PROBABILITY & STATISTICAL DATA ANALYSIS
SECTION-01

SECI2143

2024/2025

GROUP PROJECT TITLE:

Cybersecurity Awareness Among Internet Users

LECTURER'S NAME:

DR SEAH CHOON SEN

GROUP MEMBERS:

NAME	MATRIC NO.
IZWAN AZIZ BIN ISMAIL @ ABD MALEK	SX241894ECJHF01
YUARAJ A/L PARTHIPAN	SX241919ECRHF01
SITI NURNAJIHAH BINTI MOHAMAD ANUAR	SX232351ECRHF04
FATIN SYAHIRAH BINTI NOR RASHID	SX241920ECRHF01
ASWINI A/P CHANDRASAGARAN	SX242452ECRHF01

Table of Content

1.0 Introduction

The rapid advancement of information technology has made the Internet an essential medium in modern life. The Internet is widely used for various purposes including education, banking, business, entertainment, and communication. With easy access to search engines and digital platforms, society now lives in an interconnected world that merges both reality and virtual existence. This reliance on technology demonstrates that the Internet is not just a tool, but an integral part of daily life.

However, the extensive use of the Internet has also led to the emergence of numerous cybersecurity threats. Cybercrimes have become a serious issue that significantly affects the safety of individuals and organizations alike. According to the Royal Malaysia Police (PDRM), a total of **35,368 cybercrime cases** were reported in 2024, marking a 2.5% increase compared to the previous year. The estimated financial loss caused by these crimes amounted to **RM1.57 billion**, highlighting the alarming level of cyber risks faced by users today (Kosmo, 2025).

This situation clearly reflects the low level of cybersecurity awareness among Internet users. Many people navigate the online world without fully understanding the potential dangers. Therefore, having knowledge of basic cybersecurity practices is essential. This includes creating strong passwords, avoiding oversharing of personal information, and recognizing signs of online scams.

In addition, social environmental factors such as parental guidance, peer influence, workplace exposure, media coverage, and government policies play vital roles in shaping user attitudes and awareness toward cybersecurity. For instance, parents can serve as the primary educators in teaching children how to be cautious online, while peers may act as channels for sharing advice and promoting safe online habits.

Hence, this report aims to examine and analyze how social environments influence the level of cybersecurity awareness and practices among Internet users. It is hoped that this study will raise awareness and encourage various stakeholders to strengthen preventive measures and enhance digital literacy among Malaysians.

2.0 Purpose of Study

1. To examine users’ knowledge and practices related to the online risks.
2. To study their experiences with the cyber threats and the steps they take to protect their online passwords.
3. To analyze the impact of demographic factors such as gender, age, and occupation on awareness of cybersecurity.
4. To interpret the data gathered using various types of graphs and make a conclusion based on the findings.

2.1 Method of Data Analysis

To begin our study on Cybersecurity Awareness Among Internet Users, we developed a structured questionnaire using Google Forms. The questionnaire was designed to include all the necessary questions to gather relevant data for our research. After finalizing the form, we distributed Google Forms via popular messaging platforms such as WhatsApp and Telegram to collect responses from a diverse group of participants. A copy of the questionnaire is included in the appendix of this report for reference.

3.0 Data Collection

The target **population** for this study is **internet users**, as the research focuses on assessing the level of **cybersecurity awareness** among this group. A **sample** of **112 internet users** was selected to represent the population. The data was collected through an online questionnaire designed specifically to measure various aspects of cybersecurity awareness, such as knowledge of online threats, safe practices, and password management.

The questionnaire was distributed digitally via social media platforms such as WhatsApp, Instagram, and email, allowing broad and convenient reach to respondents. A non-probability sampling method, specifically convenience sampling, was employed due to its practicality and accessibility. All participants were assured of the confidentiality and anonymity of their responses, and participation was entirely voluntary.

Variable	Type of Variable	Level of Measurement	Representation
Gender	Qualitative	Nominal	Male / Female
Age	Qualitative	Ordinal	18–24, 25–34, 35–44, Below 55
Occupation	Qualitative	Nominal	Student, Govt Staff, Private, Self-employed, Other
Received suspicious communication	Qualitative	Nominal	Yes / No
Primary device to access internet	Qualitative	Nominal	Smartphone, Laptop, Desktop, Tablet, Other
Frequency of password change	Qualitative	Ordinal	Every month, Every 3–6 months, Once a year, rarely
Importance of antivirus software (1–5)	Qualitative	Ordinal	Linear scale: 1 (Strongly Disagree) to 5 (Strongly Agree)
Phishing understanding (1–5 stars)	Qualitative	Ordinal	Star rating
Confidence in identifying phishing (1–5)	Qualitative	Ordinal	Linear scale
Daily hours spent online	Qualitative	Ordinal	<1, 1–3, 4–6, 7–9, 10+ hours
Meaning of “https://”	Qualitative	Nominal	Multiple choice (Knowledge question)
Most secure password option	Qualitative	Nominal	Multiple choice (Knowledge-based)
Safety of public Wi-Fi	Qualitative	Nominal	Yes / No
Action on Unfamiliar Email	Qualitative	Nominal	Multiple choice (Behavioral)

Attended cybersecurity talks/courses	Qualitative	Nominal	Yes / No
Talk/course improved cybersecurity knowledge	Qualitative	Nominal	Yes / No
Main source of cybersecurity knowledge	Qualitative	Nominal	Social media, Online courses, News,etc,

4.0 Data Analysis

Data analysis is a systematic process of collecting, processing, interpreting, and presenting data to extract useful information. This process involves several steps, including data collection, data cleaning, data transformation, statistical analysis, and result visualization. The primary goal of data analysis is to understand data, identify patterns and trends, make predictions, and support better decision-making.

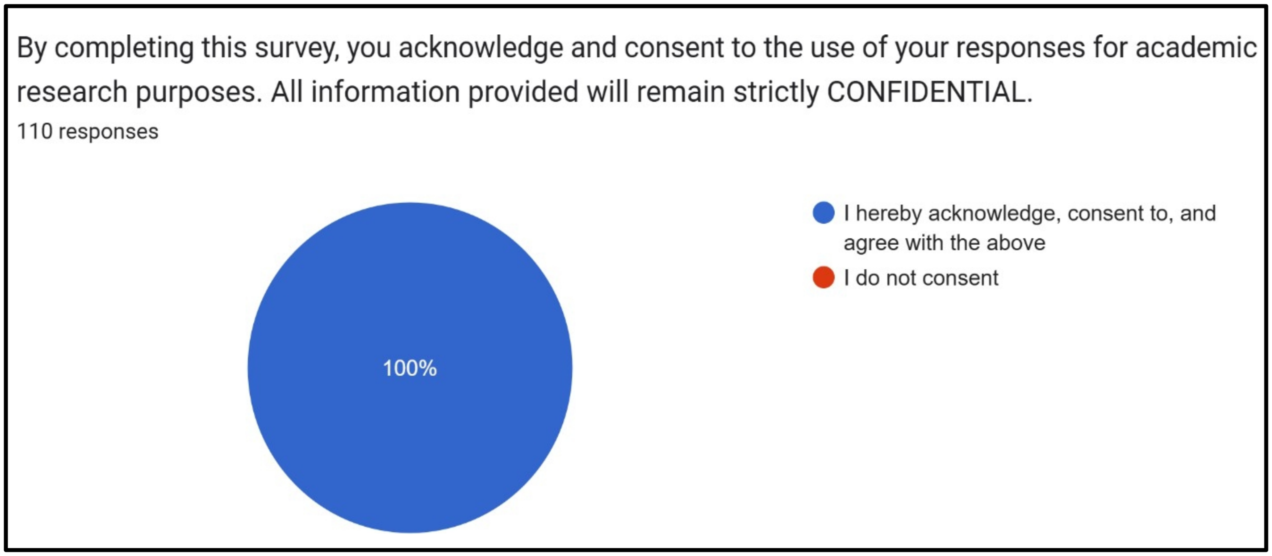
There are two main approaches to data analysis: qualitative and quantitative. Qualitative data analysis focuses on a deep understanding of concepts, experiences, and meanings behind descriptive data, such as text or narratives. This method is often used in social and humanities research. On the other hand, quantitative data analysis concentrates on measuring and analyzing numerical data to test hypotheses and generalize. This method is commonly used in science and business fields.

The steps in data analysis include:

1. **Data Collection**: Gathering relevant data from various sources.
2. **Data Cleaning**: Removing or correcting inconsistent or incomplete data.
3. **Data Transformation**: Converting data into a suitable format for analysis.
4. **Data Analysis**: Using statistical techniques or algorithms to analyze data and identify patterns.
5. **Result Interpretation**: Interpreting the analysis results to gain actionable insights.
6. **Data Visualization**: Presenting data in graphical or diagrammatic forms to facilitate understanding.

Data analysis plays a vital role in various fields, including business, healthcare, education, and government. By effectively understanding and applying data analysis, organizations and individuals can make more accurate and strategic decisions.

4.1 Categorical Data

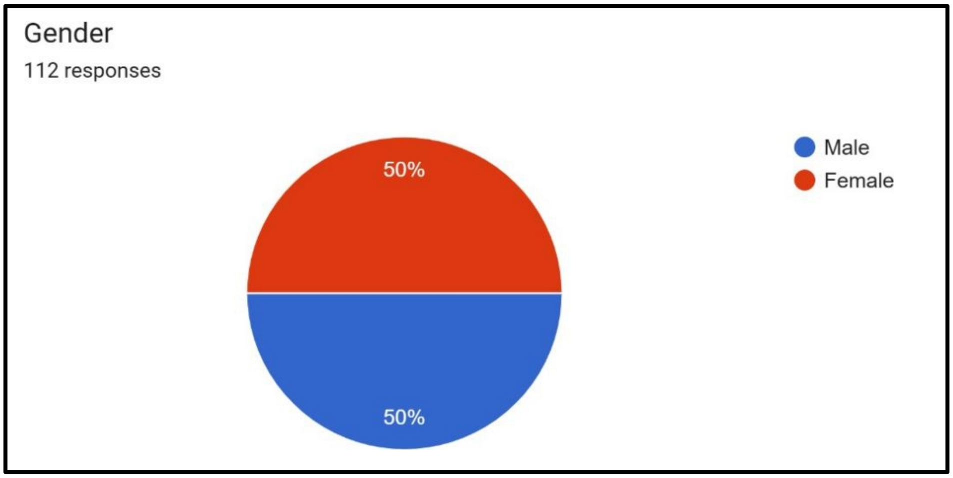


By completing this survey, you acknowledge and consent to the use of your responses for academic research purposes. All information provided will remain strictly CONFIDENTIAL.

110 responses

The pie chart above shows the results of the question regarding respondents' consent for the use of their data for academic research purposes. Out of a total of 110 respondents, **100% agreed** ("I hereby acknowledge, consent to, and agree with the above") and **0% did not consent**. This demonstrates that all respondents gave their full consent for their information to be used confidentially and in accordance with the stated conditions.

4.2 Section A: Demographic Information



Gender

112 responses

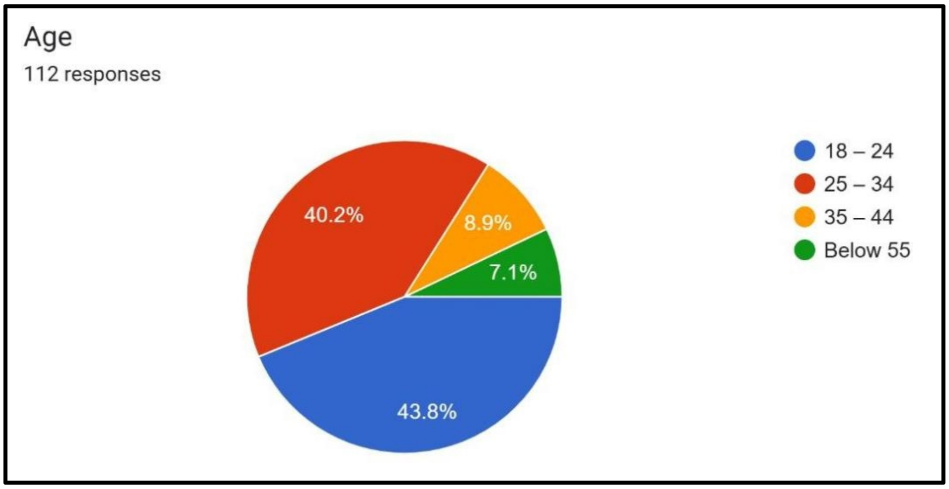
Gender Distribution of Respondents

The pie chart above presents the gender distribution of the 112 respondents who participated in the study on *Cybersecurity Awareness Among Internet Users*. The chart indicates an equal representation of genders, with:

- **50% (56 respondents)** identified as **Male**
- **50% (56 respondents)** identified as **Female**

This balanced distribution ensures that the findings of this research are not biased toward one gender and provide a more representative overview of cybersecurity awareness levels across both male and female internet users.

4.3 Age Distribution of Respondents

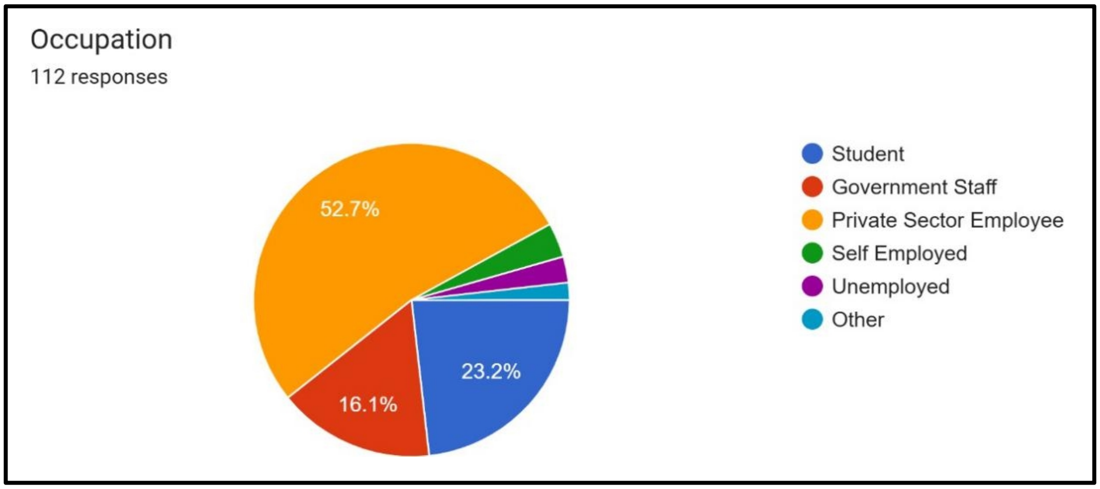


The pie chart above illustrates the age distribution of the 112 respondents who participated in the study on *Cybersecurity Awareness Among Internet Users*. The findings reveal that many respondents belong to the younger age groups. The detailed breakdown is as follows:

- **43.8%** of respondents are aged **18–24 years old**
- **40.2%** are aged **25 – 34 years old**
- **8.9%** are aged **35 – 44 years old**
- **7.1%** are aged **below 55 years old**

This distribution indicates that individuals aged between 18 and 34 years constitute approximately 84% of the total respondents, highlighting that the study predominantly reflects the perspectives of the most active internet users. Therefore, the results are highly relevant in evaluating cybersecurity awareness among the digital-native generation.

4.4 Occupation Distribution of Respondents



The pie chart above presents the occupation distribution of the 112 respondents who participated in this study. The data revealed that participants come from various professional backgrounds, with the majority being employed in the private sector. The breakdown is as follows:

- **52.7%** are **Private Sector Employees**
- **23.2%** are **Students**
- **16.1%** are **Government Staff**
- Approximately **3%** are **Self-Employed**
- The **Unemployed** and **Other** categories each account for less than **3%**

This diverse distribution provides a broad view of cybersecurity awareness among internet users from different occupational backgrounds. Those who are employed, particularly in the private and public sectors, are more likely to be exposed to cybersecurity threats through daily interactions with organizational systems such as corporate emails, cloud platforms, online banking, and remote work applications.

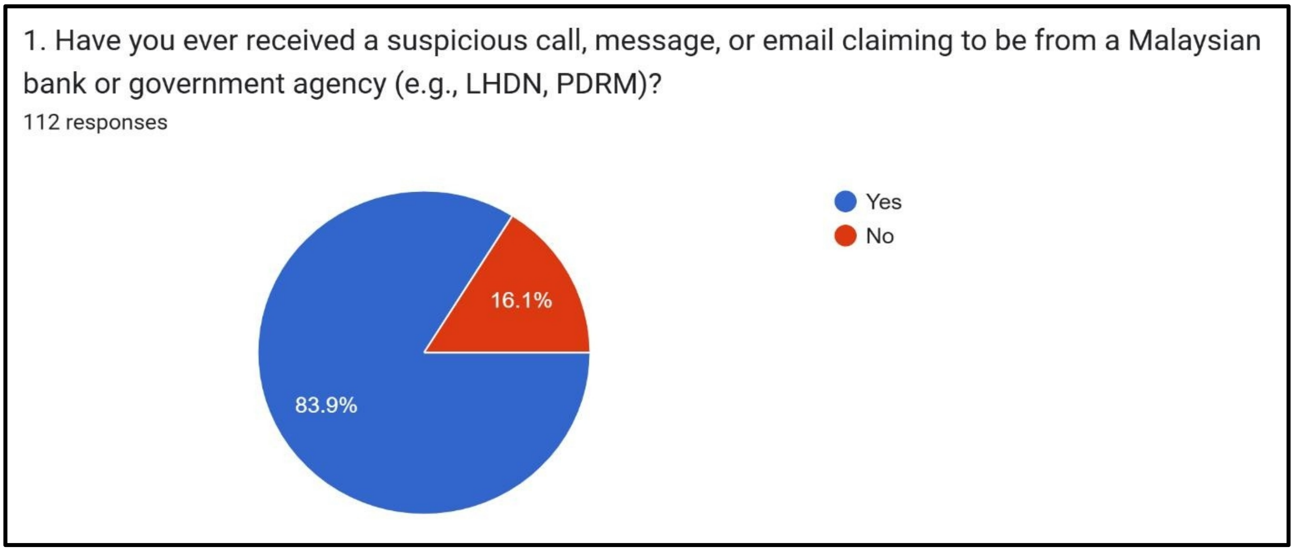
Meanwhile, students represent the younger generation who are consistently connected to the internet for learning, entertainment, and social networking. Although they are digitally savvy, not all may be fully aware of cyber threats such as phishing, malware, or identity theft.

The inclusion of respondents from the **self-employed**, **unemployed**, and **other** categories adds further value to the study, as they represent individuals who may access the internet independently for business purposes, job seeking, or personal activities.

Overall, this occupational distribution allows for a more comprehensive analysis of cybersecurity awareness across various types of internet users based on their work status and digital engagement.

4.5 Section B: Knowledge on Cybersecurity

Question 1



1. Have you ever received a suspicious call, message, or email claiming to be from a Malaysian bank or government agency (e.g., LHDN, PDRM)?

112 responses

Response	Count
Yes	94
No	18

- **Mode:** The most frequent response is "Yes" (94 respondents).
- **Median :** Yes (as over half respondent “Yes”)
- **Mean :** Not applicable for categorical data.

The pie chart above illustrates the responses to the question:
“Have you ever received a suspicious call, message, or email claiming to be from a Malaysian bank or government agency (e.g., LHDN, PDRM)?”
A total of **112 respondents** participated in this section of the survey.

Key findings are as follows:

- **83.9%** of respondents answered **“Yes”**, indicating that they have received suspicious communications that appeared to be scams.
- Only **16.1%** answered **“No”**, meaning they have not encountered such incidents.

Analysis and Significance:

More than 4 out of every 5 respondents have received suspicious calls or messages strongly indicates that **cyber threats are widespread in Malaysia**, particularly those involving **the impersonation of government agencies and financial institutions**. This attack is commonly known as **phishing** or **social engineering**, where scammers trick individuals into revealing sensitive information such as bank account numbers, identity card numbers, or login credentials.

This trend is concerning because:

- It shows that many Malaysians are still being targeted through digital platforms such as SMS, email, and phone calls.
- Cybercriminals often impersonate trusted institutions like **LHDN, PDRM, Bank Negara**, or commercial banks to gain the victim's trust.

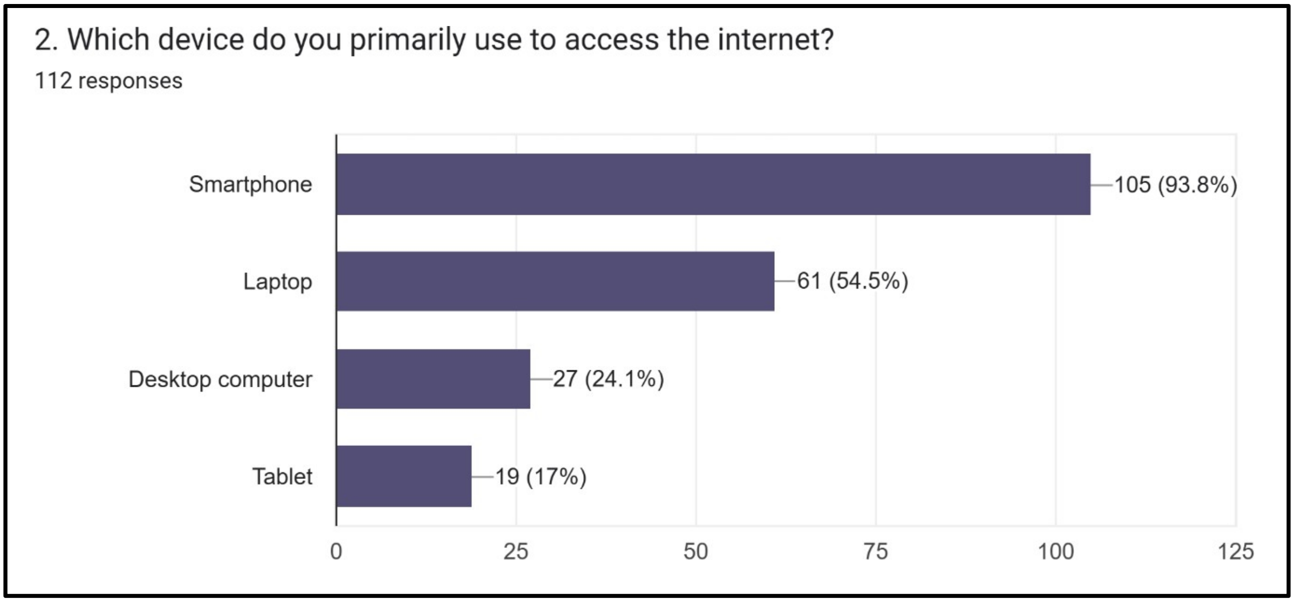
Implications for Cybersecurity Awareness:

These results highlight the urgent need to **enhance public awareness and education** about cybersecurity. While many have encountered such scams, not all may be equipped to recognize or respond to them effectively.

Therefore, this calls for greater efforts from authorities, educators, and organizations to:

- Conduct more public cybersecurity awareness campaigns.
- Provide training on how to identify and report phishing and scam attempts.
- Educate users about common signs of fraud, such as urgent language, suspicious links, and requests for personal information.

Question 2


2. Which device do you primarily use to access the internet?

112 responses

Device	Frequency
Smartphone	105
Laptop	61
Desktop computer	27
Tablet	19

- **Mode**: The most frequent response is "Smartphone" (105 respondents).
- **Median / Mean :** Not applicable.

The bar chart above presents the responses to the question:
“Which device do you primarily use to access the internet?”
A total of **112 respondents** participated in this section of the survey, and they were allowed to select more than one device.

Key findings are as follows:

- **93.8% (105 respondents)** use a **Smartphone** as their primary device to access the internet.
- **54.5% (61 respondents)** reported using a **Laptop**.
- **24.1% (27 respondents)** use a **Desktop computer**.
- **17% (19 respondents)** use a **Tablet**.

Analysis and Implications:

The data clearly indicates that smartphones are the **most used device** for internet access among respondents. This finding aligns with current trends in digital behaviour, where mobile internet usage continues to dominate due to convenience, portability, and affordability.

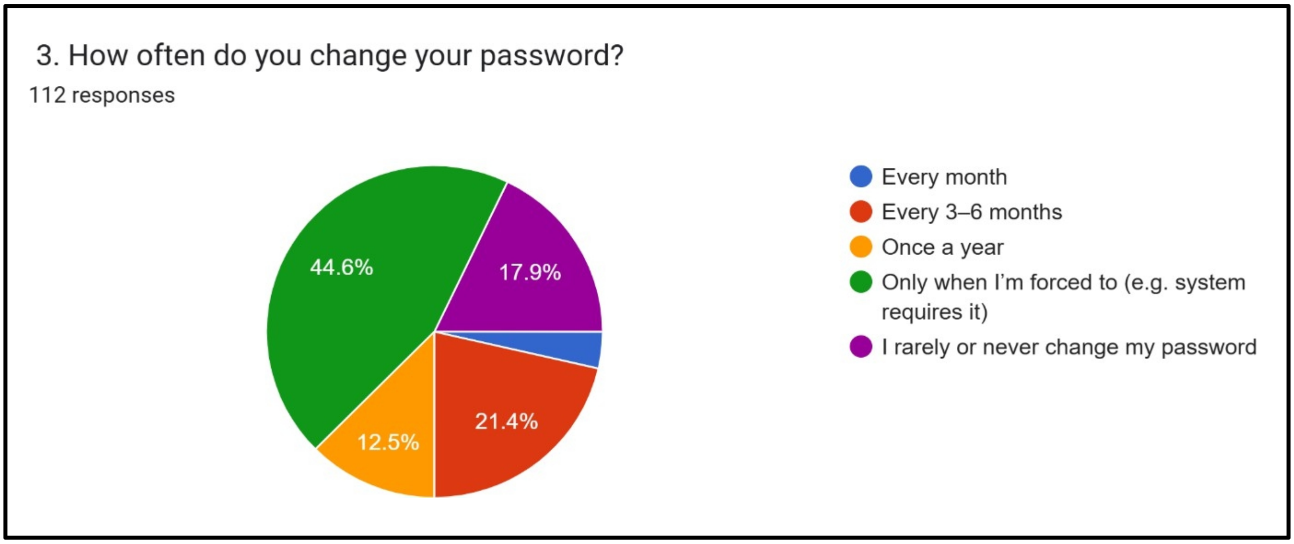
The high usage of smartphones also suggests that cybersecurity awareness campaigns should be **optimized for mobile platforms**, especially since many cyber threats—such as phishing links, malicious apps, and fraudulent messages are often encountered via mobile devices.

Meanwhile, the use of laptops and desktops, although less dominant, still reflects the presence of users accessing the internet for educational, work, or productivity purposes. The lower percentage of tablet users indicates that tablets are not a primary choice for internet access among most respondents.

Conclusion:

This information is critical in tailoring cybersecurity strategies, as different devices present different types of risks. It emphasizes the need for **mobile-first cybersecurity education**, particularly in teaching users how to recognize threats on smartphones and manage security settings effectively.

Question 3


3. How often do you change your password?

112 responses

How Often ?	Frequency	Cumulative frequencies
Every month	4	4
Every 3-6 months	24	28
Once a year	14	42
Only when forced	50	92
Rarely or never	20	112

- **Mode:** The most frequent response is "Only when forced" (50 respondents).
- **Median:** (112+1)/2 = 56.5, so the **56th and 57th** respondents fall under "Only when forced"
- **Mean :** Not precisely computable without numerical coding, but ordinal central tendency is "Only when forced"

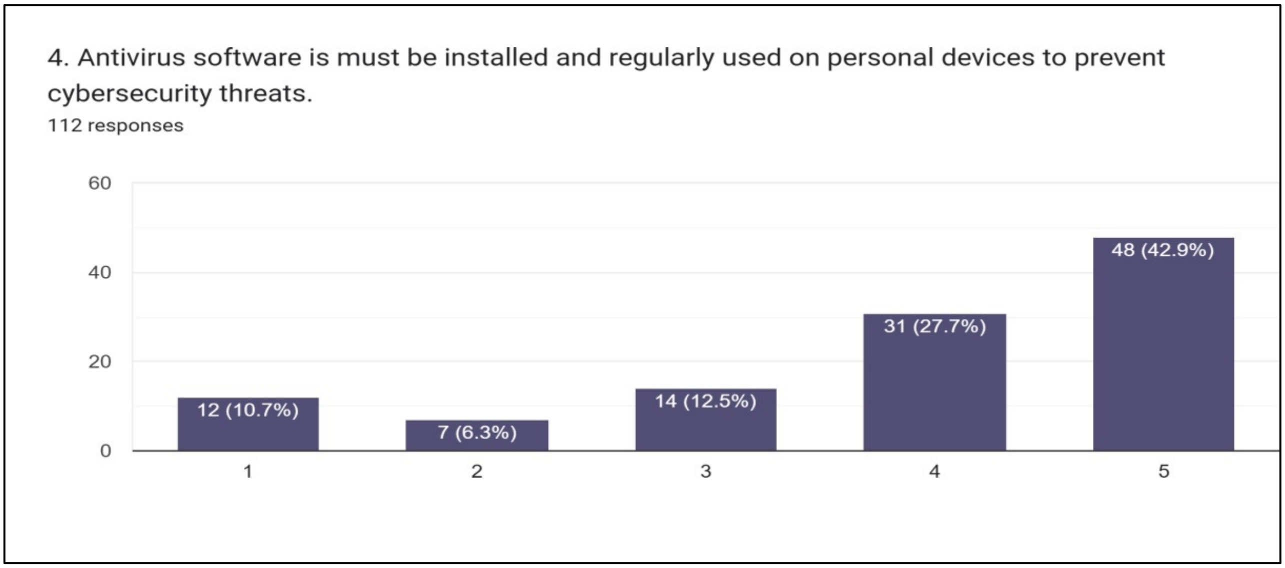
Based on the responses from 112 participants, the findings reveal that the practice of regularly updating passwords is still not widely adopted among internet users. A significant portion of respondents, **44.6%**, stated that they only change their passwords **when they are forced to do so by a system requirement**, such as receiving a prompt to update their login credentials. In addition, **17.9%** admitted that they **rarely or never change their passwords**, which is a highly risky habit in terms of cybersecurity.

Only a small percentage of users demonstrated higher awareness by changing their passwords more frequently. **21.4%** reported changing their passwords **every 3 to 6 months**, while **12.5%** do so **once a year**. The smallest group, just **3.6%**, indicated that they change their passwords **monthly**. These results suggest that only a minority of users are taking proactive steps to secure their data and accounts against potential cyber threats such as account breaches, identity theft, and data leaks.

Failing to change passwords regularly increases a user's vulnerability, especially for those who reuse the same passwords across multiple accounts. Relying solely on system prompts to change passwords also reflects a lack of personal initiative and understanding of basic cybersecurity hygiene. This is particularly concerning given the growing sophistication and frequency of cyberattacks, which include tactics such as brute-force attacks, phishing, and credential stuffing.

Therefore, these findings highlight a critical need to improve **public awareness and education on proper password management practices**. Emphasis should be placed on encouraging the use of secure password creation methods, implementing two-factor authentication (2FA), and utilizing password managers to store and manage complex passwords safely. Integrating these practices into cybersecurity awareness campaigns would significantly enhance users' ability to protect themselves in today's digital environment.

Question 4


4. Antivirus software is must be installed and regularly used on personal devices to prevent cybersecurity threats.

112 responses

Response	Count
Strongly Agree	48
Agree	31
Neutral	14
Disagree	7
Strongly Disagree	12

- **Mode :** The most frequent response is 5 "Strongly Agree" (48 respondents).
- **Median :** Middle value is between **56th and 57th**, respondents fall under 4 "Agree"
- **Mean :** (5×48)+(4×31)+(3×14)+(2×7)+(1×12)/112 = 432/112 = 3.86

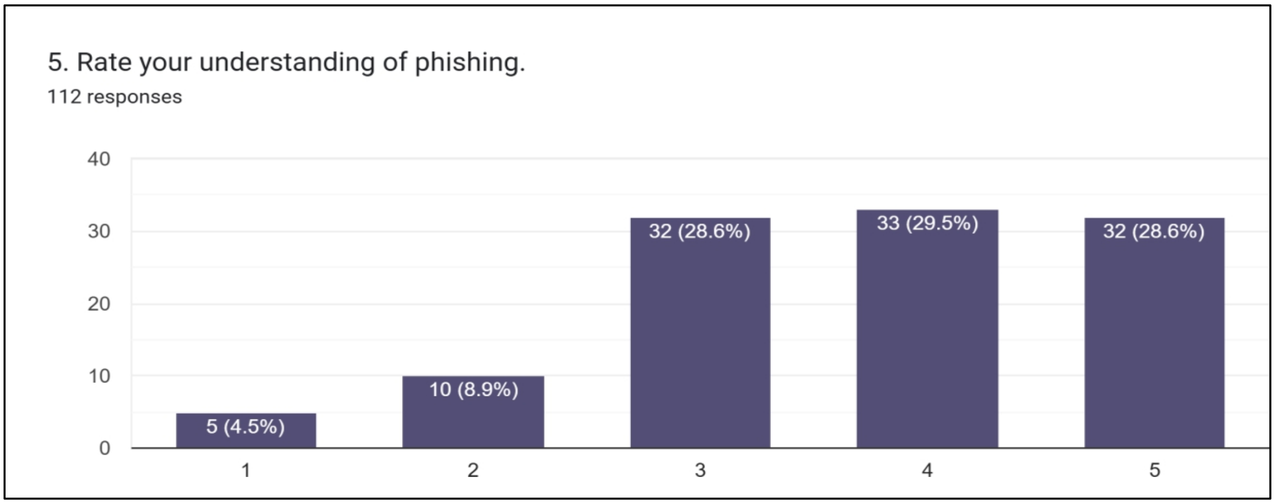
This question evaluates the **general opinion on the necessity of antivirus software for personal devices**. Most respondents recognize its importance in preventing cybersecurity threats, with **42.9%** (48 respondents) strongly agreeing that antivirus software must be installed and regularly used. This indicates a high level of awareness about the necessity of antivirus software in safeguarding devices from cyber threats. However, there are also some mixed opinions :

27.7% (31 respondents) agree that antivirus software is important, though they might not consider it as critical as those selecting the highest rating (5).
12.5% (14 respondents) remain neutral, suggesting that they either do not have a strong opinion on the matter or may not see antivirus software as a priority.

A smaller portion of respondents disagree or feel that antivirus software is not essential :

6.3% (7 respondents) disagree, possibly believing in alternative security measures.
10.7% (12 respondents) strongly disagree, possibly due to overconfidence in other security practices or a lack of concern regarding cyber threats.

Question 5



Rating	Count
Excellent	32
Good	33
Moderate	51
Minimal	10
None	5

- **Mode :** The most frequent response is "Moderate" (51 respondents).
- **Median :** Middle value is between **56th and 57th,** respondents fall under "Moderate"
- **Mean :** (5×32) + (4×33) + (3×51) + (2×10) + (1×5) / 131 = 470/131= **3.59**

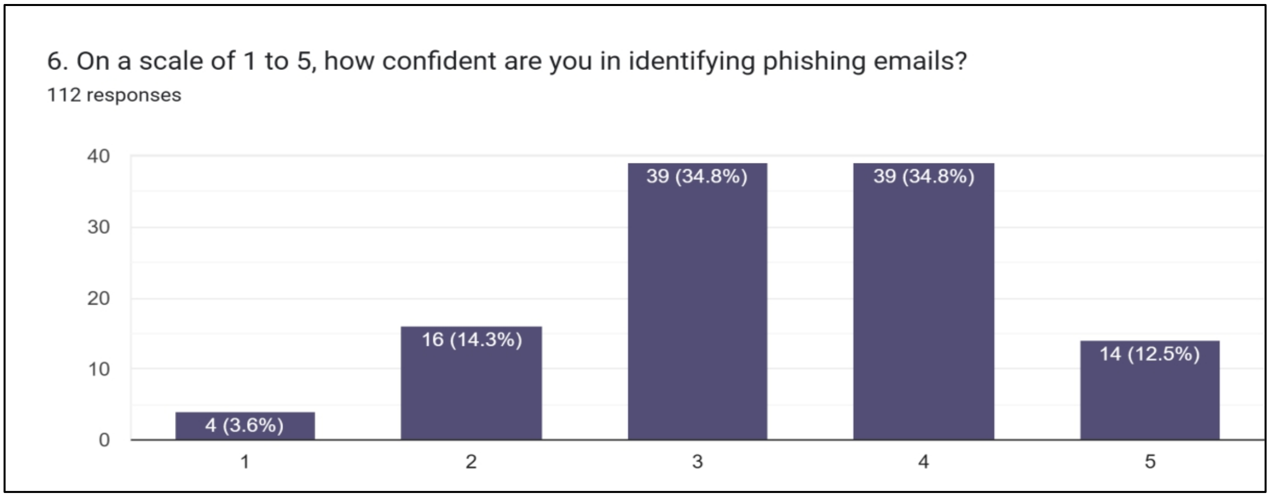
When asked to rate their understanding of phishing, the responses show a general awareness but also a significant portion of respondents with limited or moderate understanding :

45.5% (51 respondents) have a **moderate understanding**, which suggests that they are familiar with phishing but may not be fully knowledgeable about the latest threats or phishing techniques. **29.5%** (33 respondents) rated their understanding as good, indicating that they know about phishing and its risks but may not consider themselves experts.

A smaller group of respondents rated their understanding as excellent:
28.6% (32 respondents) feel confident in their knowledge of phishing, meaning they likely recognize common phishing tactics and know how to avoid them.

However, there are still gaps in understanding:
8.9% (10 respondents) have a **minimal understanding**, which indicates that these individuals might not recognize phishing attempts or may fall victim to such attacks. **4.5%** (5 respondents) have **no understanding**, highlighting a need for further educational efforts to address this vulnerability.

Question 6


6. On a scale of 1 to 5, how confident are you in identifying phishing emails?
112 responses

Confidence Level	Count
Very Confident	14
Confident	39
Somewhat Confident	39
Not Very Confident	10
Not Confident at All	5

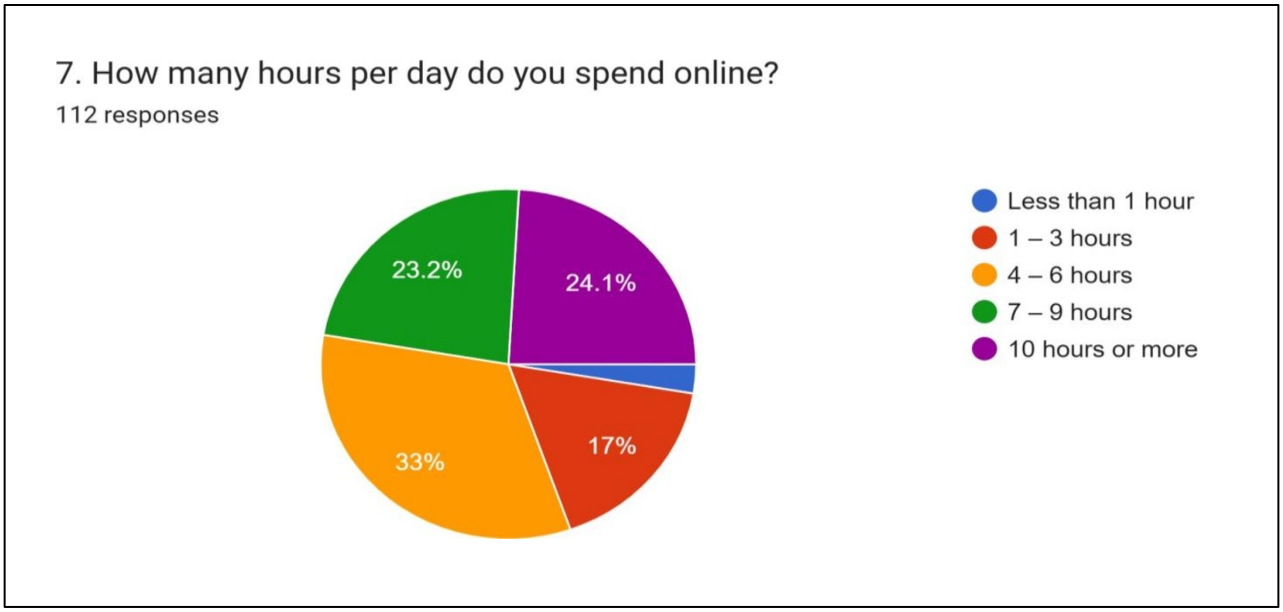
- **Mode :** The most frequent response is "Confident & Somewhat Confident" (39 each respondents).
- **Median :** Middle value is between **56th and 57th,** respondents fall under "Somewhat respondent"
- **Mean :** (5×14)+(4×39)+(3×39)+(2×10)+(1×5)/107 = 368/107 = **3.44**

Regarding the confidence in identifying phishing emails, the responses show a generally positive outlook but also a notable portion of users lacking full confidence:

34.8% (39 respondents) feel **confident** (rating 4) in identifying phishing emails, and an equal number, 34.8% (39 respondents), are somewhat confident (rating 3). This suggests that while many users can recognize phishing attempts, they may not feel fully certain or may second-guess themselves in ambiguous situations.
12.5% (14 respondents) rated themselves as very confident (5), indicating they are highly capable of detecting phishing emails, likely due to prior training or experience.

However, there remains a portion of the survey population with **lower confidence** :
8.9% (10 respondents) rated themselves as ***not very confident** (2), implying that they might struggle to distinguish between legitimate and phishing emails.
4.5% (5 respondents) rated themselves as **not confident at all** (1), a concerning statistic indicating these users are highly vulnerable to phishing attacks.

Question 7



Time Spent Online (hours)	Count
Less than 1 hour	3
1-3 hours	19
4-6 hours	37
7-9 hours	26
10 hours and more	27

Class Interval (hours)	Frequency (*f*)	Cumulative Frequency (*cf*)	Midpoint (x)	x^2	*fx*
Less than 1	3	3	0.5	0.25	1.5
1 - 3	19	22	2	4	38
4 - 6	37	59	5	25	185
7 - 9	26	85	8	64	208
10 and more (24 hours)	27	112	17	289	459
Total	**112**	**-**	**-**	**-**	**891.5**

- **Mode :** The most frequent response is "4 - 6 hours" (37 respondents).
- **Median :** Middle value from 112 respondents is (112 + 1) / 2 = 56.5, so the median from class interval is **5 hours**.
- **Variance :** $s^2 = (10468.75 / 112) - (7.96)^2$

  $s^2 = 93.47 - 63.36$

  $s^2 = 30.11$
- **Standard deviation :** Variance (s^2) = 30.11

  Standard Deviation (s) = $\sqrt{30.11}$= 5.48 hours

This image presents a pie chart summarizing responses to the questions:
"How many hours per day do you spend online?" With data collected from 112 respondents, the responses are broken down into five-time ranges.

Analysis and observation:

Time spent online (per day)

1. Less than 1 hour

- Represented in **blue**
- **2.7%** of respondents, which is equivalent to 3 individuals.
- The smallest segment

2. 1 - 3 hours

- Represented **red**
- **17%** of respondents, which is equivalent to 19 individuals.

3. 4 - 6 hours

- Represented in **orange**
- **33%** of respondents, which is equivalent to 37 individuals.
- The largest segment

4. 7 - 9 hours

- Represented in **green**
- **23.2%** of respondents, which is equivalent to 26 individuals.

5. 10 hours or more

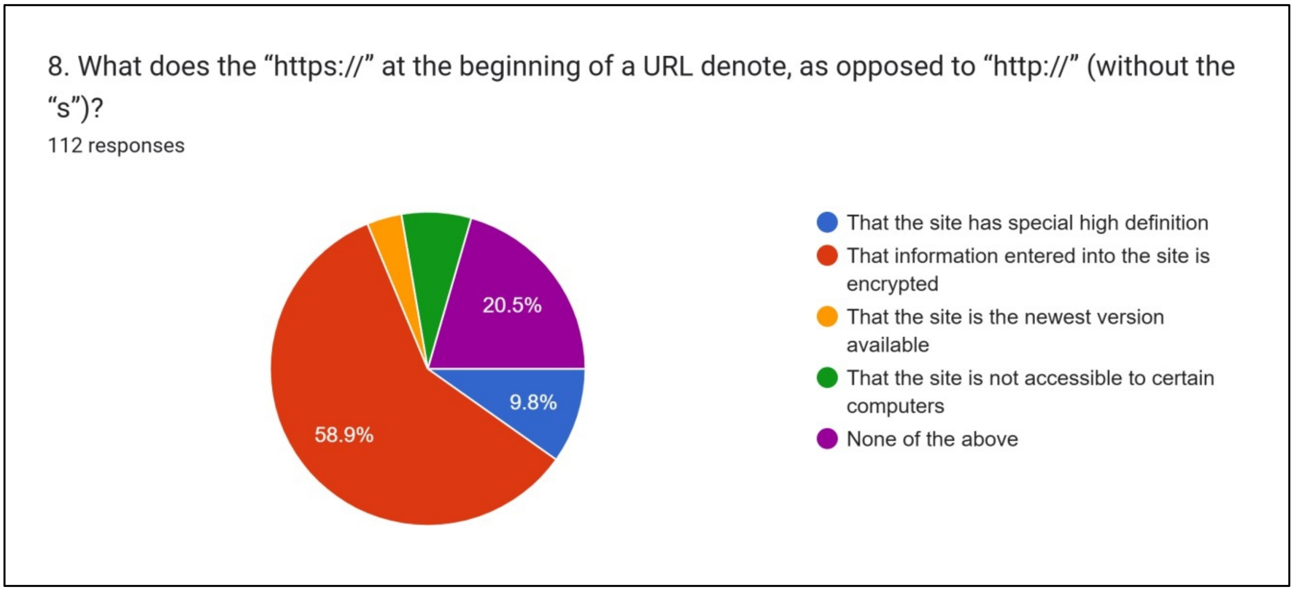
- Represented in **purple**
- **24.1%** of respondents, which is equivalent to 27 individuals.

The data shows that most respondents (over 80%) are spending more than 4 hours online each day, with 33% falling within the 4 - 6-hour range, 23.2% falling within the 7 - 9 hours, and 24.1% exceeding 10 hours. This indicates a high level of dependence on the internet, highlighting the urgent need to raise awareness and promote cybersecurity practices among internet users.

Conclusion:

With over 80% of users spending more than 4 hours online daily, the data shows a strong reliance on the internet and a higher exposure to cyber threats. This highlights the importance of enhancing cybersecurity awareness and promoting safe online practice, particularly among frequent internet users.

Question 8



8. What does the “https://” at the beginning of a URL denote, as opposed to “http://” (without the “s”)?

112 responses

Answer	Frequency
That the site has special high definition	11
That information entered is encrypted	66
That the site is the newest version available	4
That the site is not accessible to certain computers	8
None of the above	23

- **Mode :** The most frequent response is "That information entered is encrypted” (66 respondents).

This pie chart displays the responses of 112 participants regarding their understanding of the question: **“What does the ‘https:// at the beginning of a URL denote, as opposed to ‘http://” (without the “s”)?.** the correct answer to this question is “**That information entered into the site is encrypted”, which** refers to a protocol that secures communication and data transfer between the user’s web browser and the website.

Analysis and observation:

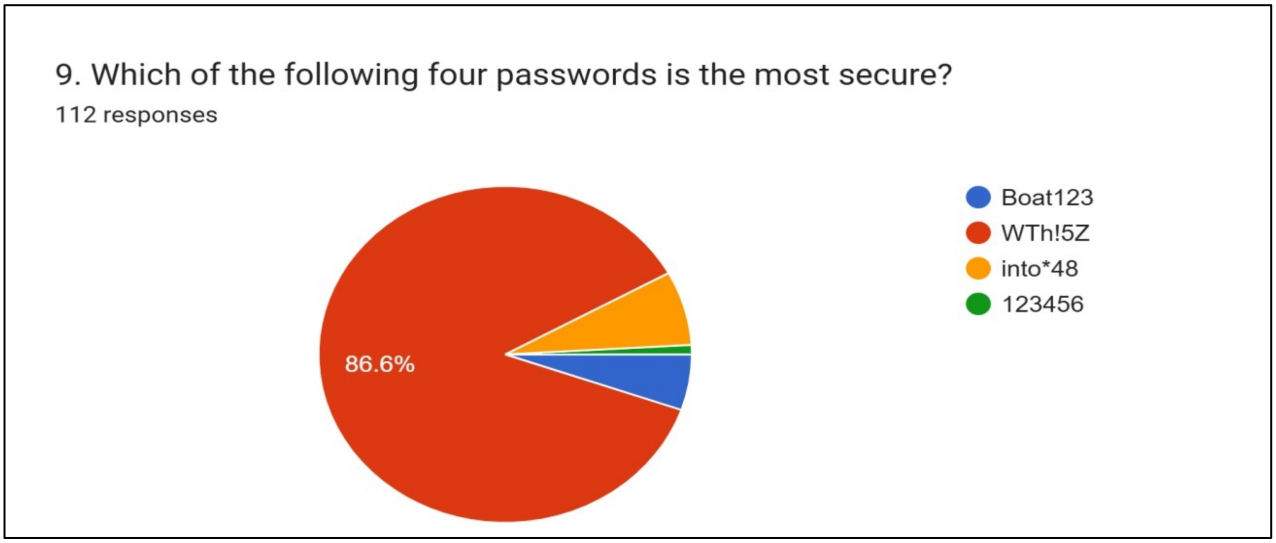
- 🟦 - That the site has special high definition - **9.8%** respondents**,** which is equivalent to **11** individuals.
- 🟥 - That information entered the site is encrypted - **58.9%** respondents **(the highest respond),** which is equivalent to **66** individuals.
- 🟧 - That the site is the newest version available - **3.6%** respondents**,** which is equivalent to **4** individuals.
- 🟩 - That the site is not accessible to certain computers - **7.1%** respondents**,** which is equivalent to **8** individuals.
- 🟪 - None of the above - **20.5%** respondents**,** which is equivalent to **23** individuals.

Even though the majority respondents (58.9%) correctly identified the meaning of “https://” with the correct answer, there were still a number (41.1%) who indicated incorrect or uncertain answer (None of the above). This indicated that while more than half of the respondents had a basic understanding of secure web protocols, there was still a large minority that still lacked clarity and displayed incorrect perceptions regarding basic aspects of online security.

Conclusion:

The results show that while most internet users recognize that "https://" signifies as a protocol that secures communication and data transfer between the user’s web browser and the website, awareness still not comprehensive. With over 40% demonstrated confusion or misunderstanding, there is a clear need for more effective education on basic cybersecurity concepts, particularly about secure browsing practices, which are essential for safe internet use in everyday life.

Question 9



9. Which of the following four passwords is the most secure?

112 responses

Password Option	Frequency
Boat123	6
WTh!5Z	97
into*48	8
123456	1

- **Mode :** The most frequent response is "WTh!5Z" (97 each respondents).

This pie chart reflects responses from 112 participants evaluating four different passwords based on "**Which of the following four password is the most secure?"**. The correct answer is **"WTh!5Z",** as it combines uppercase and lowercase letters, numbers, and special character, making it the strongest password by complexity standards.

Analysis and observation:

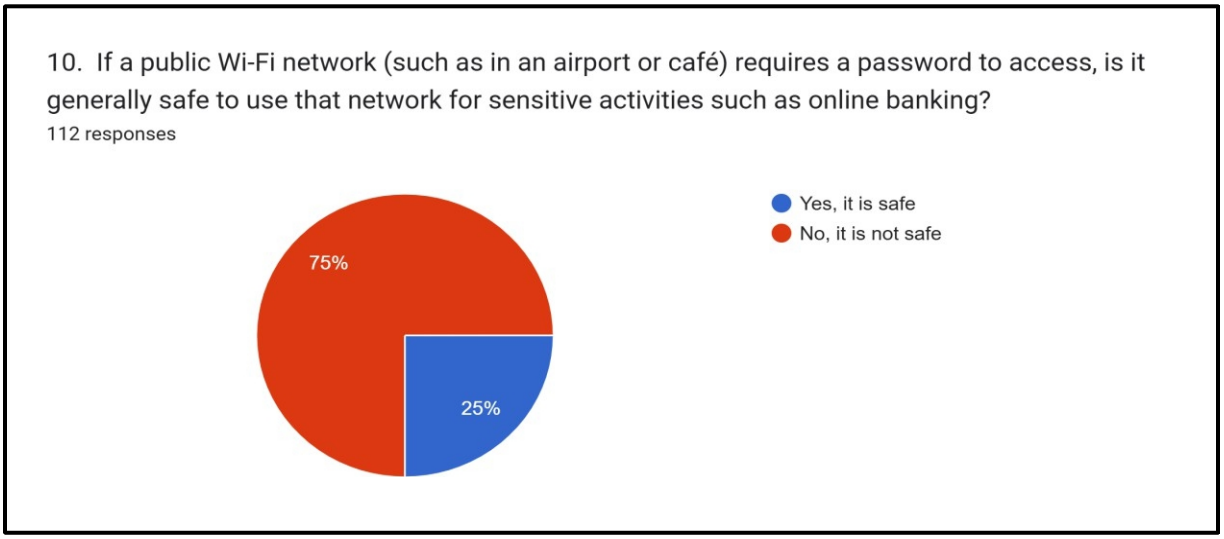
- 🟦 - Boat123 **- 5.4%** respondents**,** which is equivalent to **6** individuals.
- 🟥 - **WTh!5Z - 86.6%** respondents (the correct answer and most secure), which is equivalent to **97** individuals.
- 🟧 - **into*48 - 7.1%** respondents, which is equivalent to **8** individuals.
- 🟩 - **123456** - **0.9%** respondents, which is equivalent to **1** individual.

Most participants (**86.6%**) correctly identified **WTh!5Z** as the most secure password, indicating a strong awareness of good password practices among respondents. Only a small percentage (**13.4%**) have selected a weaker option such as **Boat123** (simple and easily guessable), **into*48** (moderately secure but less weak than WTh!5Z), and **123456** (very common and highly insecure).

Conclusion:

These results indicate that most internet users in this group have a good understanding of what makes a password strong, such as using mixed characters and complexity. However, the small percentage who selected a weak or a simplistic password indicates that there is still room for improvement in reinforcing best practice in password security, particularly for users who may default to simple or similar patterns.

Question 10



10. If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

112 responses

Is it safe ?	Frequency
Yes	28
No	84

- **Mode :** The most frequent response is "No” (84 respondents).

Shown here are the results of the question which about whether the public Wi-Fi network accessed using password are safe for sensitive activities. About 112 responses were acquired and the question only allowed one answer to be picked for each respondent.

Key Findings:

- 25% of the respondents (blue-colored segment) believe that it is safe for sensitive activities.
- While the remaining 75% (red-colored segment) thinks otherwise.

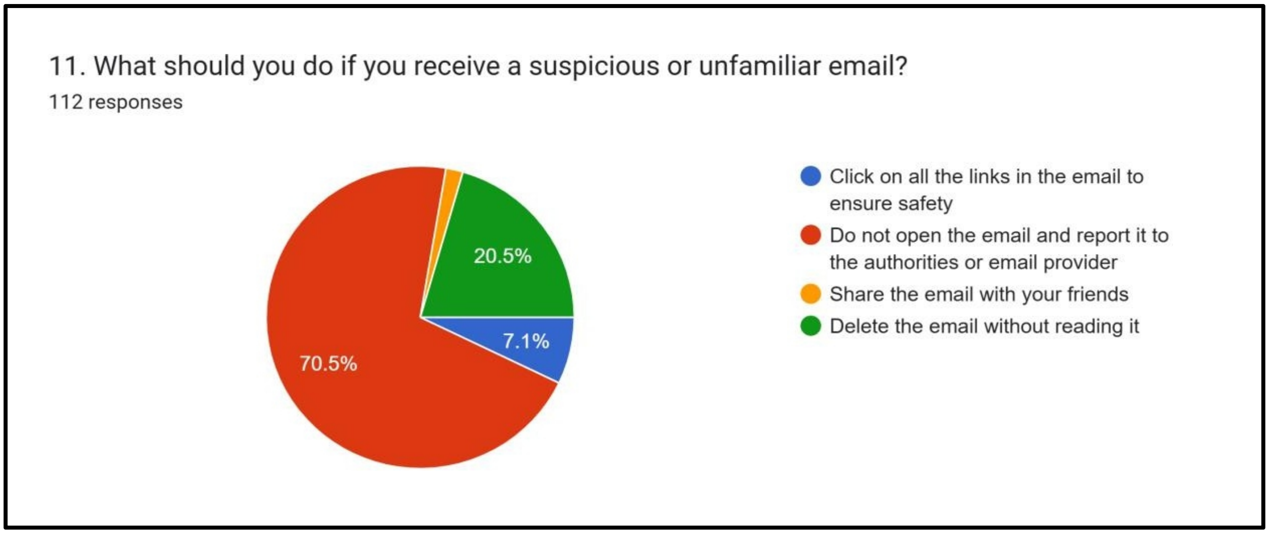
Analysis & Significance:

The result shows a majority (3/4) of respondents thinks public Wi-Fi that’s accessed with password are deemed unsafe for sensitive activities such as online banking. This shows that there's a huge awareness of the potential risks that are related to public networking although it's encrypted with password. Public Wi-Fi networks, even with guarded access are still exposed to safety threats like rogue hotspots, session hijacking or "man in the middle" attacks. About 25% that considered it safe probably underestimate the risk or believe that additional safety precautions such as HTTPS and VPN are enough to minimize the hazard.

Conclusion:

Data proved most of the users are aware about the public Wi-Fi safety limits, even though protected by password, and being cautious in using it for sensitive activities. This reflects the increase in digital literacy among users regarding online safety. However, 25% that trust the network highlights the need for continuous education in the best practices of cyber protection, ultimately in the public digital environment.

Question 11



11. What should you do if you receive a suspicious or unfamiliar email?

112 responses

Action	Frequency
Do not open and report it	79
Delete it without reading	23
Click all the links in the email to ensure safety	8
Share it with your friends	2

- **Mode :** The most frequent response is "Do not open and report it" (79 respondents).

The pie chart above summarizes responses to the question of what the respondents would do if they received an unfamiliar or suspicious email. Out of all 112 respondents, majority of them chose the option that focuses primarily on safety.

Key Findings :

- 70.5% of the respondents picked “Do not open the email and report it to the authorities or email provider”
- The second highest choice are green-colored segments, with a percentage of 20.5% that will delete the email.
- Blue-colored segment shows 7.1% of respondents will open the email just to check it as they are aware of the risk.
- Small remaining of the respondents, which are less than 2%, will go for sharing emails with friends.

Analysis & Significance :

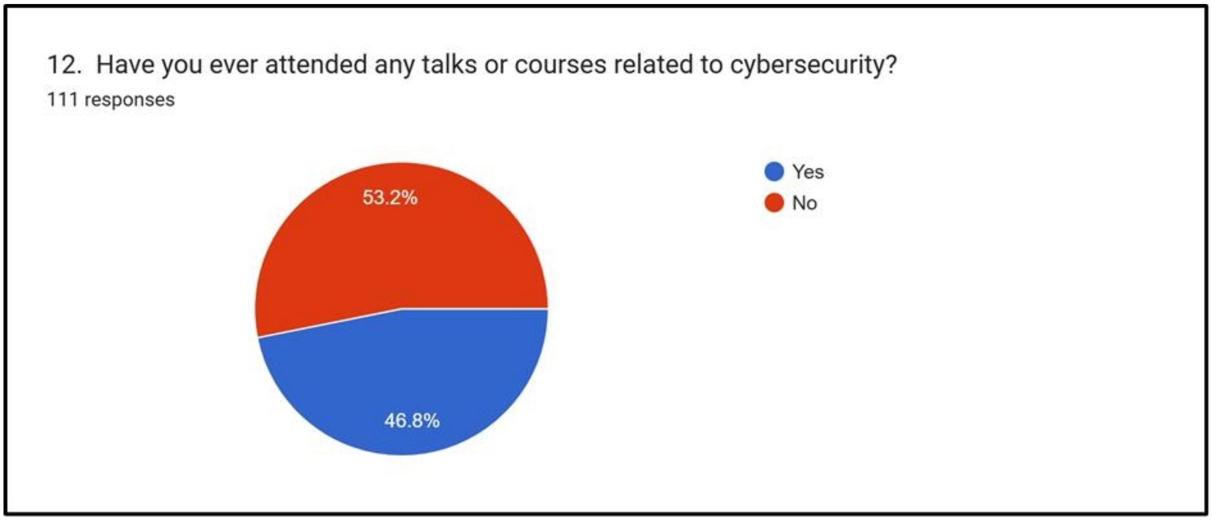
The result of this question proved that a large majority of the respondents (more than 70%) understand the correct and safe approaches in handling suspicious email, which is to report it to the authority or email provider. This showed the high awareness level of data phishing and cyber threats. However, 7.1% that will click all the links, as well as those who will share suspicious email, reflect worrying weaknesses in cyber safety awareness. These choices can cause malware infection, data to be stolen and account compromises.

Conclusion :

Most of the respondents appear to be applying good cyber safety practices by deciding to report or delete suspicious email. But the existence of the unsafe responses highlights the needs for continuous education of identifying and handling data phishing attempts. Solidifying safe digital practices through awareness campaigns or training courses can help to close this gap and next to reduce the risk of social engineering attacks.

4.6 Section C : Awareness & Training

Question 12



12. Have you ever attended any talks or courses related to cybersecurity?

111 responses

Response	Frequency
Yes	52
No	60

- **Mode :** The most frequent response is "No" (60 respondents).

The responses of the question "Have you ever attended any talks or courses related to cybersecurity" are illustrated by pie chart shown above. Out of 112 respondents, only 111 answered, leaving one skipped this question. The chart is divided into two response categories following 2 options available: yes and no.

Key Findings :

- 53.2% of respondents admit that they have never attended any talks or courses related to cybersecurity.
- The rest in blue, 46.8%, attended the talks or course.

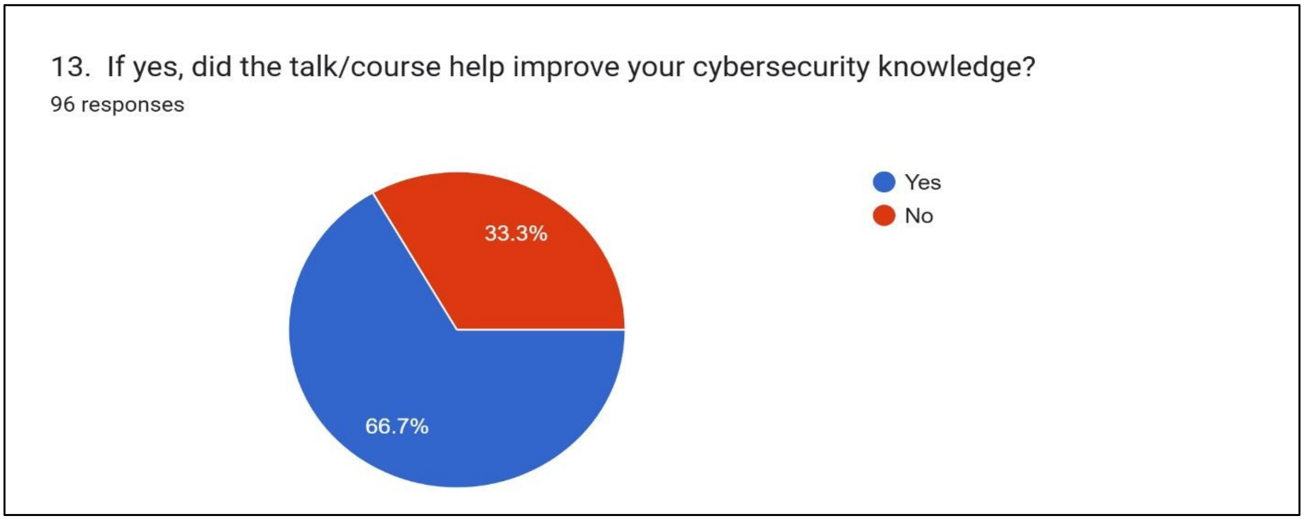
Analysis & Significance :

Data showed that more than half of the respondents lack formal exposure to cyber safety literacy. This is important because lack of training can contribute to risky online behaviors, such as trapped in data phishing frauds, or wrongly handling suspicious email (as seen on the previous chart). From the positive view, nearly half of the respondents have been exposed to the efforts of cyber safety awareness, suggesting the foundation that can be built upon.

Conclusion :

While it is encouraging that a sizeable portion of individuals have attended events related to cyber safety, the majority of those who haven't attended any represents clear opportunity for awareness establishment initiatives. Promoting cyber safety literacy through talks, workshops, or easily accessed online modules could solve these matters and elevate digital safety in the community.

Question 13



13. If yes, did the talk/course help improve your cybersecurity knowledge?

96 responses

Response	Frequency
Yes	64
No	32

- **Mode :** The most frequent response is "Yes" (64 each respondents).

The Pie Chart shows out of 96 participants, 66.7% reported that the talk/course helped improve their cybersecurity knowledge, while 33.3% did not find it beneficial.

Key Findings:

1. A majority (two-thirds) of attendees acknowledged gaining cybersecurity knowledge from the session.
2. A significant portion (one-third) felt no improvement, indicating potential gaps in content delivery or relevance.

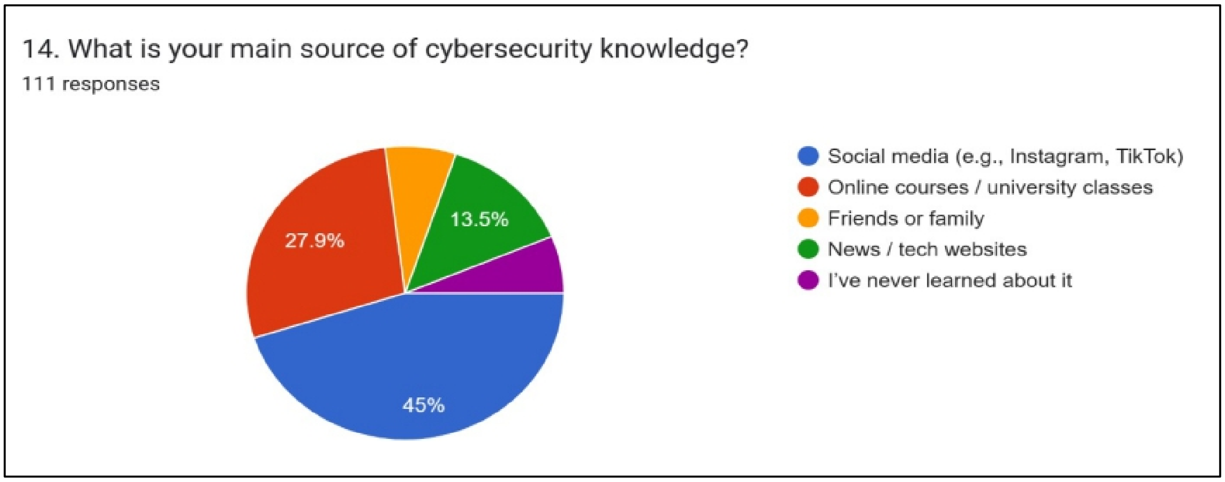
Analysis & Significance:

The data highlights that while the talk/course had a positive impact on most participants, there's room for improvement. Tailoring the content to diverse knowledge levels and including more interactive or practical examples could bridge the gap for those who didn’t benefit

Conclusion:

The session was generally effective in enhancing cybersecurity awareness, but future iterations should consider feedback-driven adjustments to ensure broader engagement and impact.

Question 14



14. What is your main source of cybersecurity knowledge?

111 responses

Source	Frequency
Social media	50
Online Courses	31
Friends or Family	15
News/Tech Websites	10
Never learned about it	4

- **Mode :** The most frequent response is "Social Media” (50 respondents).

Based on 111 responses, the largest group (45%) reported social media (e.g., Instagram, TikTok) as their primary source of cybersecurity knowledge. This is followed by online courses/university classes (27.9%), friends or family (13.5%), news/tech websites, and a small portion who admitted they’ve never learned about cybersecurity.

Key Findings:

1. Social media is the dominant source (45%) for cybersecurity learning, indicating a shift towards bite-sized, accessible content
2. Traditional learning platforms (like courses/university classes) still hold relevance but trail behind social media by a significant margin.

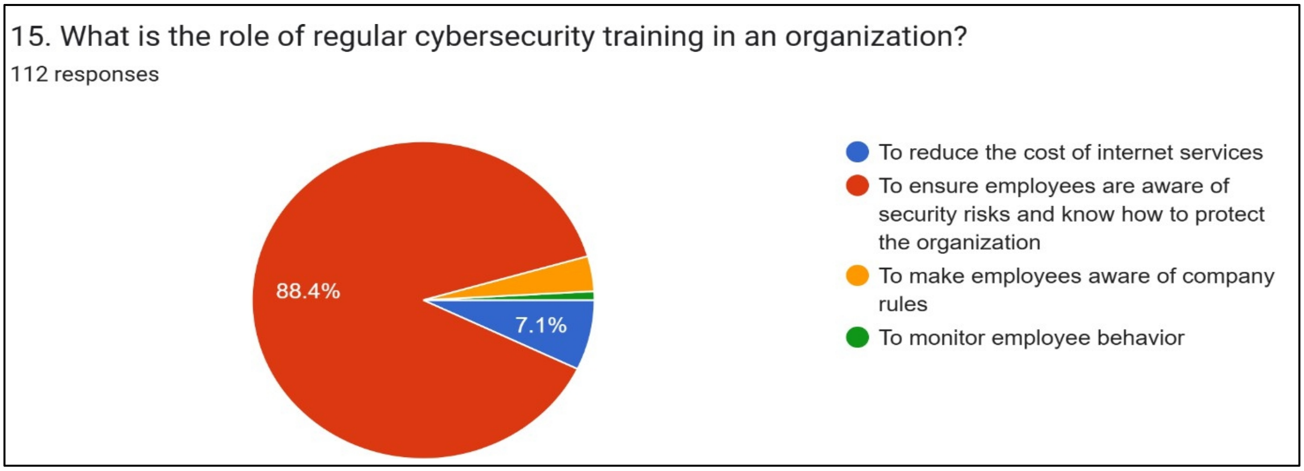
Analysis & Significance:

The findings suggest a growing dependency on social platforms for cybersecurity information, which can be both a strength (accessibility) and a risk (misinformation). Educational institutions may need to adapt their delivery methods to match learners' preferences and ensure credible content is also available in popular formats.

Conclusion:

Cybersecurity education is increasingly influenced by social media. While this democratizes access to knowledge, it underscores the need for accurate, credible content to be shared across these platforms, and for formal educators to engage where learners already are.

Question 12



15. What is the role of regular cybersecurity training in an organization?

112 responses

Role	Frequency
To ensure employees are aware of security risks	99
To reduce the cost of internet services	8
To make employees aware of company rules	3
To monitor employee behavior	2

- **Mode :** The most frequent response is "To ensure employees are aware of security risks" (99 respondents).

Out of 112 respondents, a vast majority (88.4%) believe the primary role of regular cybersecurity training is to ensure employees are aware of security risks and know how to protect the organization. A smaller percentage (7.1%) think it helps reduce internet service costs, while even fewer chose other roles such as enforcing company rules or monitoring behavior.

Key Findings:

1. **88.4%** of participants recognize awareness of security risks and protective practices as the key purpose of training.
2. Minimal emphasis is placed on secondary benefits like reducing costs or monitoring behavior.

Analysis & Significance:

This dominant response underscores the critical role of human factors in cybersecurity. Organizations increasingly understand that informed employees are their first line of defense. Investing in training not only reduces vulnerability but also fosters a culture of security awareness.

Conclusion:

Regular cybersecurity training is widely seen as essential for empowering employees with the knowledge to mitigate risks. Organizations should continue to prioritize training programs focused on practical threat awareness and response to build a resilient workforce.

5.0 Conclusion

The analysis of the survey results on cybersecurity awareness among Internet users in Malaysia highlights several key findings that emphasize the need for improved digital literacy and awareness in the face of rising cyber threats. Despite the increasing prevalence of cybercrimes, most respondents demonstrate a basic understanding of essential cybersecurity practices, such as password management and phishing detection. However, gaps remain, particularly among users who do not regularly update their passwords or lack confidence in identifying phishing attempts.

The results also underline the importance of cybersecurity education, with a significant portion of respondents indicating that they have attended cybersecurity talks or courses, but a larger number have not. This discrepancy reveals an opportunity for further engagement through educational campaigns and the integration of cybersecurity topics into everyday digital interactions.

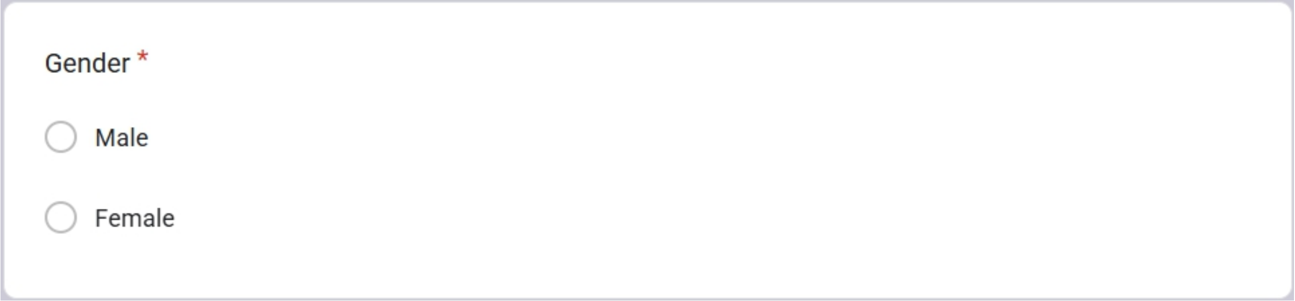
Furthermore, the study suggests that mobile devices, particularly smartphones, are the primary means of Internet access for most users, highlighting the importance of optimizing cybersecurity awareness programs for mobile platforms. Given the widespread use of mobile phones and the higher susceptibility to mobile-specific threats, campaigns should prioritize educating users on securing their devices and recognizing threats on mobile platforms.

In conclusion, while some progress has been made in raising awareness, the study's findings indicate a clear need for continuous education and outreach to equip users with the skills necessary to protect themselves from evolving cyber threats. This can be achieved through sustained, targeted efforts from both government and private sector organizations.

6.0 Questionnaire

https://forms.gle/6r3NrB5ZsgJFCB3J8

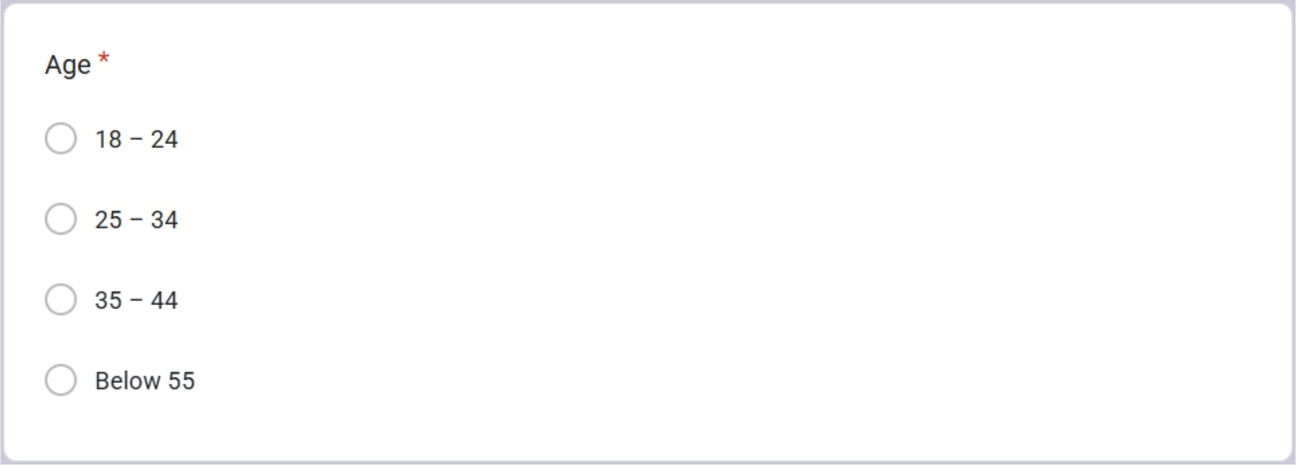
6.1 Section A: Demographic Information



Gender *

○ Male

○ Female



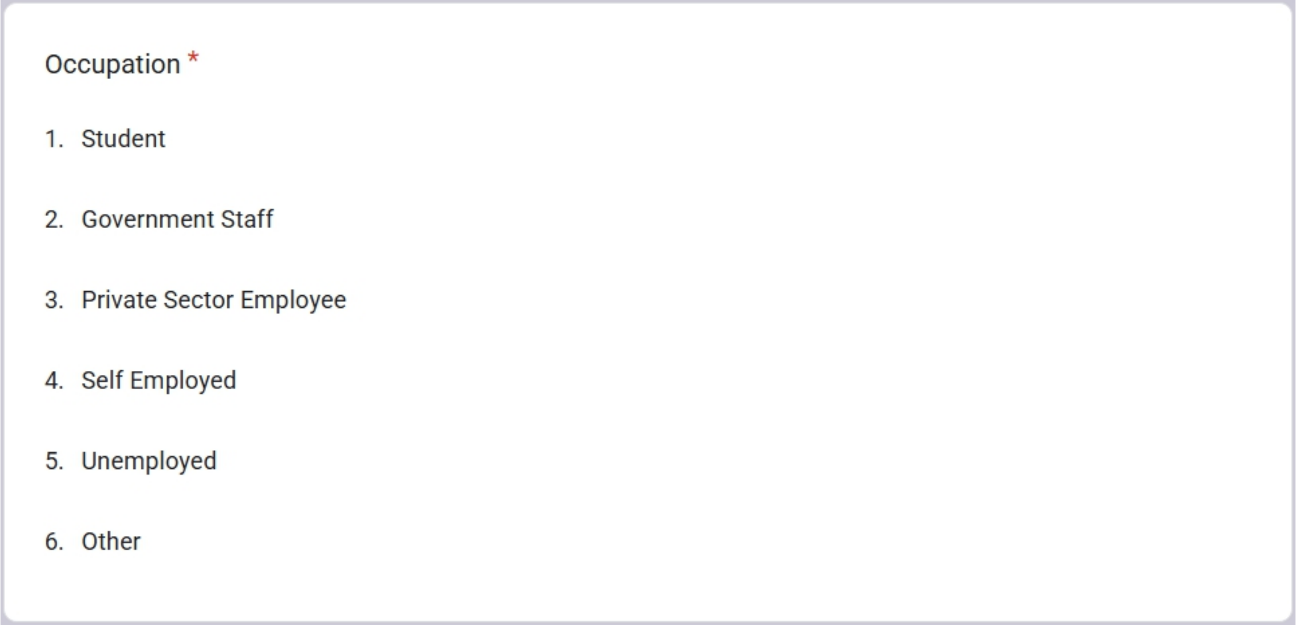
Age *

○ 18 – 24

○ 25 – 34

○ 35 – 44

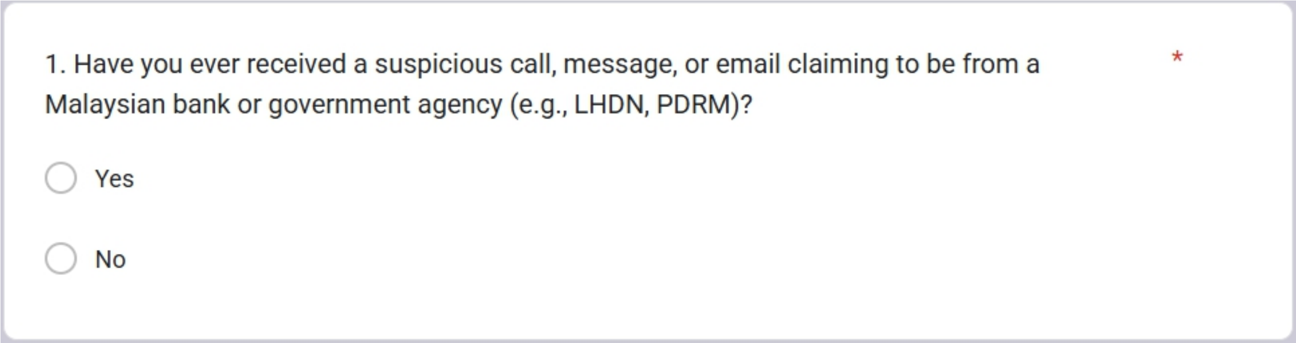
○ Below 55



Occupation *

1. Student
2. Government Staff
3. Private Sector Employee
4. Self Employed
5. Unemployed
6. Other

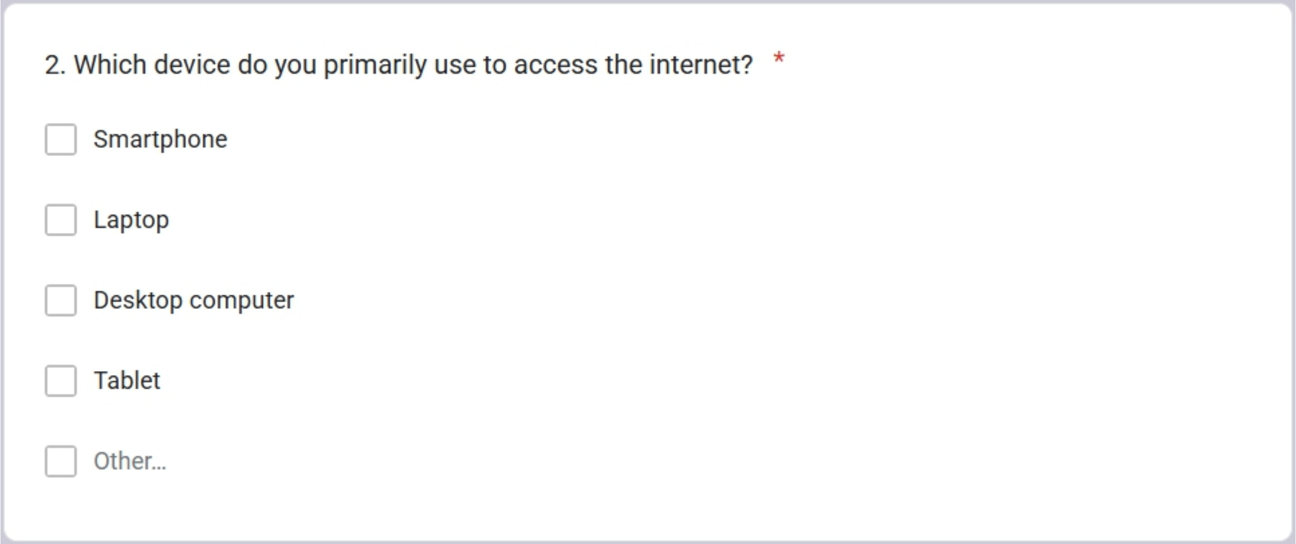
6.2 Section B: Knowledge of cybersecurity



1. Have you ever received a suspicious call, message, or email claiming to be from a Malaysian bank or government agency (e.g., LHDN, PDRM)? *

○ Yes

○ No



2. Which device do you primarily use to access the internet? *

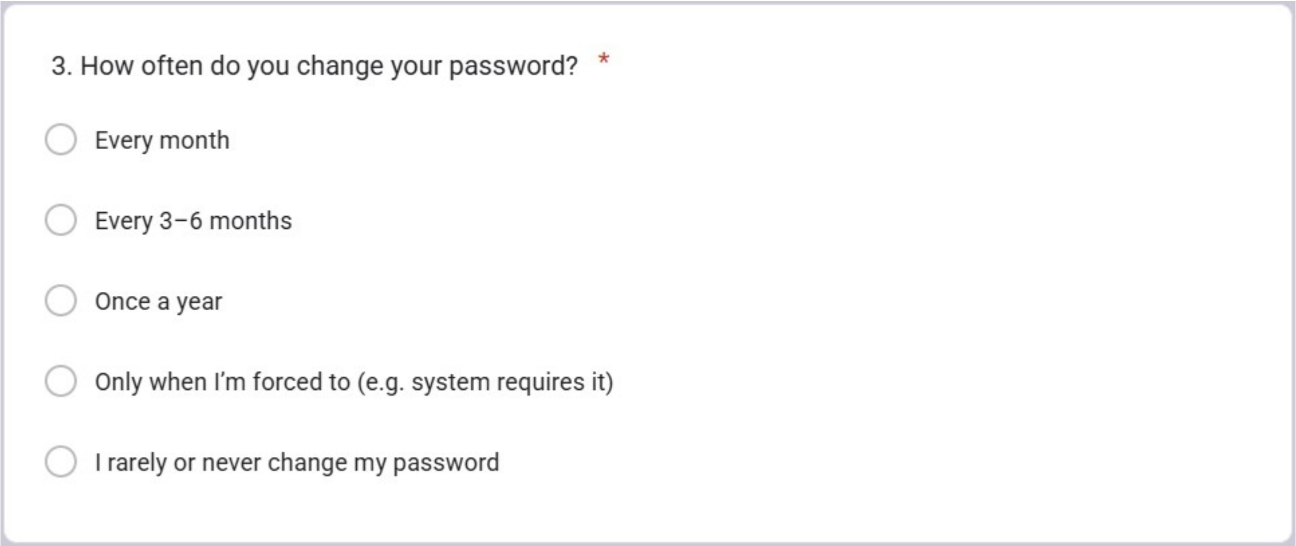
□ Smartphone

□ Laptop

□ Desktop computer

□ Tablet

□ Other...



3. How often do you change your password? *

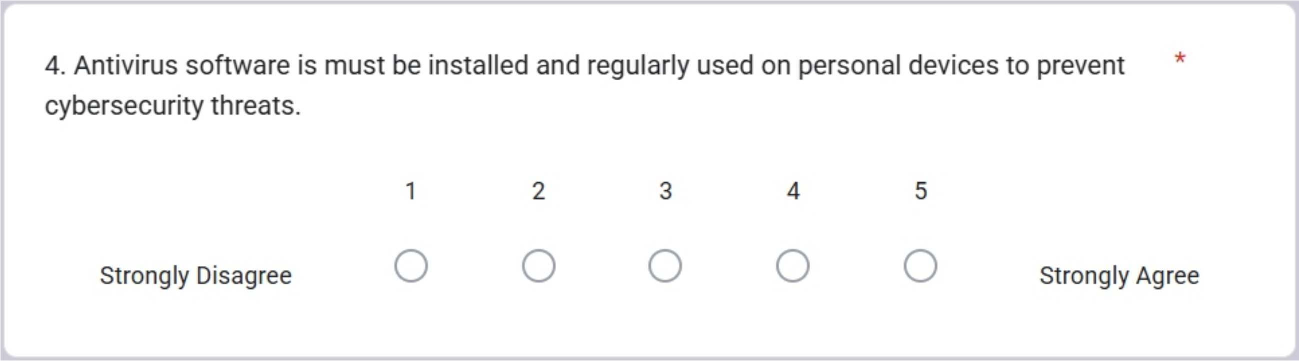
○ Every month

○ Every 3–6 months

○ Once a year

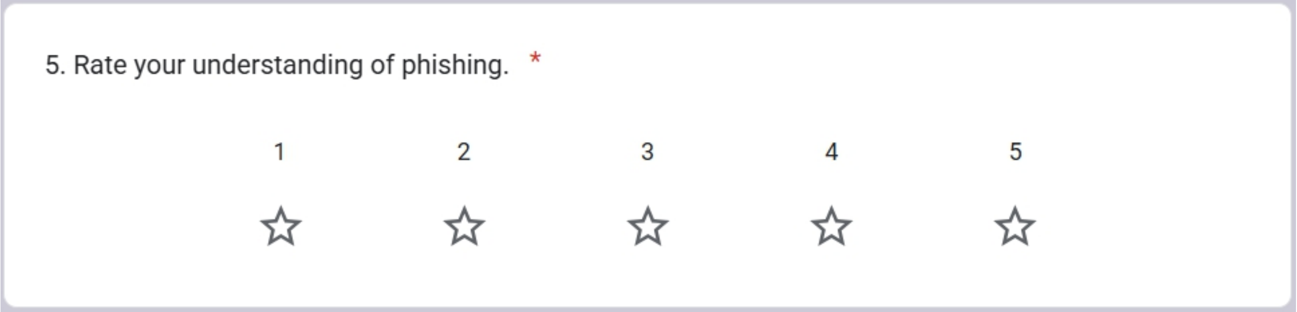
○ Only when I'm forced to (e.g. system requires it)

○ I rarely or never change my password



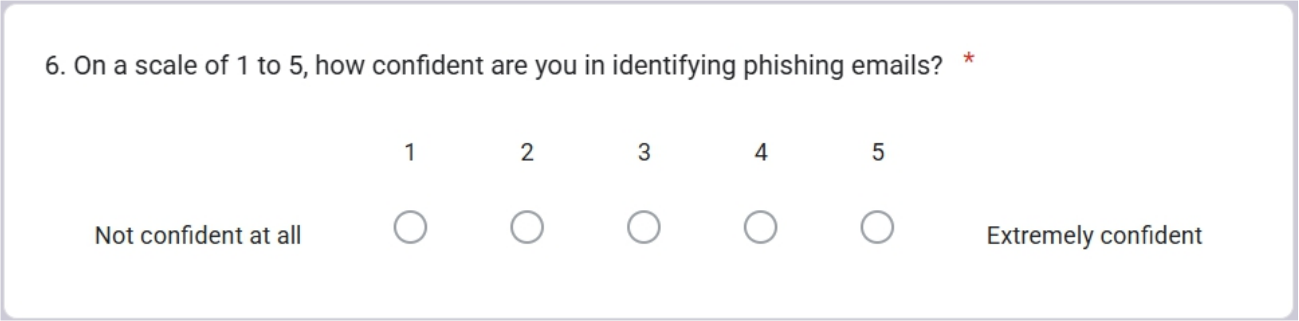
4. Antivirus software is must be installed and regularly used on personal devices to prevent cybersecurity threats. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



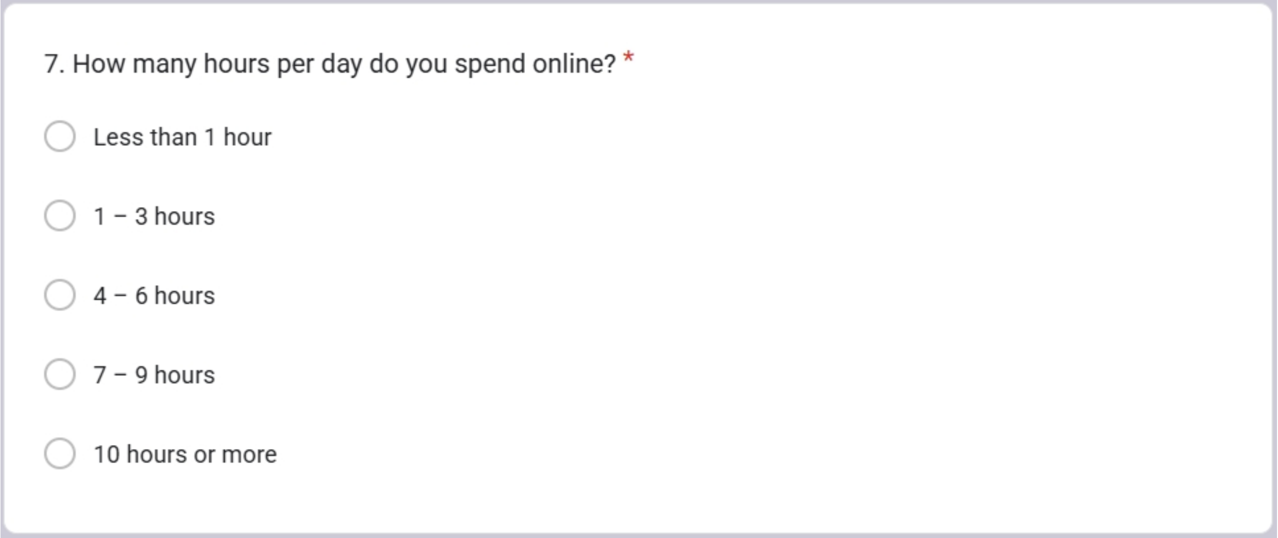
5. Rate your understanding of phishing. *

1	2	3	4	5
☆	☆	☆	☆	☆



6. On a scale of 1 to 5, how confident are you in identifying phishing emails? *

	1	2	3	4	5	
Not confident at all	○	○	○	○	○	Extremely confident



7. How many hours per day do you spend online? *

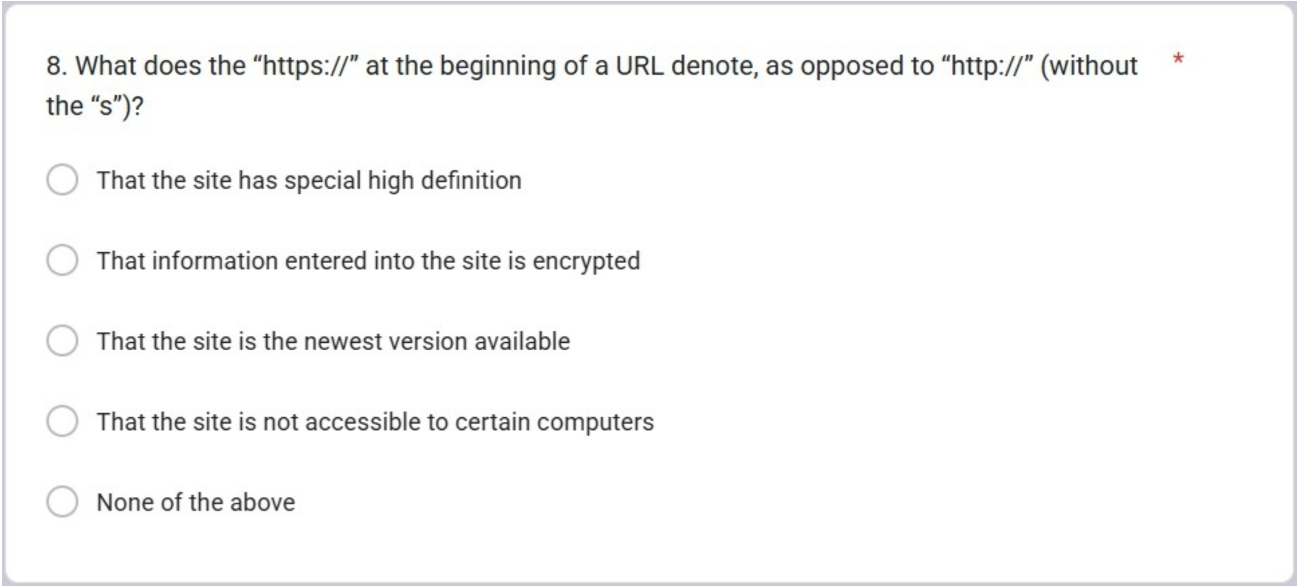
○ Less than 1 hour

○ 1 – 3 hours

○ 4 – 6 hours

○ 7 – 9 hours

○ 10 hours or more



8. What does the “https://” at the beginning of a URL denote, as opposed to “http://” (without the “s”)? *

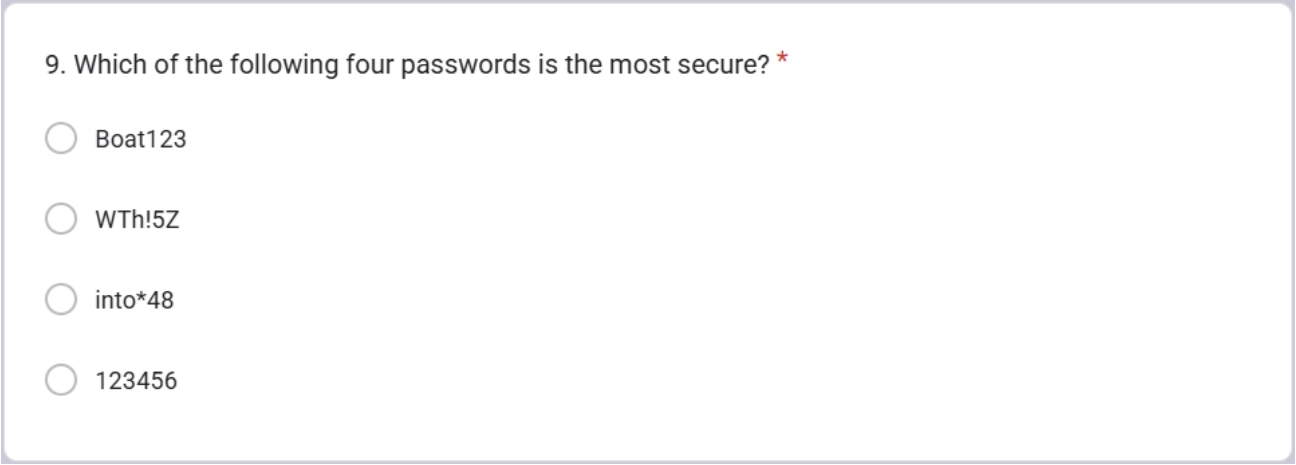
○ That the site has special high definition

○ That information entered into the site is encrypted

○ That the site is the newest version available

○ That the site is not accessible to certain computers

○ None of the above



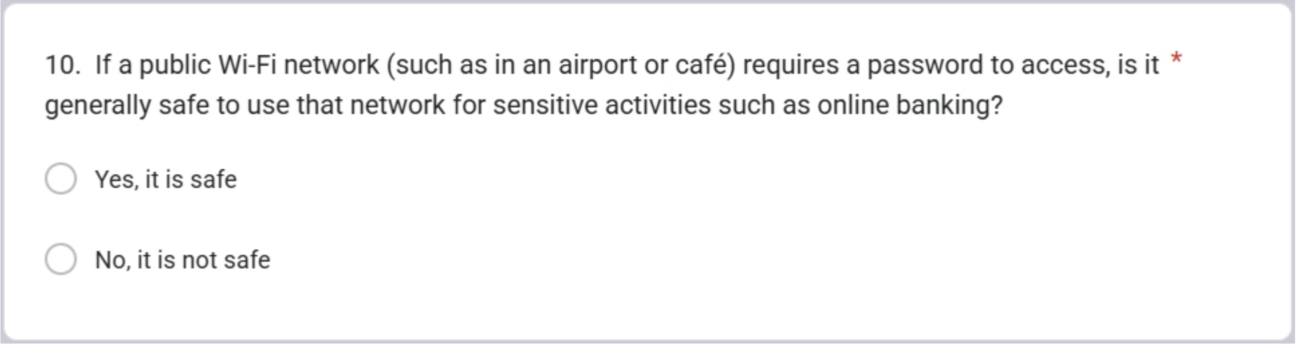
9. Which of the following four passwords is the most secure? *

○ Boat123

○ WTh!5Z

○ into*48

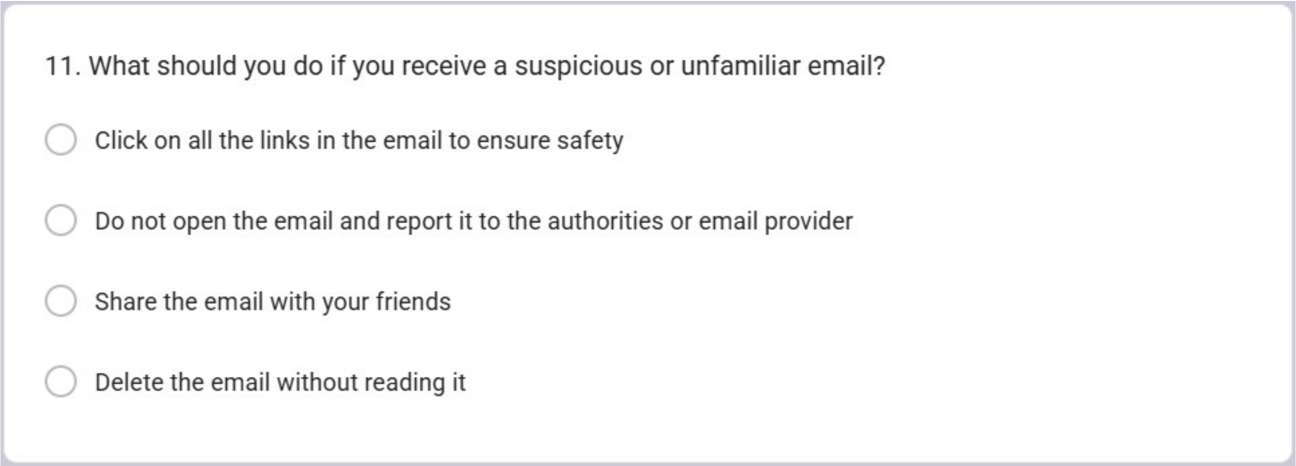
○ 123456



10. If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking? *

○ Yes, it is safe

○ No, it is not safe



11. What should you do if you receive a suspicious or unfamiliar email?

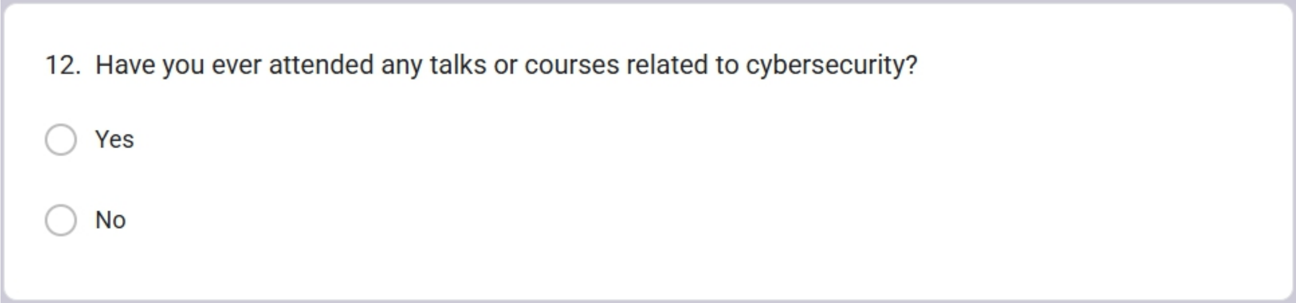
○ Click on all the links in the email to ensure safety

○ Do not open the email and report it to the authorities or email provider

○ Share the email with your friends

○ Delete the email without reading it

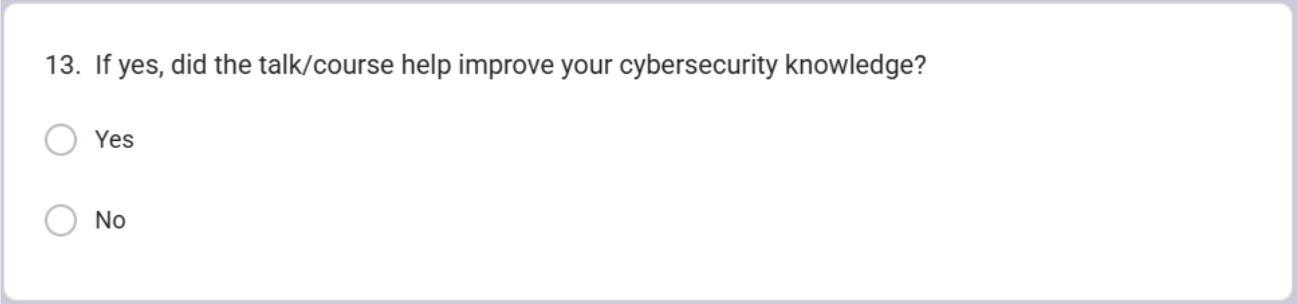
6.3 Section C: Awareness Training



12. Have you ever attended any talks or courses related to cybersecurity?

○ Yes

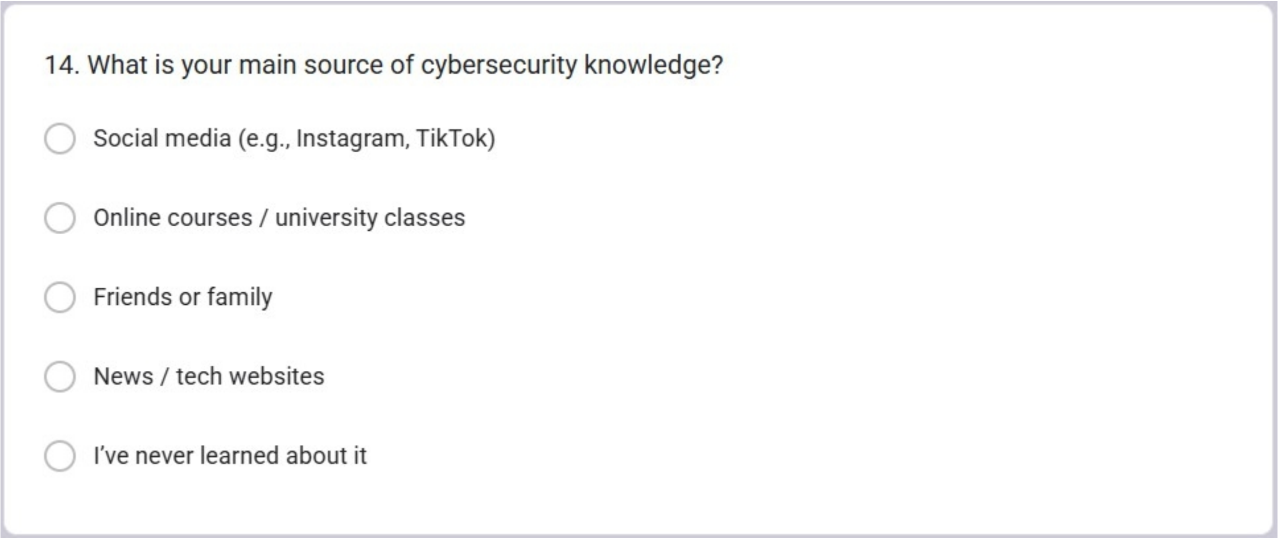
○ No



13. If yes, did the talk/course help improve your cybersecurity knowledge?

○ Yes

○ No



14. What is your main source of cybersecurity knowledge?

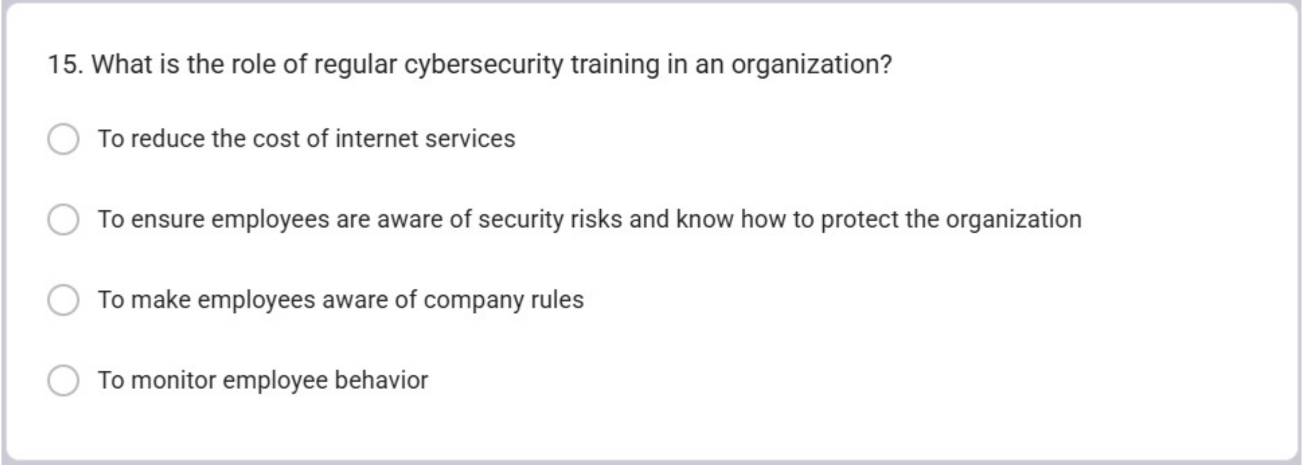
○ Social media (e.g., Instagram, TikTok)

○ Online courses / university classes

○ Friends or family

○ News / tech websites

○ I've never learned about it



15. What is the role of regular cybersecurity training in an organization?

○ To reduce the cost of internet services

○ To ensure employees are aware of security risks and know how to protect the organization

○ To make employees aware of company rules

○ To monitor employee behavior

6.4 Responses

https://docs.google.com/spreadsheets/d/e/2PACX-1vS7a7a7H2C9DagOEDzjgb5JckJ5fTbuVzmO3202Spb0JXT2_tkck3n0LLJr0oY-C0jg7K0Mvh6FThHU/pub?output=pdf

7.0 Reference

1. **Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://doi.org/10.3390/app12052589MDPI**

2. **Mittal, C. (2024). An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks. *International Journal of Scientific Research and Management, 12*(04), 1144–1158. https://doi.org/10.18535/ijsrm/v12i04.ec05ResearchGate**

3. **Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 223–228). IEEE. https://doi.org/10.1109/PST.2016.7906931ResearchGate**

4. **Cybersecurity & Infrastructure Security Agency. (2024, April 10). Cybersecurity awareness for internet users. *CISA*. https://www.cisa.gov/cybersecurity-awareness**

5. **Rahul Awati, Informa TechTarget. (2022, March 02). Definition Hypertext Transfer Protocol Secure (HTTPS). https://www.techtarget.com/searchsoftwarequality/definition/HTTPS**