Vidhyayana - ISSN 2454-8596

An International Multidisciplinary Peer-Reviewed E-Journal

www.vidhyayanaejournal.org

Indexed in: Crossref, ROAD & Google Scholar

29

Analysis and Survey on Cybersecurity: Threats and Solutions

Om Dhule

MSc. Computer Science, MIT-WPU,

omdhule2000@gmail.com

Hrishikesh Bhorde

MSc. Computer Science, MIT-WPU,

hrishikeshbhorde7@gmail.com

Shail Alavani

MSc. Computer Science,

MIT-WPU, shailalavani@gmail.com

Avinash Janbhare

MSc. Computer Science, MIT-WPU,

avinashjanbhare29@gmail.com

Mentor

Gauri Dhongade

Asst. Prof., School of Computer Science,

MIT WPU Pune

gauri.dhongade@mitwpu.edu.in

Abstract

This research paper will explore the various types of cyber attacks that are currently impacting individuals and organizations, and the solutions that are available to mitigate these threats. The paper will begin by providing an overview of the current state of cybersecurity, including the types of attacks that are most commonly seen and the industries that are most at risk.

The paper will then delve into specific types of attacks, such as ransomware and phishing, and examine the methods that are used to carry out these attacks, as well as the potential consequences for victims. The paper will also provide data about cybersecurity awareness amongst the people.

Index Terms*- CyberSecurity, Cyber-Threats, Malware, Countermeasures, Awareness, Hacking, Phishing, DDOS,*

I. INTRODUCTION

In today's digital age, the need for robust cybersecurity measures has never been greater. With the increasing number of internet-connected devices and the growing dependence on technology in all aspects of life, cyber attacks have become a major concern for individuals and organizations. These attacks can take many forms, from hacking and phishing to malware and ransomware, and can have serious consequences for victims, including the loss of sensitive data and financial loss.

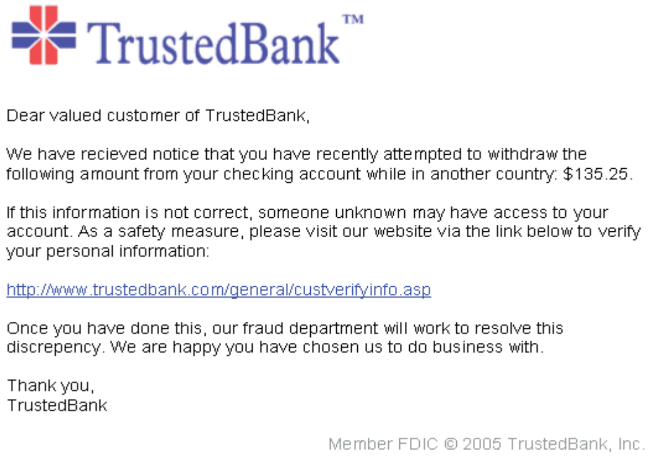
As the threat landscape continues to evolve, it is important to stay informed about the latest cybersecurity threats and the solutions that are available to mitigate them. This research paper aims to provide the various types of attacks that are being seen, and the solutions that are available to protect against these threats.

II. OBJECTIVE

1. To perform an in-depth analysis of the existing research on Cybersecurity Threats and the available solutions.
2. To check the awareness about cybersecurity amongst people.

III. TYPES OF CYBERSECURITY THREATS

- **Phishing:** Phishing is a type of cyber attack that involves the use of fraudulent emails, text messages, or websites to obtain sensitive information such as usernames, passwords, and credit card details. The attackers typically pose as legitimate entities, such as banks or e-commerce sites, to trick the victims into providing their personal information. The most effective solution to prevent phishing attacks is to educate users about how to identify fraudulent emails, texts, or websites. An example of fishing is given below.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

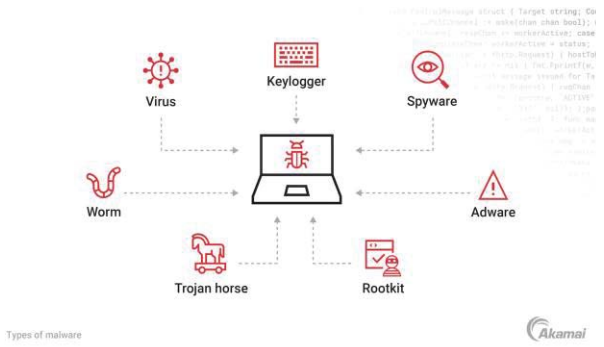
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Example of a Phishing disguised as a bank. (*File: PhishingTrustedBank.png*, n.d.)

- **Malware:** Malware is a type of software designed to harm computer systems, steal data, or gain unauthorized access to networks. Malware can take many forms, such as viruses, worms, Trojans, and spyware. The most effective solution to prevent malware attacks is to use antivirus software and keep it updated regularly.



Types of Malwares. (*What Is Malware?* n.d.)

- **DDoS Attacks:** DDoS (Distributed Denial of Service) attacks are designed to overwhelm a website or network with a large number of requests, rendering it inaccessible to legitimate users. DDoS attacks are often carried out using a network of compromised devices, such as botnets. The most effective solution to prevent DDoS attacks is to use firewalls, intrusion detection systems, and load balancers.
- **Man-in-the-middle (MitM) attacks:** In a MitM attack, a cybercriminal intercepts and alters communication between two parties to steal sensitive information, such as login credentials or financial data.
- **SQL injection:** A SQL injection attack involves injecting malicious code into a website or application's database, allowing the attacker to access and manipulate sensitive data.
- **Cross-site scripting (XSS):** XSS attacks allow cybercriminals to inject malicious code into a website or application that can then be executed by unsuspecting users, leading to data theft or other malicious activity.
- **Password attacks:** Password attacks involve using various techniques, such as brute force or dictionary attacks, to gain unauthorized access to a user's account or system by guessing or cracking passwords.

IV. CYBERSECURITY SOLUTIONS

- **Firewalls:** Firewalls are a critical component of cybersecurity. They are designed to prevent unauthorized access to a network by monitoring incoming and outgoing traffic.
- **Intrusion Detection Systems:** Intrusion detection systems (IDS) are designed to detect and prevent unauthorized access to a network. IDS can monitor network traffic in real-time and alert network administrators if suspicious activity is detected.
- **Antivirus Software:** Antivirus software is designed to detect and remove malware from computer systems. Antivirus software can be installed on individual devices or on a network to provide comprehensive protection against malware.

- **Encryption:** The process of transforming data into an unreadable format that can only be understood with a decryption key is known as encryption. Encryption is a critical component of cybersecurity, as it can prevent unauthorized access to sensitive data.
- **Virtual Private Network (VPN):** A VPN provides secure and private communication between two or more devices over a public network, such as the Internet.
- **API Security:** Application programming interfaces (APIs) enable communication between different applications. Since this process let's, you transfer information between services and applications, it is highly vulnerable to interceptions. API security solutions help protect APIs and prevent exploitations of transmissions or vulnerabilities. (*Cyber Security Solutions | Protect Enterprise Networks | Imperva*, n.d.)
- **Zero Trust Cybersecurity:** Zero trust is a security model that enforces strict access controls. A laptop connected to the network, a mobile device connected to the corporate cloud, a SaaS environment shared with external parties—all of these should be treated with zero trust. At the most basic level, this means applying strict authentication across granular user types. Organizations also leverage endpoint security to enforce zero trust. (*Cyber Security Solutions | Protect Enterprise Networks | Imperva*, n.d.)
- **Access Control:** Access control systems limit access to certain areas or information to authorized users only, preventing unauthorized access or tampering.
- **Security Information and Event Management (SIEM):** SIEM is a software system that collects and analyzes security data from multiple sources, including network devices, servers, and applications, to identify potential security threats.

V. QUESTIONNAIRE

- We conducted a small survey about the awareness of cybersecurity among 50 people.
- The survey tool used for this was a Questionnaire.
- The response was either a yes/no or a scale of 1 to 5 depending on the question.

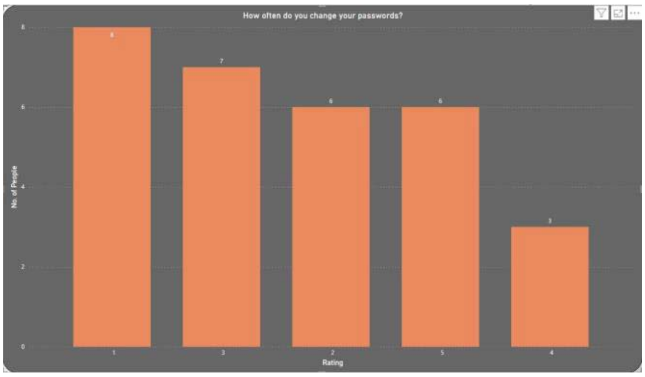
- The survey consisted of the following questions:

  1. How often do you change your passwords?
  2. How often do you update your software and security patches?
  3. Do You Use Two-factor authentication?
  4. How often do you back up your data?
  5. Have you ever shared your passwords with anyone else?
  6. Have you ever accessed sensitive information on a public Wi-Fi network?
  7. How often do you review your privacy settings on social media?
  8. How genuine do you think this mail is?
  9. How much do you trust this screenshot of "Java Installation" is genuine?

- These are the graphs that were created based on the data collected via this survey.
- Form Link: https://forms.gle/K8X8CSR39zgfFkRd7

VI. OBSERVATIONS

- How often do you change your passwords?

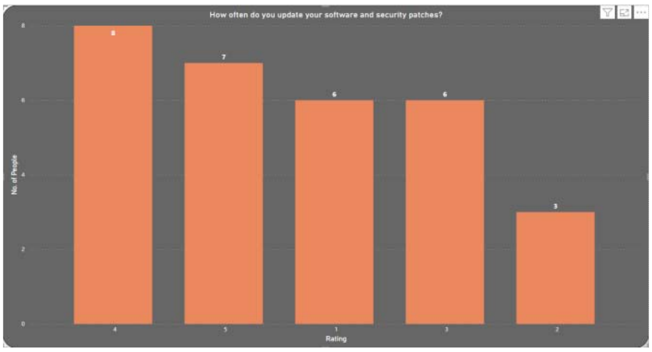


The above bar graph shows how often people change their passwords on a scale of 1 to 5, 1 being never and 5 being regularly.

From all the gathered 30 records, about 41.5% of the people come under the "actively or regularly changing password" category while the other 59.5% are from "sometimes to never updation of password" category.

As we can see, the majority of people don't update/change their passwords which can make their accounts vulnerable to password hacking.

- How often do you update your software and security patches??



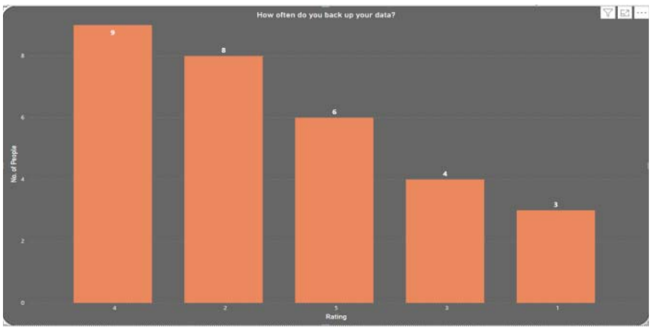
The above bar graph shows how often people update their software and security patches on a scale of 1 to 5, 1 being never and 5 being regularly.

From all the gathered 30 records, about 60% of the people come under the "actively or regularly changing password" category while the other 40% are from "sometimes to never updation of password" category.

As we can see, the majority of people update their security patches which makes their system more secure and ready for new emerging threats. Not downloading the latest software patches can leave the software vulnerable to new threats and the user can also miss on new features.

Eg. New viruses get introduced everyday and antivirus softwares rolls out updates to handle these viruses. If the user does not download the latest patch of the antivirus software, there are high chances that the system can be infected by the new virus because of the incapability of the antivirus software to handle the new threat.

- How often do you back up your data?

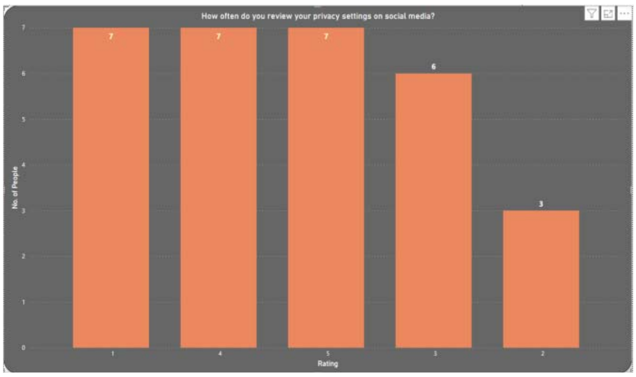


The above bar graph shows how often people backup their data on a scale of 1 to 5, 1 being never and 5 being regularly.

From all the gathered 30 records, about 63.33% of the people come under the "actively or regularly changing password" category while the other 36.67% are from "sometimes to never updation of password" category.

As we can see, the majority of people backup their data on a regular basis. Creating data backup from time to time is very important when it comes to data security. If by any chance, the data of the user is lost due to any attack or human error, he/she can recover the data from the last updated data recovery file.

- How often do you review your privacy settings on social media?

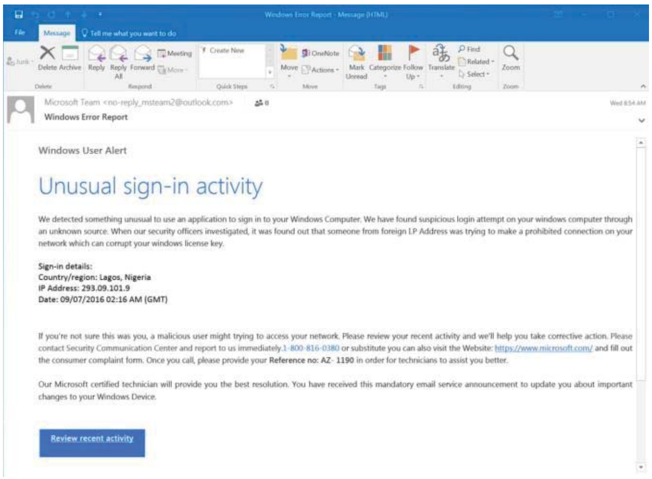


The above bar graph shows how often people review their privacy settings on social media on a scale of 1 to 5, 1 being never and 5 being regularly.

From all the gathered 30 records, about 56.66% of the people come under the "actively or regularly changing password" category while the other 43.34% are from "sometimes to never updation of password" category.

As we can see, the majority of people review the privacy setting on social media on a regular basis. Reviewing privacy settings on social media helps the user decide who gets the consent to use the user's data and personal information. Ignoring these settings can lead to people misusing the user's data from social media which creates a case of breach of personal privacy.

- How genuine do you think this mail is?



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Wed 8:54 AM

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

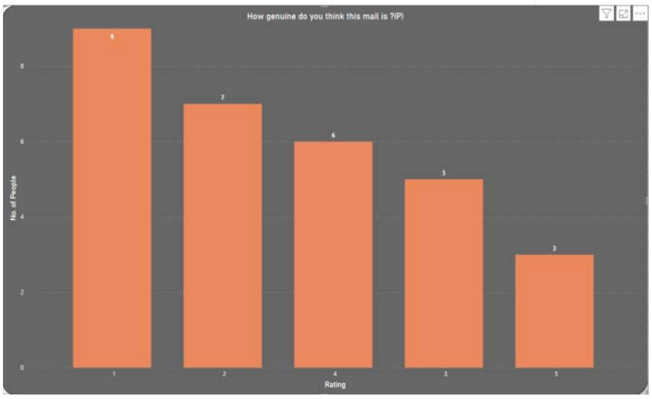
Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

In this question, we showed the above image and asked the people how genuine this image looks.

This image is a fake microsoft notice of “Unusual Sign-in” which looks identical to the official one which microsoft sends when it notices unusual sign-in. This fake email points to a phony-number “1-800” and suggests the user to contact this number. This is commonly known as credentials phishing which can lead the user to expose his/her credential to the fake support employee.

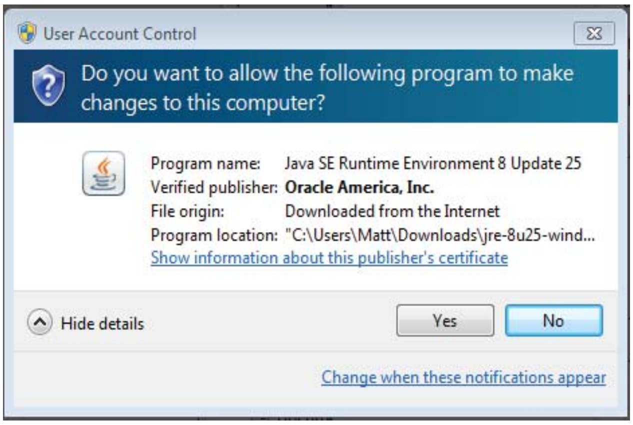


The above bar graph shows how genuine people think this mail is, on a scale of 1 to 5, 1 being Total Scam and 5 being Legit.

From all the gathered 30 records, about 61.66% of the people think that the mail shown in the image is a Scam while the other 38.33% people think that the mail is legit.

Unusual Sign-in mails are very important and people should always keep a lookout for such mails but identifying if the mail is legit or not is also very important. If not careful, people can fall for such scams while being in the illusion of taking security steps. (*Phishing Examples*, n.d.)

- How much do you trust this screenshot of "Java Installation" is genuine?

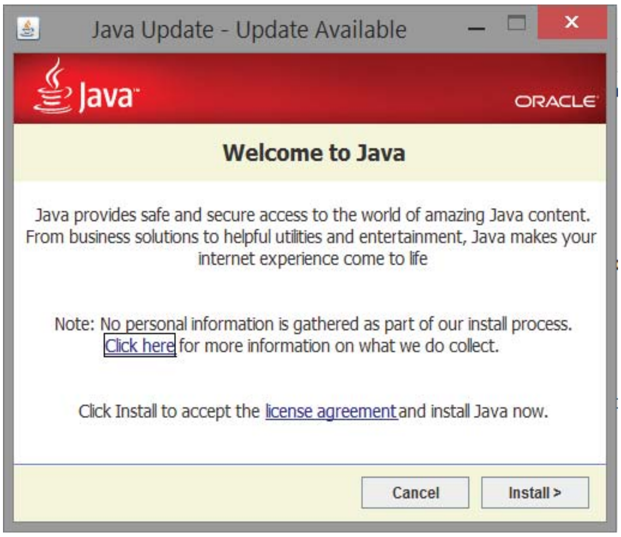


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Java SE Runtime Environment 8 Update 25
Verified publisher: **Oracle America, Inc.**
File origin: Downloaded from the Internet
Program location: "C:\Users\Matt\Downloads\jre-8u25-wind...
Show information about this publisher's certificate

We first show the image above to the people and ask the question based on the image below.



Java Update - Update Available

Welcome to Java

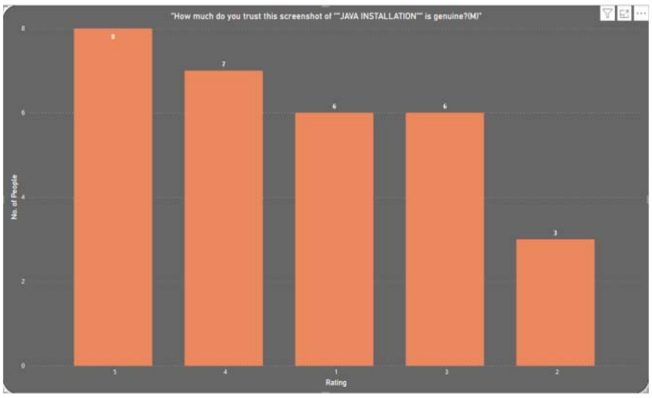
Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life

Note: No personal information is gathered as part of our install process. Click here for more information on what we do collect.

Click Install to accept the license agreement and install Java now.

In this question, we showed the above two images and asked the people how genuine this java installer image looks after seeing the first one.

The above image is an example of an attack called "Placeholder Trojan". In this example, the user downloads the version of java here and the installation window is also identical to the original installer. However, when it asks for permission to User Account Control, it is actually asking access for trojan to be injected in the user's system.

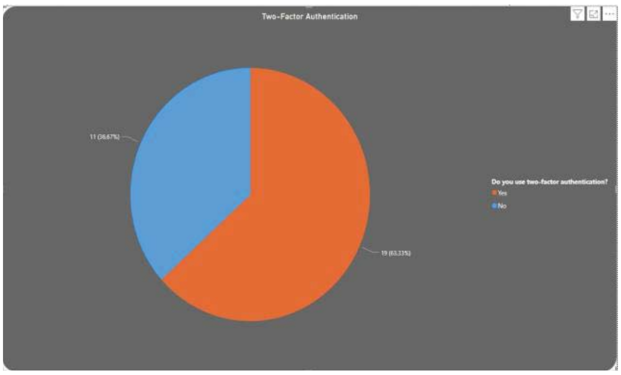


The above bar graph shows how much people trust that this is the legit java installer, on a scale of 1 to 5, 1 being Fake and 5 being Legit.

From all the gathered 30 records, about 60% of the people think that the installer is genuine while the other 40% people think that the installer can be fake.

When the user clicks on the "Yes" button, no matter what the user does after that, the trojan will be installed. It runs in the background stalking and stealing all the running program information. (*Trojan Placeholder*, 2014)

- Do You Use Two-factor authentication?

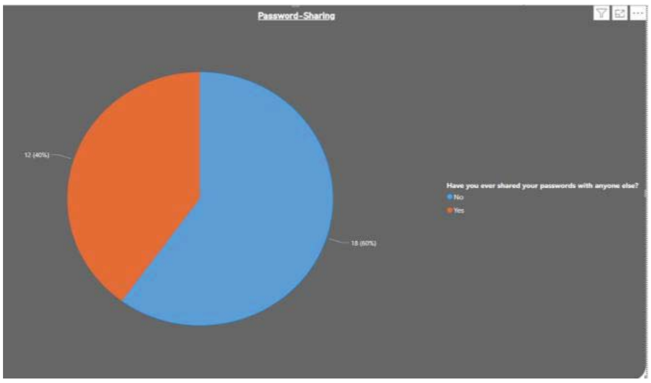


The pie chart depicts the distribution of how many people use 2- Factor Authentication.

According to the data collected we can see more than 63% of people are not using 2-Factor Authentication.

It is important and suggested to use *2 - Factor Authentication as it immediately neutralizes the risks associated with compromised passwords, and also adds an additional layer of security to your online accounts.* (*Why Use 2FA?: TechWeb*, n.d.)

- Have you ever shared your passwords with anyone else?

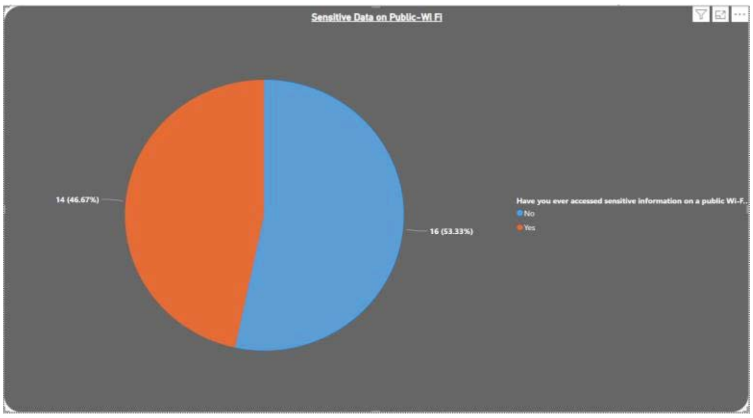


The pie chart depicts the distribution of how many people have shared their passwords with others.

According to the data collected we can see 60% of people have shared their passwords with other's.

The sharing of passwords can be done via verbal communication or a text message, either way it's not suggested to share your passwords. By sharing passwords your security could be compromised.

- Have you ever accessed sensitive information on a public Wi-Fi network?



The pie chart depicts the distribution of people who have accessed sensitive information on a public Wi-Fi network.

Here, by sensitive information we mean use of financial services, social media logins etc.

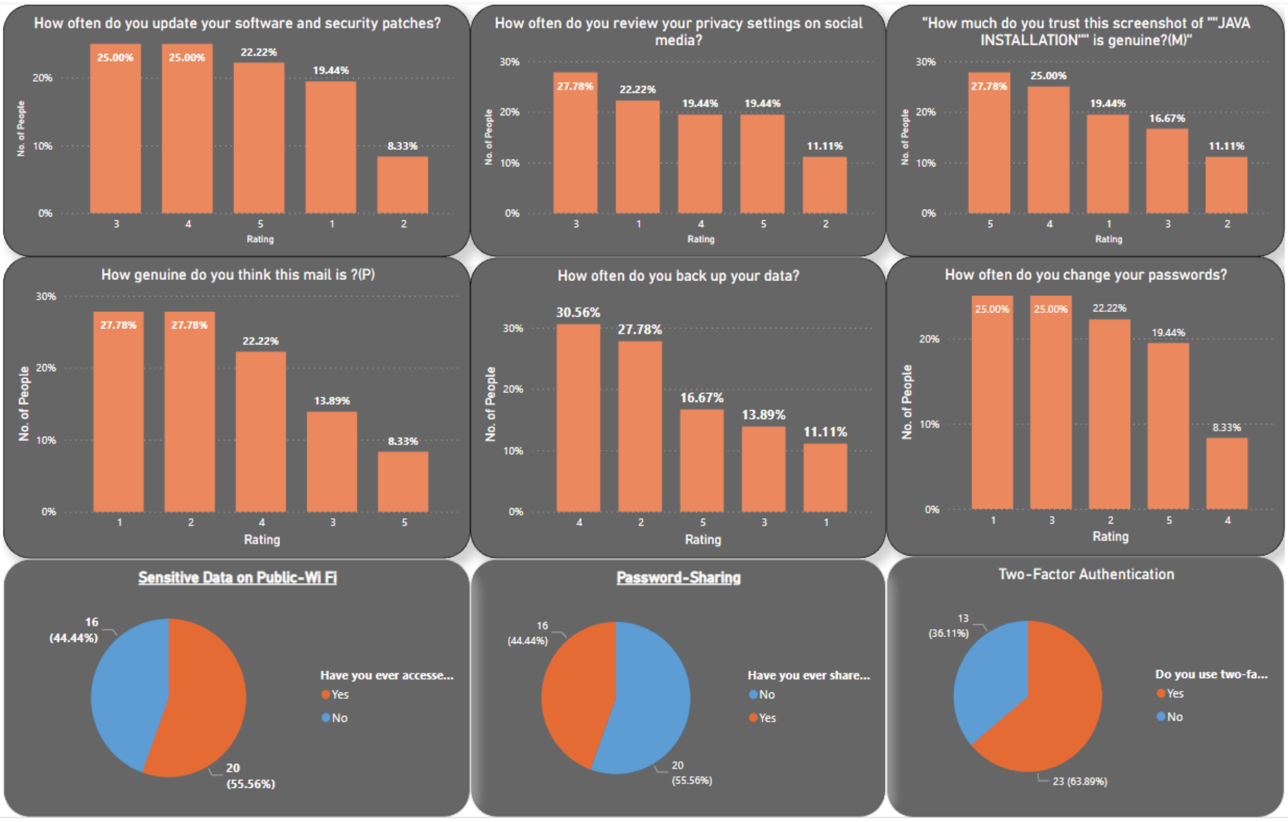
According to the data collected we can see more than 53% of people have accessed sensitive information on a public Wi-Fi network.

There are many security risks associated with public Wi-Fi like lack of encryption, Malware Attacks.

Fake Wi-Fi Network is one of the major issues, also termed as "Honeypots"

Honeypots basically allows a user to view all the websites he/she would visit normally, while doing so the hacker would steal all the usernames, password (Login Credentials) of the user. (Gray, 2022)

- Below are the graphs of all the observations collected via the questionnaire.



VII. CONCLUSION

We have provided all the prominent threats and solutions related to cybersecurity. In today's world, cyber-threats are definitely a major concern and the need for cyber-security is rising day by day. Everyday a new threat emerges and a new solution is needed to handle the threat. So, the first step people need to take is to stay aware.

From the gathered data through the survey, we can see that about 50-60% of people still are not aware about cyberattacks. To increase this percentage of awareness, we need to educate people about the different threats and solutions about cybersecurity.

REFERENCES

1. *File: PhishingTrustedBank.png*. (n.d.). Wikimedia Commons. Retrieved April 15, 2023, from https://en.wikipedia.org/wiki/File:PhishingTrustedBank.png
2. *What Is Malware?* (n.d.). Akamai. Retrieved April 15, 2023, from https://www.akamai.com/glossary/what-is-malware
3. *Phishing Examples*. (n.d.). Phishing.org. Retrieved April 15, 2023, from https://www.phishing.org/phishing-examples
4. Bourg, G., Bullock, M., & Miller, R. (2014, December 1). *Trojan Placeholder*. Placeholder Trojan: Writing a Malware Software. Retrieved April 15, 2023, from https://www.cse.wustl.edu/~jain/cse571-14/ftp/p_trojan/index.html
5. *Why Use 2FA? : TechWeb*. (n.d.). Boston University. Retrieved April 15, 2023, from https://www.bu.edu/tech/support/information-security/why-use-2fa/
6. Gray, K. (2022, October 17). Fake Wi-Fi HotSpots: A Criminal's Tool to Steal from You. Retrieved April 15, 2023, from https://blog.envisionitsolutions.com/computer-security-and-fake-wi-fi-hotspots-a-criminals-tool-to-steal-from-you
7. *Cyber Security Solutions | Protect Enterprise Networks | Imperva*. (n.d.). Imperva, Inc. Retrieved April 15, 2023, from https://www.imperva.com/learn/application-security/cyber-security-solutions/