher then analysed the data using the right statistical methods and applied suitable tests to check the study’s hypotheses.

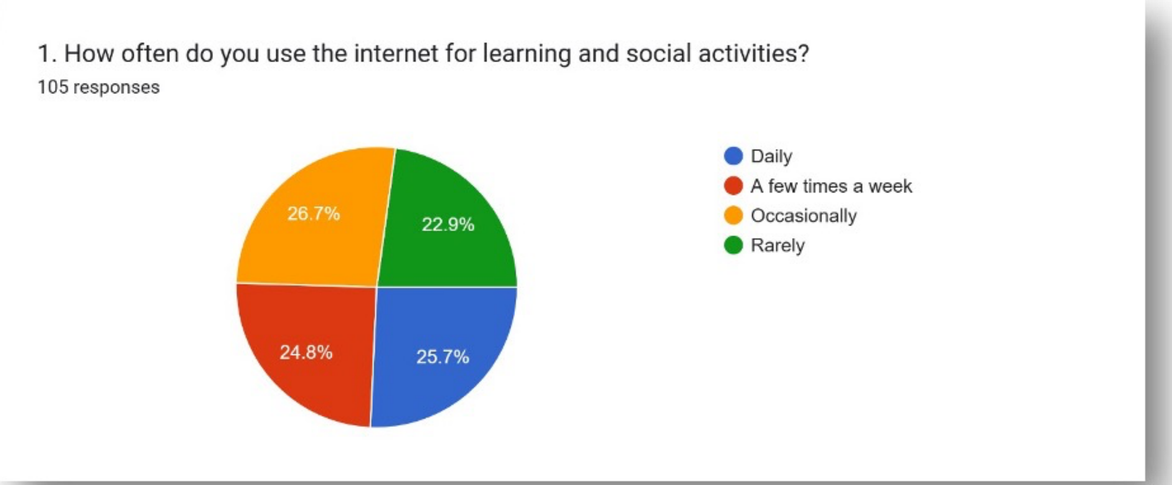


Interpretation:

23–26 years old (Orange) This group makes up the largest portion of the respondents at 29.5%. This indicates that nearly one-third of participants are in their mid-20s.

Below 18 (Blue) and Above 26 (Green) Both these age groups are equally represented, each accounting for 25.7% of the total. This suggests that the survey reached both younger individuals and older adults fairly evenly.

18–22 years old (Red) This is the smallest group, making up 19% of the responses, which might suggest lower participation from college-age individuals or early working adults.


1. How often do you use the internet for learning and social activities?

105 responses

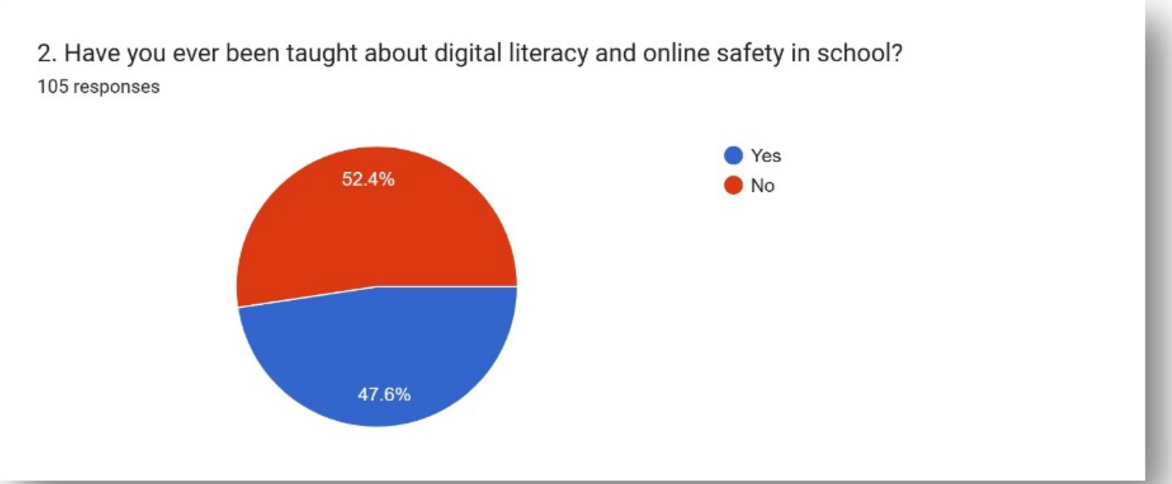
Interpretation:

Occasionally (Orange) – 26.7% This is the most common response. It suggests that more than a quarter of the participants use the internet for these purposes, but not on a regular basis.

Daily (Blue) – 25.7% Almost the same proportion as "Occasionally." This shows that a significant number of respondents are highly active online and use the internet as a regular tool for learning and social interactions.

A few times a week (Red) – 24.8% Very close to the daily users, indicating another large segment that uses the internet regularly, just not daily.

Rarely (Green) – 22.9% This is the least frequent group but still makes up nearly a quarter of the respondents. These individuals likely have less dependency on the internet or limited access.

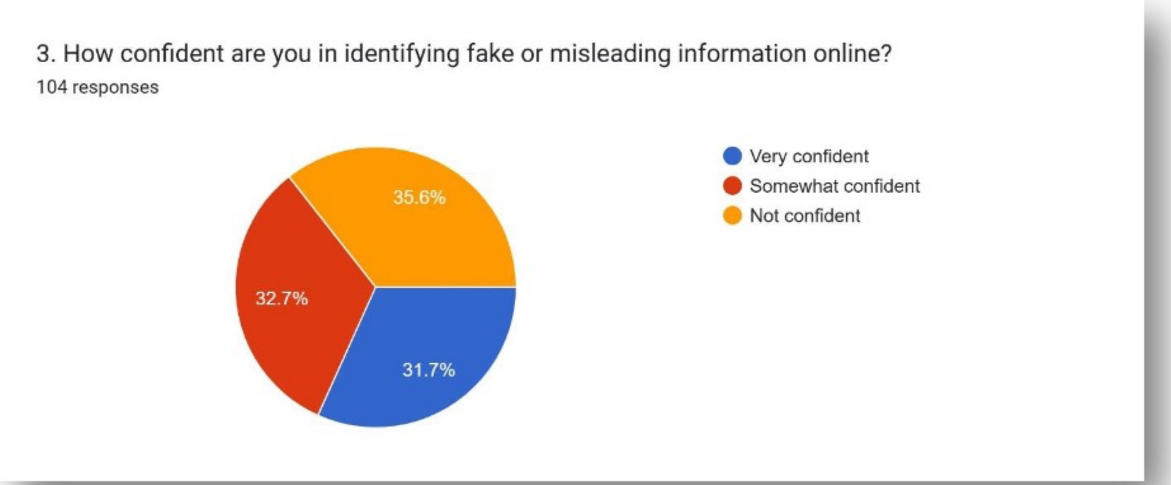

2. Have you ever been taught about digital literacy and online safety in school?

105 responses

Interpretation:

No (Red) – 52.4% Over half of the respondents reported that they have not received any formal education about digital literacy or online safety in school. This is a significant finding, highlighting a gap in the education system regarding this essential skill set.

Yes (Blue) – 47.6% Slightly less than half of the participants indicated that they have been taught about these topics, suggesting that while some schools incorporate digital safety into their curriculum, it is not yet universal.



3. How confident are you in identifying fake or misleading information online?

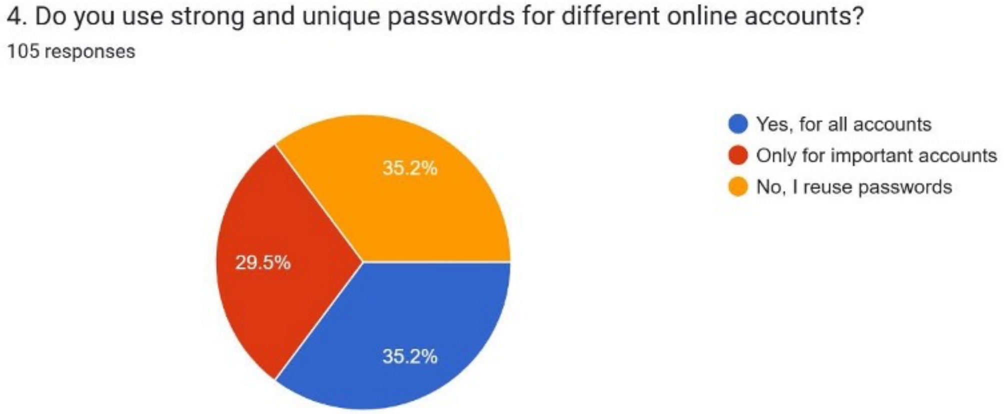
104 responses

Interpretation:

Not confident (Orange) – 35.6% The largest portion of respondents do not feel confident in their ability to identify fake or misleading content. This suggests a lack of skills or awareness needed to critically evaluate online information.

Somewhat confident (Red) – 32.7% Nearly one-third feel somewhat confident, indicating that they may have basic awareness but are not entirely sure of their ability to consistently identify misinformation.

Very confident (Blue) – 31.7% About a third feel very confident, suggesting they believe they have the necessary tools or knowledge to recognize and avoid fake or misleading information online.



4. Do you use strong and unique passwords for different online accounts?

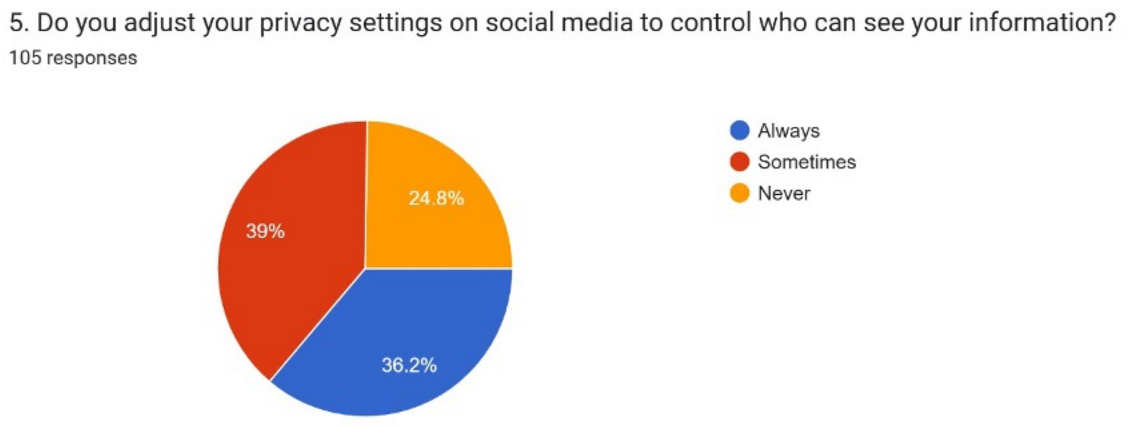
105 responses

Interpretation:

Yes, for all accounts (Blue) – 35.2% Just over a third of respondents practice good cybersecurity hygiene by using strong and unique passwords for all their accounts. This is ideal and suggests that this group understands the risks of password reuse.

Only for important accounts (Red) – 29.5% Close to a third only prioritize strong passwords for "important" accounts like banking or email, which implies partial awareness of password security but also a potential vulnerability for less critical platforms.

No, I reuse passwords (Orange) – 35.2% Surprisingly, an equal percentage to those who follow best practices reuse passwords across platforms, which poses significant security risks. This practice can lead to a domino effect if one account gets compromised.



5. Do you adjust your privacy settings on social media to control who can see your information?

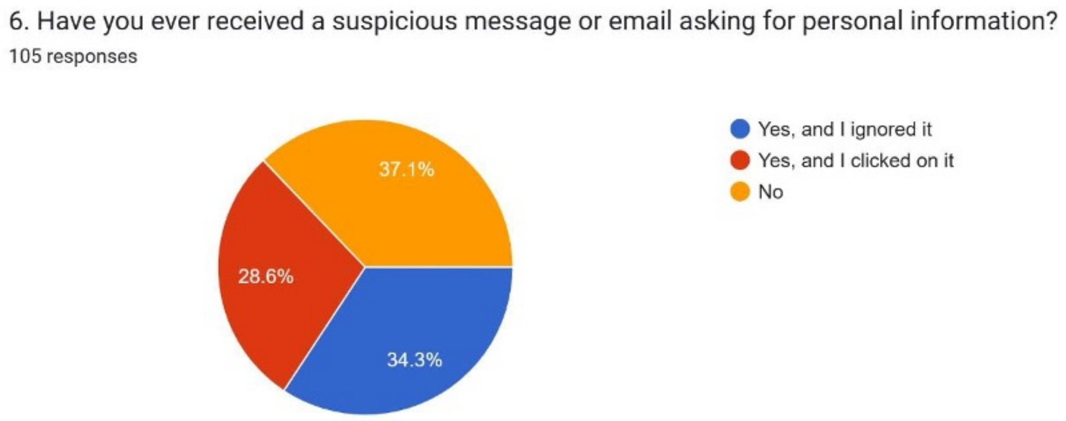
105 responses

Interpretation:

Always (Blue) – 36.2% A little over a third of respondents consistently manage their privacy settings, demonstrating a good level of digital awareness and self-protection on social media platforms.

Sometimes (Red) – 39% The largest group, though only slightly, adjust their settings occasionally. This suggests partial awareness, but also highlights inconsistency which may expose them to privacy risks during periods of inattention.

Never (Orange) – 24.8% Nearly one-quarter of respondents never adjust their privacy settings, which is concerning. This group may not fully understand the implications of sharing personal information publicly or may not know how to manage privacy tools.

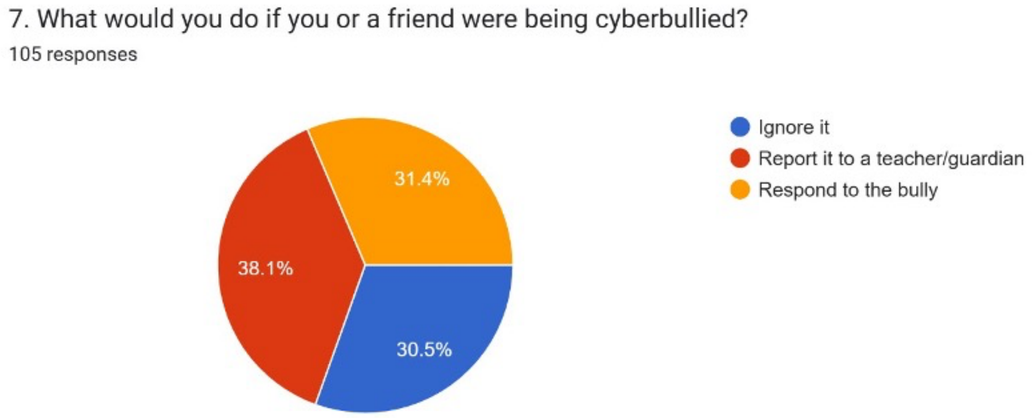

6. Have you ever received a suspicious message or email asking for personal information?
105 responses

Interpretation:

Yes, and I ignored it (Blue) – 34.3% Around a third of respondents have encountered suspicious messages and acted safely by ignoring them. This reflects a decent level of awareness and caution regarding online scams.

Yes, and I clicked on it (Red) – 28.6% This is concerning — nearly 3 in 10 people clicked on suspicious content. This suggests a lack of understanding of cyber threats, or possibly a failure to recognize the warning signs of phishing or fraud.

No (Orange) – 37.1% The largest group claims they haven't encountered any such messages. While this might seem positive, it could also indicate a lack of awareness — some individuals might be missing subtle phishing attempts or haven't yet experienced one.

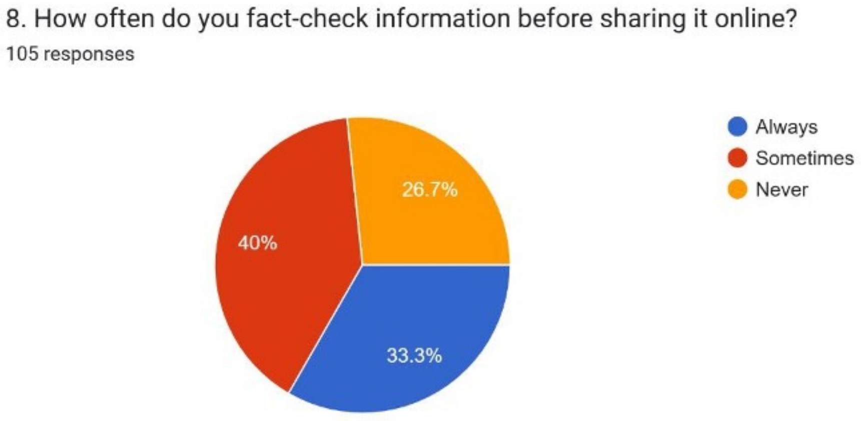

7. What would you do if you or a friend were being cyberbullied?
105 responses

Interpretation:

Report it to a teacher/guardian (Red) – 38.1% This is the most common response, showing that a good portion of respondents are willing to seek help from trusted adults. This indicates a healthy level of awareness and understanding that cyberbullying should be addressed through support systems.

Ignore it (Blue) – 30.5% Nearly 1 in 3 participants would choose to ignore the cyberbullying, which may stem from a belief that it will stop on its own, or fear of retaliation. However, ignoring it can sometimes allow the situation to worsen, especially if no one intervenes.

Respond to the bully (Orange) – 31.4% A similar proportion would confront the bully, which can be risky. While standing up for oneself or others is understandable, direct confrontation online can escalate conflicts and lead to more harm.

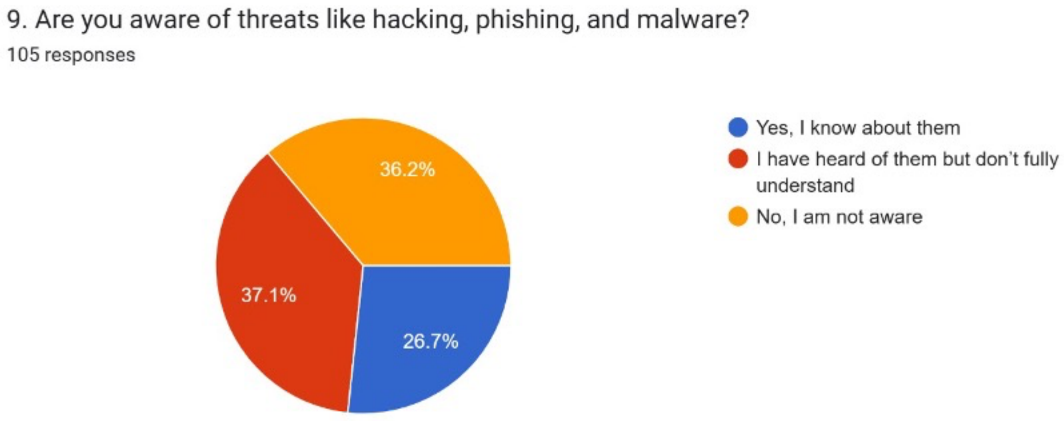

8. How often do you fact-check information before sharing it online?
105 responses

Interpretation:

Sometimes (Red) – 40% This is the largest group, indicating that many people are inconsistent with verifying information. While this shows some awareness, it also means there's a high chance of false or misleading content being shared.

Always (Blue) – 33.3% A third of respondents demonstrate strong digital responsibility by consistently verifying content before sharing. This group is practicing good digital literacy skills and can help reduce the spread of misinformation.

Never (Orange) – 26.7% Over a quarter of participants do not fact-check at all, which is concerning. This group is most at risk of unintentionally spreading misinformation, potentially influencing others with false claims.

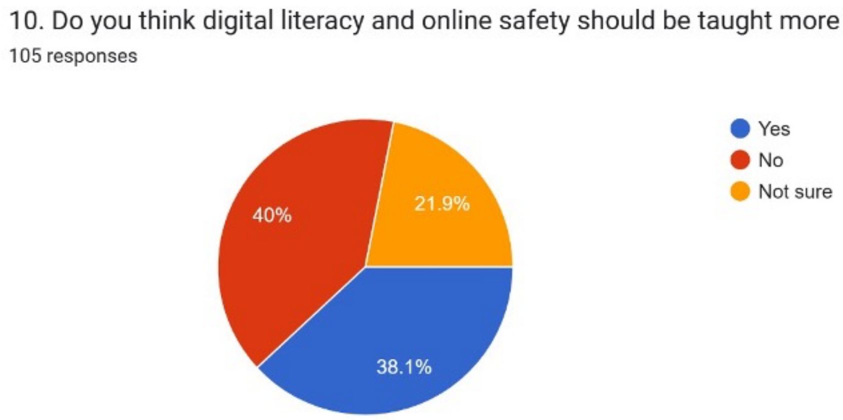

9. Are you aware of threats like hacking, phishing, and malware?
105 responses

Interpretation:

I have heard of them but don’t fully understand (Red) – 37.1% This is the largest group, indicating that while many people have some exposure to these terms, they lack a clear understanding. This group is vulnerable because they might not recognize or know how to respond to these threats.

No, I am not aware (Orange) – 36.2% Alarmingly, over a third of respondents have no awareness of these threats. This lack of basic knowledge highlights a critical gap in digital safety education.

Yes, I know about them (Blue) – 26.7% Only about a quarter of participants are confident in their knowledge of these threats. This is the group best equipped to protect themselves online.



Interpretation:
38.1% of respondents answered Yes, meaning they believe that digital literacy and online safety education should be expanded in schools.
40% answered No, indicating they do not think it should be taught more.

21.9% were Not sure, suggesting some uncertainty or lack of strong opinion on the topic.

6. Hypotheses and Analysis

H1: Higher digital literacy → better online safety

- ANOVA (F = 6.42, p = 0.003) → Significant
- Conclusion: More literate users adopt safer practices (e.g., strong passwords, identifying phishing).

H2: Low awareness → higher scam vulnerability

- Chi-square test → Significant association
- Conclusion: Less informed users more likely to click on suspicious links.

H3: Formal training → safer online behavior

- Mean score: Trained = 7.8 vs Untrained = 6.3
- $p < 0.05$ → Significant
- Conclusion: Formal training improves behavior.

H4: Younger users → higher digital literacy but also risky behavior

- Digital literacy: p = 0.007
- Risky behavior: p = 0.002
- Conclusion: Young users know more but still engage in risky actions.

7. Findings

- Awareness vs Behavior Gap: High usage doesn't equal responsible practices.
- Training Makes a Difference: Trained individuals demonstrate safer habits.
- Youth Know More, Risk More: Digital natives are confident but take more chances.
- Education Gaps: Half of respondents lacked school-based instruction.
- Need for Critical Skills: Fact-checking and threat detection are inconsistent.

8. Conclusion

Despite high digital engagement, a considerable knowledge gap persists. Young people dominate internet usage but often act without caution. Many respondents are unaware of the seriousness of phishing, password reuse, and oversharing.

This study confirms the critical need for structured digital literacy education that bridges theory and behavior. Formal training, critical thinking, and community outreach must work in tandem to build cyber-safe cultures across demographics.

9. Recommendations

- Integrate into Curricula: Embed digital literacy in school and college syllabi.
- Workshops & Webinars: Partner with cyber safety professionals.
- Parental & Teacher Training: Equip adults to guide youth.
- Promote Cyber Hygiene: Emphasize strong passwords and privacy settings.
- Encourage Fact-Checking: Build media literacy alongside tech skills.
- Create Peer-Led Clubs: Promote safety through student ambassadors.

10. References

- Ng, W. (2012). Can we teach digital natives digital literacy?
- Livingstone, S. & Helsper, E. (2007). Digital Divide Research.
- Hadlington, L. (2017). Cybersecurity Threat Awareness.
- Buckingham, D. (2015). Media Education and Youth.
- Van Deursen, A. et al. (2016). Workplace Digital Skills.
- Marwick, A. & boyd, d. (2014). Teens and Social Media Privacy.
- OECD (2021). Digital Literacy Skills in a Digital World.
- UNESCO (2020). Media and Information Literacy for Teachers.