CYBERSECURITY AWARENESS SURVEY

Mr.Shabzada Betab Badar

SHARON JINO
SHARAN V K
VISHAK V
PRANATHI CHOWDARY
PINKY RK

Table of content

Motivation

- Cyber Security threats are increasingly affecting individuals and organizations. withe the rise of online activities, cyber attacks like phishing, ransomware, and identity theft are becoming more frequent.

- The motivation behind this survey is to understand how aware individuals are about these syber threats and how prepared they are to handle them. as digital activity grows, the number of cyber attacks also increases, making it crucial for individuals to stay informed and proactive about their online security practices

Introduction

Objective:

Cybersecurity awareness involves understanding the risks associated with online activities and implementing protective measures to avoid cyber threats. This study aims to assess how familiar individuals are with common cybersecurity threats and the security measures they use to safeguard their personal information.

Scope:

Data from the participants aged 16-32 from diverse background. Focuses on both genders and varying levls of familiarity with cybersecurity practices.

Methadology

01

Survey Tool:
google forms
Respondents: the survey collected responses from 59 participants aging from 16-30 years old

02

Data Analyzed:
gender distribution
cyberseurity awareness
security practices
threat concerns

03

Tool for analysis:
microsoft excel for data processing and chart creation

Work flow

Survey creation

↓

Data collection

↓

Data cleaning and categorization

↓

Analysis and visualization

↓

Insights generation and report writing

Data organization

Data cateogories

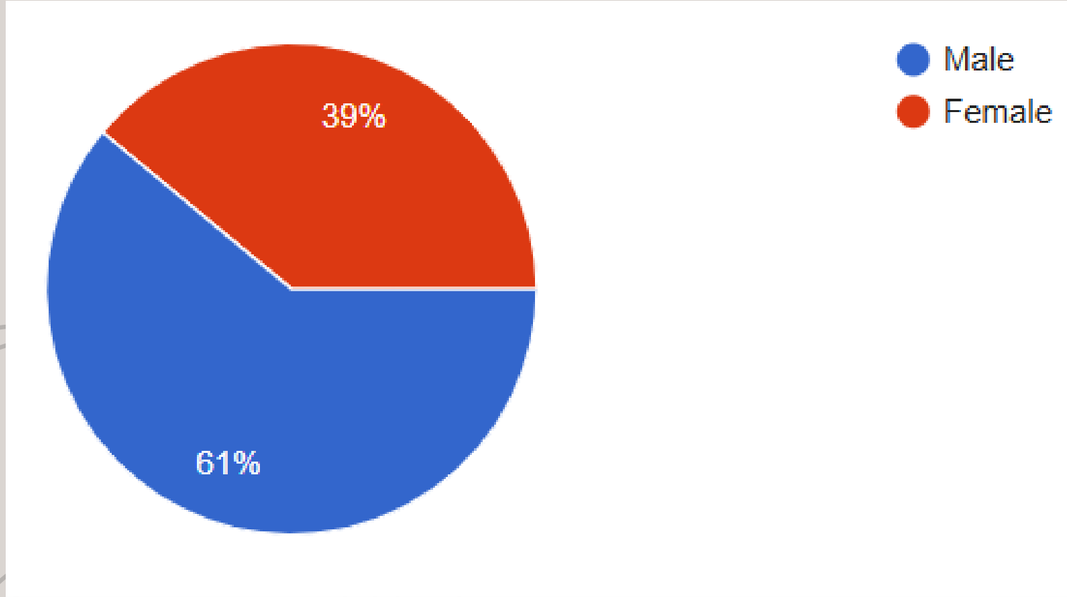
- Gender and Demographics: This section analyzes the gender distribution and demographic characteristics of the respondents, providing insights into the diversity of the survey participants.
- General Awareness: This section examines the general awareness levels of respondents regarding cybersecurity, highlighting their knowledge and understanding of key concepts.
- Password Management: This section investigates the password management practices of respondents, including the frequency of password changes and the use of strong passwords.

- Device Security: This section analyzes the security measures taken by respondents to protect their devices, such as the use of antivirus software and regular updates.
- Online Behaviour: This section studies the online behavior and practices of respondents, including their activities on social media and their approach to online shopping and banking.
- Awareness and Training: This section evaluates the awareness and training levels of respondents regarding cybersecurity, focusing on their ability to recognize phishing emails and their participation in cybersecurity training programs.

Analysis

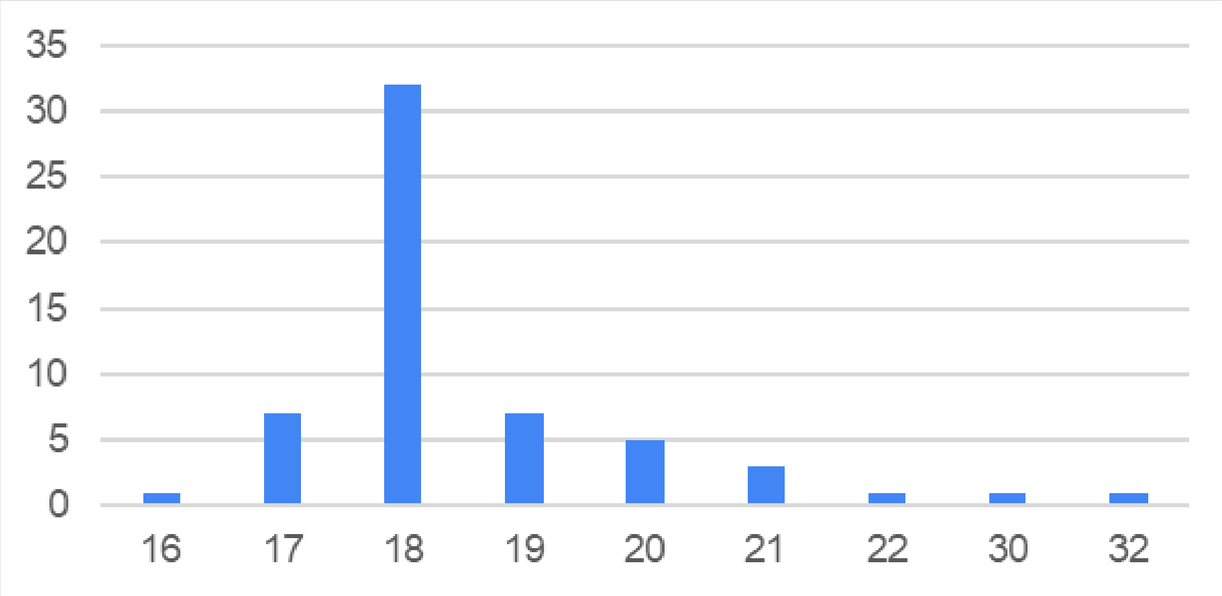
GENDER AND DEMOGRAPHICS

Gender Ratio



·Male respondants: 61% (35)
·Female respondants: 39% (23)
·Gender distribution is fairly balanced.

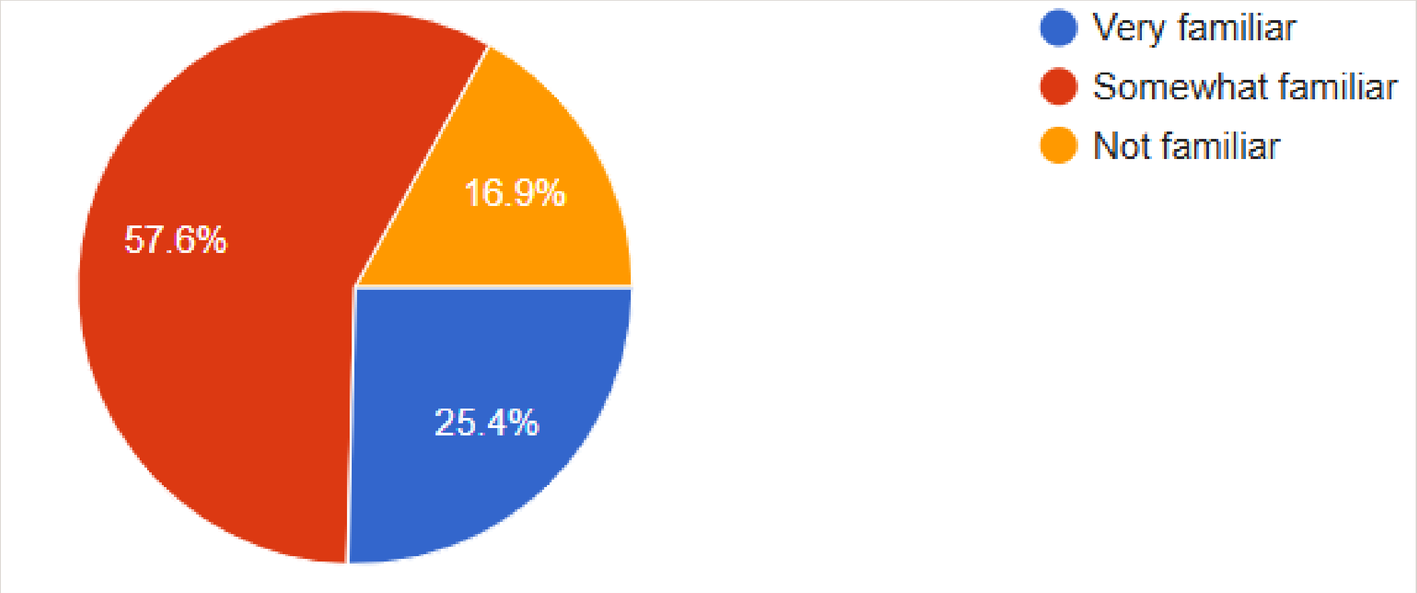
Age distribution:



·Most of the respondents are of the age 16-18.
·A few members are from the age group of 19–21
·A very few members are between the age 21-32

GENERAL AWARENESS

- How familiar are you with different types of cyber threats?

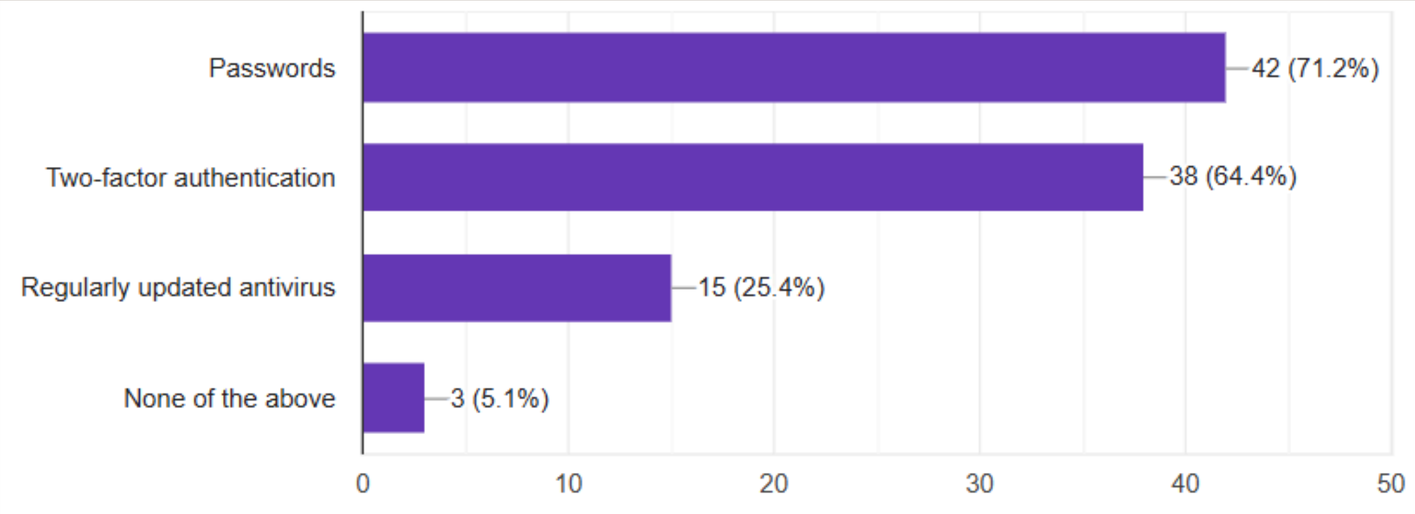


very familiar: 25.4%

Somewhat failiar: 57.6%

Not familiar: 16.9%

- Which of the following security measures do you use for your online accounts?



Passwords: 42(71.2)%

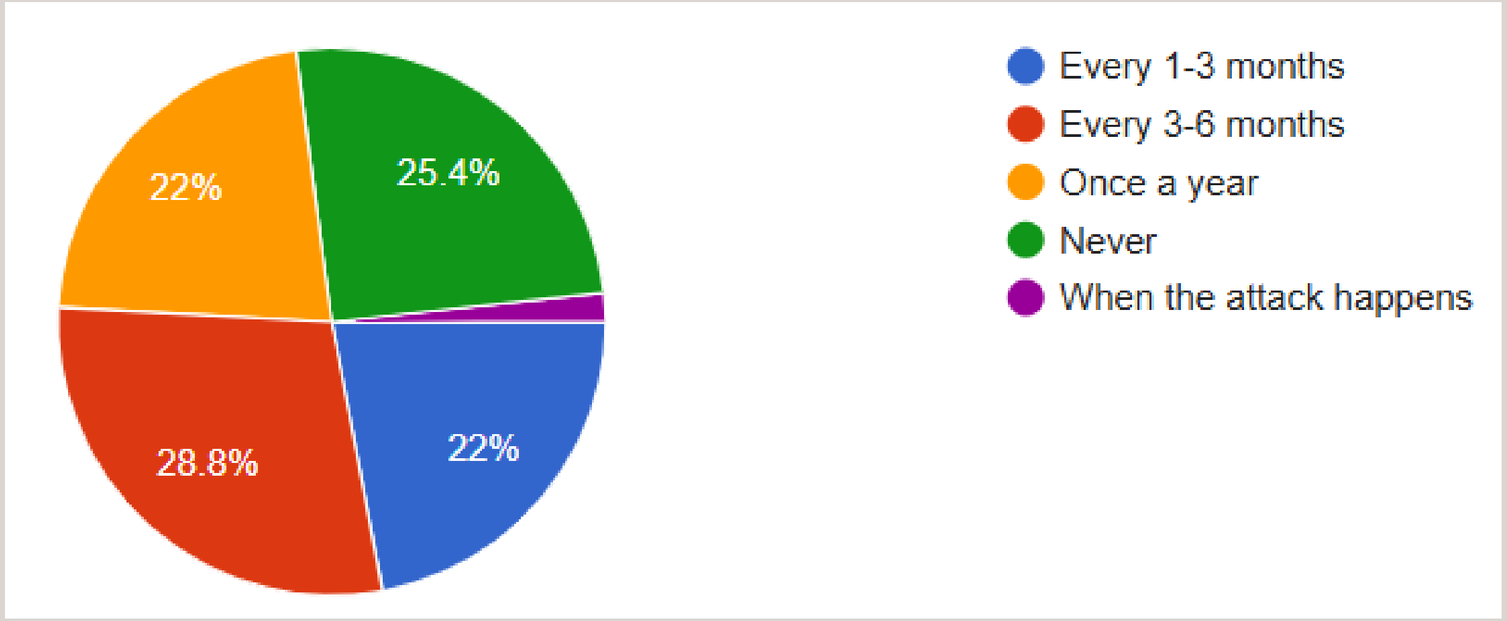
Two-factor authentication:38(64.4)%

Regularly updated anti-virus:15(25.4)%

None of the above:3(5.1)%

PASSWORD MANAGEMENT

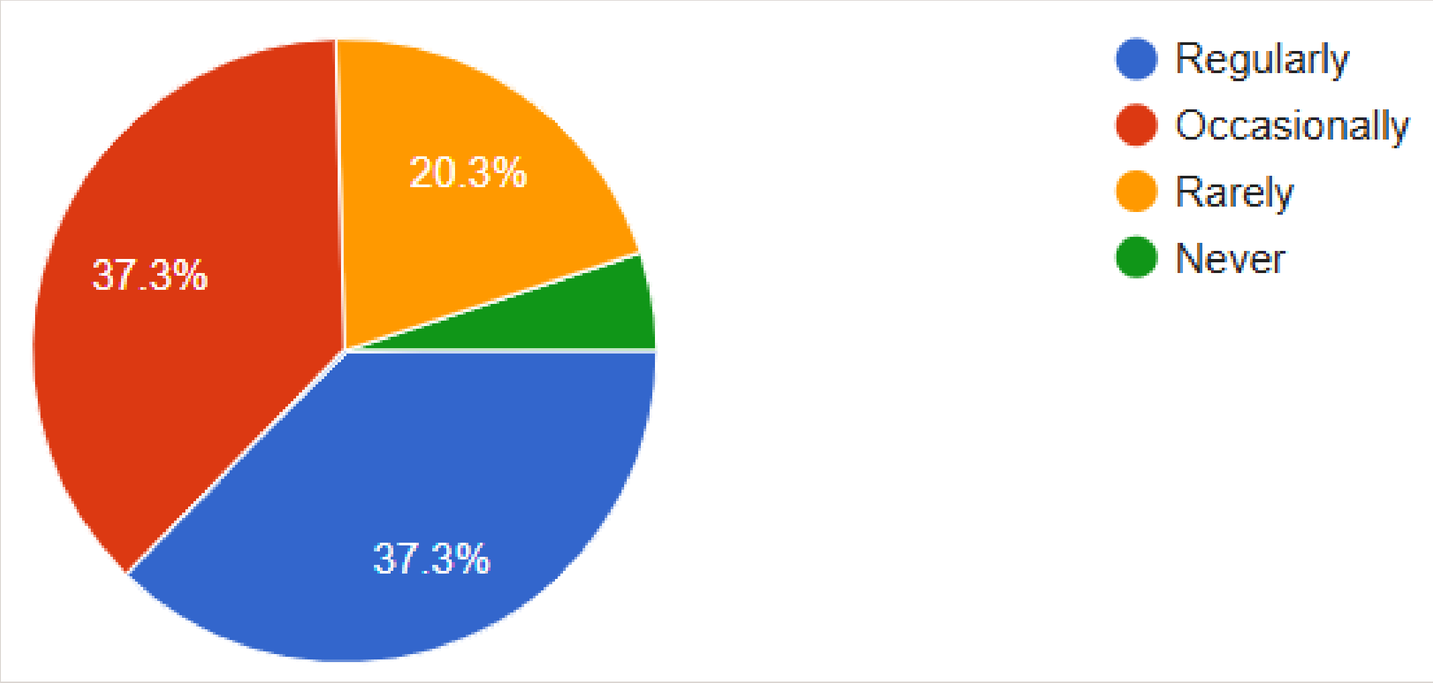
- How often do you change your passwords for online accounts?



- Every 1-3 months - 13
- Every 3-6 months- 16
- Never- 15
- Once a year- 13
- When the attack happens - 1

DEVICE SECURITY

- How often do you update your computers operating system and software appliaction?



Regularly: 37.3%

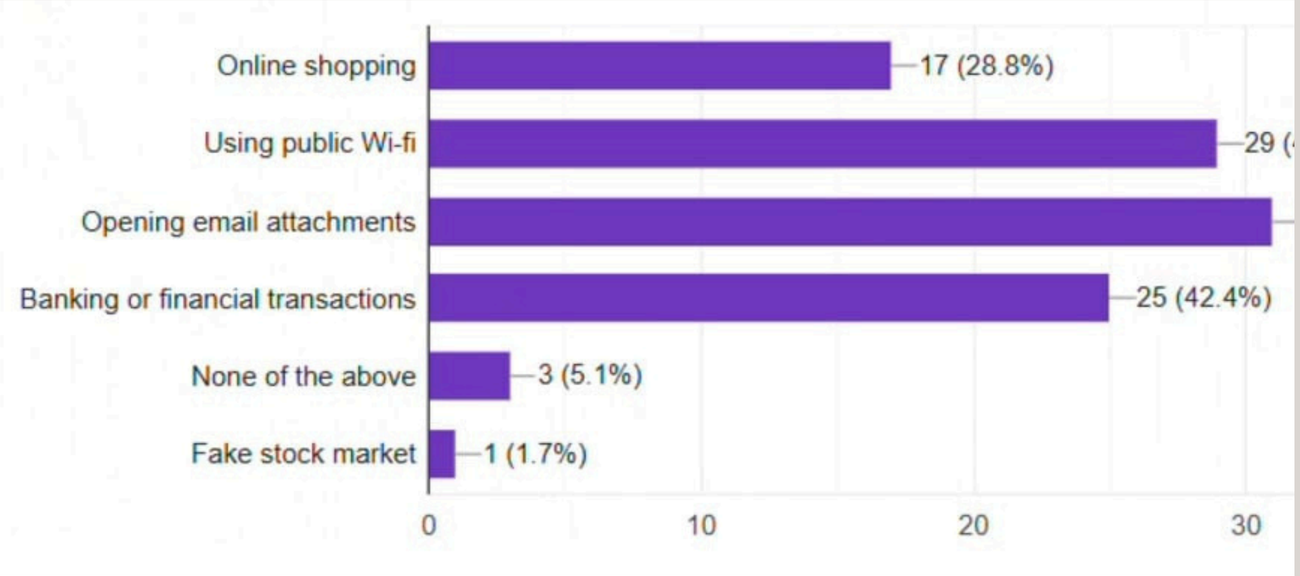
Occasionally: 37.3%

Rarely: 20.3%

Never: 5.1%

ONLINE BEHAVIOUR

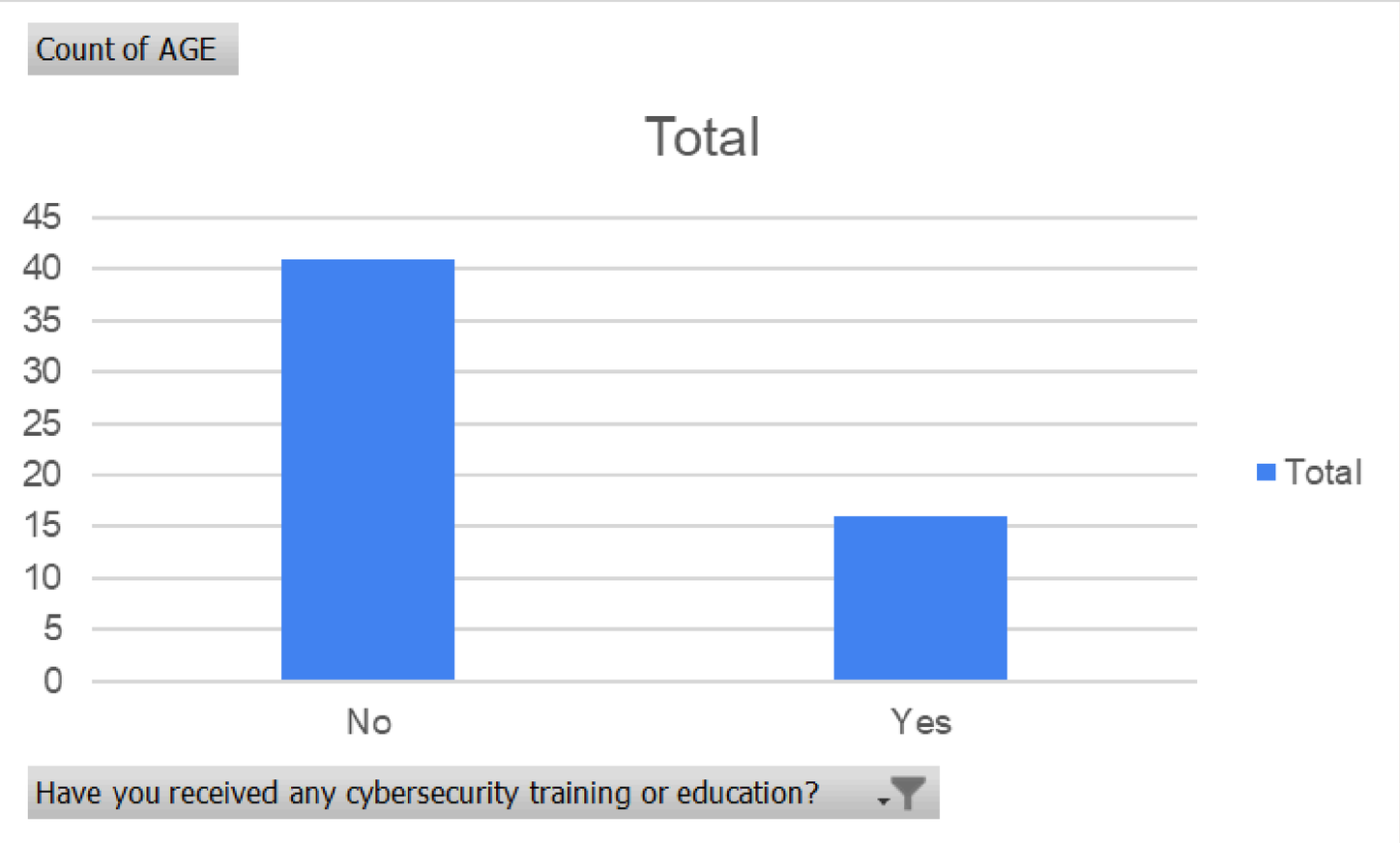
- Which of the following online activities do you consider to have the highest risk interms of cybersecurity?



- Opening email attachments: 52.5% (31).
- Using public Wi-Fi: 49.2% (29).
- Banking or financial transactions: 42.4% (25).
- Online shopping: 28.8% (17).
- None of the above: 5.1% (3)

AWARENESS AND AND TRAINING

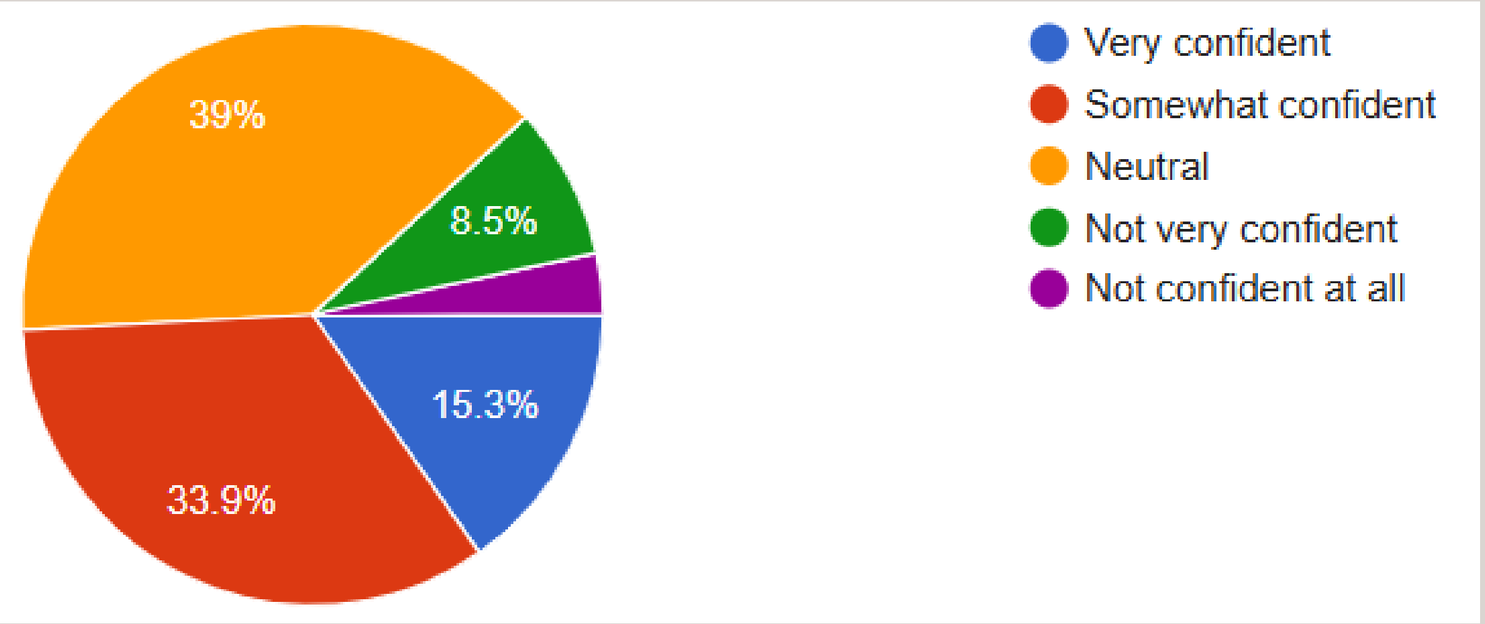
- Have you received any cybersecurity training or education?



No: Count: 41
Yes: Count: 16

- The data highlights significant gaps in cybersecurity awareness and practices among respondents, emphasizing the need for increased education and training.

- How confident are you in your ability to recognize phising emails?



Very confident: 15.3%

Somewhat confident: 33.9%

Neutral: 39%

Not very confident: 8.5%

Inference and key insights

- The cybersecurity awareness survey showed varying levels of familiarity with cyber threats and diverse cybersecurity practices among employees.
- Key findings include a significant awareness of common cyber threats, but a lack of confidence in recognizing phishing emails.
- Common practices include using two-factor authentication and regularly updating operating systems.
- Major concerns revolve around phishing attacks, malware, and identity theft. These insights highlight the need for ongoing cybersecurity education and training

Recommendations

- Increase Cybersecurity Training: Implement regular cybersecurity training programs to educate individuals on recognizing phishing emails, using strong passwords, and maintaining overall online security
- Promote Regular Updates: Encourage users to regularly update their operating systems, applications, and antivirus software to protect against the latest threats and vulnerabilities.
- Enhance Awareness Campaigns: Launch awareness campaigns to highlight the importance of avoiding password reuse, using secure networks, and being cautious with online activities such as shopping and banking.

Conclusion

- In conclusion, the survey highlights a gap between cybersecurity awareness and action.
- While many respondents are familiar with threats, critical measures like two-factor authentication and regular updates are underutilized.
- Addressing these gaps through education and better practices can significantly enhance online safety.

Thank You