****

**CYBERSECURITY AWARENESS**

**School of Computer Science and Information Technology**

**Department of Computer Science and Information Technology**

**Semester: I**

**Specialisation: COMMON**

**SHARAN VK**

Advisor: **Mr. Sahabzada Betab Badar**

Department of Computer Science and Information Technology

Jain (Deemed-to-be) University

This report is submitted for the degree of

***Bachelor of Computer Application***

Jain University, Bengaluru November 2024

**DECLARATION**

I hereby declare that except where specific reference is made to the work of others, the contents of this report are original and have not been submitted in whole or in part for consideration for any other degree or qualification or course in this or any other university. This report is the collective work of myself and my team and contains nothing that is the outcome of work done in collaboration with others except my team members as specified in the text and Acknowledgements.

SHARAN VK

USN no: JUUG24BCA44993

Department of Computer Science and Information Technology, Jain (Deemed-to-be) University, Bengaluru

**ACKNOWLEDGEMENT**

I acknowledge Prof. Ferdous Sahabzada Betab Badar’s invaluable guidance and support throughout this project. My gratitude for their mentorship extends to all the Department of Computer Science and Information technology faculty at the Jain (Deemed-to-be) University, Bangalore. I would like to extend my heartfelt thanks to all my friends who took the time to respond to the survey. Your valuable input and support are greatly appreciated and have significantly contributed to the success of this project. My appreciation goes out to my parents and family members for their unwavering encouragement and support throughout all my assignment.

**ABSTRACT**

This report presents the findings of a comprehensive survey conducted to assess cybersecurity awareness among individuals. The primary objective of the survey was to evaluate the current level of understanding and practices related to cybersecurity, identify common threats, and highlight areas requiring improvement.

The survey methodology involved distributing questionnaires to a diverse group of participants. The questions covered topics such as password management, phishing awareness, data protection, and incident response.

The results indicate a moderate level of cybersecurity awareness, with significant variations across different demographics. While most participants demonstrated a basic understanding of cybersecurity principles, there were notable gaps in advanced knowledge and practical application. Common threats identified include identity theft, phishing attacks and malware infections.

The report concludes with recommendations for enhancing cybersecurity awareness through targeted training programs, regular updates on emerging threats, and the implementation of robust security policies. By addressing these areas, organizations can better protect their digital assets and reduce the risk of cyber incidents.

**TABLE OF CONTENTS**

List of figures……………………………………………………………………………vi

List of tables………………………………………………………………………...…. vii

1.Introduction

1.1 Objective…………………………………………………………………....1

1.2 Organization……………………………………………………………….2

1.3 Contribution………………………………………………………..............3

2. Data description

2.1 Data description……………………………………………………….…...4

2.2 Technical description…………………………………………………….10

2.3 Work flow diagram………………………………………………………14

3. Data analysis

3.1 Gender and demographics ………………………………………….….15

3.2 General awareness……………………………………………………….16

3.3 Password management……………………………………………….….20

3.4 Device security……………………………………………………………22

3.5 Online behaviour ………………………………………………………...24

3.6 Awareness and training …………………………………………………26

4. Key insights

4.1 Key insights of Gender and demographics ……………………….….28

4.2 Key insights of General awareness ……………………………………29

4.3 Key insights of Password management ………………………………30

4.4 Key insights of Device security …………………………………….….31

4.5 Key insights of Online behaviour ………………………………….….32

4.6 Key insights of Awareness and training………………………………33

Conclusion ……………………………………………………………………….34

References………………………………………………………………………..35

LIST OF FIGURES

FIGURE 2.1: Workflow diagram……………………………………………………...14

FIGURE 3.1: Bar chart– Gender ratio………………………………………………...15

FIGURE 3.2: Bar graph - Age distribution…………………………………………...15

FIGURE 3.3: Clustered graph – Counts of cyber threat familiarity……………….16

FIGURE 3.4: Conditional formatting in excel sheet………………………………...17

FIGURE 3.5: Pie chart – Security measures used for online accounts…………….18

FIGURE 3.6: Pivot chart- Same password usage & frequency of password changing………………………………………………………………………………...20

FIGURE 3.7: Pivot chart – Frequency of updating OS and installation of antiviruses………………………………………………………………………………22

FIGURE 3.8: Pivot chart – Review online accounts activity and regularity to check security and privacy settings………………………………………………………….24

FIGURE 3.9: Pie chart– Confidence in recognizing phishing emails……………...26

LIST OF TABLES

TABLE 3.1: Counts of cyber threat familiarity……………………………….….…16

TABLE 3.2: Security measures used for online accounts………………………….18

TABLE 3.3: Same password usage & frequency f password changing………………………………………………………………………………...21

TABLE 3.4: Frequency of updating OS and installation of antivirus…………....22

TABLE 3.5: Review online account activity and regularity to check security and privacy settings………………………………………………………………………....24

TABLE 3.6: Confidence in recognizing phishing emails………………………….26

**CHAPTER 1**

**INTRODUCTION**

* 1. Objectives

The Cybersecurity Awareness Survey aims to get a clear picture of how well people understand cybersecurity. It looks into what people know about threats like phishing and malware, and how they feel about the importance of protecting data. The survey also checks how often and how well people follow good cybersecurity practices, such as updating software, using strong passwords, and spotting suspicious activity. By finding out where people might lack knowledge or follow unsafe practices, the survey helps pinpoint areas that need more education and training. The ultimate goal is to boost everyone’s overall cybersecurity habits, making both individuals and organizations more secure against potential threats.

* 1. ORGANIZATION

The document is organized into several sections, each focusing on different aspects of the study. The **Introduction** section outlines the main goals and objectives of the study, describes the structure and organization of the document, and highlights the contributions and significance of the study.

The **Data Description** section provides a detailed description of the data used in the study, explains the technical aspects and methodologies used for data collection and analysis, and presents a visual representation of the workflow and processes involved in the study.

The **Data Analysis** section analyses various aspects of the data, including gender distribution and demographic characteristics of the respondents, general awareness levels, password management practices, security measures taken to protect devices, online behaviour and practices, and awareness and training levels regarding cybersecurity.

The **Key Insights** section summarizes the key findings from the data analysis, highlighting the main insights related to gender and demographics, general awareness, password management, device security, online behaviour, and awareness and training.

Finally, the **Conclusion** section provides a summary of the study's findings and their implications, and the **References** section lists the sources and references used in the study.

* 1. Contribution

Cybersecurity Awareness: Protecting Yourself in the Digital Age

Introduction

In today's digital age, cybersecurity awareness is more critical than ever. With the increasing number of cyber threats and data breaches, it's essential to educate individuals and organizations on how to protect themselves online. According to recent reports, cyber attacks have increased by 30% over the past year, affecting millions of users worldwide. This article aims to provide valuable insights and practical tips on enhancing cybersecurity awareness.

Common Cyber Threats

- Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.

- Malware: Malicious software designed to damage or gain unauthorized access to systems.

- Ransomware: A type of malware that locks users out of their systems until a ransom is paid.

Best Practices

-Use Strong Passwords: Create complex passwords and change them regularly.

-Enable Two-Factor Authentication: Add an extra layer of security to your accounts.

-Regular Software Updates: Keep your systems and software up to date to protect against vulnerabilities.

Practical Tips

-Stay Informed: Follow reputable cybersecurity blogs and news sources to stay updated on the latest threats and trends.

-Educate Others: Share your knowledge with friends, family, and colleagues to help them understand the importance of cybersecurity. Simple actions like explaining how to recognize phishing emails can make a big difference.

**CHAPTER 2**

**DATA ORGANIZATION**

* 1. Data description

2.1.1. Demographics:

1. **Name**: Open-ended input capturing the respondent's name.
2. **Gender**: Categorical variable with options (Male and female).
3. **Age**: Open-ended input capturing the respondent's age

**NOTE**: All questions are mandatory.

2.1.2. General Awareness:

1. **Familiarity with Different Types of Cyber Threats**:

* **Description**: Measures the respondent's awareness of various cyber threats.
* **Data Type**: Categorical
* **Format:** Options include "Very Familiar", "Somewhat Familiar", "Not Familiar"

1. **Victim to a Cyber Attack or Online Scam**:

* **Description**: Captures whether the respondent has ever been a victim of a cyber-attack or online scam.
* **Data Type**: Categorical
* **Format:** Options include "Yes", "No"

1. **Security Measures Used for Online Accounts**:

* **Description**: Identifies the security measures the respondent uses for their online accounts.
* **Data Type**: Categorical (Multiple Selection)
* **Format:** Options include "Strong Passwords", "Two-Factor Authentication", "Regularly Updated Antivirus", "Avoiding Suspicious Emails/Links", "None of the Above"

### Password Management:

1. **Frequency of Changing Passwords**:

* **Description**: Measures how often the respondent changes their passwords for online accounts.
* **Data Type**: Categorical
* **Format:** Options include "Every 1-3 months", "Every 3-6 months", "Once a year", "Rarely", "Never"

1. **Use of Same Password for Multiple Accounts:**

* **Description**: Captures whether the respondent uses the same password for multiple online accounts.
* **Data Type**: Categorical
* **Format**: Options include "Yes", "No"

1. **Password Storage Methods**:

* **Description**: Identifies how the respondent stores their passwords.
* **Data Type**: Categorical (Multiple Selection)
* **Format**: Options include "Password Manager", "Written Down", "Memorized", "Saved in Browser", "Other (please specify)"

2.1.4 Device Security:

1. Devices Used to Access the Internet:

* Description: Identifies the types of devices the respondent uses to access the internet.
* Data Type: Categorical (Multiple Selection)
* Format: Options include "Desktop Computer", "Laptop", "Smartphone", "Tablet", "Smart TV", "Other (please specify)"

1. Antivirus and Anti-Malware Software:

* Description: Captures whether the respondent has reliable antivirus and anti-malware software installed on their devices.
* DataType: Categorical
* Format: Options include "Yes", "No"

1. Frequency of Updating Operating System and Software:

* Description: Measures how often the respondent updates their computer's operating system and software applications.
* DataType: Categorical
* Format**:** Options include "Regularly", "Occasionally", "Rarely", "Never**"**

2**.**1.5 Online Behaviour:

1. Online Activities with Highest Cybersecurity Risk:

* Description: Identifies which online activities the respondent considers to have the highest risk in terms of cybersecurity.
* Data Type: Categorical (Multiple Selection)
* Format: Options include "Online Shopping", "Using Public Wi-Fi", "Opening Email Attachments", "Social Media Usage", "Banking or Financial Transactions", "None of the Above"

1. Regularly Checking Security and Privacy Settings of Social Media Accounts:

* Description: Captures whether the respondent regularly checks the security and privacy settings of their social media accounts.
* Data Type: Categorical
* Format: Options include "Yes", "No"

1. Frequency of Reviewing Online Account Activity:

* Description: Measures how often the respondent reviews their online account activity for any unauthorized access or suspicious transactions.
* Data Type: Categorical
* Format: Options include "Daily", "Weekly", "Monthly", "Rarely", "Never"
  + 1. Awareness and Training:

1. Received Cybersecurity Training or Education:

* Description: Indicates whether the respondent has received any formal training or education related to cybersecurity.
* Data Type: Categorical
* Format: Options include "Yes", "No"

1. Confidence in Recognizing Phishing Emails:

* Description: Measures the respondent's confidence in their ability to recognize phishing emails.
* Data Type: Categorical
* Format: Options include "Very Confident", "Somewhat Confident", "Neutral", "Not Very Confident", "Not Confident at All"

1. Types of Cyber Threats of Most Concern:

* Description: Identifies which types of cyber threats concern the respondent the most.
* Data Type: Categorical (Multiple Selection)
* Format: Options include "Malware", "Phishing Attacks", "Identity Theft", "Ransomware", "Data Breaches", "None of the Above"
  1. Technical description
     1. Data collection methodology
* Survey Platform:

The data was collected using Google Forms, a user-friendly online platform for creating structured questionnaires with a variety of response formats (e.g., multiple-choice, Likert scale, and open-ended).

* Question Design:
  + The survey contained 18 questions designed to capture demographic information, general awareness, password management, device security, online behaviour and awareness and training.
  + Responses were designed to generate both categorical data (e.g., gender, familiarity of cyber threats) and ordinal data (e.g., Likert-scale questions measuring confidence).
* Target Audience:
  + The survey targeted students, aiming to uncover patterns in cybersecurity awareness and to understand any training received

### 2.2.2 Data Processing Tools

* Platform for Analysis:

The data collected via Google Forms was exported to **Microsoft Excel** for organization, cleaning, and analysis.

* Data Cleaning and Preparation:
  + 59 rows of data were reviewed to identify and remove incomplete or invalid responses.
  + Data was organized into structured tables, where each row represents a respondent, and each column represents a survey question

2.2.3 Data Analysis Techniques

Statistical Tools Used**:** Various functionalities in Microsoft Excel were leveraged, including:

1. **Formulas:** For aggregation and computation, such as calculating response frequencies, percentages, and averages.

* COUNTIF: The COUNTIF function in Excel is used to count the number of cells that meet a specific condition within a range. It is particularly useful for data analysis when you need to count occurrences of a particular value or condition.

SYNTAX: COUNTIF(range, criteria)

=COUNTIFS(F2:F59,"No")

The number of respondents to ‘No’ are 51.

=COUNTIFS(F2:F59,"Yes")

The number of respondents to ‘Yes’ are 6.

1. **Conditional Formatting:** Conditional formatting is a feature in Excel that allows you to apply specific formatting to cells that meet certain criteria. This helps to highlight important information, identify trends, and make data analysis more intuitive.
2. **Charts & graphs:**
3. Bar Chart:

* **Description**: A bar chart displays data using rectangular bars with lengths proportional to the values they represent. It is useful for comparing different categories or groups.
* **Example**: Comparing the number of respondents using different security measures for online accounts.

1. Clustered Bar Chart:

* **Description**: A clustered bar chart groups multiple bars together to show comparisons between different categories and subcategories. It is useful for comparing multiple variables within each category.
* **Example**: Comparing the frequency of updating computer's OS and applications across different groups with and without reliable antivirus software.

1. Pie Chart:

* **Description**: A pie chart displays data as slices of a circle, with each slice representing a proportion of the whole. It is useful for showing the relative proportions of different categories.
* **Example**: Showing the distribution of respondents' confidence levels in recognizing phishing emails.

### 2.2.4 Pivot Table and Pivot Chart in Data Analysis

**Pivot Table**: A pivot table is a powerful tool in Excel that allows you to summarize, analyse, and explore large datasets. It enables you to reorganize and group data dynamically, making it easier to identify patterns and trends. By dragging and dropping fields into different areas (Rows, Columns, Values, and Filters), you can create customized views of your data. Pivot tables are particularly useful for performing calculations, such as sums, averages, and counts, and for generating quick insights from complex datasets.

**Pivot Chart**: A pivot chart is a graphical representation of the data in a pivot table. It provides a visual way to analyse and present data, making it easier to understand and communicate insights. Pivot charts are dynamic and update automatically when the underlying pivot table data changes. They support various chart types, including bar charts, line charts, pie charts, and more. Pivot charts are useful for visualizing trends, comparisons, and distributions, and they enhance the overall data analysis experience by providing an intuitive and interactive way to explore data.

2.4 Flowchart

The workflow diagram presented in this report illustrates the step-by-step process followed in the collection, analysis, and interpretation of survey data. It provides a visual representation of the sequence of tasks, tools, and methods used from the initial survey creation to the final reporting of findings.

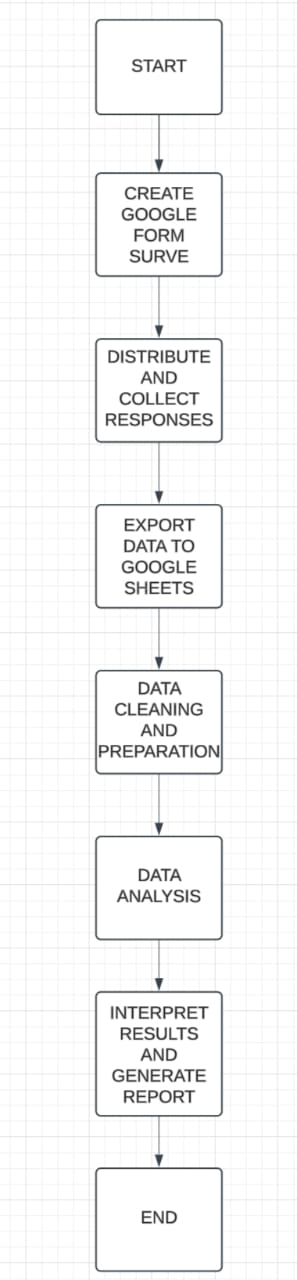
****

FIGURE 2.1: WORKFLOW DIAGRAM

**CHAPTER 3**

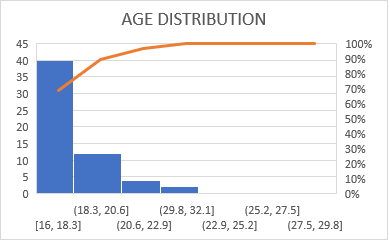
DATA ANALYSIS

* 1. Gender and demographics

1. Gender ratio:

* Male respondants:35
* Female respondants:23
* Gender distribution is fairly balanced.

FIGURE 3.1 : BAR CHART – GENDER RATIO

1. Age ratio:

* Most of the respondents are between 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

FIGURE 3.2: BAR GRAPH- AGE DISTRIBUTION

3.2 GENERAL AWARENESS

3.2.1 Exploring general awareness of cyber threats among individuals.

This section analyses the familiarity of individuals with the cyber threats. A clustered bar chart is used for the purpose. This chart is used when the category text is long.

FIGURE 3.3: CLUSTURED GRAPH COMPARING COUNTS OF CYBER THREAT FAMILIARITY

The clustered bar chart represents the respondents' familiarity with different types of cyber threats. The chart includes three categories: "Not familiar," "Somewhat familiar," and "Very familiar." Each bar's length corresponds to the number of respondents in each category.

|  |  |
| --- | --- |
| Familiarity with types of cyber threats? | Count |
| Not familiar | 10 |
| Somewhat familiar | 34 |
| Very familiar | 14 |
| Grand Total | 58 |

TABLE 3.1: COUNT OF FAMILIARITY OF CYBER THREAT AMONG INDIVIDUALS

* **Not familiar**: This category has the shortest bar, indicating that 10 respondents are not familiar with cyber threats.
* **Somewhat familiar**: This category has the longest bar, showing that 34 respondents have a moderate level of familiarity with cyber threats.
* **Very familiar**: This category has a medium-length bar, representing 14 respondents who are very familiar with cyber threats.

3.2.2 Exploring the number of individuals faced cyber attack

In this section, we have examined the number of individuals who have faced cyber threats or online scams.

To highlight the individuals who have fallen victim to cyber-attack, conditional formatting is used to highlight cells that contain the text “Yes”. Using Conditional Formatting one can easily spot trends and patterns in their data using bars, colours, and icons to visually highlight important values.

Using COUNTIF function one can count the number of cells within a range that meet the given condition.

SYNTAX: COUNTIF(range, criteria)

=COUNTIFS(F2:F59,"No")

* The number of respondents to ‘No’ are 51.

=COUNTIFS(F2:F59,"Yes")

* The number of respondents to ‘Yes’ are 6.

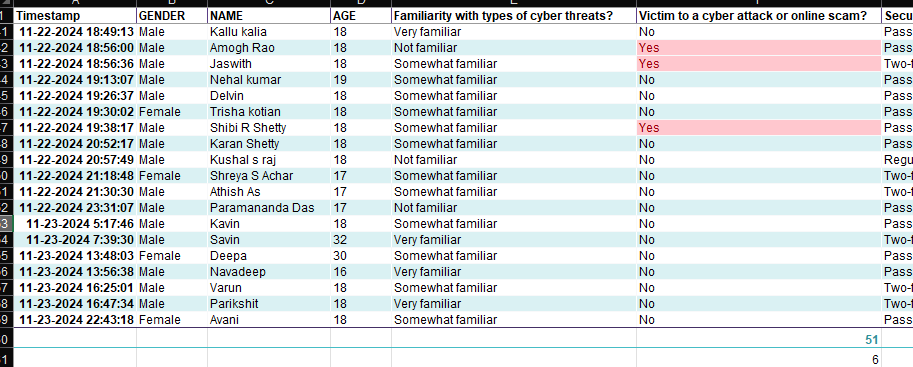


FIGURE 3.4: CONDITIONAL FORMATTING IN EXCEL SHEET

3.2.3 Exploring the security measures used for online accounts

This part of the survey is helpful in understanding the different ways by which individuals secure their online accounts.

FIGURE 3.5: PIE CHART – SECURITY MEASURES USED FOR ONLINE ACCOUNTS

|  |  |  |
| --- | --- | --- |
| Security measures used for online accounts | Count of AGE | PERCENTAGE |
| None of the above | 3 | 5% |
| Passwords | 15 | 26% |
| Passwords, regularly updated antivirus | 1 | 2% |
| Passwords, Two-factor authentication | 14 | 24% |
| Passwords, Two-factor authentication, regularly updated antivirus | 11 | 19% |
| Regularly updated antivirus | 2 | 3% |
| Two-factor authentication | 12 | 21% |
| Grand Total | 58 | 100% |

TABLE 3.2: SECURITY MEASURES USED FOR ONLINE ACCOUNTS

Each slice of the pie corresponds to the percentage of respondents using each security measure.

* The largest segment (26%) of respondents use passwords as their primary security measure.
* A significant portion (24%) of respondents use both passwords and two-factor authentication, indicating a higher level of security awareness.
* Additionally, 19% of respondents use a combination of passwords, two-factor authentication, and regularly updated antivirus, showing a comprehensive approach to security.
* Furthermore, 21% of respondents use two-factor authentication, highlighting its importance in securing online accounts.
* A small percentage (5%) of respondents do not use any of the listed security measures, indicating a potential area for improvement in cybersecurity practices.
* Smaller segments include respondents using "Passwords, regularly updated antivirus" (2%) and "Regularly updated antivirus" (3%).
  1. PASSWORD MANAGEMENT

3.3.1 Exploring the frequency of changing the password for online accounts and usage of same password for multiple accounts

In this section it is discussed about the count of frequency of changing the passwords. The analysis is categorized in 5 groups (“Every 1-3 months”, “Every 3-6 months”, “Never”, “once a year” & “When the attack happens”). It is also analysed the count of individuals who use the same password for multiple accounts under 2 categories (‘yes’ & ’no’).

FIGURE 3.6: PIVOT CHART- SAME PASSWORD USAGE AND FREQUENCY OF PASSWORD CHANGING

|  |  |  |
| --- | --- | --- |
| Same password usage for multiple accounts? | Frequency of changing password | Count of AGE |
| No |  | 44 |
|  | Every 1-3 months | 10 |
|  | Every 3-6 months | 14 |
|  |  |  |
|  | Never | 10 |
|  | Once a year | 10 |
| Yes |  | 14 |
|  | Every 1-3 months | 3 |
|  | Every 3-6 months | 2 |
|  | Never | 5 |
|  | Once a year | 3 |
|  | When the attack happens | 1 |
| Grand Total |  | 58 |

TABLE 3.3: SAME PASSWORD USAGE AND FREQUENCY OF PASSWORD CHANGING

* 44 respondents (about 76%) do not use the same password for multiple accounts.
* 14 respondents (about 24%) use the same password for multiple accounts.
* Among those who don’t use the same password for multiple accounts:
  + Most change their password every 3-6 months (14 respondents).
  + 10 respondents never change their passwords, which could be a security concern.
* Among those who use the same password for multiple accounts:
  + 5 respondents never change their passwords.
  + 1 respondent only changes their password when an attack happens.

3.4 DEVICE SECURITY

3.4.1 Exploring the reliability of antivirus and anti-malware software installed on devices and frequency of updating computer's OS & applications?

FIGURE 3.7: PIVOT CHART – FREQUENY OF UPDATING OS AND INSTALLATION OF ANTIVIRUS

|  |  |  |
| --- | --- | --- |
| Frequency of updating computer's OS & applications | Reliable antivirus and anti-malware software installed on your devices | Count of AGE |
| Never |  | 3 |
|  | No | 3 |
| Occasionally |  | 22 |
|  | I don't know | 1 |
|  | No | 9 |
|  | Yes | 12 |
| Rarely |  | 12 |
|  | No | 9 |
|  | Yes | 3 |
| Regularly |  | 21 |
|  | No | 5 |
|  | Yes | 16 |
| Grand Total |  | 58 |

TABLE 3.4: FREQUENY OF UPDATING OS AND INSTALLATION OF ANTIVIRUS

Frequency of Updates and Antivirus Usage:

* Regular Updates: Majority (16) of users with antivirus/anti-malware installed update their OS and applications regularly. Only 5 users do not install such software but still update regularly.
* Occasional Updates: A significant number (12) occasionally update their systems and also have antivirus installed. 9 users do not have antivirus yet occasionally update.
* Rarely Update: Few users (3) with antivirus software rarely update their systems, while 9 without antivirus software fall into this category.
* Never Update: 3 users do not update their systems and have no antivirus installed.
* Awareness ("I don’t know"): 1 user indicated uncertainty about their antivirus or update practices, showing potential lack of awareness regarding cybersecurity practices.

3.5 ONLINE BEHAVIOUR

3.5.1 Exploring the relation of how often do you review your online account activity for any unauthorized access and Regularity to check security and privacy settings of social media accounts?

FIGURE 3.8: PIVOT CHART – REVIEW ONLINE ACCOUNT ACTIVITY AND REGULARITY TO CHECK SECURITY AND PRIVACY SETTINGS

|  |  |  |
| --- | --- | --- |
| Review your online account activity | Regularity to check security settings | Count of AGE |
| Daily |  | 11 |
|  | No | 2 |
|  | Yes | 9 |
| Monthly |  | 14 |
|  | No | 4 |
|  | Yes | 10 |
| Never |  | 5 |
|  | No | 5 |
| Rarely |  | 18 |
|  | No | 5 |
|  | Yes | 13 |
| Weekly |  | 10 |
|  | No | 3 |
|  | Yes | 7 |
| Grand Total |  | 58 |

TABLE 3.5: REVIEW ONLINE ACCOUNT ACTIVITY AND REGULARITY TO CHECK SECURITY AND PRIVACY SETTINGS

This data represents how often individuals review their online account activity for security and privacy settings, along with whether they take actions to review these settings (Yes or No).

1. Frequency of Reviewing Online Account Activity**:**
   * **Daily**: 11 respondents
   * **Monthly**: 14 respondents
   * **Never**: 5 respondents
   * **Rarely**: 18 respondents
   * **Weekly**: 10 respondents
2. Actions Taken to Check Security & Privacy Settings:
   * **No**: Number of respondents who do **not** check security & privacy settings.
   * **Yes**: Number of respondents who **do** check security & privacy settings.

General Trend:

* Those who regularly review their online activities (daily/weekly/monthly) are more likely to also review their privacy settings ("Yes").
* Conversely, those who rarely or never review their activity are less likely to engage in privacy checks.

3.6 AWARENESS AND TRAINING

3.6.2 Exploring the confidence in recognizing phishing emails

FIGURE 3.9: PIE CHART – CONFIDENCE IN RECOGNIZING PHISHING EMAILS

|  |  |
| --- | --- |
| How confident are you in your ability to recognize phishing emails? | Count of AGE |
| Neutral | 23 |
| Not confident at all | 2 |
| Not very confident | 5 |
| Somewhat confident | 20 |
| Very confident | 8 |
| Grand Total | 58 |

TABLE 3.6: CONFIDENCE IN RECOGNIZING PHISHING EMAILS

Here is the breakdown of the responses:

* Neutral (40%): The largest portion of participants feel neither confident nor unconfident, suggesting uncertainty or lack of strong opinions about their ability to recognize phishing emails.
* Somewhat Confident (34%): A significant portion of respondents have some degree of confidence, indicating moderate awareness or experience in identifying phishing emails.
* Very Confident (14%): A smaller percentage of respondents are highly confident in their ability, showing strong awareness or expertise.
* Not Very Confident (9%): A smaller segment indicates limited confidence, suggesting they feel somewhat unprepared or unsure.
* Not Confident at All (3%): Only a small fraction of respondents reports complete lack of confidence, indicating minimal or no familiarity with recognizing phishing emails.

The results show that while a substantial portion of participants (48%) have some level of confidence, 43% are either neutral or lack confidence, highlighting the need for better training or awareness programs on phishing email detection.

CHAPTER 4

INFERENCES & KEY INSIGHTS

* 1. Key insights of Gender and demographics

1. **Gender Ratio**:

* The gender distribution among respondents is fairly balanced, with 35 male respondents and 23 female respondents. This indicates a diverse representation of genders in the survey.

2. **Age Ratio**:

* The majority of respondents are between the ages of 16-18, suggesting that the survey primarily reached a younger demographic.
* A smaller group of respondents falls within the age range of 19-21, indicating some representation of young adults.
* A very few respondents are between the ages of 21-32, showing limited participation from this age group.
  1. Key insights of General awareness

1. **Majority Awareness**: The majority of respondents (34 out of 58) are somewhat familiar with types of cyber threats, indicating a moderate level of awareness.
2. **High Awareness**: A significant portion (14 out of 58) are very familiar with cyber threats, showing a good level of understanding among some respondents.
3. **Low Awareness**: A smaller group (10 out of 58) are not familiar with cyber threats, highlighting the need for increased awareness and education.

These insights suggest that while there is a reasonable level of awareness about cyber threats, there is still room for improvement, especially for those who are not familiar with these threats. Targeted training and educational programs could help bridge this gap.

* 1. Key insights of Password management

1. **Passwords**: The largest segment (26%) of respondents use passwords as their primary security measure.
2. **Passwords and Two-Factor Authentication**: A significant portion (24%) of respondents use both passwords and two-factor authentication, indicating a higher level of security awareness.
3. **Passwords, Two-Factor Authentication, and Regularly Updated Antivirus**: 19% of respondents use a combination of passwords, two-factor authentication, and regularly updated antivirus, showing a comprehensive approach to security.
4. **Two-Factor Authentication**: 21% of respondents use two-factor authentication, highlighting its importance in securing online accounts.
5. **None of the Above**: A small percentage (5%) of respondents do not use any of the listed security measures, indicating a potential area for improvement in cybersecurity practices.
6. **Other Combinations**: Smaller segments include respondents using "Passwords, regularly updated antivirus" (2%) and "Regularly updated antivirus" (3%).
   1. Key insights of Device security
7. **Regular Updates**: A significant portion of respondents (21 out of 58) regularly update their computer's OS and applications, with the majority (16) also having reliable antivirus and anti-malware software installed.
8. **Occasional Updates**: The largest group (22 out of 58) updates their OS and applications occasionally, with a mix of antivirus software usage: 12 have it installed, 9 do not, and 1 is unsure.
9. **Rare Updates**: 12 respondents rarely update their OS and applications, with the majority (9) not having reliable antivirus and anti-malware software installed.
10. **Never Updates**: A small group (3 out of 58) never updates their OS and applications, and none of them have reliable antivirus and anti-malware software installed.
11. **Security Awareness**: The data suggests a need for increased awareness and education on the importance of regularly updating OS and applications and having reliable antivirus and anti-malware software to enhance overall cybersecurity.
    1. Key insights of Online behaviour
12. **Daily Review**: 11 respondents review their online account activity daily, with the majority (9) also regularly checking their security and privacy settings.
13. **Monthly Review**: 14 respondents review their online account activity monthly, with most (10) also regularly checking their security and privacy settings.
14. **Never Review**: 5 respondents never review their online account activity, and none of them check their security and privacy settings.
15. **Rarely Review**: 18 respondents rarely review their online account activity, with the majority (13) regularly checking their security and privacy settings.
16. **Weekly Review**: 10 respondents review their online account activity weekly, with most (7) also regularly checking their security and privacy settings.
17. **Security Awareness**: The data suggests that those who review their online account activity more frequently are also more likely to regularly check their security and privacy settings, indicating a higher level of security awareness.
    1. Key insights of Awareness and training
18. **Neutral Confidence**: The largest group of respondents (23 out of 58) feel neutral about their ability to recognize phishing emails.
19. **Somewhat Confident**: A significant portion (20 out of 58) are somewhat confident in their ability to recognize phishing emails.
20. **Very Confident**: A smaller group (8 out of 58) are very confident in their ability to recognize phishing emails.
21. **Low Confidence**: A combined total of 7 respondents (2 not confident at all and 5 not very confident) have low confidence in their ability to recognize phishing emails.
22. **Overall Confidence**: The data suggests that while a majority of respondents have some level of confidence in recognizing phishing emails, there is still a need for increased awareness and training to boost confidence levels, especially for those who are not confident.

CONCLUSION

The cybersecurity awareness survey conducted via Google Forms and distributed through WhatsApp revealed 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.

**Future Work**

**Enhanced Training Programs:** Develop targeted training to boost confidence in recognizing phishing emails and update employees on new cyber threats.

**Policy and Procedure Improvements:** Update cybersecurity policies and ensure mandatory training for all.

**Advanced Data Analysis:** Conduct deeper analysis, including regression and correlation, and explore machine learning for predictive insights.

**Follow-Up Surveys:** Regularly assess the effectiveness of training programs and track changes in awareness levels.

**Broader Engagement:** Expand the survey to include more diverse groups and promote a culture of cybersecurity awareness through ongoing communications and interactive sessions.

REFERENCES

[1] Microsoft. (n.d.). COUNTIF function. Microsoft Support. Retrieved November 25, <https://support.microsoft.com/en-us/office/countif-function-e0de10c6-f885-4e71-abb4-1f464816df34>

[2] Microsoft. (n.d.). Conditional formatting. Microsoft Support. Retrieved November 25, <https://support.microsoft.com/en-us/office/conditional-formatting-7957ee2d-c54e-4230-961f-175fad32972c>

[3] Microsoft. (n.d.). Create a PivotChart. Microsoft Support. Retrieved November 25,<https://support.microsoft.com/en-us/office/create-a-pivotchart-c1b1e057-6990-4c38-b52b-8255538e7b1c>

[4] Microsoft. (n.d.). Available chart types in Office. Microsoft Support. Retrieved November 25, 2024, from <https://support.microsoft.com/en-us/office/available-chart-types-in-office-a6187218-807e-4103-9e0a-27cdb19afb90>