CHRIST NAGAR COLLEGE

MARANALLOOR,
THIRUVANANTHAPURAM

Submitted to the **University of Kerala** in partial fulfillment of the requirements of the BA Degree Course in **Journalism, Mass Communication and Video Production** for the Sixth Semester.

By

Students of Group-2

Abdul Munaf Z (12917825004)
Anand S (12917825008)
Arun S Kumar (12917825011)
Mohammed Yazeen N (12917825022)
Sivabalan B (12917825028)
Sooraj S Kumar (12917825030)

CYBER & DIGITAL SECURITY AWARENESS IN THIRUVANANTHAPURAM

Abdul Munaf, Anand S, Arun S Kumar, Mohammed Yazeen, Sooraj S Kumar

Christ Nagar College, Maranalloor, Trivandrum

ABSTRACT

The Internet has and is becoming increasingly interwoven in the daily lives of individuals, organisations, and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business; and it has given nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users are not aware. Though cyber-security awareness and education measures to counter the perceived ignorance of the Internet users have been implemented at different levels, the effectiveness is questionable. The primary research objective is to determine the scale of awareness that currently exists in various spheres among the populace of Thiruvananthapuram, including the impact of factors like age, gender, and financial position on the same. With digital financial transactions becoming more popular each day, and the number of cybercrimes increasing rapidly, this information is of immense relevance as to whether the users are aware of the potential risks, user permissions, internet terminologies, security-breach vulnerabilities, and about how to avoid such risks.

INTRODUCTION

Now-a-days, protecting the integrity and confidentiality of the information in the system of complex networks is very important and challenging. While social networks and bank account details are also at high risk, institutions are also facing risks of losing valuable intellectual property. Despite this being the digital era, or the ‘Internet Age’, awareness about the potential risks has been limited to a few minutes of awareness classes to the students. The real problem is yet to be dealt with, as the populace, including not only students but also the adult individuals, still is vulnerable to becoming prey for cheating attempts. With the usage of digital money transactions skyrocketing in recent years with the growth of applications like Google Pay, the potential risks are much more.

CHAPTER 1

INTRODUCTION

1.1 ABOUT CYBER AND DIGITAL SECURITY

Computer security, cybersecurity, information technology security (IT security) are terms that refer to protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data. It also includes protection from the disruption or misdirection of the services they provide. Cyber security is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, and televisions. Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world. Computer security, mobile security, internet and network security, are some of the related categories. Threats include personal information breach, malware attacks, data encryption, gaining illegal access into private data, et cetera. With the payment and money transactions becoming more and more in the digital realm these days, money related frauds are also a potential risk factor. Steps have been and have to be taken at both the personal level and at the governmental level to effectively handle the concerns. Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000.

1.2 TYPES OF CYBER ATTACKS

1.2.1 DENIAL-OF-SERVICE (DOS) AND DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

A denial-of-service attack interrupts a system's resources so that it cannot respond to service requests. A DDoS attack is a type of cyber attack which attacks a system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike other attacks that are structured to enable the attacker to gain or increase access, denial-of-service does not provide direct benefits for attackers. Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be created. One example is session hijacking.There are different types of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.

1.2.1.1 TCP SYN FLOOD ATTACK

In this mode of attack, an attacker misuse the buffer space during a Transmission Control Protocol (TCP). The attacker's device interrupts the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This makes the target system to become timed out while waiting for the response from the

attacker's device, which makes the system crash or become unstable when the connection queue fills up.

1.2.1.2 BOTNETS

Botnets are the millions of systems which get infected with malwares under the control of the hacker in order to carry out DDoS attacks. These bots are used to carry out attacks against the target systems, often interrupting the target system's bandwidth and processing abilities. These DDoS attacks are difficult to identify because botnets are located in varying geographic locations.

1.2.2 MAN-IN-THE-MIDDLE (MitM) ATTACK

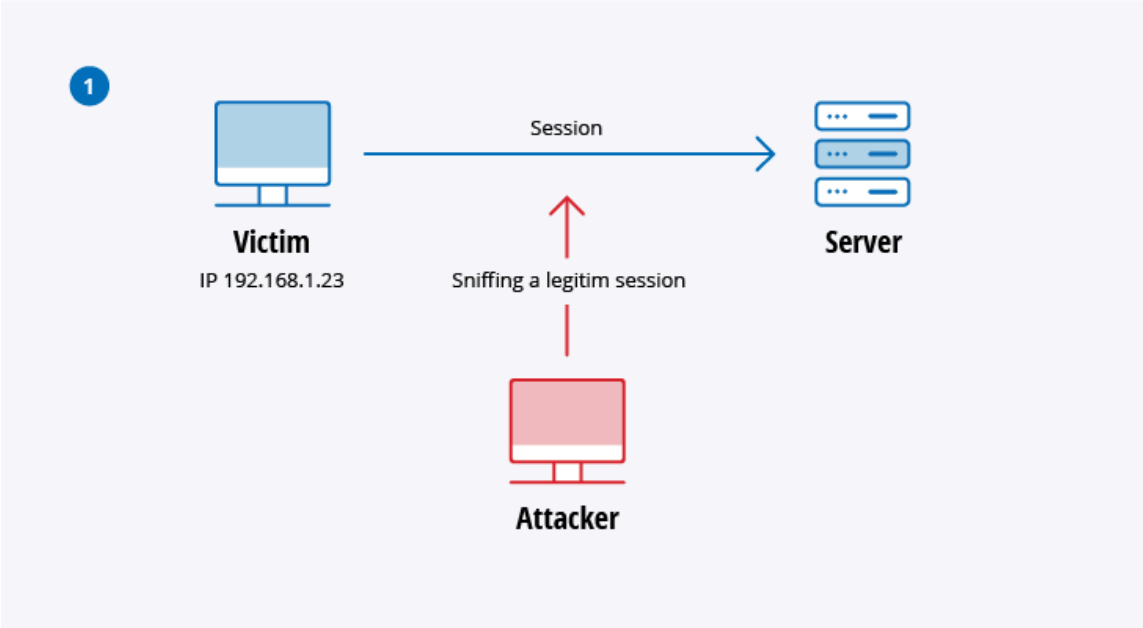
A MitM attack occurs when a hacker comes across in between the communications of a client and a server. Some common types of man-in-the-middle attacks are:

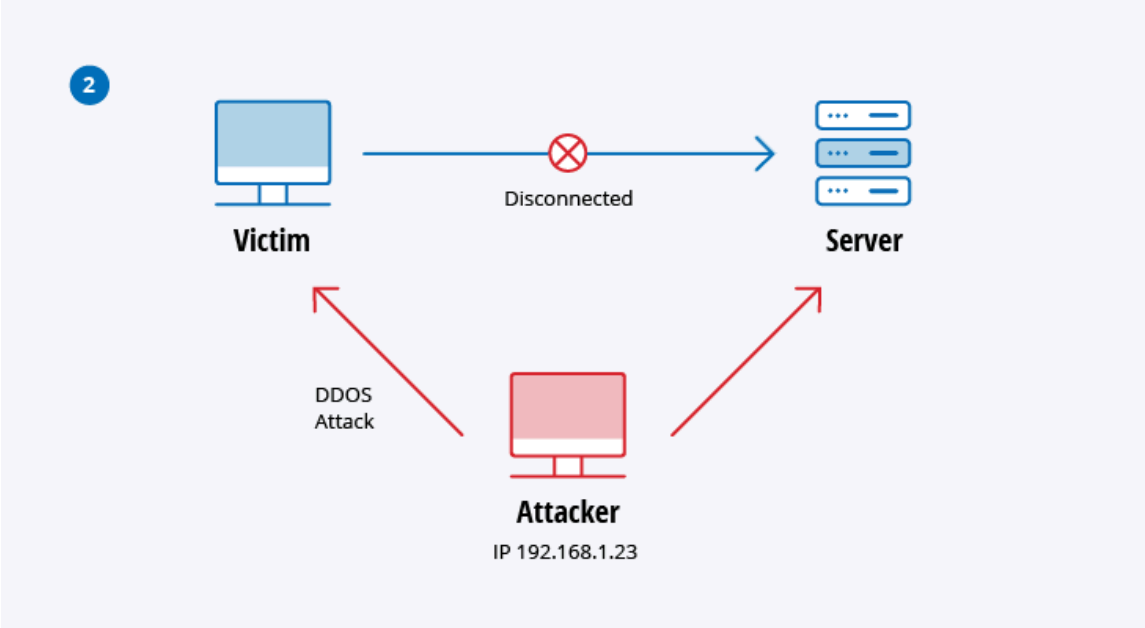
1.2.2.1 SESSION HIJACKING

In this mode of MitM attack, an attacker hacks a session between a trusted client and network server. The attacking computer alters its IP address for the trusted client while the server continues the session, believing it is performing with the client.The attack might go like this:

- A client connects to a server.
- The attacker's computer gains control of the client.

- The attacker’s computer disconnects the client from the server.
- The attacker’s computer replaces the client’s IP address with its own IP address and spoofs the client’s sequence numbers.
- The attacker’s computer continues to dialog with the server and the server believes it is still communicating with the client.





1.2.2.2 IP SPOOFING

IP spoofing is used by a hacker to believe a system that it is communicating with a known, trusted entity and provides the hacker with access to the system. The attacker or hacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might approve the packet and act upon it.

1.2.3 PHISHING AND SPEAR PHISHING ATTACKS

Phishing is the practice of sending emails that appear to be from trusted sources with the motive to gain personal information or influencing users to do something. It is a combination of social

engineering and technical trickery. It may involve an attachment to an email that inserts malware onto your computer. It could also be a link to an illegal website that can influence you into downloading malware or handing over your personal information.

Spear phishing is a very specific type of phishing activity. Hackers take the time to conduct research into targets and create messages that are personal and important. Spear phishing can be very hard to trace and even harder to defend against. One of the easy ways that a hacker can perform a spear phishing attack is email spoofing, which is when the information in the “From” section of the email is fabricated, making it look as if it is coming from someone you know.

1.2.4 DRIVE-BY ATTACK

Drive-by download attack is a common type of spreading malware. Hackers search for insecure websites and plant a hazardous script into HTTP or PHP code on one of the pages. This malicious script might install malware directly onto the computer of someone who enters the site, or it might redirect the user to a site controlled by the hackers. Drive-by downloads can occur when a user visits a website or views an email message or a pop-up window. Unlike other types of cyber security attacks, a drive-by attack does not depend on a user to do anything to enable the attack — you do not have to click a download link or open a malicious email attachment to become infected. A drive-by download can take advantage of an application, operating system(OS) or web browser that includes security failures due to incomplete updates or lack of updates.

1.2.5 PASSWORD ATTACK

Passwords are the most commonly used mechanism to endorse users to an information system. And it is because of the same, that obtaining passwords is a common and effective attack approach.To a user's password can be acquired by looking around the person's desk, ''sniffing'' the connection to the network to access unencrypted passwords, using social engineering, getting access to a password database.

1.2.6 MALWARE ATTACK

Malicious software can be defined as an unwanted software that is installed in your operating system without permission of the user. It can attach itself to a legit code and propagate; it can enter in useful apps or multiply itself across the Internet.Some of the most common types of malware are:

1.2.6.1 MACRO VIRUSES

These types of viruses infect apps such as Microsoft Word or Excel. Macro viruses attach to an app's initialization sequence. When the application is opened, the virus implements instructions before transferring control to the application. The virus multiplies itself and attaches to other code in the computer's operating system.

1.2.6.2 FILE INFECTORS

File infectors are viruses that usually attach themselves to executable code, such as .exe files. The virus is installed when the code is entered. Other versions of a file infector relates itself with a file by creating a virus file with the exact same name, but an .exe extension. Therefore, when the file is opened, the virus code will be implemented.

1.2.6.3 TROJANS

A Trojan or a Trojan horse is a program that hides in a useful program. And it usually has a malicious function. The main difference between viruses and Trojans is that Trojans do not self-multiply. A Trojan program can establish a backdoor that can be misused by hackers.

1.2.6.4 RANSOMWARE

It is a type of malware that restricts access to the victim's data. And it threatens to publish or delete it unless a ransom is paid. Since simple computer ransomware can lock the system in a way that is easy for an informative person to reverse, some advanced malware uses a technique called cryptoviral extortion, which encrypts the user's files in a way that makes them nearly not possible to recover without the decryption key.

1.2.7 IDENTITY THEFT

Identity theft is the serious crime that obtains the personal or financial information of some other person. It is done for the sole purpose of assuming that person's name or identity to make transactions or purchases. Identity theft is done in many different ways. Some identity thieves filter through trash bins looking for bank accounts and credit card statements. Other high-tech methods involve accessing corporate databases to leak lists of customer information. Once they acquire the data they are looking for, identity thieves can destroy a person's credit rating and other personal information.

1.3 COOKIES

Cookie is a small piece of data sent from a website and stored on the user's personal computer by the user's web browser while the user is browsing on the internet. Cookies were designed to be a reliable mechanism for websites to remember information. They can also be used to remember random pieces of information that the user previously entered, such as names, addresses, passwords, and credit-card numbers.

Cookies perform important functions in the modern web. Most essentially, authentication cookies are the most frequently used method by web servers to identify whether the user is logged in or not. Without such a mechanism, the site would not be able to know whether to send a page including sensitive information.. The security of an authentication cookie is generally

based on the security of the issuing website and the user's web browser, and also depends on whether the cookie data is encrypted.

1.4 INTERNET SERVICE PROVIDERS

An Internet service provider (ISP) is an organization that provides services to access the Internet, or participating in the Internet. They can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.The services provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and colocation.Internet service provider have different classifications and they include - Access providers, Mailbox providers, Virtual ISP's, Free ISP's etc.

CHAPTER 2

REVIEW OF LITERATURE

2.1 INTRODUCTION

This chapter includes the review of studies conducted on the subject and the theoretical framework upon which this study is built on. Most of the works reviewed here are based upon cyber and digital security. The theories used to study the same cognitive dissonance theory, technology acceptance model, communication privacy management theory, social cognitive theory, protection motivation theory.

2.2 LITERATURE REVIEW

“In India, from 2011 to 2014, there has been a surge of approximately 300 per cent in cybercrime cases registered under the IT Act, 2000," found a Assocham-PwC (Associated Chambers of Commerce And Industry of India - PricewaterhouseCoopers) study on the rate of Cyber Crimes in India. In 2015, there were 11,592 cases of cyber crime registered in India, of which 33.3% had the intention of financial gain, found the National Crime Records Bureau (NCRB) in its 2016 report. The figure not only suggests the increase in the usage of the modern technology of the internet sphere, but also of the abuse of the same.

A study on Cyber-Security awareness in South Africa by Noluxolo Kortjan, Rossouw von Solms (School of ICT, Nelson Mandela Metropolitan University, South Africa) “A conceptual

framework for cyber-security awareness and education in SA" found it necessary to implement an education framework spreading knowledge on the same. It found out that the awareness among the students is very low. The paper proposed a cyber-security awareness and education framework that would assist the country in promoting its envisaged cyber-security culture as the results suggested that people are largely unaware of these risks; and so they put themselves, as well as businesses and governmental assets and infrastructure, at risk.

"A Survey on Cyber Security awareness among college students in Tamil Nadu", a study by Senthilkumar K and Sathishkumar Easwaramoorthy (VIT University, Vellore, Tamil Nadu) found that awareness about common Internet frauds including Virus Attack, Password Strength Abuse, and Misuse of Social Network, is between 64% and 65% in 3 of the 5 cities the study was based on (Madurai 64%, Salem 64.25%, Vellore 64.5%, Coimbatore 73.75%, Chennai 79.75%). The study also revealed that awareness of Social Network Misuse is as low as 18% in Madurai. Almost more than 60% of students from all the cities received phishing emails/messages in any form, but only 2.64% (10/379) claimed that they will complain about phishing to the Cyber Crime wing. More than 97% of the respondents who were victims of virus attacks did not know the source of the virus.

"Cyber Security Awareness and Education Research Cyber Security Awareness and Education Research" a study by Professor Elmarie Kritzinger (University of South Africa) found that 41% of 'School Learners', spent over 3 hours a day on the internet, and 7% strongly thought that there are no possible dangers when using the internet. Despite the moderate levels of involvement by

teachers and parents in education around cyber-security awareness, there is a strong desire for this topic to be covered within the school curriculum, particularly within the life-orientation subject, the study concluded.

“Improving Cybersecurity Awareness in Underserved Populations”, a study by Ahmad Sultan to understand the scope and nature of the underserved communities’ cybersecurity outcomes, where underserved included residents from low-income households, foreign-born and foreign-language speakers, and seniors, found that 19% of the community, do not know whether they’ve ever been a victim to a cyber scam, 41% do not know if their phone ever had a virus, and 44% think they have provided personal information to complete strangers online but cannot remember the exact details. The study also found that phishing prevention practices like hovering the mouse arrow over a link to check if it is suspicious, was not practiced by 57% of Underserved Communities, and even 25% of the Comparison Group which consisted of non-Underserved. A significant percentage of underserved residents likely have been victims of a cyber scam, and many may have been scammed multiple times, the findings of the study suggested. 47 percent of underserved respondents do not use online banking due to cybercrime, compared to eight percent in the comparison group, suggesting that the higher strata of the society trusts and employs modern technology for financial transactions.

Internet penetration rate (defined as number of individuals aged above 12 per 100 population who accessed the Internet in the last month; survey period January-March 2019) as per the report by the Internet And Mobile Association of India (IAMAI) titled 'India Internet 2019', in Kerala is

54%, which is second-most in India. This figure suggests a large number of internet users in Kerala, and their frequent use of the same. According to the Technology Acceptance Model (TAM) the ease of usage of a particular technology as well as the knowledge about the same determine the usage of that technology. This theory is consistent with the usage of net-banking usages among the public. Perceived usefulness and perceived ease of use influence consumer attitudes towards using digital technology for financial transactions.

"The Paradox of Social Media Security: A Study of IT Students' Perceptions versus Behavior on Using Facebook", a study by Zahra Alqubaiti, Master of Science in Information Technology done in December 2016, found that among Facebook participant users, only 1 student (4%) read the terms and conditions agreement of Facebook, whereas less than 50% either read fewer than 10 lines or none. More than 65% set their Facebook account profile as private and 28% as public. The results show that at least 47% of the participants changed their Facebook account password once a year, whereas 14% changed their password once every several months, 9% changed their password once every two to three years, and around 19% never changed their passwords. 57% agreed that identity theft can happen in Facebook, and interestingly, 52% disagreed that Facebook is a safe community. The study's first hypothesis stated: The users' level of perception of security severity will positively correlate to the users' safe behavior on social networking sites. Though, according to the scenario that has been tested in the survey, results showed that this hypothesis is not supported due to the very low relationship between the users' perceptions of the severity of consequence, i.e, the level of awareness of the severity of the consequences did not translate to their adopting safe measures while using social media platforms like Facebook.

In a question asking the participants to indicate their opinion on the number of statements related to Facebook security awareness, between 48% to almost 29% showed good awareness towards the security vulnerabilities and risks that the statements clarify. Moreover, only 6% and 2% agreed and strongly agreed, respectively, that Facebook is a safe community and nothing dangerous is going to happen. The study employed theories and studies including Technology Acceptance Model (TAM, Fred D. Davis, 1980s), IT adoption and use (Choi & Chung, 2013; Venkatesh & Bala, 2008), Adoption of Social Media Technologies (Kwon, Park, & Kim, 2014; Rauniar, Rawski, Yang, & Johnson, 2014), Communication privacy management (CPM) theory, also known as information boundary theory, developed by Sandra Petronio in 1991, Social cognitive theory (SCT) developed by the psychologist Albert Bandura in 1986, Influences of Online Privacy Concerns (Yao, Rice, & Wallis, 2007), et cetera.

A study was conducted to examine the influence of gender, Internet use diversity and fluency, and individual differences in need for privacy, beliefs in privacy rights, and generalized self-efficacy upon user concerns about online privacy, "Predicting User Concerns About Online Privacy", by Mike Z. Yao (Department of English and Communication, City University of Hong Kong) and Ronald E. Rice and Kier Wallis (Department of Communication, University of California). The study suggested that the more that people believe in the right to privacy and the more they desire privacy in the physical world, the more they are likely to have online privacy concerns. The results suggest that individuals' beliefs in privacy rights and the dispositional desire for privacy in general are the main factors determining concerns about privacy issues in the specific context of the Internet. The study also found that gender has no direct or indirect

impact on concerns about online privacy. The study also suggested that while Internet use diversity is positively related to Internet use fluency, it has no direct impact upon online privacy concerns.

2.3 THEORETICAL FRAMEWORK

2.3.1 TECHNOLOGY ACCEPTANCE MODEL

Studies have verified the ability of the technology acceptance model (TAM) framework to predict user acceptance of novel technologies. The TAM, which was first introduced by Davis (Fred D. Davis, 1986) in the 1980s, has been shown to be highly predictive of IT adoption and use (Choi & Chung, 2013; Venkatesh & Bala, 2008) and has been very useful in investigating the adoption of social media technologies (Kwon, Park, & Kim, 2014; Rauniar, Rawski, Yang, & Johnson, 2014). Perceived usefulness (PU) and perceived ease of use (PEOU) are the primary factors in adoption (Fred D. Davis, 1986; Sago, 2015). Attitude (ATT), and intention to use (IU) are also two factors of TAM that determine adoption of a technology (Fred D. Davis, 1986; Kwon et al., 2014). Both PU and PEOU are important factors making the TAM a very effective research model to understand and explain IT usage (Chau, 2001; Sago, 2015). Davis (F. D. Davis, 1989) defined PU as “the degree to which a person believes that using a particular system would enhance his or her job performance” and PEOU as “the degree to which a person believes that using a particular system would be free of effort”.

2.3.2 COMMUNICATION PRIVACY MANAGEMENT THEORY

Communication privacy management (CPM) theory, also known as information boundary theory, developed by Sandra Petronio in 1991 (Petronio, 1991) and suggested that "individuals believe they own their private information and have a right to control whether the information is disclosed as well as to whom it is disclosed" (Kennedy-Lightsey, Martin, Thompson, Himes, & Clingerman, 2012; Petronio, 1991, 2004). CPM theory explains how people believe in the ownership of their private information and how they usually miss the part that disclosing any information to others could make them vulnerable in a way or another. Petronio (Petronio, 2004) explains the importance of controlling our private information and that once we share such information with others we do not really own the The Paradox of Social Media Security: Users' Perceptions versus Behavior information anymore and cannot decide what happens to the information then, "when people disclose to each other, they essentially link others into a privacy boundary" (Petronio, 2004). However, the theory also shows how people tempted to develop their own privacy rules based on five criteria, which are: "(1) culture, (2) gender, (3) motivations that people have concerning privacy, (4) contextual constraints, and (5) risk–benefit ratio" (Petronio, 2004).

2.3.3 SOCIAL COGNITIVE THEORY

Social cognitive theory (SCT) was developed by the psychologist Albert Bandura in 1986 and is based on how people learn by observing others. It holds that portions of an individual's knowledge acquisition can be directly related to observing others within the context of social interactions, experiences, and outside media influences. The theory is used in a number of

sectors like psychology, education, business, health communication, and information security. SCT "founded in an agentic perspective" to provide full understanding on how human psychological and social responses work according to three reciprocal factors; which are: (1) cognitive (personal), (2) behavioral, and (3) environmental factors (Bandura, 1991, 2001). Based on SCT, observation – which individuals learn through - consists of four processes: (1) attentional, (2) retention, (3) production, and (4) motivational (Bandura, 2001), and that the individual's ability of observation proportionally correlates with the individual's level of self-efficacy (Bandura, 2001; Chai, Bagchi-Sen, Rao, Upadhyaya, & Morrell, 2009).

2.3.4 COGNITIVE DISSONANCE THEORY

Festinger's (1957) cognitive dissonance theory suggests that we have an inner drive to hold all our attitudes and behavior in harmony and avoid disharmony (or dissonance). This is known as the principle of cognitive consistency. When there is an inconsistency between attitudes or behaviors (dissonance), something must change to eliminate the dissonance.

TAM is applied here, as the major objective of this study is to analyse how much the users are changing over to the digital realm for financial transactions. CPM theory has been applied to analyse the thought processes with respect to personal privacy as well as privacy in the digital sphere. SCT and Cognitive Dissonance Theory have been applied to observe the influences of the others' beliefs and practices on an individual's actions and thought processes.

CHAPTER 3

METHODOLOGY

3.1 INTRODUCTION

This chapter contains the objectives of this study and methodology adopted to evaluate these objectives. This project uses qualitative methods to collect data and draw conclusions based on the same.

3.2 OBJECTIVES

- To determine the scale of awareness that currently exists in various digital spheres among the populace of Thiruvananthapuram
- To determine the impact of factors like age, gender, and financial position on the digital and cyber awareness
- To find correlations between socio-economic-demographic conditions and scale of awareness in internet & online banking users, frequency of usage, scale of dependency.
- To determine the actual amount of awareness, in contrast to each individual's self-estimated level of knowledge
- To validate the frequency and mode of usage of the digital cash transaction

3.3 METHODOLOGY

This study follows a qualitative method. Our survey method is a questionnaire method. It is a set of prepared questions which are distributed to a number of participants all from Trivandrum. Information would partly be collected online through Google Forms, and partly in person with fill-in forms. The data in the fill in forms were then transferred manually to Google Forms for easy analyses. The participants are selected using samples of target population and the purpose. The factors of which the awareness of the group would be measured, include potential risks, usage permissions, terminologies, cookies, and password protection, and Survey questions are framed based on the same. The first part of the questionnaire consists of demographic details while the latter contains questions concerned with objectives of the study. Collected data was organised into spreadsheets which were then organised into charts and graphs to study the data in relation with the theory applied. Percentage analysis of the data collected was used as a tool of analysis. Bar diagrams and pie charts were also used for the presentation of data. Participants of each group will be selected based on Cluster Sampling, so as to maximize the chances of representation of different economic groups and occupation. The data is classified, analysed, and conclusions drawn.

CHAPTER 4

ANALYSIS & INTERPRETATION

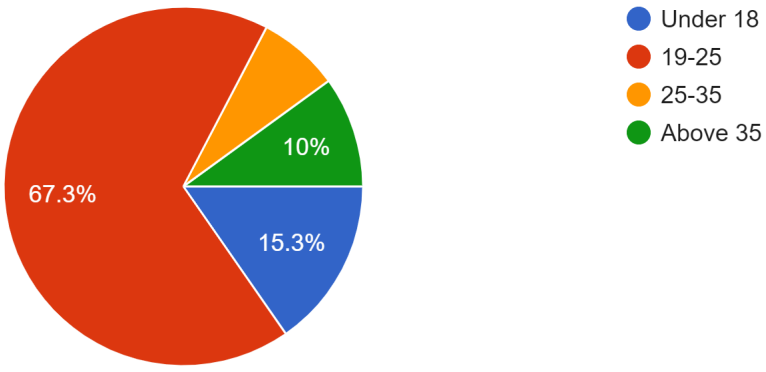
4.1 INTRODUCTION

This chapter contains the analysis and interpretation of the data collected through the survey. The survey entries of 150 individuals have been collected and analysed. The results were correlated with the applied theory to draw conclusions.

4.2 RESULTS AND DISCUSSIONS

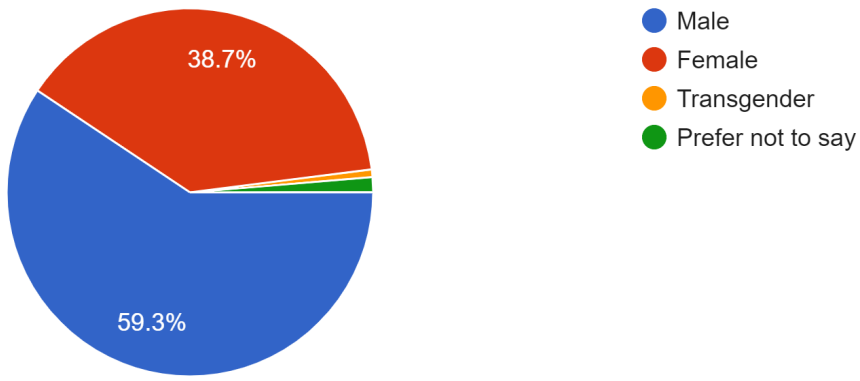
4.2.1 RESULTS OF SURVEY

Figure 4.1: Age category of respondents.



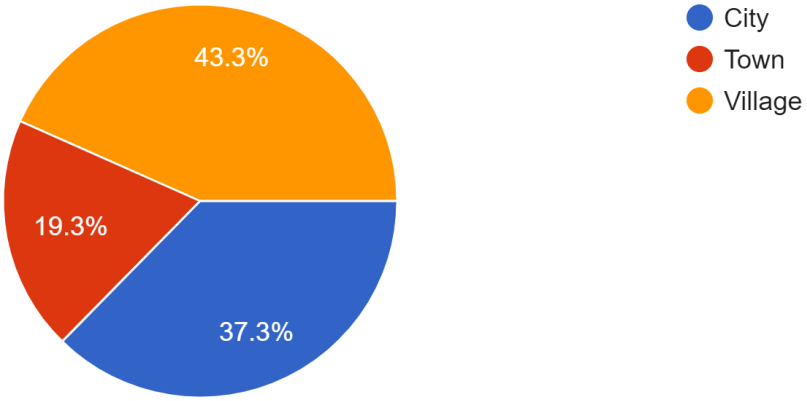
RESULT: Respondents are categorised into four age groups - Under 18, 19 - 25, 25 - 35, Above 35. The total number of respondents was 150 - 15.3% (23) from Under 18, 67.3% (101) from 19 - 25, 7.3% (11) from 25 - 35, and 10% (15) from Above 35.

Figure 4.2: Gender of respondents.



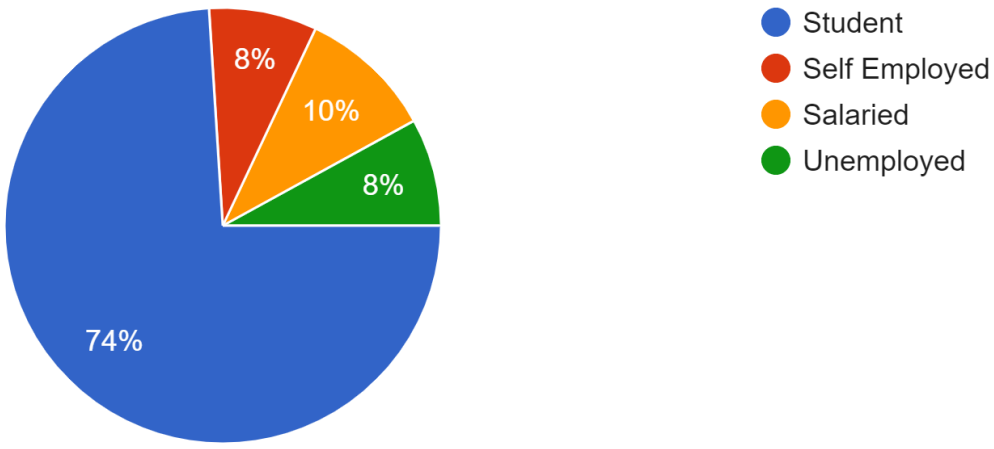
RESULT: Among the total number of respondents, 59.3% (89) are Male, 38.7% (58) are Female, 1.3% (2) Prefered not to say, and 0.7% (1) identified themselves as Transgender.

Figure 4.3: Location of respondents



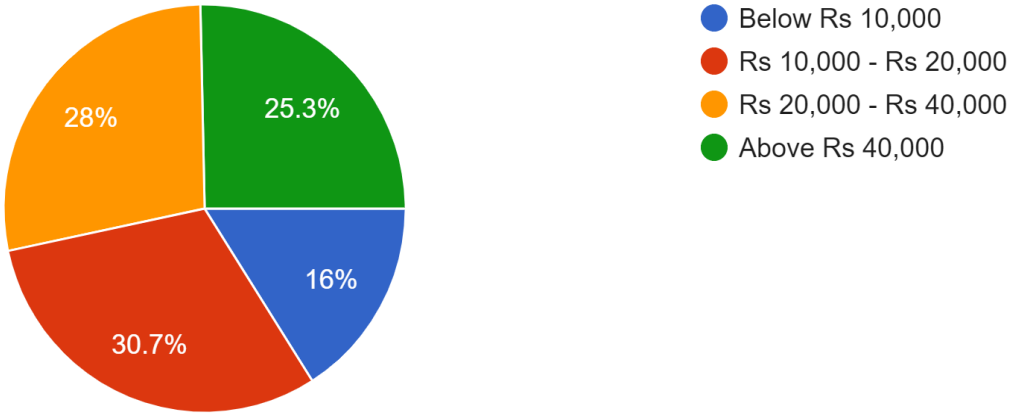
RESULT: 43.3% (65) of respondents are from Village, 37.3% (56) from City, and 19.3% (29) from Town.

Figure 4.4: Occupational status of respondents



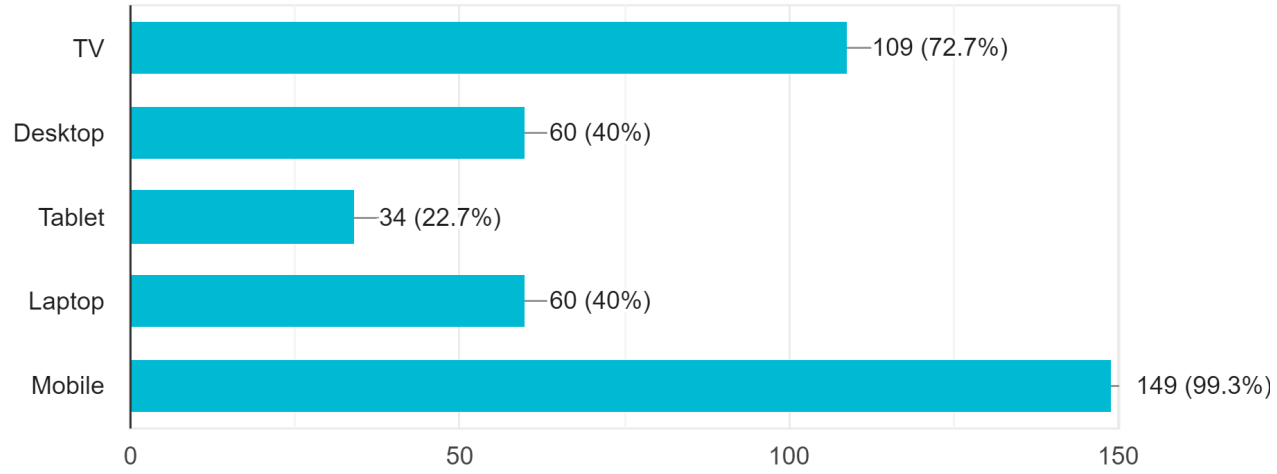
RESULT: Students formed 74% (111), Salaried 10% (15), Self Employed 8% (12), and Unemployed 8% (12), of the total respondents.

Figure 4.5: Monthly family income status of respondents



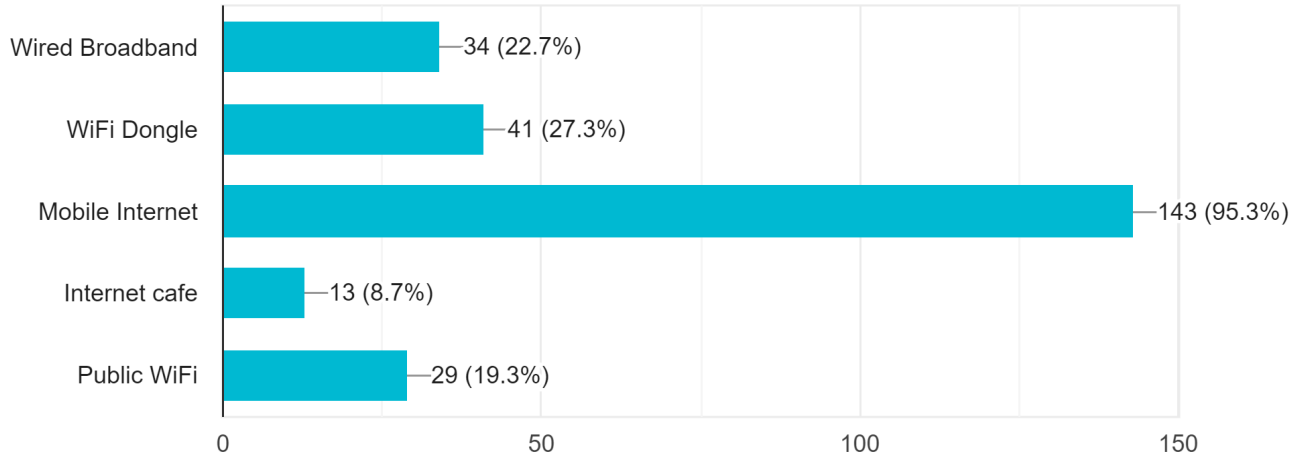
RESULT: The monthly family income of the respondents was found to be Below 10,000 for 16% (24), between 10,000 and 20,000 for 30.7% (46), between 20,000 and 40,000 for 28% (42), and Above 40,000 for 25.3% (38).

Figure 4.6: Gadgets owned by respondents



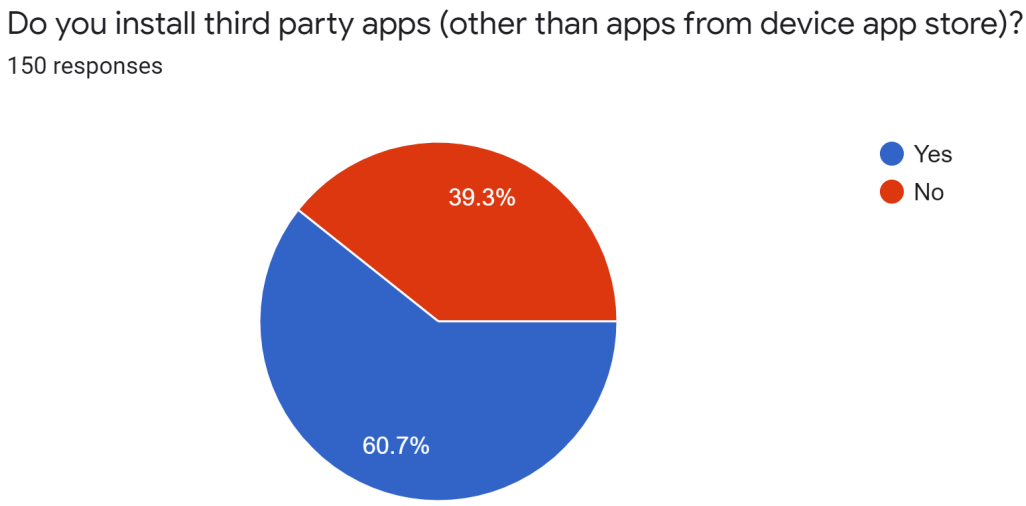
RESULT: 99.3% owned Mobile Phones, 40% owned Laptops, 22.7% owned Tablets, 40% owned Desktops, and 72.7% owned Television.

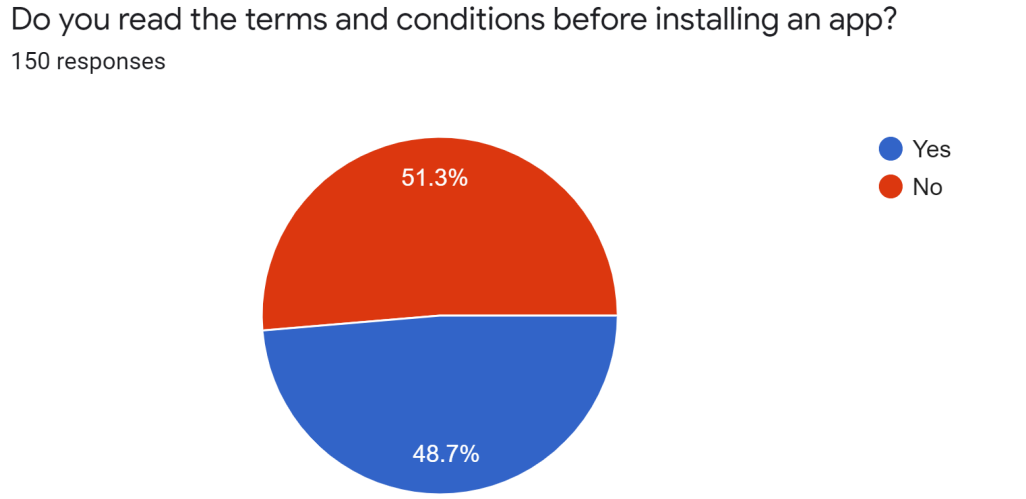
Figure 4.7: Mode of access of internet

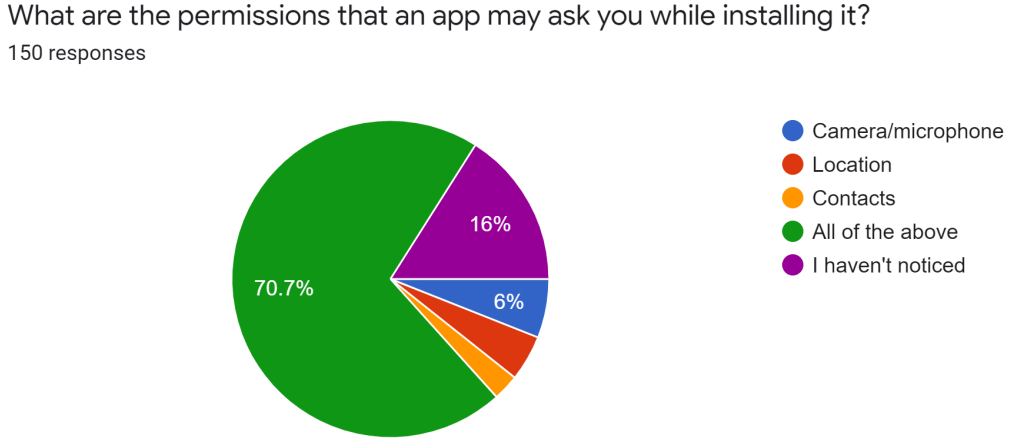


RESULT: 22.7% used Wired Broadband, 27.3% WiFi dongle, 95.3% mobile internet, 8.7% relied on Internet Cafes, and 19.3% on Public WiFi.

Figures 4.8, 4.9, 4.10: Third Party Apps and Permissions

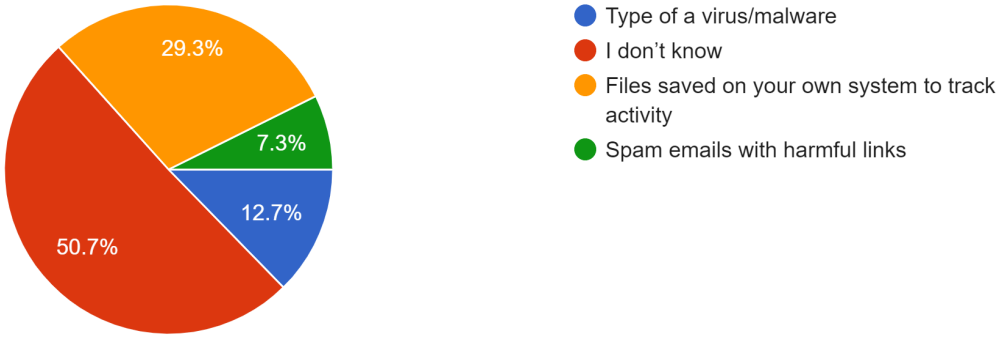






RESULT: 60.7 % of respondents install third party applications to their devices, which if done without taking necessary security steps, can potentially put the user at risk of being victim to cyber crimes and virus attacks. Only 51.3% of the respondents read the permissions and terms and conditions of an application before installing it, which also puts them under potential risk of exploitation and information theft. 16% of all respondents 'have not Noticed' what all permissions are asked by applications while they are being installed. 13.3% of all respondents believe that only Camera or Microphone or Contact or Location access permissions are seeked; 70.7% rightly marked that all permissions may be asked.

Figure 4.11: Awareness about Internet Cookies



RESULT: More than half of the respondents (50.7%) felt that they do not know about what Internet Cookies are. More interestingly, 20% of the respondents believed that Cookies are either a type of a virus/malware (12.7%) or spam emails with harmful links (7.3%). This data suggests that one in five people think that they know about what cookies are, but in reality do not know what it is. Only 29.3% rightly know what Cookies are.

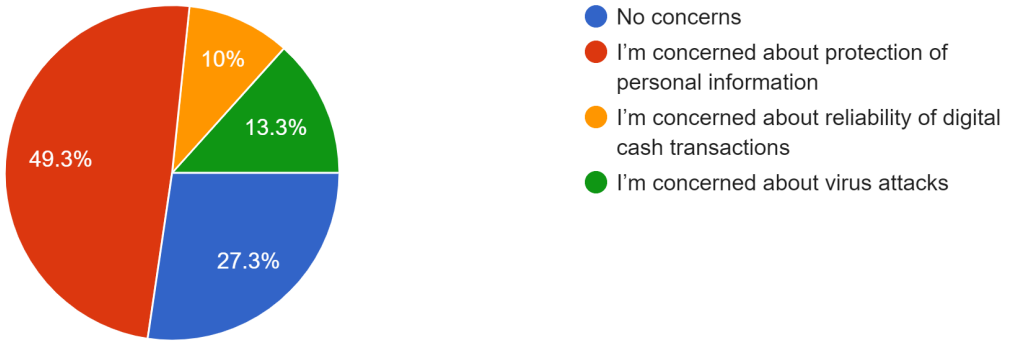
Figure 4.12, 4.13, 4.14: Personal Concerns

Do you ever feel worried about using the Internet?

150 responses

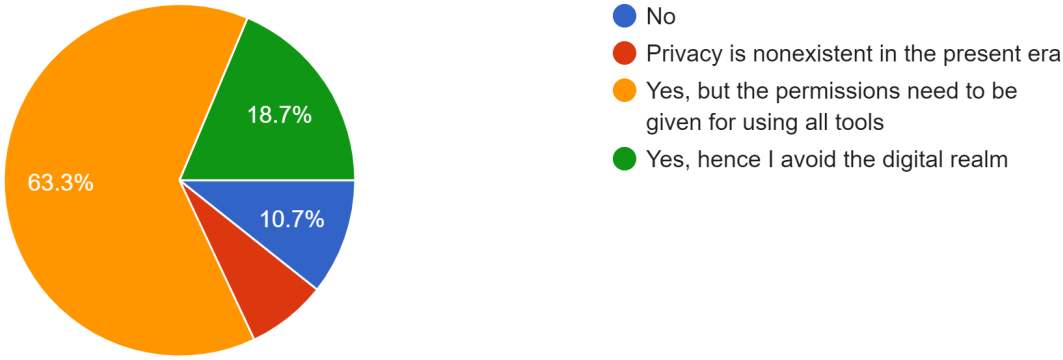
What concerns you most while using the Internet?

150 responses



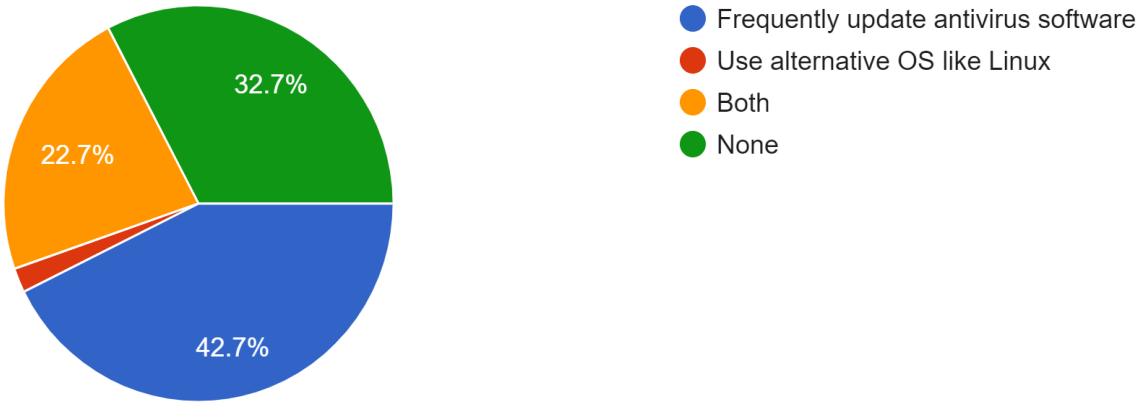
Is information security and privacy important to you?

150 responses



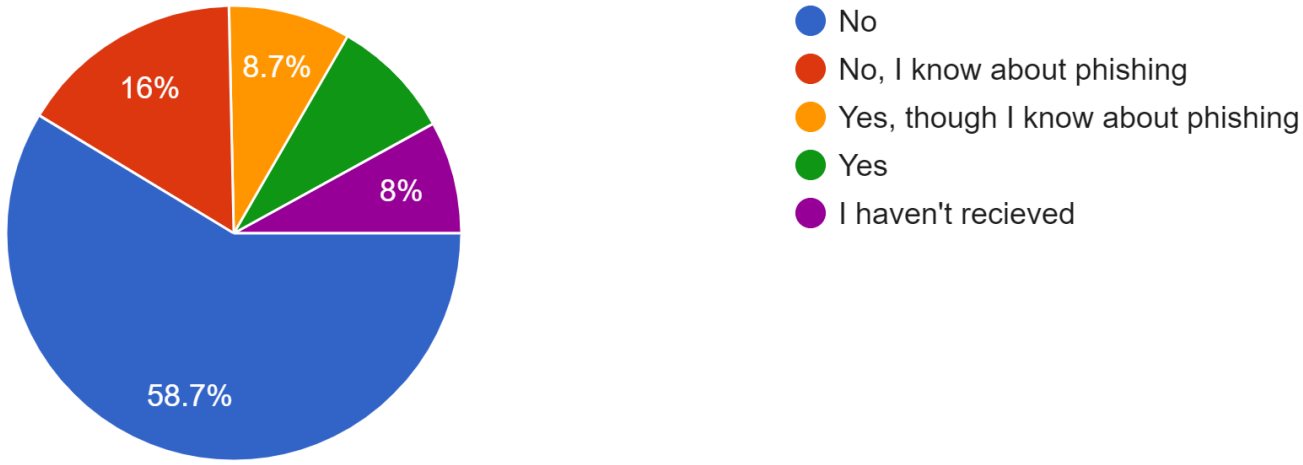
RESULT: 40.7% of all respondents are not worried about using the internet, whereas 23.3% take measures against privacy threats and still feel that they might be insufficient. 14.7% are worried, while 21.3% of all respondents feel confident that they take all the necessary security steps. Almost half (49.3%) are concerned about protection of their personal information while accessing the internet, 13.3% about virus attacks, and 10% about reliability of digital cash transactions. 10.7% of all respondents do not feel that information security and privacy is important to them. 63.3% feel that giving app permissions is a risk to their privacy, but are helpless as it is required to be able to be using all the tools. 18.7% respondents avoid the digital realm as much as possible as they feel that the medium is not secure. 7.3% feel that privacy is a myth - it does not exist in the digital era.

Figure 4.15: Security Steps



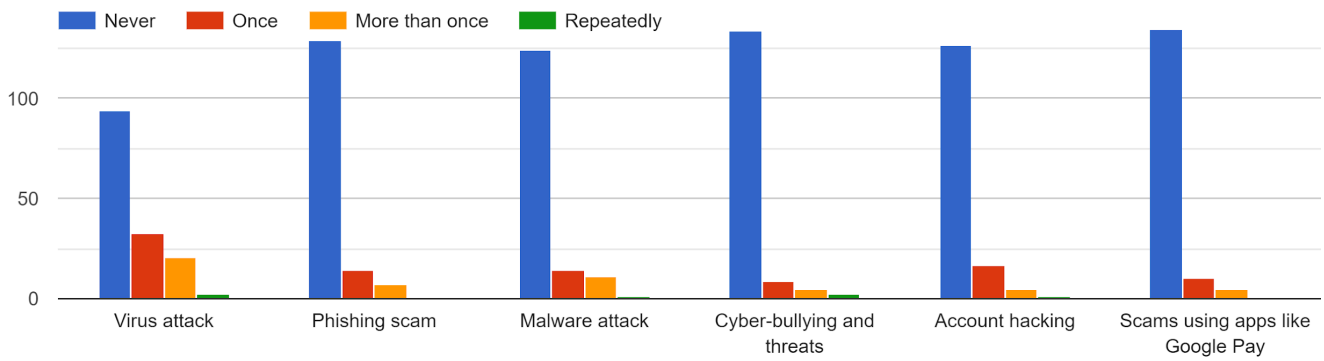
RESULT: 42.7% of the respondents frequently update their antivirus software, 2% use alternate OS like Linux, and 22.7% do both. A staggering 32.7% does neither, putting themselves at great risks of information theft and other cyber attacks, as the above mentioned are the two of the best steps of defending & troubleshooting the problem in occurance of a cyber attack.

Figure 4.16: Phishing awareness - Rate of responding to phishing messages



RESULT: A healthy 74.7% (58.7% + 16%) did not respond to phishing mails. 8.7% are unaware of phishing, 8.7% have responded to such mails though they now know about it, and 8% have not received such messages.

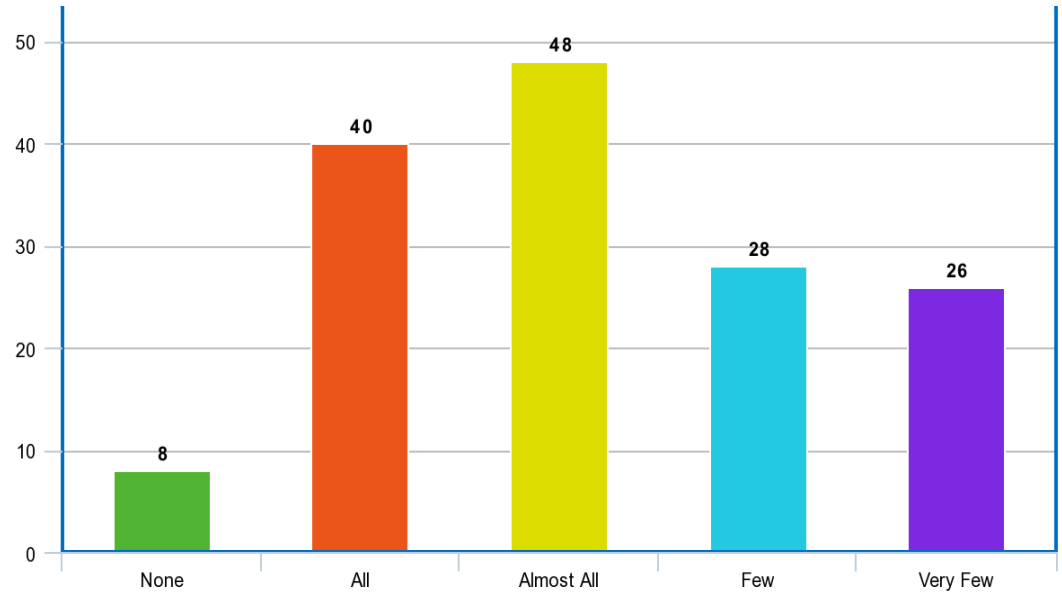
Figure 4.17: Rate of being victim to attacks



RESULT: 2 respondents were repeatedly victim to virus attacks, and 2 repeatedly faced cyber bullying and threats. 15 respondents have been victim to scams using apps using Google Pay at least once. 56 respondents have been victim to virus attacks at least once. All cyber threats had

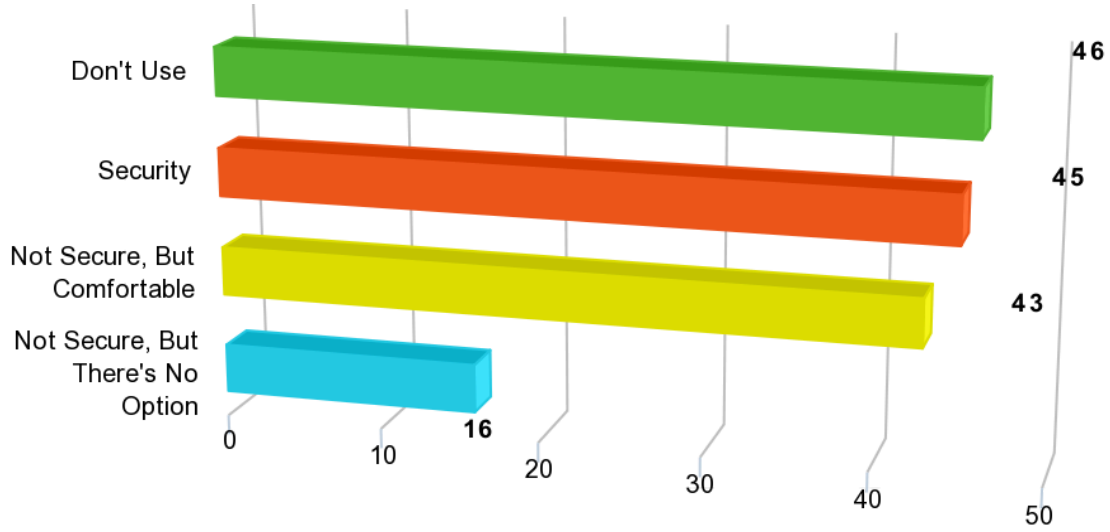
more than two-third of the whole number of respondents respond that they have never been a victim of it, other than virus attacks. 10% of all respondents fell victim to money-related scams using apps like Google Pay, putting into question the level of awareness of all the potential threats and the possibilities of the digital sphere among its users, which puts all of their financial wealth under a great risk. 14% of all have fallen for phishing attempts, 50% of the subset having been scammed repeatedly. 16.6% have faced malware attacks at least once. 14.6% have had their account hacked at least once.

Figure 4.18: Usage of same passwords



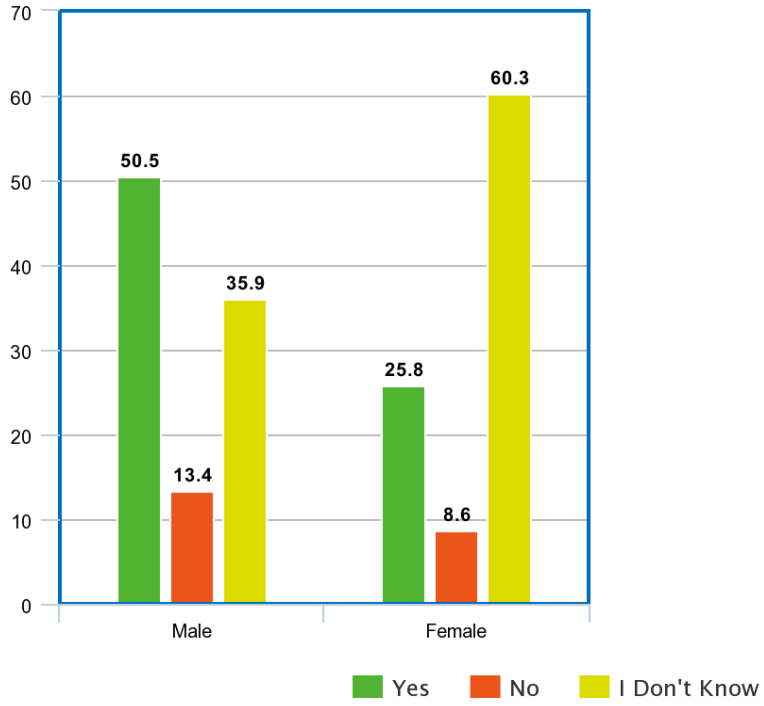
RESULT: 26.6% (40/150) use the same password for all the websites, which puts one at a serious point of risk. Adding the figure to the 48 who keep the same password for almost all the sites, a cumulative 65% of the respondents are at serious risk of being victim to cyber attacks including hacking. Only 8 of the 150 keep unique passwords for all sites.

Figure 4.19: Digital Cash Transactions - Reasons for use



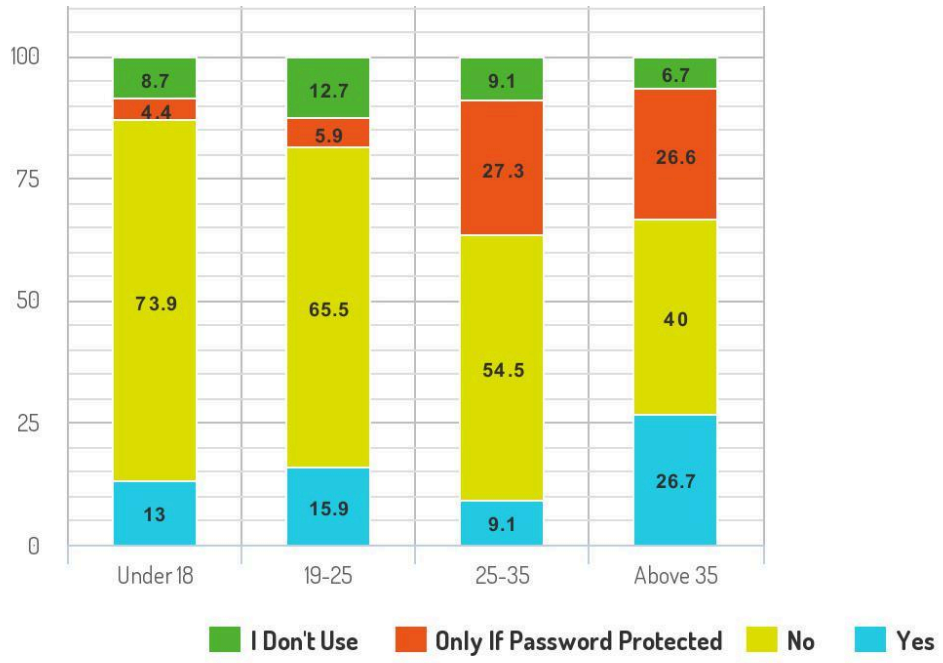
RESULT: 28.6% respondents chose digital cash transactions as they found that it is comfortable, though they believe it is not secure, whereas 30% chose it for its security. 30% do not use digital cash transactions. 11% use digital cash transactions even though they feel it is not secure, but because they feel that there is no other option. 59 of the 104 who use digital cash transactions feel that it is not secure.

Figure 4.20: Privacy from Internet Service Providers



RESULT: To the question as to whether internet service providers see the online activities when using private browsing, a wide difference was observed in the terms of gender while analysing the data. 50.5% of males thought that the activities are visible, as opposed to 25.8% among females. Though the percentage of males who felt that the service providers will not be able to see the activities is slightly higher than that of the females, the percentage of females who felt that they did not know about it, stood at 60.3%, in contrast to 35.9% among males.

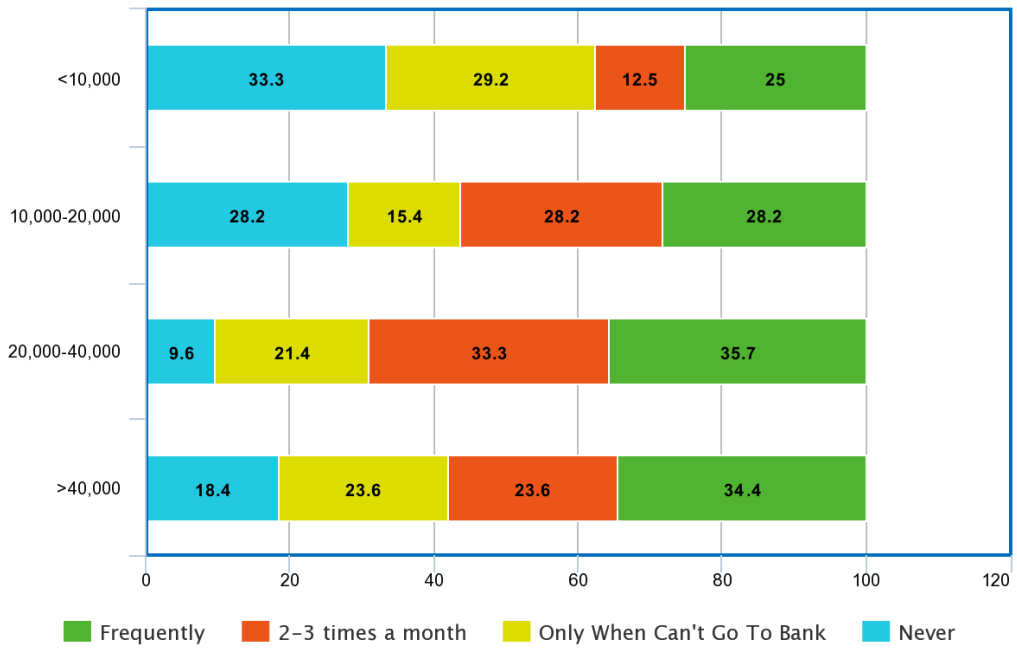
Figure 4.21: Usage of public WiFi digital cash transactions - Age Group Analysis



RESULT: The percentage of respondents who responded that it is not safe to use public WiFi for digital cash transactions, is at a healthy 73.9% and 65.5% in the Under 18 and 19-25 age groups, but the figure fals to 54.5% and 40% in the 25-35 and Above 35 categories, suggesting that the awareness is more among the youth. At the same time the percentage of respondents who believe that public WiFi is safe for financial transactions provided it is password protected, also went up from a 4.4% in the Under 18 section and 5.9% in the 19-25 section, to a staggering 27.3% and 26.6% in the 25-35 and Above 35 sections. There seems to be a noticeable difference between the responses of the former two sections over the latter two, with all figures suggesting that the former two has a better sense of awareness over the latter. Keeping in mind that the users are

more in the latter sections in terms of digital cash transactions, it is a dangerous trend that the most frequent users are the most vulnerable and exploitable. Over 26% of the respondents in the Above 35 section believe that it is completely safe to use public WiFi for cash transactions - over 50% of the respondents in the category thus believe that there is nothing wrong in using public WiFi for digital cash transactions.

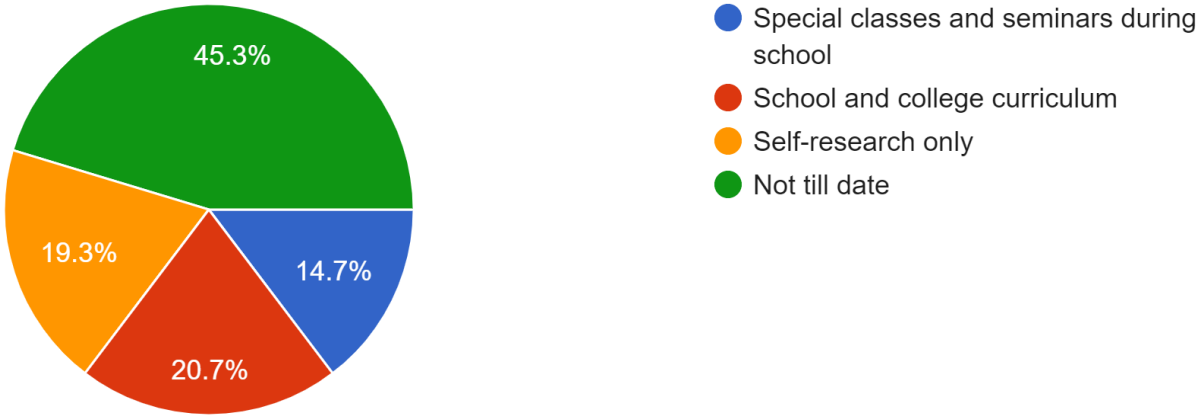
Figure 4.22: Correlation between monthly income and usage of digital cash transaction



RESULT: Digital cash transaction use is maximum in the economic class with a monthly salary between 20,000 INR to 40,000 INR. For families with lesser income, the percentage of respondents who never use digital cash transactions is higher (28.2% for 10,000 INR - 20,000

INR class and 33.3% for the below 10,000 INR class) with respect to the 20,000 to 40,000 INR class which has only 9.6%. The same class has 35.7% using digital realm frequently, and the >40,000 class also features 34.4% of its respondents in the same in terms of frequency.

Figure 4.23: Sources of Cyber Security and Digital Awareness



RESULT: The study lays bare that the majority of the respondents at 64.6% have not received any awareness classes or instructions as part of their school or college curriculum, or from special classes and seminars. 45.3% have not received awareness in any sort, whereas 19.3% have knowledge on the same only thanks to their self-research. 14.7% have received special classes and seminars on the topic, whereas only 20.7% (roughly one-fifth) of the total respondents received awareness on the topic as part of their school and college curriculum. This shows a need for the curricula to incorporate the knowledge on the same.

CHAPTER 5

CONCLUSION

5.1 CONCLUDING REMARKS

Corresponding to increased smartphone penetration along with cheap internet availability, the presence of man in the digital realm is becoming more as the days go by. Entertainment, work, studies, and more importantly, even cash transactions, have gone digital. Online payment apps and transaction software are being used in a very high frequency, and the spread of the same is as rapid as it can be. The individuals of higher age groups still tend to show a reluctance in following the same, and heavily doubt its credibility and trustworthiness, but the younger generation has completely embraced the digital sphere, as it is way more comfortable, time-saving, and effort saving. The ease of use also makes it very easy to adapt to. Though the use of the same has seen a strong growth, however, the levels of awareness - the terms, risks, challenges, security measures, et cetera - has been observed to be lower than desirable, especially in the age classes of above 25. The research project examined the levels of awareness in the public, and also analysed the various factors that could potentially affect the gauge of the same.

Contrary to common perception, the studies figures suggested that the number of users of digital cash transactions does not depend on the gender of the user. But figures also seem to suggest that females believe that the Internet Service Providers do not see one’s private browsing data, over males. The study also revealed a possible correlation between the monthly income of a

household and their usage of digital transactions. The usage frequency was found to be higher in the more economically stabler households, but hit its maximum in the households with a monthly income of 20,000 INR to 40,000 INR. Almost all users accessed the internet through their mobile phones the most.

Only around half of the users are aware of the application permissions that they grant while installing software and applications, and a large percentage of well above a half of the whole sample space installed third party applications. Around one third of the respondents have no or incomplete knowledge about the permissions that an app may ask for. This clearly shows that the knowledge of most of the internet users is insufficient to ensure that they are safe while using the various avenues of the technology, which can be a great threat to personal privacy and more so when it comes to the realms of using digital cash transactions.

In connection with the awareness of internet terminology, the study attempted to validate the awareness of the public by discussing cookies. More than half of the respondents felt that they do not know about what Internet Cookies are. More interestingly, one fifth of the respondents believed that Cookies are either a type of a virus/malware or spam emails with harmful links, which clearly signifies a dangerous fact - that people think that they know what cookies are, but in actuality are unaware. This data thus suggests that one in five people are completely misinformed as to their presence and practices in the digital media. People who think that they know about the internet but do not actually know about it, may potentially be at a higher risk of falling prey to cyber attacks.

One in four people take measures against privacy threats and still feel that they might be insufficient. Almost half of the respondents were concerned about protection of their personal information while accessing the internet, around a one tenth about virus attacks and about reliability of digital cash transactions, whereas a small percentage, roughly one tenth, went to the extent of denoting that they feel that privacy is a myth and that it does not exist in the digital era.

Less than a quarter of the respondents are aware of alternate Operating Systems like Linux, and one third of them, do not even update their antivirus software. A healthy three of four respondents did not respond to phishing mails, which is a positive statistic as almost three fourth of the respondents are aware of the potential risks. At the same time, it is alarming to notice that almost one in ten have responded to such mails though they now know about it. One tenth of all respondents fell victim to money related scams using apps like Google Pay, putting into question the level of awareness of all the potential threats and the possibilities of the digital sphere among its users, which puts all of their financial wealth under a great risk. The mere fact is threatening that the users are seldom aware of the potential threats that could take away all their hard-earned money. Only 8 of the 150 respondents keep unique passwords for all sites, which is yet another alarming fact, which shows how less the precautionary and prevention steps are taken by the various users.

One in ten respondents use digital cash transactions even though they feel it is not secure, but because they feel that there is no other option. 59 of the 104 who use digital cash transactions

feel that it is not secure. One third of the respondents chose digital cash transactions as they found that it is comfortable, though they believe it is not secure, whereas another one third chose it for its security. The percentage of respondents who believe that public WiFi is safe for financial transactions provided it is password protected, also went up five times from the Under 18 and 19-25 sections, to a staggering one third in the 25-35 and Above 35 sections. There seems to be a noticeable difference between the responses of the former two sections, over the latter two, with all figures suggesting that the former two has a better sense of awareness over the latter. Keeping in mind that the users are more in the latter sections in terms of digital cash transactions, it is a dangerous trend that the most frequent users are the most vulnerable and exploitable.

Considering the set of all respondents more than half have not received any awareness classes or instructions as part of their school or college curriculum, or from special classes and seminars. A half have not received awareness in any sort, whereas almost one fifth have knowledge on the same only thanks to their self-research. This strongly calls for subjects related to cyber and digital spheres - online money transactions, potential risks, cyber crimes, security measures, internet netiquette et cetera - to be included in the school and college curricula, as it has become an inevitable skill in the information era.

From the use of TAM, we can observe that a percentage of people in the above 35 category do not use digital cash transactions. But among the ones using, it is found that over half of the respondents in the category believe that there is nothing wrong in using public WiFi for digital

cash transactions. The Cognitive Dissonance Theory can be used to analyse the trend in internet users believing that they know what internet cookies are, though they do not know about it. Over 9 in 10 respondents feeling that privacy is important to them while being in the digital domain in various degrees, is an implication of the CPM Theory. SCT denotes that the percentage of internet users completely aware of the risks and threats of the digital realm, might go up with time.

5.2 SCOPE FOR FUTURE STUDY

On the basis of this study, we would like to make certain recommendations for further research in the areas of digital security awareness. Further studies can be carried out in different geographical locations to collect information. Analytical studies can be done at a later stage to gauge the awareness levels then, which can then be compared and analysed with the current data. Studies can also be done to measure the impact of classes and seminars that are taken on the topic to school children and college students. It can be studied as to whether incorporating the knowledge into the syllabi and curricula would make a positive change. With the debate of Right to information v/s Right to privacy being active as ever, the public perception of digital security and digital privacy can also be studied. The influence of a group of people around an individual on the awareness of the person can also be a point of further research. Research can also be done to calculate precisely as to how much of a risk are individuals in, if they do not possess a basic awareness of the internet and its use cases.

5.3 LIMITATIONS OF THE STUDY

- Total number of respondents participating in the survey is very limited.
- Study is conducted in a limited geographical area. For a broader analysis study could be extended across the state.
- The number of respondents in the above 35 age class needs to be more to make the outcomes evident.
- Some respondents were not interested in answering the questionnaire.
- The study being purely quantitative, could not exactly tap into the details of the depth of awareness that each individual possesses.
- Study having collected information primarily through Google Forms, had to not consider multiple entries thanks to spamming and random selections.
- The dependence of one's awareness on the awareness of the people around them, could not be established or any interesting relationship proven.

REFERENCES

1. Sultan, Ahmad. (2017) Improving Cybersecurity Awareness in Underserved Populations. Retrieved from: https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC_Underserved_Populations.pdf

2. Kumar, Shubha & Kumar, Uday. (2015) Present scenario of cybercrime in INDIA and its preventions. Retrieved from: https://www.ijser.org/paper/Present-scenario-of-cybercrime-in-INDIA-and-its-preventions.html

3. Kortjan, Noluxolo & Solms, Rossouw von. (2014) A conceptual framework for cyber-security awareness and education in SA. Retrieved from: https://www.researchgate.net/publication/290139259_A_conceptual_framework_for_cyber_security_awareness_and_education_in_SA

4. Tsohou, Aggeliki & Kokolakis, Spyros & Karyda, Maria & Kiountouzis, Evangelos. (2014) Investigating information security awareness: research and practice gaps. Retrieved from: https://www.researchgate.net/publication/220449896_Investigating_Information_Security_Awareness_Research_and_Practice_Gaps?enrichId=rgreq-9d22fb4e3d66db1bedbddd3700f8ec3d-XXX&enrichSource=Y292ZXJQYWdlOzIyMDQ0OTg5NjtBUzo5ODU1NTc5NjY1NjE0NkAxNDAwNTA4OTQxODI5&el=1_x_3&_esc=publicationCoverPdf

5. Salni, Hemraj. (2006) A Study on Cyber Crime in India. Retrieved from: https://www.researchgate.net/publication/241689595_A_Study_on_Cyber_Crime_in_India?enrichId=rgreq-a70e165837f76589473ce941fd18a7e2-XXX&enrichSource=Y292ZXJQYWdlOzI0MTY4OTU5NTtBUzo0NzMxNzM1MjAwNjQ1MTJAMTQ4OTgyNDc2NjY2NA%3D%3D&el=1_x_3&_esc=publicationCoverPdf

6. Senthilkumar, K & Easwaramoorthy, Sathishkumar (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. Retrieved from: https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043

7. Kritzinger, Elmarie. CYBER SECURITY AWARENESS AND EDUCATION RESEARCH. Retrieved from: http://eagle.unisa.ac.za/elmarie/images/Pdf/r1.pdf

8. Iqbal, Juneed. (2017) Cybercrime in India: Trends and Challenges. Retrieved from: https://www.researchgate.net/publication/322245372_Cybercrime_in_India_Trends_and_Challenges

9. PTI (2016). Cybercrime in India up 300% in 3 years: Study. Economic Times. Bennett, Coleman & Co. Ltd. Retrieved from: https://economictimes.indiatimes.com/tech/internet/cybercrime-in-india-up-300-in-3-years-study/articleshow/53858236.cms

10. Hasan, S. (2010). Mass Communication Principles and Concepts (2nd edition). Daryaganj, New Delhi: CBS Publishers & Distributors Pvt Ltd.

11. Das, Shaswati (2017). 11,592 cases of cyber crime registered in India in 2015: NCRB. LineMint. HT Media Ltd. Retrieved from: https://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html

12. Kumar, K.J. (1994). Mass Communication in India (4th edition). Mumbai, Maharashtra: Jaico Publishing House.

13. Krishnan, Varun, B. (2019). Where does Kerala's Internet Access Stand Compared to Other States.The Hindu. Retrieved from: https://www.thehindu.com/news/national/where-does-kerala-internet-access-stand-compared-to-other-states/article29910398.ece

14. Venkatesh, Thong J.Y.L & Xu, X. (2003).User Acceptance Of Information Technology: Toward a Unified View. MIS Quarterly Journal. Vol. 27 No. 3, pp. 425-478. Retrieved from: www.vvenkatesh.com/wp-content/upload/2016/01/2016_JAIS_Venkates-et-al-UTAUT.pdf

15. Venkatesh, Thong J.Y.L. & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly Journal. Vol. 36, No.1, pp. 157-178. Retrieved from: https://pdfs.semanticscholar.org

16. Williams, A., Noorin, M.I. & Holmes, C.M. (2018). The scientifically proven best ways to be happy. Retrieved from: www.qz.com

APPENDIX 1

CYBER & DIGITAL SECURITY AWARENESS IN THIRUVANANTHAPURAM

QUESTIONNAIRE

We, students of BJMC, are conducting a study on cyber and digital awareness among the people of Trivandrum. This is only for academic purposes.

1. Which option describes you?

   A. Male
   B. Female
   C. Transgender
   D. Other
   E. Prefer Not To Say

2. Location:

   A. City
   B. Town
   C. Village

3. Age:

   A. Below 18
   B. 18-25
   C. 25-35
   D. Above 35

4. Which option describes you?

   A. Student
   B. Self Employed
   C. Salaried
   D. Unemployed

5. Which of these describes your monthly income?

   A. Below Rs 10,000
   B. Rs 10,000 - Rs 20,000
   C. Rs 20,000 - Rs 40,000
   D. Above Rs 40,000

6. Tick the gadgets that you own?

TV	⬜	Desktop	⬜	Tablet	⬜
Laptop	⬜	Mobile	⬜		

7. How do you access the internet?

Wired Broadband	⬜	WiFi Dongle	⬜		
Mobile Internet	⬜	Internet cafe	⬜	Public WiFi	⬜

8. How often do you use online money transfer?

A. Frequently
B. 2-3 times a month
C. Only if I cannot go to the bank
D. Never

9. For how many platforms do you use the same password?

A. All
B. Almost All
C. Few
D. Very Few
E. None

10. Do you use a public Wi-Fi network (eg: airport, cafe) for online banking?

A. I do not use online banking
B. Only if password protected
C. No
D. Yes

11. Why do you use Digital cash transactions?

A. do not use
B. Security
C. Not secure, but comfortable
D. Not secure, but there’s no option
E. Other:

12. Do you think internet service providers see online activities when using private browsing?

A. Yes
B. No
C. I do not know

13. Do you install third party apps (other than apps from the device app store)?

Yes No

14. Do you read the terms and conditions before installing an app?

Yes No

15. What are the permissions that an app may ask you while installing it?

A. Camera/microphone
B. Location
C. Contacts
D. All of the above
E. I have not noticed

16. What are cookies on the internet?

A. I do not know
B. Spam emails with harmful links
C. Files saved on your own system to track activity
D. Type of a virus/malware

17. Do you ever feel worried about using the Internet?

A. No
B. I know security threats exist, but I'm not concerned as I take preventative measures
C. I take measures against security threats; however, I'm concerned as they are insufficient
D. Yes

18. What concerns you most while using the Internet?

A. No concerns
B. I'm worried about protection of personal information
C. I'm worried about reliability of digital cash transactions
D. I'm worried about virus attacks

19. Is information security and privacy important to you?

A. No
B. Privacy is nonexistent in the present era
C. Yes, but the permissions need to be given for using all tools
D. Yes, hence I avoid the digital realm

20. Which of the following steps do you take?

A. Frequently update antivirus software
B. Use alternative OS like Linux
C. Both
D. None

21. Have you responded to emails or SMS from reputable companies giving you offers and prizes?

A. No
B. No, I know about phishing
C. Yes, though I know about phishing
D. Yes
E. I have not received

22. Have you ever been victim to: (Tick Appropriate Options)

	Never	Once	More than once	Repeatedly
Virus attack				
Phishing scam				
Ransomware/ Malware attack				
Cyberbullying				
Account hacking				
Scams using apps like Google Pay				

23. Have you ever attended classes on Cyber Security and Digital Awareness?

A. Special classes and seminars during school
B. School and college curriculum
C. Self-research only
D. Not till date