

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Rishikesh Ram Shankaran
184509IVCM

**COMPARATIVE STUDY ON PERCEPTION
AND PREPAREDNESS OF A USER
TOWARDS CYBERSECURITY THREATS IN
IOT AND MOBILE DEVICES.**

Master's thesis

Supervisor: Prof. Stefan Sütterlin

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Rishikesh Ram Shankaran

19.05.2020

Abstract

Over the years, there has been substantial growth in the amount of information processing devices that can interact with one another, especially small handheld devices like mobiles, tablets, and different IoT devices. Smart devices communicate with mobile devices like tablets or smartphones that allow users to control these appliances remotely. These devices can also interact with the smart grid, responding to signals that give users with reminders to use these devices. The smart devices market is discerning prompt growth day by day, but the lack of knowledge on these device vulnerabilities are deficient. Cybersecurity is a global phenomenon representing a complex socio-technical challenge. Although cybersecurity is one of the most critical challenges faced today, visibility and public awareness remains limited. Nearly everybody has heard of risks in different devices. However, the urgency and behavior of persons do not reflect a high level of knowledge. Understanding the user's perception of different IoT or mobile device threats would help to streamline the focus areas to mitigate the incidents. In this research, we address this gap and focus on investigating the comparative analysis on the preparedness and perception of a user towards different privacy or security concerns they face in IoT and mobile devices.

The thesis is in English and contains 67 pages of text, 6 chapters, 15 figures, 52 tables.

Annotatsioon

Võrdlev uurimus kasutaja tajumisse ja valmidusse küberohutuse ähvardustesse IoT ja mobiilseadmete

Aastate jooksul on märkimisväärselt kasvanud üksteisega suheldavate andmetöötlusseadmete arv, eriti väikeste käeshoitavate seadmete, näiteks mobiilide, tahvelarvutite ja erinevate IoT seadmed jaoks. Nutiseadmed suhtlevad mobiilseadmetega nagu tahvelarvutid või nutitelefonid, mis võimaldavad kasutajatel neid seadmeid eemalt juhtida. Need seadmed saavad ka nutivõrguga suhelda, reageerides signaalidele, mis annavad kasutajatele meeldetuletusi nende seadmete kasutamise kohta. Nutiseadmete turg näeb iga päev kiiret kasvu, kuid nende seadmehaavatavuse kohta pole piisavalt teavet. Küberturvalisus on globaalne nähtus, mis kujutab endast keerulist sotsiaal-tehnilist väljakutset. Kuigi küberturvalisus on üks kriitilisemaid väljakutseid, millega silmitsi seisab, on nähtavus ja üldsuse teadlikkus piiratud. Peaaegu kõik on kuulnud ohtudest erinevates seadmetes. Inimeste kiireloomulisus ja käitumine ei kajasta siiski kõrgetasemelisi teadmisi. Kasutaja ettekujutuse mõistmine asjade IoT või mobiilseadmed erinevatest ohtudest aitaks juhtumite leevendamiseks fookusvaldkondi sujuvamaks muuta. Selles uurimistöös käsitleme seda lünka ja keskendume võrdleva analüüsi uurimisele kasutaja valmisoleku ja taju kohta IoT ja mobiilsetes seadmetes esinevatele erinevatele ohtudele.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 67 leheküljel, 6 peatükki, 15 joonist, 52 tabelit.

List of abbreviations and terms

IoT	Internet of things
MD	Mobile Device
IT	Information Technology
ANOVA	Analysis of Variance
EFA	Exploratory Factor Analysis
Wi-Fi	Wireless Fidelity
OODA	Observe Orient Decide Act
DEF CON	Defence readiness condition
REDDIT	Read Every Damn Dumb Internet Thing
CSV	Comma-Separated Values
JASP	Jeffreys's Amazing Statistics Program
IP	Internet Protocol
Ph. D.	Doctor of Philosophy
SD	Standard deviation
M	Mean
N	Sample Size
RQ	Research Question
Sig	Significance

Table of contents

<i>Author's declaration of originality</i>	2
<i>Abstract</i>	3
<i>Annotatsioon</i>	4
<i>List of abbreviations and terms</i>	5
<i>List of figures</i>	8
<i>List of tables</i>	9
1 Introduction	11
1.1 Problem	11
2 Background	12
2.1 Cyber Risks in Digital Environment	12
2.1.1 Cybersecurity Awareness	12
2.1.2 Ever-Rising Concern of Cyber Threats	12
2.1.3 Cyber Vulnerabilities of IoT and Mobile devices	13
2.2 Impact of Cyberpsychology	13
2.3 Role of End-users in Cybersecurity	14
2.4 Cybersecurity Perception and Preparedness	14
2.5 Gap in Literature	15
2.6 Novelty, Goals and Research Questions	15
2.7 Assumptions	17
3 Methodology	18
3.1 Research Approach	18
3.2 Instrumentation	18
3.3 Data Analysis Plan	18
3.3.1 Data Coding	19
3.3.2 Defining Statistical Significance	19
3.3.3 Pearson Correlation	20
3.3.4 Spearman Rank Correlation	20
3.3.5 ANOVA	20
3.3.6 Independent-samples <i>t</i> -test	20
3.3.7 Kruskal-Wallis Test.....	21
3.3.8 Mann-Whitney U Test.....	21
3.3.9 Paired-sample <i>t</i> -test	21
3.3.10 Cohen's <i>d</i>	21
3.4 Ethical Considerations	22
4 Results	23
4.1 Demographics	23
4.2 Descriptive Statistics of the Collected Data	23
4.2.1 Data Preparation	23
4.2.2 Normality of Data	23
4.2.3 Descriptive Analysis	24
4.3 Reliability Test and Correlation	25

4.3.1 Reliability Test	25
4.3.2 Correlation	26
4.4 EFA	27
4.4.1 EFA - Mobile Devices Perception	27
4.4.2 EFA - IoT Devices Perception	28
4.4.3 EFA - Mobile Devices Preparedness	30
4.4.4 EFA - IoT Devices Preparedness	31
4.5 Analysis of Mobile and IoT Devices Perception	33
4.5.1 Tests on Mobile Devices Perception	33
4.5.2 Tests on IoT Devices Perception	35
4.5.3 Comparison Between Mobile and IoT devices Perception	38
4.6 Analysis of Mobile and IoT Devices Preparedness.....	39
4.6.1 Tests on Mobile Devices Preparedness	39
4.6.2 Tests on IoT Devices Preparedness	41
4.6.3 Comparison between Mobile and IoT devices Preparedness	42
4.7 Analysis of Mobile Devices Perception and Preparedness	43
4.8 Analysis of IoT Devices Perception and Preparedness	45
5 Discussion.....	47
5.1 Research Implications.....	47
5.2 Practical Implications	48
5.3 Limitations	49
5.4 Future Work	49
6 Conclusion.....	50
References	51
Appendix 1 – Survey Consent Form.....	57
Appendix 2 – Questionnaire	58

List of figures

Figure 1- Research design.....	16
Figure 2- Path diagram of Mobile devices perception.....	28
Figure 3- Scree plot of Mobile devices perception.....	28
Figure 4- Path diagram of IoT devices perception.....	29
Figure 5- Scree plot of IoT devices perception.....	30
Figure 6- Path diagram of Mobile devices preparedness.....	31
Figure 7- Scree plot of Mobile devices preparedness.....	31
Figure 8- Path diagram of IoT devices preparedness.....	32
Figure 9- Scree plot of IoT devices preparedness.....	33
Figure 10- Effect size difference MD & IoT perception.....	38
Figure 11- Assumption Check Q-Q plot Mobile devices preparedness.....	40
Figure 12- Assumption Check Q-Q plot IoT preparedness.....	41
Figure 13- Effect size difference MD & IoT preparedness.....	43
Figure 14- Effect size difference MD perception & preparedness.....	44
Figure 15- Effect size difference IoT perception & preparedness.....	46

List of tables

Table 1- Data coding.....	19
Table 2- Demographics.....	23
Table 3- Descriptive statistics (Age group)	24
Table 4- Descriptive statistics (Gender)	24
Table 5- Descriptive statistics (IT-background)	24
Table 6- Descriptive statistics (Education level) perception	24
Table 7- Descriptive statistics (Education level) preparedness	25
Table 8- Reliability statistics MD perception	25
Table 9- Reliability statistics IoT devices perception.....	25
Table 10- Reliability statistics MD preparedness	25
Table 11- Reliability statistics IoT devices preparedness.....	25
Table 12- Correlation matrix MD perception	26
Table 13- Correlation matrix IoT devices perception.....	26
Table 14- Correlation matrix MD preparedness	26
Table 15- Correlation matrix IoT devices preparedness.....	27
Table 16- Factor loadings of MD perception.....	27
Table 17- Factor correlations of MD perception	27
Table 18- Factor loadings of IoT devices perception	29
Table 19- Factor correlations of IoT devices perception	29
Table 20- Factor loadings of MD preparedness.....	30
Table 21- Factor correlations of MD preparedness	30
Table 22- Factor loadings of IoT devices preparedness	32
Table 23- Factor correlations of IoT devices preparedness	32
Table 24- ANOVA MD_perception_3	33
Table 25- ANOVA MD_perception_4	34
Table 26- ANOVA MD_perception_5	34
Table 27- Post HOC comparison age groups MD perception	34
Table 28- Post HOC comparison education level MD perception	34
Table 29- Independent samples t-test MD perception (Gender).....	35
Table 30- Independent samples t-test MD perception (IT-background)	35
Table 31- ANOVA IoT_perception_3_1	35
Table 32- ANOVA IoT_perception_3_3	36
Table 33- ANOVA IoT_perception_4_1	36
Table 34- ANOVA IoT_perception_4_3	36
Table 35- Post HOC comparison age groups IoT devices perception	36
Table 36- Post HOC comparison education level IoT devices perception	37
Table 37- Independent samples t-test IoT devices perception (Gender)	37
Table 38- Independent samples t-test IoT devices perception (IT-background)	37
Table 39- Paired sample t-test.....	38
Table 40- One sample t-test	39
Table 41- Kruskal-Wallis test (MD preparedness)	39
Table 42- Mann-Whitney U test MD preparedness (Gender)	40
Table 43- Mann-Whitney U test MD preparedness (IT-background)	40
Table 44- Kruskal-Wallis test (IoT preparedness).....	41
Table 45- Mann-Whitney U test IoT preparedness(Gender)	42
Table 46- Mann-Whitney U test IoT preparedness(IT-background).....	42

Table 47- Wilcoxon signed-rank test	43
Table 48- One sample t-test (Wilcoxon signed-rank test)	43
Table 49- Paired sample t-test (MD perception and preparedness)	44
Table 50- One sample t-test MD perception & preparedness	45
Table 51- Paired sample t-test (IoT perception and preparedness)	45
Table 52- One sample t-test (IoT perception and preparedness)	46

1 Introduction

We are in a period where privacy and security have become the most complicated challenge for technology experts. The last decade saw tremendous adoption and advancements in technology. This has resulted in mobile devices, and the internet has become increasingly accessible and cheaper for end users. Stats reveal that more than half of the world population is using the internet as of 2019 [1]. Among mobile devices, the adoption of smartphones has seen an incomprehensible increase. The advancement in technology has provided a means for smartphone manufacturers to make their phones more powerful and smarter. On top, the increased popularity and adoption of cloud computing has paved the way for millions of users to be connected in cyberspace. This has led to some significant trends like e-commerce, social networking, online banking, etc. Almost every daily activity of an individual is performed via a device connected to the internet. This has resulted in an enormous increase in an individual's online presence meaning all the shopping preferences, social interactions, financial information, and internet usage is no longer a private affair. Instead, it is stored as data on cyberspace.

While these advancements have improved the living standards of end-users, they come with some serious repercussions. This widespread use of technology and connected devices means the blast radius of a security problem is very high. This has led to the rise in cybercrime. Since all this data is stored in cyberspace, how this data is stored, protected, or used is a complete black box for the end-user. Any breaches on these cloud storage can lead to loss of data, which would ultimately affect the end-users severely. Also, every device used in our day-to-day activities is connected to the internet, exposing each of us as a potential target for cyberattacks.

1.1 Problem

Mobile devices like smartphones, laptops, etc. and IoT devices are the most common ways end-users interact with or are connected to the internet. More than half of the world population is using the internet in their mobile/ IoT devices as of 2019 [1]. The most severe part of IoT is that users are surrendering their privacy, bit by bit, without discerning it [1]. Users have no clear understanding of the permissions they grant in their devices. Also, they are more ignorant about reading the terms and conditions before installing or using an application without knowing the side effects of these applications collecting sensitive data. This would mean that the probability of users facing privacy concerns via these mediums is exceptionally high. It is also essential for the end-user to consider the security aspects of their day to day activities. It is more likely that a user uses outdated and unsigned software, operate their devices using an unsafe network, having a weak/old password without knowing that these aspects help a hacker to exploit their devices. As a recent analysis by The Federal Bureau of Investigation provides an insight that, on average, 4000 ransomware attacks are occurring daily [2]. In addition to that, 7.2 billion malware attacks were launched in the first three quarters of 2019, and the number of malware attacks on IoT devices increased by 215% between 2017 and 2018 [3, 4]. Almost 81% of all the hacking-related breaches leveraged weak passwords [5]. Considering the fact that user's cyber risk is predominantly affected by these day-to-day activities on mobile and IoT devices, it is critical to understand whether user perceives these actions as a security threat and how well they are prepared in handling them.

2 Background

2.1 Cyber Risks in Digital Environment

2.1.1 Cybersecurity Awareness

A distinct study on cognitive science explains the situational awareness and cognitive-oriented aspect of decision-making with adapted processes of perception, comprehension, and projection [6]. A cognitive OODA loop was designed in 2018 explains the relationship between the cognitive phase and process to establish a capability of self-awareness to different computational systems [7]. This evaluates the threat actor's cognitive aspect towards gaining a competitive advantage over the patterns or process of the attack. The demonstration of situation awareness is the main activity of the security operation center. The conjecture of situation awareness describes the organization's current situation about threats and attacks, the impact of a possible attack, and the identification of the attacker and user behavior [8].

Cybersecurity awareness evaluation demands a mix of methodologies because assessing humans cannot be based merely on the quantitative approach. Specific details need the intentness of qualitative methods, such as determining human behavior. Different frameworks were developed to measure security behavior in the workplace and examine the impact of cybersecurity policy awareness on various threats metrics, coping procedures, and security compliance [9]. But the peer behavior on cybersecurity is controlled by the employee's actions as both central and external motivators [10]. However, previous studies symbolize that peer behavior is a source of social impact and that social impact is a type of trigger for various cyber incidents due to the lack of motivators. A security framework created by K C Park and D H Shin. (2016) [11] used a fuzzy decision-making method to identify the interrelationship between the cause and effect of various security concerns due to IoT devices.

2.1.2 Ever-Rising Concern of Cyber Threats

Cyberspace encompasses "the entire spectrum of networked information and communication technologies and systems worldwide as well as the physical hardware," [12] including various exhibits of information and communication technologies. In the current scenarios, human activities are predominately carried out on the internet. This change ends in an asymmetric, low-risk environment for attackers maintaining environmental remoteness from the target of an attack and avoiding exposure to defensive forces, in which even insignificant opponents with evil intentions can challenge the resources of major corporate entities [13, 14]. Cyber threats comprise any socially harmful activity, including online crime and terrorism. According to Weimann, cyberterrorism constitutes a terrorist element in cyberspace attacks [15]. Divided from infringements in general, terrorism refers to "violence, or the threat of violence, used and directed in pursuit of, or service of, a political aim" [16].

The growing dependence of today's community on information and communication technologies has produced a new sort of vulnerability allowing cybercriminals to go after various targets [17]. The scope of cyber threats to the public encompasses sophisticated malicious software, disruptive activity by online activists and nationalist groups, and even organized crime and electronic cyber espionage activities.

2.1.3 Cyber Vulnerabilities of IoT and Mobile devices

IoT development dramatically transformed the cyber threat aspect. The mass-scale deployment of such fundamentally unsafe devices produces an increase in more vectors for the attack [18, 19]. A critical security difficulty in the IoT is the development of the overall attack factor for malicious threats as analyzed to isolated systems. IoT devices are essential enablers for sensing the significant features and assets to increase operational and computational efficiencies. Due to the crucial elements of IoT technologies, the perceived risk tends to be restricted to security and privacy [20]. According to the study in 2015, more than 70% of potential customers of IoT technologies are very concerned about their private data being shared or leaked to third parties [21]. A study on privacy concerns observed that users with more security knowledge and experience never save or share personal information through emails [22]. Also, those users had various privacy concerns with social media sites such as Instagram and Twitter, where they felt images are “the most privacy-invasive data” on social networking sites [23, 24].

The Hewlett Packard in 2015 explained that over 60 percent of IoT devices carry dangerous vulnerabilities [25]. This is because the massive amount of data transferred between different IoT devices is through the cloud and different mobile applications. According to an article on IoT, device vulnerability states that amazon echo and google home are prone to various privacy attacks due to different applications used as a phishing application to collect privacy details from the user [26]. Various attack scenarios observed by researchers in google home and amazon echo during DEF CON 2019 has found that smart home devices are prone to multiple privacy-related concerns [27]. In the first half of 2019, Kaspersky analyzed different attack vectors using a honey pot program in which 105 million attacks were related to IoT devices compared to the count of 12 million in 2018 [28]. Another report published by F-secure states that Over 2.9 billion events observed by our global network of honeypots in the first half of 2019 [29].

Digital attacks on different IoT devices pose dangers in the digital environment and, even more critically, privacy challenges to these IoT device users. [30]. Various researches used an open-source simulation that emulated different IoT scenarios with which they proposed various new cybersecurity exercises to eliminate the attack vectors [31]. Also, multiple IoT security taxonomy was proposed, respect to the architectural communication layers [32]. Furthermore, some studies present a set of standard threats and vulnerabilities in the IoT environments and suggest possible solutions for fixing the IoT security design.

2.2 Impact of Cyberpsychology

Cyberpsychology aims to understand the interaction of humans with digital devices, various emerging technologies, and how they utilize it. A newly developing practice on cyberpsychology is defined as “the study of how new communication technologies influence and are influenced by, human behaviors and subjectivities” [33, 34]. The most generally studied aspects of cyberpsychology are to examine the areas of human interactions with many devices, including mobile computing, gaming consoles, virtual reality, and artificial intelligence [35]. A rapid rise in computing and mobile technology, changing human behavior due to adverse factors like digital addiction and stress, was detrimental to the users. This increased the scope of knowledge areas to study user’s change in behavior to emerging digital trends. The lack of intellectual knowledge on cybersecurity threats and concise human decision-making was figured out to be the most vulnerable link among several users like random guessers, low, moderate, and high cybersecurity decision-makers [36].

2.3 Role of End-users in Cybersecurity

Awareness of user's security decisions towards smart devices and other security products differs from the vast culture [37]. This leads to a mismatch between knowledge and existence. Knowledgeable users show contrast to responders with a lack of awareness, which changes the approach to how those devices are used among these two categories. Lack of perception of cyber risk coupled with expectancy bias leads to users assuming that their smart devices are more secure [38]. The behavior of users is a significant talking point on how humans are the main problem for cybersecurity threats and how users themselves are the solution to that problem [39].

A study carried out in 2017 analyzed a decade's publications in major human-centred security conferences, in terms of whether they focused on the individual, social aspects of human-centred security, or their more significant role in the socio-technical system [40]. The researchers found that most articles focused on the individual, with a tiny number focusing on the social aspects. The primary focus was on the human-computer interaction layer in how it acts as a significant factor in the individual role in cybersecurity.

Human error is the common cause of adverse incidents and "a serious threat to the viability of computer-based systems, and thereby to the industrialized world at large" [41]. Some say that the on average computer users lack knowledge and perception of cybersecurity issues and of the security practices they ought to be carried out [42].

2.4 Cybersecurity Perception and Preparedness

"There are those who have been breached, and those who don't know it yet," [43] is a truism about computer security that has been circulating for almost a decade. Cybersecurity can be technically regarded as computer security plus securitization, but the knowledge of the preparedness for cybersecurity goes beyond a mere technical understanding of the acceptance of societal effects invoked by cyber threats [44]. A common error enterprise makes to view data security preparedness and maturity as something that can be measured by listing the layers of defence an IT department has in place. By viewing cybersecurity through this lens, enterprises cannot distinguish between self-perception and reality, only by analysing several critical elements collectively [45]. A Bit Sight Insight report, while examining the cyber health of the U.S. economy, discovered that 82% of the 460 companies evaluated had an externally observable security compromise. However, despite this evidence of widespread understanding among America's most significant corporate and IT leaders, it appears to feel quite confident about their security aspect [46].

Individuals tend to understand the level of cyber threat and their readiness, not as the outcome of fact or evidence-based decisions, but as a result of psychological reactions [47]. The impacts on psychological responses may increase the sense of vulnerability and also trigger actions to reduce individual risks. People's perceptions of more common risks usually are reduced, due to which it invokes fear [48]. Cybersecurity awareness raises the understanding that a given threat may exploit an asset's vulnerabilities, whereas ignorance promotes the fear of cyberattacks [16]. In many studies, such perception means attracting users' attention to security issues or their understanding of and commitment to security [49, 50]. Users' perceptions of security can affect their attitudes and behaviors directly and indirectly. For example, an individual's knowledge of security is the building block of trust (indirect) towards any form of

an electronic transaction that can fuel users' behavioral intentions (direct), such as their intention to share private information with websites. Few studies specifically examine how an individual's perceptions of security can trigger coping and compliance behaviors. Examples of coping behaviors include avoidance, protective actions, and seeking help from others, which justifies the motivations behind individuals' self-protection in online environments [51]. For instance, security perceptions could indirectly lead to organizational security compliance, which is a significant problem in various organizations [51].

2.5 Gap in Literature

“Cybersecurity systems are only as strong as their potentially weakest links: the end-users that are using them” [52]. An individual's cyber hygiene is not just about protecting themselves, it is also protecting users around them. For example, a single compromised individual can be the doorway to infecting a large number of machines, thus greatly amplifying their ability to reach millions of users[53]. In general, the literature so far produced seems to consider the perception and preparedness of cybersecurity in terms of large, medium, and small enterprises. But it is clear that individuals play an equally important role in ensuring a secure environment. A good example of this would be that employees predominantly use personal devices, which are unprotected, for email and other work functions. Enterprise emphasized security software, and restrictions typically do not go beyond work computers, making every individual employee a potential security threat[54]. Most of security/data breaches result from an employee not following safe email and internet practices [55]. So it is clear that measuring the perception and preparedness of an individual is very important. And it is well established that technical knowledge is one of the roadblocks for an individual in understanding cybersecurity risks[56]. So this study tries to mitigate this by scoring an individual's perception and preparedness towards privacy and security based on their day-to-day interaction with mobile and IoT devices and identifying how dimensions like education, work background and age affect perception and preparedness. Also as part of this study we try to understand the differences in perception and preparedness between mobile and IoT devices.

2.6 Novelty, Goals and Research Questions

Despite the growing concern of prevalent cybersecurity issues, little research has been done on individual perceptions of threats to and preparedness for cybersecurity, nor has it focused on the gap between these two viewpoints.

In this study the user's perception is calculated using the following dimensions,

- Is the user aware that sensitive data like voice, videos, pictures are being stored or collected when they use mobile or IoT devices.
- Do users use location services while using an application.
- Do users use open/ password less protected networks while using their mobile/ IoT devices.
- Do users share financial information online.

In contrast to the perception, the user's preparedness is calculated using the following dimensions,

- Do users use VPN when using an open/ password less networks.

- Does the user have read/understand the terms and conditions when accepting them.
- Do users know what kind of permissions they grant while using an application in their devices.
- Do they use adblockers to block unnecessary ads while using their browsers in their devices.
- Do users update their device software regularly.

Given the scarcity of relevant research, the goal of this study is to discuss perception and preparedness in terms of security in day-to-day interactions with mobile and IoT devices. Each dimension from fig 1 is related to a privacy or security concern and helps to answer the following four research questions to understand from the user’s perspective.

RQ1. Whether the user’s perception towards cybersecurity threats for older mobile devices differ when compared to newer IoT devices?

RQ2. Whether the user’s preparedness towards cybersecurity threats for older mobile devices differ when compared to newer IoT devices?

RQ3. Whether the user’s perception towards cybersecurity threats in mobile devices is associated with preparedness?

RQ4. Whether the user’s perception towards cybersecurity threats in IoT devices is associated with preparedness?

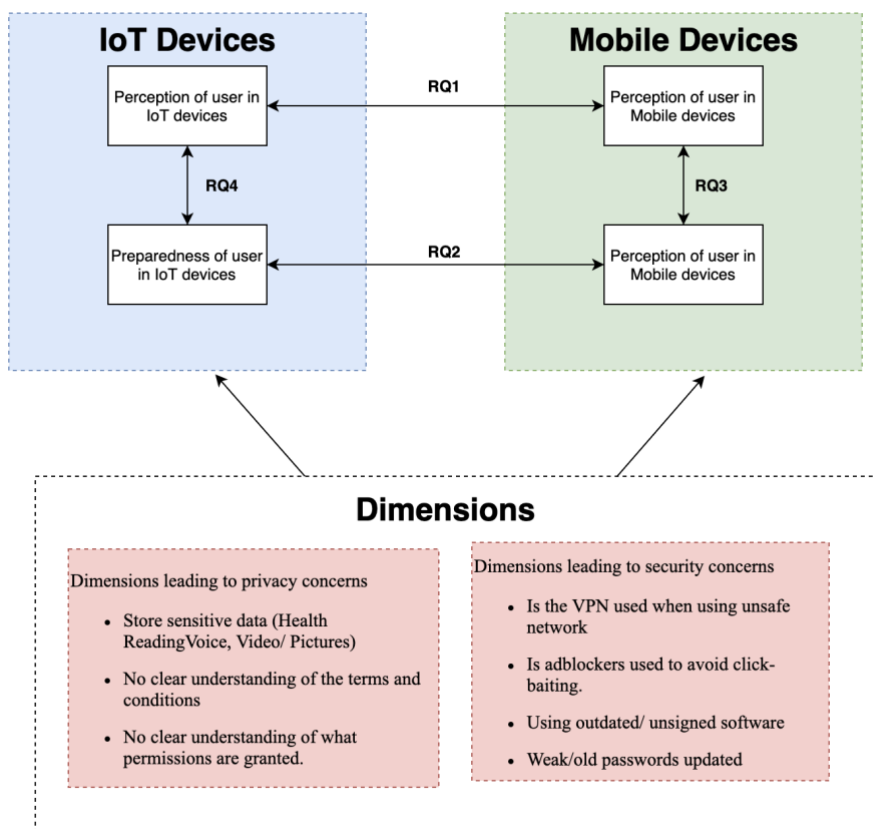


Figure 1- Research design

The RQ1 and RQ2 address the gap between the user's perception and preparedness in older mobile devices to the newer IoT. Further expanding on this, RQ3 and RQ4 identifies whether the age of products availability in the market affects the user's knowledge towards cybersecurity threats. This is to determine whether, the users understanding and readiness of cybersecurity threats in mobile devices, which are available in the market for a more extended period are better than IoT devices or there is a Dunning-Kruger-Effect, meaning people are less careful with IoT devices because they know less about it and have more problems assessing their perception and preparedness.

2.7 Assumptions

The assumptions listed below are boundaries set to ensure there is a clear scope that encapsulates the study. This is to ensure that the sample data obtained is targeted and the findings can be justified. This study is conducted based on the following:

- The survey is completed with genuine and authentic feedback from participants.
- The participants took a genuine interest in completing the survey and had no other motive.
- The participants considered are from different age-groups, education, gender and IT background.

3 Methodology

This chapter briefly discusses the approach taken, followed by the data collection instrument used and the analysis plan. The chapter is concluded with ethical considerations.

3.1 Research Approach

The methodology used in this thesis utilises a quantitative, self-administered, closed-ended questionnaire to collect data to measure the user's perception and preparedness towards cybersecurity threats in IoT and mobile devices.

3.2 Instrumentation

The online survey was used as the data collection instrument. The benefits of using a web-based survey are the speed and breadth at which the survey can be sent out and received [59]. Furthermore, the obtained data can be quickly transformed into an analysis [60] [61]. Web-based surveys are also extremely cost-effective [59] [61] [62].

However, there are also some challenges associated with web-based surveys. For example, due to the anonymity of the surveys, it is hard to follow up [61] and discuss the answers face to face with participants. Noting all the pros and cons, as long as the survey was conducted diligently, a quantitative approach will save time and still provide credible outcomes.

For this research, Google Forms was used as the survey tool as it was free, and it also can develop graphs and export raw data to excel. The online survey was conducted in English and consisted of two parts. The first part has undertaken the demographic variables, and the second part has done the measurement of the conceptual variables. The measure of the conceptual variables was divided into two sections, perception and preparedness, each incorporated with ten closed-ended questions. Each question was framed with an idea of having one threat or vulnerability indirectly associated with the question to understand the user's approach towards it. The survey takes approximately 5 minutes to complete.

The participants are the general public in various age groups from various levels of education and different backgrounds who use various mobile and IoT devices in their day to day life. The linear snowball sampling approach was followed to collect data. The online survey was posted on social media, sent to different participants via WhatsApp messages, and email. The survey was also published in many community sites like Reddit to collect from various responders. Each post had a link to the Google Form questionnaire that can be completed on any device with an internet connection. The online survey that was used is attached in appendix 2.

3.3 Data Analysis Plan

Once the survey data were obtained from participants, the first step was to check each questionnaire to possibly eliminate incomplete questionnaires [57][58]. After which, the data was later coded to allocate numeric values to answers for performing statistical techniques [57]. This sample data is then transcribed and converted into CSV format to allow for more data analysis. Cleaning the data then follows by observing and identifying any outliers or errors that could skew the overall results.

To achieve the results of the survey, data analysis was systematically conducted to examine the quantitative data and extract valuable conclusions. The survey consists of 25 questions comprising different types of variables. All variables in this survey can be classified as nominal variables. Choosing the type of analysis depends on how the research and survey were designed. There are two parts to this analysis: descriptive and inferential. In the first section, the descriptive analysis includes explains the data in descriptive form using minimum, maximum, frequency, and measures of central tendency. In the second section, inferential analysis employs statistical tests to evaluate the pattern that forms from the data. Datasets obtained through Google Forms were directly exported to Microsoft Excel, where the data was cleaned and outliers removed [63]. The data was then converted into a CSV file to perform statistical analysis using JASP [64] and data analysis tools. Data was validated using EFA was used to statistically measure the correlation of the underlying variables [65]. To find the reliability of the collected data, Cronbach alpha coefficients were used [66]. Once the data was validated, statistical tests are chosen based on the design of the research, types of variables, and distribution of the data (parametric, non-parametric).

Considering all the parameters and variables for mobile and IoT devices perception, four different parametric statistical tests are performed to answer the research questions presented in this study [Pearson Correlation, ANOVA, Independent-samples t-test and Cohen’s d]. Four non-parametric tests [Spearman Correlation, Kruskal-Wallis test, Mann-Whitney U test, and Cohen’s d] are done for the mobile and IoT devices preparedness. A paired sample *t*-test was conducted for the comparative study of perception and preparedness.

3.3.1 Data Coding

The data collected from the survey is coded to a numerical form to facilitate the statistical analysis of the data, as seen in Table 1. Each level on the scale of concerns is assigned a number or code, starting from 1, with an equal increment to 6.

Questions 8_1, 8_2, 8_3, 8_4	Questions 9_1, 9_2, 9_3, 10_1, 10_2, 10_3	Gender	Age Groups	IT- Background	Education Level
1 – Very uncomfortable	1 - Strongly disagree	1 - Male	1 - 18-24	1 - Yes	1 - High school degree or equivalent
2 - Slightly uncomfortable	2 - Slightly disagree	2 - Female	2 - 25-34	2 - No	2 - Bachelor’s degree
3 - Uncomfortable	3 - Disagree		3 - 35-50		3 - Master’s degree
4 - Comfortable	4 - Agree		4 - 50+		4 - PhD or higher
5 - Slightly comfortable	5 - Slightly agree				
6 - Very comfortable	6 - Strongly agree				

Table 1- Data coding

3.3.2 Defining Statistical Significance

In statistical analysis, the null hypothesis, H_0 is a theory that has not been proved but is believed to be true. Whereas, the alternative hypothesis, H_a is determined by the outcome of the statistical test [67]. If the difference in mean between the two samples is substantial, then the null hypothesis, H_0 is rejected [68]. The significance level is a pre-chosen probability that compares the calculated significance value (p-value) of the hypothesis test to a statistically significant value [61]. Typical p-values are 0.1, .05, and 0.01; in this study p-value = .05.

Therefore, if the p-value of the sample statistic is less than or equal to .05, then the decision is to reject the null hypothesis, else we fail to reject the null hypothesis [69]. Choosing a significance level is purely arbitrary, and in the case of p-value = .05, signifies a 95% level of confidence in the result.

3.3.3 Pearson Correlation

This test was used to “measure the strength of a linear association between two variables” [69]. This strength of the relationship between two variables is represented through the correlation coefficient, r . To interpret the resultant r -value, if the value is near zero, there is no correlation. If the value is between 0 to ± 0.15 , signifies weak correlation, and a value between ± 0.45 to ± 1 signifies a strong negative or positive strength in the relationship [67]. Another useful descriptor is the significance of the relationship that is calculated through the p-value. The correlation is statistically significant if the p-value is less than .05 [68]. This study Pearson correlation was carried out for the first research question mentioned in section 2.5.

3.3.4 Spearman Rank Correlation

The Spearman correlation is a non-parametric test not requiring normally distributed data. The correlation between the two variables is equal to the Pearson correlation within the two variables' rank values to assess the monotonic relationships [76]. If there are no duplicated data values, a precise Spearman correlation of +1 or -1 occurs when each of the variables is an absolute monotone function of the opposite [77]. One way to test whether a found value of p is significantly different from zero if r will perpetually sustain $-1 \leq r \leq 1$ to determine the likelihood that it would be higher than the observed r [78].

3.3.5 ANOVA

The ANOVA is used to identify the variables in a multidimensional model that influence the model most or check whether the means of several samples are the same [64]. Before an ANOVA can be performed as a precondition, it is necessary to test the ‘assumption of homogeneity of variance’ [69]. The significance level, p-value .05, is used as a measure to classify whether the samples have violated the assumption of homogeneity of variances [69]. The theory shows that if the significance value (p -value) is greater than .05, then variances are considered equal. If the p-value is lesser than .05, then the assumption of homogeneity has been violated with unequal variances [69]. The sample data is then combined with the individual samples (whose means are not equal) into a larger collective sample, in which we can see that the variance of the new sample will be greater than the variance of the individual samples. The increase in the variance of the combined sample allows us to test for the equality of the individual samples' means by merely comparing the individual samples' variances to the variance of the collective sample. This would help in investigating the collective variance.

3.3.6 Independent-samples t -test

“The Student’s t -test is an inferential statistical test that determines whether there is a statistically significant difference between the means in two unrelated groups [69]”. To accept or reject the null hypothesis H_0 , the calculated p-value should be less than .05 [59]. Since this is a two-tailed test, indicating that we would have to define rejection regions associated with p-value < .05 as $z_{0.025} = \pm 1.96$ [60]. The reason we choose p values of $z_{0.025} = \pm 1.96$ is that

we need to split the 0.05 p-value across both tails of the curve. Thus, the null hypothesis will be rejected if the resultant test statistic is less than -1.96 or greater than 1.96 [60].

3.3.7 Kruskal-Wallis Test

The Kruskal–Wallis test by ranks is a non-parametric method for testing whether samples originate from the same distribution [60]. It is used for associating two or more independent variables of similar or varied sample sizes [75]. In this study, the Kruskal-Wallis test was conducted for samples (mobile devices and IoT devices preparedness), considering the distribution of data to be non-parametric. The choice to reject or not the null hypothesis is made by comparing H_0 to a critical value H_c obtained from a significant p-value $< .05$, else if H_0 is bigger than H_c , the null hypothesis is rejected [76]. Otherwise, the order of H can be approximated by a chi-squared distribution [77].

3.3.8 Mann-Whitney U Test

The Mann–Whitney U test is a nonparametric analysis of the null hypothesis that it is reasonably likely that a randomly chosen value from one group will be less than or greater than a randomly chosen value from another group [78].

3.3.9 Paired-sample *t*-test

This test was done by making several inferences about the difference between the two groups mean scores (gender, IT-background) based on paired samples (for example, IoT perception and mobile devices perception). The null hypothesis (H_0) assumes that the actual mean difference (μ_d) is equal to zero. The variable is statistically significant when the p-value is less than .05 [59].

3.3.10 Cohen's d

This statistical test completes the *t*-test by computing the Cohen's d measure. It is a unitless effect size and shows the strength of the difference between two sample means [71]. In other words, this represents the distance between the mean of the observations compared to the mean of the null hypothesis. Cohen's d can be calculated using Equation (1) [72]

$$d = \left| \frac{\bar{x} - \mu}{\sigma} \right| \quad (1)$$

x = sample size

μ = null hypothesis population mean

σ = null hypothesis population standard deviation

According to Cohen's definition of resultants the small effect size has a value between 0 to 0.20, medium effect size for values between 0.20 to 0.50 and finally the large effect size has values larger than 0.50 [73].

3.4 Ethical Considerations

From the participant's side, it was essential to confirm consent before starting the survey. Participants were notified that the questions could be skipped at any time if they do not feel comfortable answering. They were informed that the survey is entirely anonymous, that no personal information is stored, and that participants cannot be identified from the results of this study in any way. Even though the survey is online-based, no geographical locations or IP addresses were retrieved. No identification or personal information was requested from the participants. The consent form is attached in appendix 1.

4 Results

This chapter presents the findings and statistical analysis of the sample data collected using the online survey. The study first provides an overview of the demographics of the sample, followed by validation of data and different tests conducted to answer research questions statistically.

4.1 Demographics

The sample consisted of people from different countries between different age groups with both IT and non-IT backgrounds. Overall the data includes 515 eligible participants in the survey. Table 2 represents the age-groups, gender, education, and IT Background demographic data. Overall, 186 participants were female, with 329 males. The ratio of females to males was 36% to 64%. The age range was across different groups, with which 50% of people were from the age group between 25-34. The education level of the participants varied from high school to Ph.D. level or higher, in which 63% of the respondents had bachelor level education. Respondent's background was almost equally distributed, with 53% from IT background and rest 46% from non-IT experience.

Demographics		Frequency	Percent	Total
Please select your age group	18 - 24	179	34.757	515
	25-34	262	50.874	
	35-50	64	12.427	
	50+	10	1.942	
Please select your gender	Female	186	36.117	
	Male	329	63.883	
Select your level of education	Bachelor's degree	325	63.107	
	High school degree or equivalent	6	1.165	
	Master's degree	164	31.845	
	PhD or higher	20	3.883	
Are you working in an IT-related field	No	240	46.602	
	Yes	275	53.398	

Table 2- Demographics

4.2 Descriptive Statistics of the Collected Data

4.2.1 Data Preparation

Data preparation entails examining the data for accuracy, assigning a variable name for each item, and documenting it in an excel sheet. The next step is to understand the attributes of the data to build awareness of any assumption violations and the associations they may have for the evaluation process or the analysis of the results.

4.2.2 Normality of Data

The normality tests are additional to the graphical assessment of normality [81]. The primary test used for the evaluation of normality is the Kolmogorov-Smirnov test. It is used to compare the scores in the sample to a normally distributed set of scores with the identical mean and standard deviation. The null hypothesis is that sample distribution is normal [81]. For smaller

sample sizes, normality tests have the control to reject the null hypothesis, and often pass the normality tests [82]. The data which are normalized are considered for parametric tests, and for the data which are not normalized, non-parametric tests are conducted.

4.2.3 Descriptive Analysis

Table 3,4,5,6 shows some descriptive for the constructs, namely minimum (min), maximum (max), mean, standard deviation. Minimum and maximum values show that all the constructs were consistently measured within the point on the scale that they had been measured on, i.e., from 1 to 6, where respondents to the items were measured on a six-point Likert scale where the value representation is explained in the data coding section 3.4.1.

	MD_Perception				IoT_Perception				MD_Preparedness				IoT_Preparedness			
	18 - 24	25-34	35-50	50+	18 - 24	25-34	35-50	50+	18 - 24	25-34	35-50	50+	18 - 24	25-34	35-50	50+
Valid	179	262	64	10	179	262	64	10	179	262	64	10	179	262	64	10
Missing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mean	1.323	1.307	1.348	1.301	3.644	3.677	3.656	3.700	2.776	2.992	2.849	2.268	2.825	2.882	2.694	3.140
Std. Deviation	0.342	0.300	0.372	0.304	1.200	1.119	0.967	1.123	1.243	1.194	1.045	1.087	1.137	0.969	0.859	0.938
Minimum	0.733	0.733	0.750	1.000	1.000	1.000	1.750	2.250	1.000	1.000	1.000	1.000	1.000	1.000	1.400	1.400
Maximum	2.233	2.167	2.233	1.789	6.000	6.000	6.000	6.000	6.000	6.000	5.330	4.000	5.800	5.600	5.800	4.600

Table 3- Descriptive statistics (Age group)

	MD_Perception		IoT_Perception		MD_Preparedness		IoT_Preparedness	
	Female	Male	Female	Male	Female	Male	Female	Male
Valid	186	329	186	329	186	329	186	329
Missing	0	0	0	0	0	0	0	0
Mean	1.309	1.323	3.591	3.704	2.613	3.039	2.701	2.925
Std. Deviation	0.314	0.330	1.115	1.135	1.137	1.203	1.046	0.994
Minimum	0.733	0.733	1.000	1.000	1.000	1.000	1.000	1.000
Maximum	2.167	2.233	6.000	6.000	6.000	6.000	5.800	5.800

Table 4- Descriptive statistics (Gender)

	MD_Perception		IoT_Perception		MD_Preparedness		IoT_Preparedness	
	No	Yes	No	Yes	No	Yes	No	Yes
Valid	240	275	240	275	240	275	240	275
Missing	0	0	0	0	0	0	0	0
Mean	1.327	1.310	3.626	3.695	2.882	2.888	2.786	2.895
Std. Deviation	0.305	0.340	1.080	1.168	1.197	1.198	1.062	0.977
Minimum	0.733	0.733	1.000	1.000	1.000	1.000	1.000	1.000
Maximum	2.233	2.194	6.000	6.000	6.000	6.000	5.800	5.800

Table 5- Descriptive statistics (IT-background)

	MD_Perception				IoT_Perception			
	Bachelors degree	High school degree or equivalent	Masters degree	PhD or higher	Bachelors degree	High school degree or equivalent	Masters degree	PhD or higher
Valid	325	6	164	20	325	6	164	20
Missing	0	0	0	0	0	0	0	0
Mean	1.295	1.454	1.365	1.264	3.718	3.250	3.573	3.625
Std. Deviation	0.320	0.301	0.327	0.341	1.145	1.432	1.093	1.037
Minimum	0.733	1.167	0.750	0.733	1.000	1.000	1.000	2.000
Maximum	2.233	1.778	2.233	1.833	6.000	5.000	6.000	6.000

Table 6- Descriptive statistics (Education level) perception

	MD_Preparedness				IoT_Preparedness			
	Bachelors degree	High school degree or equivalent	Masters degree	PhD or higher	Bachelors degree	High school degree or equivalent	Masters degree	PhD or higher
Valid	325	6	164	20	325	6	164	20
Missing	0	0	0	0	0	0	0	0
Mean	2.810	2.665	3.041	2.900	2.792	2.867	2.957	2.750
Std. Deviation	1.201	1.520	1.151	1.355	1.052	0.909	0.973	0.810
Minimum	1.000	1.330	1.000	1.000	1.000	1.200	1.000	1.400
Maximum	6.000	5.330	6.000	5.330	5.800	3.800	5.800	4.200

Table 7- Descriptive statistics (Education level) preparedness

4.3 Reliability Test and Correlation

4.3.1 Reliability Test

Cronbach's alpha coefficient was used to measure the internal consistency of the scales applied in this study. Nunnally (1978) recommend a minimum level of 0.70 for the scale of the construct to be deemed highly reliable. Table 8,9,10,11 shows all the constructs revealing Cronbach's alpha values greater than 0.70 concluding that the constructs are reliable.

Scale Reliability Statistics Mobile devices Perception (3 Items)

	mean	sd	Cronbach's α	95.0% Confidence Interval	
				Lower	Upper
scale	2.279	0.343	0.778	0.743	0.809

Note. Of the observations, 515 were used, 0 were excluded listwise, and 515 were provided.

Table 8- Reliability statistics MD perception

Scale Reliability Statistics IoT devices Perception (4 Items)

	mean	sd	Cronbach's α	95.0% Confidence Interval	
				Lower	Upper
Scale	3.663	0.340	0.726	0.685	0.763

Note. Of the observations, 515 were used, 0 were excluded listwise, and 515 were provided.

Table 9- Reliability statistics IoT devices perception

Scale Reliability Statistics Mobile devices Preparedness (3 Items)

	mean	sd	Cronbach's α	95.0% Confidence Interval	
				Lower	Upper
scale	2.885	0.849	0.733	0.449	0.591

Note. Of the observations, 515 were used, 0 were excluded listwise, and 515 were provided.

Table 10- Reliability statistics MD preparedness

Scale Reliability Statistics IoT devices Preparedness (5 Items)

	mean	sd	Cronbach's α	95.0% Confidence Interval	
				Lower	Upper
scale	2.844	0.572	0.788	0.625	0.711

Note. Of the observations, 515 were used, 0 were excluded listwise, and 515 were provided.

Table 11- Reliability statistics IoT devices preparedness

4.3.2 Correlation

Pearson's correlation was used to explore the relationship between all the variables of IoT devices perception and mobile devices perception. Spearman correlation was used to explore the relationship between all the variables of IoT devices preparedness and mobile devices preparedness. Correlations coefficients are capable of giving a numerical sense of the direction and strength of the linear relation between all the variables. Pearson 's correlation coefficients (r) and Spearman correlation coefficient (rho) produce either positive correlation or negative correlation (Pallant, 2007). Cohen (1998) proposes the subsequent guidelines to define the strength of the association.

r or rho = $\pm .10$ to $\pm .29$ -> small

r or rho = $\pm .30$ to $\pm .49$ -> medium

r or rho = $\pm .50$ to ± 1.0 -> large

	MD_Perception_1	MD_Perception_2	MD_Perception_3	MD_Perception_4	MD_Perception_5
MD_Perception_1	—				
MD_Perception_2	0.454***	—			
MD_Perception_3	-0.222***	-0.164***	—		
MD_Perception_4	-0.213***	-0.073	0.588***	—	
MD_Perception_5	-0.181***	-0.122**	0.473***	0.559***	—

* p < .05, ** p < .01, *** p < .001

Table 12- Correlation matrix MD perception

	IoT_Perception_1	IoT_Perception_2_1	IoT_Perception_2_2	IoT_Perception_2_3	IoT_Perception_3_1	IoT_Perception_3_2	IoT_Perception_3_3	IoT_Perception_4_1	IoT_Perception_4_2	IoT_Perception_4_3
IoT_Perception_1	—									
IoT_Perception_2_1	0.048	—								
IoT_Perception_2_2	0.067	0.231***	—							
IoT_Perception_2_3	0.074	0.207***	0.504***	—						
IoT_Perception_3_1	-0.028	0.036	0.035	0.162***	—					
IoT_Perception_3_2	0.080	-0.004	0.105*	0.209***	0.204***	—				
IoT_Perception_3_3	-0.107*	0.079	0.021	-0.023	0.293***	0.150***	—			
IoT_Perception_4_1	0.074	0.028	-0.094*	0.017	0.557***	0.087*	0.230***	—		
IoT_Perception_4_2	0.099*	0.149***	0.204***	0.332***	0.189***	0.460***	0.153***	0.220***	—	
IoT_Perception_4_3	-0.074	0.052	0.070	0.105*	0.308***	0.017	0.658***	0.346***	0.227***	—

* p < .05, ** p < .01, *** p < .001

Table 13- Correlation matrix IoT devices perception

	MD_Preparedness_1	MD_Preparedness_2	MD_Preparedness_3	MD_Preparedness_4	MD_Preparedness_5
MD_Preparedness_1	—				
MD_Preparedness_2	0.091*	—			
MD_Preparedness_3	0.263***	0.038	—		
MD_Preparedness_4	0.348***	0.235***	0.139**	—	
MD_Preparedness_5	0.219***	0.152***	-0.013	0.147***	—

* p < .05, ** p < .01, *** p < .001

Table 14- Correlation matrix MD preparedness

	IoT_Preparedness_1	IoT_Preparedness_2	IoT_Preparedness_3	IoT_Preparedness_4	IoT_Preparedness_5
IoT_Preparedness_1	—				
IoT_Preparedness_2	0.326***	—			
IoT_Preparedness_3	0.279***	0.124**	—		
IoT_Preparedness_4	0.088*	0.270***	0.436***	—	
IoT_Preparedness_5	0.493***	0.267***	0.240***	0.187***	—

* p < .05, ** p < .01, *** p < .001

Table 15- Correlation matrix IoT devices preparedness

4.4 EFA

EFA is utilized to classify latent factors. It is usually done to reduce variables into a smaller set to preserve time and expedite more spontaneous interpretations. There are various extraction methods such as principal axis factor and maximum likelihood. EFA is mathematically complex, and the measures used to determine the number and significance of the factors. There are two kinds of rotation methods, orthogonal rotation, and oblique rotation. Orthogonal rotation (e.g., Varimax) includes uncorrelated factors, whereas oblique rotation (e.g., promax) involves correlated factors. The interpretation of EFA is based on rotated factor loadings, rotated eigenvalues, and scree test. In this study EFA is carried out for mobile devices perception, IoT devices perception, mobile devices preparedness and IoT devices preparedness.

4.4.1 EFA - Mobile Devices Perception

The EFA for mobile devices perception is done by considering three items which are correlated with an internal consistency of .778 (Table 8). To determine the number of factors associated with the variables, an eigenvalue of 1.0 was set with oblique rotation (promax). Oblique rotation is used to simplify the loading structure, allowing us to interpret the factor loadings more easily. From table 16, we can see that all the variables of mobile devices perception primarily load onto only one factor.

Factor Loadings

	Factor 1	Uniqueness
MD_Perception_3	0.705	0.502
MD_Perception_4	0.834	0.305
MD_Perception_5	0.670	0.550

Note. Applied rotation method is promax.

Table 16- Factor loadings of MD perception

Factor Correlations

	Factor 1
Factor 1	1.000

Table 17- Factor correlations of MD perception

The path diagram given in figure 2 represents the number of factors the variables are associated with, and the thick lining explains how well they are associated with that factor. The Scree plot given in figure 3 is a line plot of the eigenvalues of components in the analysis. It also used to determine the number of factors to retain for further analysis.

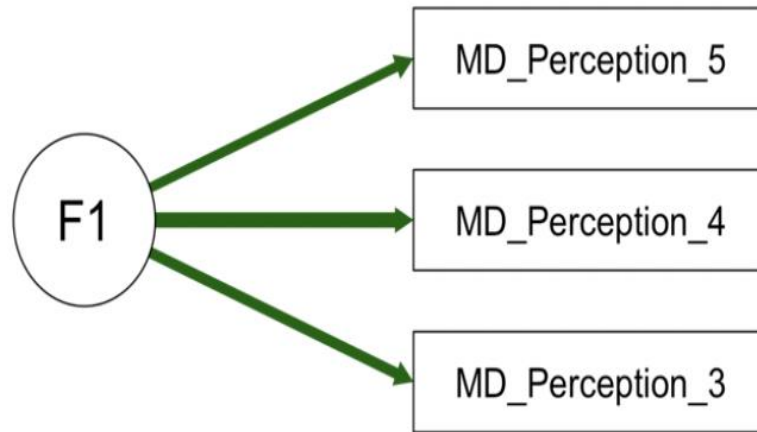


Figure 2- Path diagram of MD perception

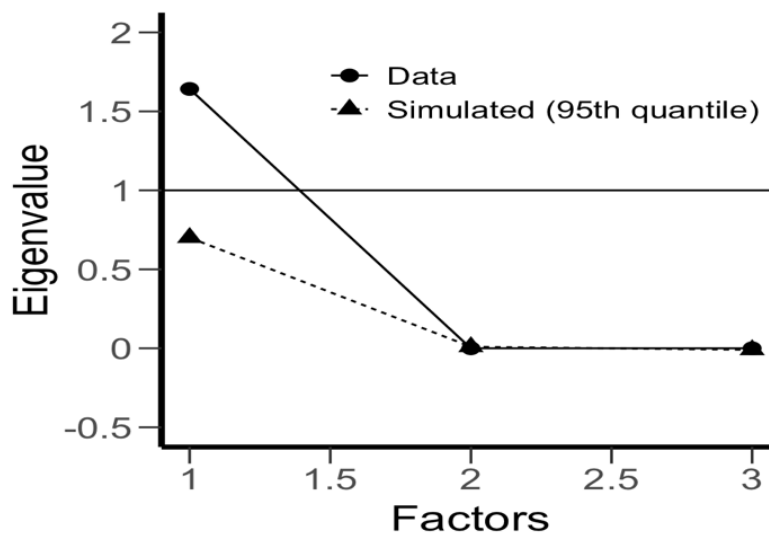


Figure 3- Scree plot of MD perception

4.4.2 EFA - IoT Devices Perception

The EFA for IoT devices perception is done by considering three items which are correlated with an internal consistency of .726 (Table 9). To determine the number of factors associated with the variables, an eigenvalue of 1.0 was set with oblique rotation (promax). Oblique rotation is used to simplify the loading structure, allowing us to interpret the factor loadings more easily. From table 18, we can see that all the variables of IoT devices perception primarily load onto only one factor.

Factor Loadings

	Factor 1	Uniqueness
IoT_Perception_3_1	0.555	0.691
IoT_Perception_3_3	0.666	0.556
IoT_Perception_4_1	0.545	0.702
IoT_Perception_4_3	0.761	0.421

Note. Applied rotation method is promax.

Table 18- Factor loadings of IoT devices perception

Factor Correlations

	Factor 1
Factor 1	1.000

Table 19- Factor correlations of IoT devices perception

The path diagram given in figure 4 represents the number of factors the variables are associated with, and the thick lining explains how well they are associated with that factor. The Scree plot given in figure 5 is a line plot of the eigenvalues of components in the analysis. It also used to determine the number of factors to retain for further analysis.

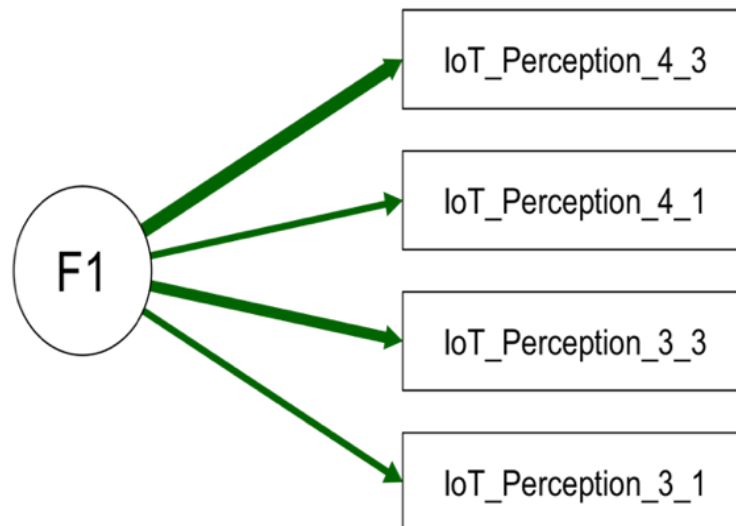


Figure 4- Path diagram of IoT devices perception

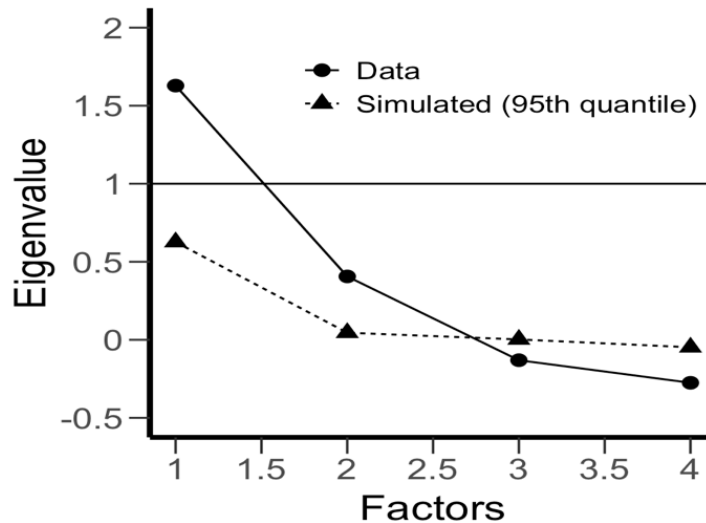


Figure 5- Scree plot of IoT devices perception

4.4.3 EFA - Mobile Devices Preparedness

The EFA for IoT devices perception is done by considering three items which are correlated with an internal consistency of .733 (Table 10). To determine the number of factors associated with the variables, an eigenvalue of 1.0 was set with oblique rotation (promax). Oblique rotation is used to simplify the loading structure, allowing us to interpret the factor loadings more easily. From table 20, we can see that all the variables of mobile devices preparedness primarily load onto only one factor.

Factor Loadings

	Factor 1 Uniqueness	
MD_Preparedness_1	0.641	0.589
MD_Preparedness_4	0.583	0.660
MD_Preparedness_5	0.371	0.862

Note. Applied rotation method is promax.

Table 20- Factor loadings of MD preparedness

Factor Correlations

	Factor 1
Factor 1	1.000

Table 21- Factor correlations of MD preparedness

The path diagram given in figure 6 represents the number of factors the variables are associated with, and the thick lining explains how well they are associated with that factor. The Scree plot given in figure 7 is a line plot of the eigenvalues of components in the analysis. It also used to determine the number of factors to retain for further analysis.

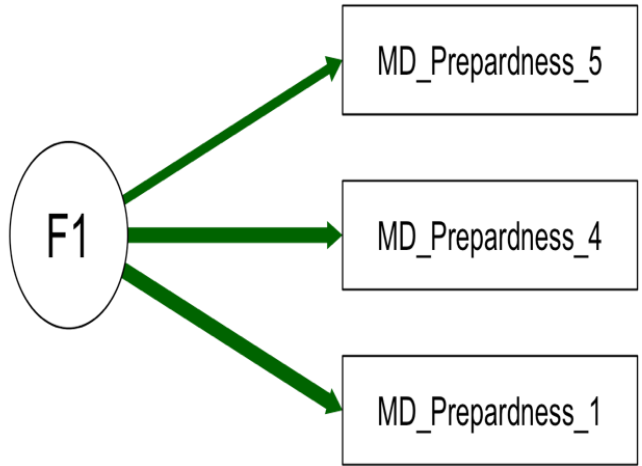


Figure 6- Path diagram of MD preparedness

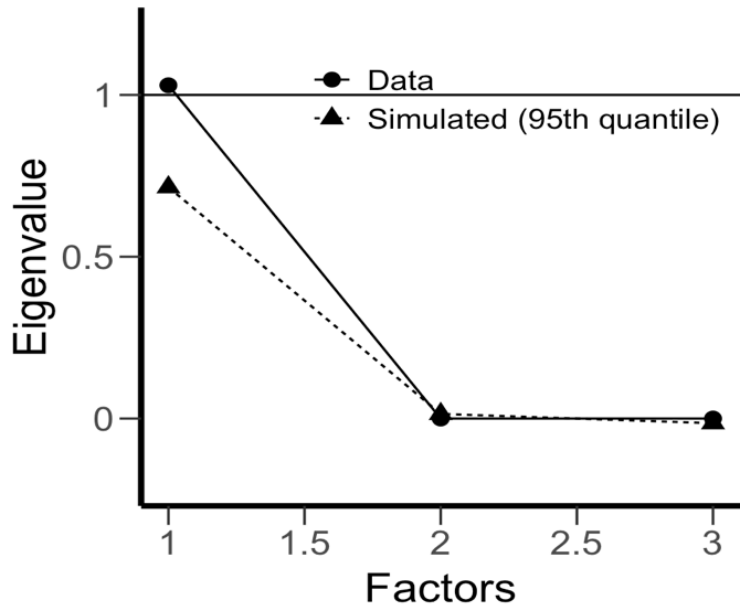


Figure 7- Scree plot of MD preparedness

4.4.4 EFA - IoT Devices Preparedness

The EFA for IoT device's perception is done by considering three items that are correlated with an internal consistency of .788 (Table 11). To determine the number of factors associated with the variables, an eigenvalue of 1.0 was set with oblique rotation (promax). Oblique rotation is used to simplify the loading structure, allowing us to interpret the factor loadings more easily. From table 22, we can see that all the variables of IoT devices preparedness primarily load onto only one factor.

Factor Loadings

	Factor 1	Uniqueness
IoT_Preparedness_1	0.681	0.537
IoT_Preparedness_2	0.459	0.789
IoT_Preparedness_3	0.543	0.705
IoT_Preparedness_4	0.413	0.830
IoT_Preparedness_5	0.627	0.606

Note. Applied rotation method is promax.

Table 22- Factor loadings of IoT devices preparedness

Factor Correlations

	Factor 1
Factor 1	1.000

Table 23- Factor correlations of IoT devices preparedness

The path diagram given in figure 8 represents the number of factors the variables are associated with, and the thick lining explains how well they are associated with that factor. The Scree plot given in figure 9 is a line plot of the eigenvalues of components in the analysis. It also used to determine the number of factors to retain for further analysis.

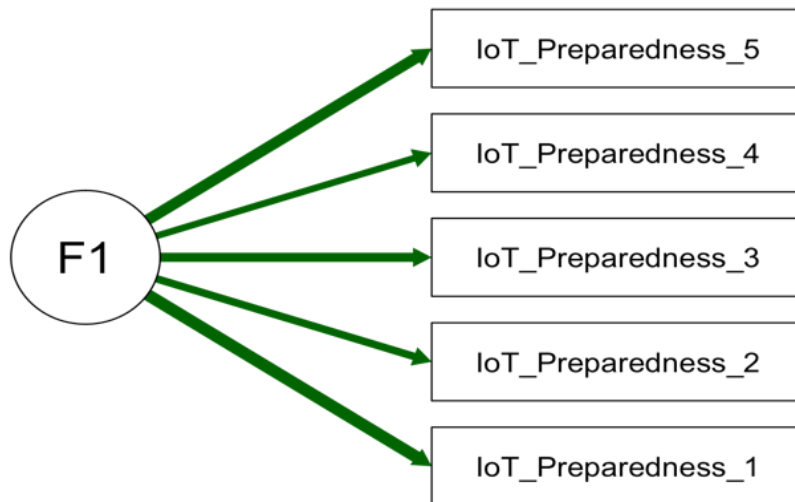


Figure 8- Path diagram of IoT devices preparedness

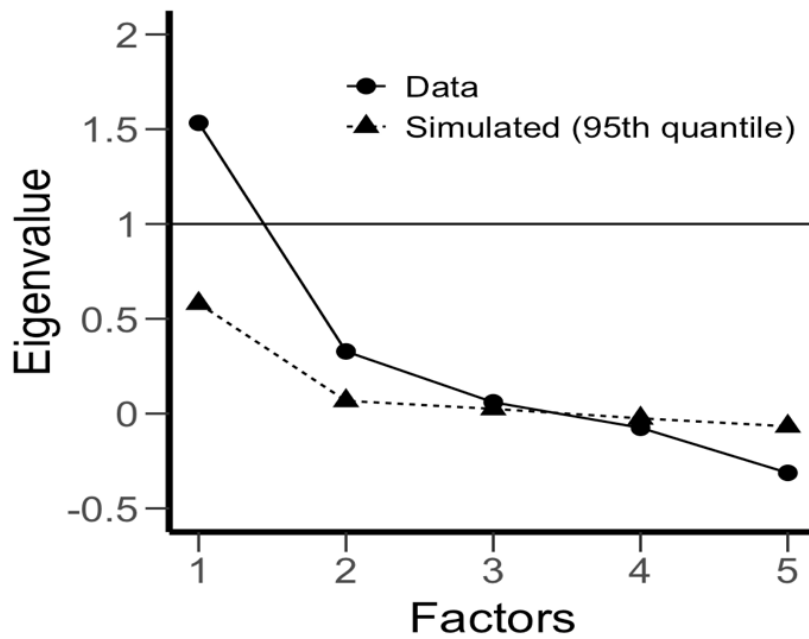


Figure 9- Scree plot of IoT devices preparedness

4.5 Analysis of Mobile and IoT Devices Perception

To answer the first research question, Do users have more perception towards cybersecurity threats for older mobile devices compared to newer IoT devices? various parametric tests were performed for both mobile device's perception and IoT device's perception and compared their scores to understand how different is the perception of users on those devices.

4.5.1 Tests on Mobile Devices Perception

4.5.1.1 ANOVA

ANOVA was conducted considering each correlated variable from table 8 as dependent variable with two factors age-group and education having different levels. From the results it was found that dependent variables statistically significant with p value is less than .05 with small effect.

ANOVA - MD_Perception_3

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	1.387	3.000	0.462	4.625	0.003
Select your level of education	1.496	3.000	0.499	4.988	0.002
Residual	50.795	508.000	0.100		

Note. Type III Sum of Squares

Table 24- ANOVA MD_perception_3

ANOVA - MD_Perception_4

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	10.214	3.000	3.405	2.281	0.078
Select your level of education	16.366	3.000	5.455	3.655	0.013
Residual	758.218	508.000	1.493		

Note. Type III Sum of Squares

Table 25- ANOVA MD_perception_4

ANOVA - MD_Perception _5

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	19.032	3.000	6.344	3.836	0.010
Select your level of education	14.842	3.000	4.947	2.991	0.031
Residual	840.199	508.000	1.654		

Note. Type III Sum of Squares

Table 26- ANOVA MD_perception_5

Post Hoc Comparisons - Please select your age group

		95% CI for Mean Difference			SE	t	Cohen's d
		Mean Difference	Lower	Upper			
18	24	0.111	0.207	0.016	0.037	2.995	0.210
	24	0.118	0.243	0.008	0.049	2.422	0.01
	24	0.257	0.523	0.009	0.103	2.493	0.031
25-34	35-50	0.007	0.122	0.109	0.045	0.149	0.021
	50+	0.146	0.412	0.120	0.103	1.417	0.459
35-50	50+	0.139	0.418	0.139	0.108	1.292	0.420

Note. Confidence level used: 0.95

Table 27- Post HOC comparison age groups MD perception

Post Hoc Comparisons - Select your level of education

		Mean Difference	95% CI for Mean Difference		SE	t	Cohen's d
			Lower	Upper			
Bachelor's degree	High school degree or equivalent	0.124	-0.213	0.461	0.131	0.948	0.381
	Master's degree	0.097	0.004	0.191	0.036	2.682	0.302
	PhD or higher	0.241	0.047	0.435	0.075	3.205	0.748
High school degree or equivalent	Master's degree	0.027	-0.375	0.322	0.135	0.197	0.085
	PhD or higher	0.117	-0.270	0.504	0.150	0.782	0.459
Master's degree	PhD or higher	0.144	-0.051	0.338	0.075	1.908	0.466

Note. Confidence level used: 0.95

Table 28- Post HOC comparison education level MD perception

4.5.1.2 Independent Sample t-test

Independent t-test was conducted considering all the correlated variables from table 7 with Gender and IT-background as grouping variables. From the results table (29, 30) it was evident that for variable MD_Perception_5 the effect size was small and for MD_Perception_4 and MD_Perception_3 the effect size was trivial. Considering a very small effect size of .001 in a

large population can have a large economic or political relevance. For example, sending 100,000 phishing emails and getting 10 hits is a very bad hit rate, but when considering the gain even one hit can produce a large gain.

Independent Samples *t*-test (Gender)

	t	df	p	Mean Difference	SE Difference	Cohen's d
MD_Perception_3_N	0.810	513.000	0.418	0.024	0.029	0.074
MD_Perception_4	0.977	513.000	0.329	0.110	0.113	0.090
MD_Perception_5_N	1.476	513.000	0.040 ^a	0.044	0.030	0.135

Note. Student's *t*-test.

^a Levene's test is significant ($p < .05$), suggesting an equal variance assumption

Table 29- Independent samples *t*-test MD perception (Gender)

Independent Samples *t*-test (IT-background)

	t	df	p	Mean Difference	SE Difference	Cohen's d
MD_Perception_3_N	0.167	513.000	0.867	0.005	0.028	0.015
MD_Perception_4	0.475	513.000	0.635	0.052	0.109	0.042
MD_Perception_5_N	0.218	513.000	0.027 ^a	0.006	0.029	0.119

Note. Student's *t*-test.

^a Levene's test is significant ($p < .05$), suggesting an equal variance assumption

Table 30- Independent samples *t*-test MD perception (IT-background)

4.5.2 Tests on IoT Devices Perception

4.5.2.1 ANOVA

ANOVA was conducted considering each correlated variable from table 8 as dependent variable with two factors age-group and education having different levels. From the results it was found that dependent variables statistically significant with p value is less than .05 with small effect.

ANOVA - IoT_Perception_3_1

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	2.139	3.000	0.713	0.319	0.012
Select your level of education	3.033	3.000	1.011	0.452	0.016
Residual	1136.037	508.000	2.236		

Note. Type III Sum of Squares

Table 31- ANOVA IoT_perception_3_1

ANOVA - IoT_Perception_3_3

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	1.276	3.000	0.425	0.200	0.896
Select your level of education	8.635	3.000	2.878	1.357	0.255
Residual	1077.813	508.000	2.122		

Note. Type III Sum of Squares

Table 32- ANOVA IoT_perception_3_3

ANOVA - IoT_Perception_4_1

Cases	Sum Squares	of df	Mean Square	F	p
Please select your age group	14.374	3.000	4.791	1.938	0.122
Select your level of education	9.728	3.000	3.243	1.312	0.270
Residual	1255.788	508.000	2.472		

Note. Type III Sum of Squares

Table 33- ANOVA IoT_perception_4_1

ANOVA - IoT_Perception_4_3

Cases	Sum of Squares	df	Mean Square	F	p
Please select your age group	0.878	3.000	0.293	0.120	0.949
Select your level of education	9.410	3.000	3.137	1.283	0.279
Residual	1241.883	508.000	2.445		

Note. Type III Sum of Squares

Table 34- ANOVA IoT_perception_4_3

Post Hoc Comparisons - Please select your age group

			95% CI for Mean Difference				
Mean Difference			Lower	Upper	SE	t	Cohen's d
18	24	0.156	0.609	0.297	0.176	0.886	0.019
	24	0.182	0.775	0.411	0.230	0.790	0.012
	24	0.079	1.337	1.179	0.488	0.162	0.036
25-34	35-50	0.026	0.571	0.519	0.211	0.124	0.018
	50+	0.077	1.180	1.333	0.487	0.157	0.052
35-50	50+	0.103	1.212	1.418	0.510	0.202	0.073

Note. Confidence level used: 0.95

Table 35- Post HOC comparison age groups IoT devices perception

Post Hoc Comparisons - Select your level of education

		Mean Difference	95% CI for Mean Difference		SE	t	Cohen's d
			Lower	Upper			
Bachelor's degree	High school degree or equivalent	0.203	1.798	1.391	0.619	0.329	0.134
	Master's degree	0.177	0.265	0.619	0.172	1.032	0.118
	PhD or higher	0.057	0.975	0.860	0.356	0.161	0.038
High school degree or equivalent	Master's degree	0.380	1.267	2.028	0.639	0.595	0.254
	PhD or higher	0.146	1.683	1.976	0.710	0.206	0.111
Master's degree	PhD or higher	0.234	1.154	0.685	0.357	0.657	0.161

Note. Confidence level used: 0.95

Table 36- Post HOC comparison education level IoT devices perception

4.5.2.2 Independent Sample *t*-test

Independent *t*-test was conducted considering all the correlated variables from table 9 with gender and IT-background as grouping variables. From the results table (37, 38) it was evident that for all the variables the effect size was trivial.

Independent Samples *t*-test (Gender)

	t	df	p	Mean Difference	SE Difference	Cohen's d
IoT_Perception_3_1	0.561	513.000	0.575	0.077	0.137	0.051
IoT_Perception_3_3	0.864	513.000	0.388	0.115	0.133	0.079
IoT_Perception_4_1	0.825	513.000	0.01 ^a	0.119	0.145	0.076
IoT_Perception_4_3	0.959	513.000	0.338	0.138	0.143	0.088

Note. Student's *t*-test.

^a Levene's test is significant ($p < .05$), suggesting an equal variance assumption

Table 37- Independent samples *t*-test IoT devices perception (Gender)

Independent Samples *t*-test (IT-background)

	t	df	p	Mean Difference	SE Difference	Cohen's d
IoT_Perception_3_1	1.501	513.000	0.134	-0.197	0.131	0.133
IoT_Perception_3_3	0.529	513.000	0.597	-0.068	0.129	0.047
IoT_Perception_4_1	0.834	513.000	0.015	-0.116	0.139	0.074
IoT_Perception_4_3	0.751	513.000	0.453	0.104	0.138	0.066

Note. Student's *t*-test.

Table 38- Independent samples *t*-test IoT devices perception (IT-background)

4.5.3 Comparison Between Mobile and IoT devices Perception

From table 8,9 the items which are correlated for both mobile devices and IoT devices perception were combined by taking the average of each item to form two variables, MD_Perception and IoT_perception.

Paired sample *t*-test was performed having MD_Perception as first variable pair and IoT_Perception as the second. From table 39 we find that the variables are statistically significant $p < .05$ with trivial effect size. Again the same process was followed by considering IoT_Perception as factor variable pair and MD_Perception as the second. From table 39 we find that the variables are statistically significant $p < .05$ with very large effect size. Which explains how the perception of IoT and mobile devices vary with huge increases in various new technologies and devices.

Paired Samples *t*-test

	t	df	p	Mean Difference	SE Difference	Cohen's d
MD_Perception - IoT_Perception	-45.870	514	< .001	-2.345	0.051	-3.042
IoT_Perception - MD_Perception	45.870	514	< .001	2.345	0.051	3.042

Note. Student's *t*-test.

Table 39- Paired sample *t*-test

Group 1 – Mobile devices perception

Group 2 – IoT devices perception

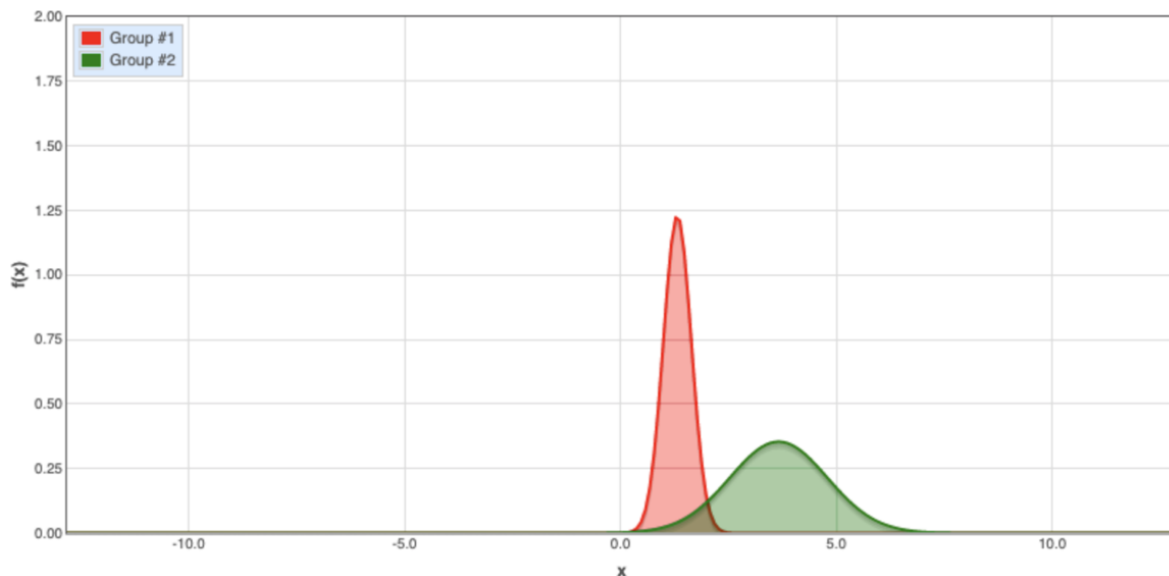


Figure 10- Effect size difference MD & IoT perception

One sample *t*-test was performed for the correlated variable and from table 40 we found that, independently both the mobile and IoT devices perceptions are statistically significant $p < .05$ and have a large effect size.

One Sample *t*-test

	t	df	p	Mean Difference	Cohen's d
MD_Perception	92.306	514	< .001	1.318	4.067
IoT_Perception	73.715	514	< .001	3.663	3.248

Note. Student's *t*-test.

Note. For the Student *t*-test, location parameter is given by mean difference *d* .

Note. For the Student *t*-test, effect size is given by Cohen's *d* .

Table 40- One sample *t*-test

4.6 Analysis of Mobile and IoT Devices Preparedness

To answer the second research question, do users have more preparedness towards cybersecurity threats for older mobile devices compared to newer IoT devices? various non-parametric tests were performed for both mobile device's preparedness and IoT device's preparedness and compared their scores to understand how different is the preparedness of users on those devices.

4.6.1 Tests on Mobile Devices Preparedness

4.6.1.1 Kruskal-Wallis Test

Kruskal-Wallis test was performed considering the correlated variable from table 10 as dependent variable with two fixed factors age-group and education. From table 41 we find that there is a statistically significant difference in the continuous variables across the two factors and have a small effect size.

Kruskal-Wallis test

Factor	Statistic	df	p	Effect Size
Please select your age group	3.171	3	0.066	0.201
Select your level of education	3.338	3	0.042	0.135

Table 41- Kruskal-Wallis test (MD preparedness)

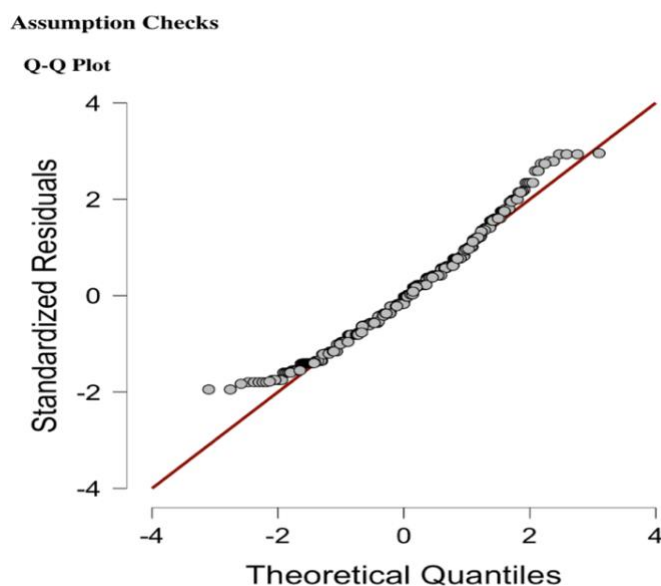


Figure 11- Assumption Check Q-Q plot MD preparedness

4.6.1.1 Mann-Whitney U Test

Mann-Whitney U test was performed considering the correlated variables from table 10 with two groups (Male, Female for Gender and IT , non-IT for IT-background). From table 42, 43 we find that the preparedness of the two groups (Gender, IT-background) were statistically significant $p < .05$ and have a small effect size.

Mann-Whitney U test (Gender)

	W	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
MD_Preparedness_1	26191.500	0.005	7.198e -6	0.144
MD_Preparedness_4	28251.000	0.108	5.668e -5	0.077
MD_Preparedness_5	25049.500	< .001	1.000	0.181

Note. For the Mann-Whitney test, effect size is given by the rank biserial correlation.

Table 42- Mann-Whitney U test MD preparedness (Gender)

Mann-Whitney U test (IT-background)

	W	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
MD_Preparedness_1	34443.500	0.380	3.265e -5	0.144
MD_Preparedness_4	32112.500	0.559	1.645e -5	0.027
MD_Preparedness_5	31956.500	0.529	8.189e -5	0.132

Note. For the Mann-Whitney test, effect size is given by the rank biserial correlation.

Table 43- Mann-Whitney U test MD preparedness (IT-background)

4.6.2 Tests on IoT Devices Preparedness

4.6.2.1 Kruskal-Wallis Test

Kruskal-Wallis test was performed by considering the correlated variable from table 11 as dependent variable with two fixed factors age-group and education. From table 44 we find that there is a statistically significant difference in the continuous variables across the two factors and have a small effect size.

Kruskal-Wallis test

Factor	Statistic	df	p	Effect Size
Please select your age group	2.987	3	0.394	0.221
Select your level of education	7.191	3	0.066	0.102

Table 44- Kruskal-Wallis test (IoT preparedness)

Assumption Checks

Q-Q Plot

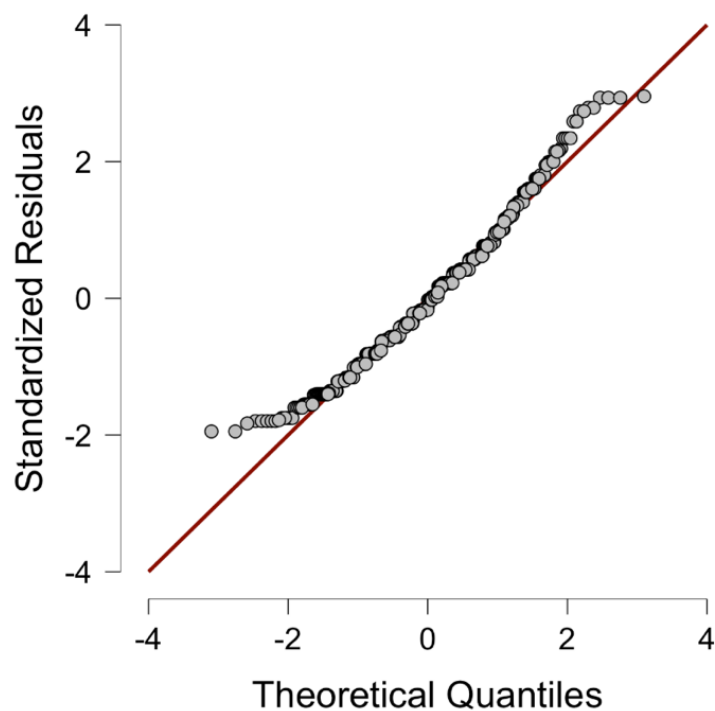


Figure 12- Assumption Check Q-Q plot IoT preparedness

4.6.2.1 Mann-Whitney U Test

Mann-Whitney U test was performed considering the correlated variables from table 11 with two groups (male, female for gender and IT , Non-IT for IT-background). From table 45, 46 we find that the preparedness of the two groups (gender, IT-background) were statistically significant $p < .05$ and have a small effect size.

Mann-Whitney U test (Gender)

	W	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
IoT_Preparedness_1	29289.500	0.041	6.128e -5	0.043
IoT_Preparedness_2	26634.500	0.013	4.199e -5	0.130
IoT_Preparedness_3	28734.000	0.024	1.134e -5	0.061
IoT_Preparedness_4	27877.000	0.088	1.980e -5	0.089
IoT_Preparedness_5	27326.000	0.040	2.862e -5	0.107

Note. For the Mann-Whitney test, effect size is given by the rank biserial correlation.

Table 45- Mann-Whitney U test IoT preparedness(Gender)

Mann-Whitney U test (IT-background)

	W	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
IoT_Preparedness_1	30819.000	0.177	1.120e -6	0.066
IoT_Preparedness_2	28834.500	0.012	2.365e -5	0.126
IoT_Preparedness_3	33675.000	0.672	4.439e -5	0.020
IoT_Preparedness_4	31605.500	0.400	3.535e -5	0.042
IoT_Preparedness_5	34438.500	0.384	3.858e -5	0.044

Note. For the Mann-Whitney test, effect size is given by the rank biserial correlation.

Table 46- Mann-Whitney U test IoT preparedness(IT-background)

4.6.3 Comparison between Mobile and IoT devices Preparedness

From table 10,11 the items which are correlated for both mobile devices and IoT devices preparedness were combined by taking the average of each item to form two variables, MD_Preparedness and IoT_Preparedness. Paired sample *t*-test (*Wilcoxon* signed-rank test) was performed having MD_Preparedness as first variable pair and IoT_Preparedness as the second. From table 47 we find that the variables are statistically significant $p < .05$ with large effect size. Again the same process was followed by considering IoT_Preparedness as factor variable pair and MD_Preparedness as the second. From table 47 we find that the variables are statistically significant $p < .05$ with very trivial effect size. Which gives an indication that being prepared for different cybersecurity threats in mobile devices are more easier and well known compared to that of the newer IoT devices.

Wilcoxon signed-rank test

	W	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
MD_Preparedness - IoT_Preparedness	64571.500	0.047	0.035	0.46
IoT_Preparedness - MD_Preparedness	60678.500	0.047	-0.035	-0.46

Table 47- Wilcoxon signed-rank test

Group 1 – Mobile devices preparedness

Group 2 – IoT devices preparedness

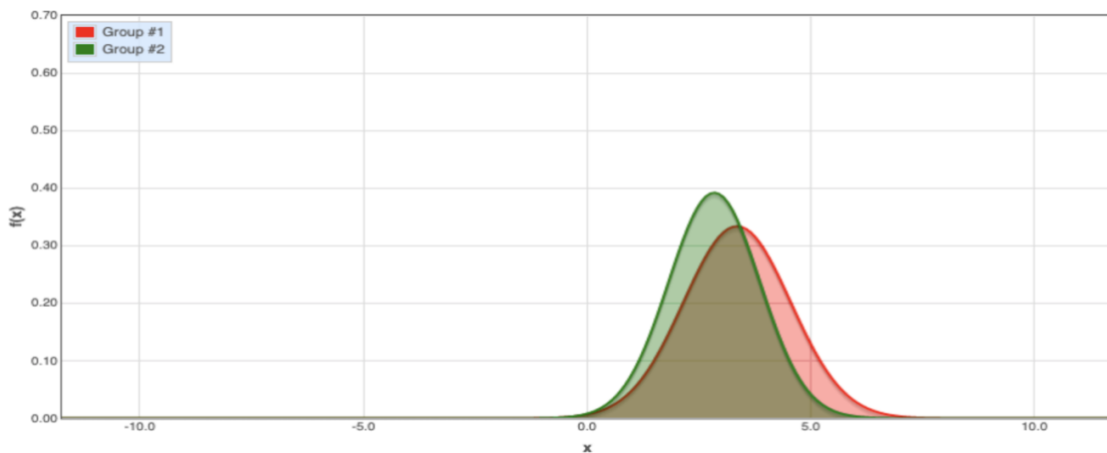


Figure 13- Effect size difference MD & IoT preparedness

One sample *t*-test (Wilcoxon signed-rank test) was performed for the correlated variable and from table 48 we found that, independently both the mobile and IoT devices preparedness are statistically significant $p < .05$ and have a large effect size.

One Sample *t*-test

	V	p	Hodges-Lehmann Estimate	Rank-Biserial Correlation
MD_Preparedness	132870.000	< .001	2.835	1.000
IoT_Preparedness	132870.000	< .001	2.800	1.000

Note. Wilcoxon signed-rank test.

Note. For the Wilcoxon test, location parameter is given by the Hodges-Lehmann estimate.

Note. For the Wilcoxon test, effect size is given by the matched rank biserial correlation.

Table 48- One sample *t*-test (Wilcoxon signed-rank test)

4.7 Analysis of Mobile Devices Perception and Preparedness

To answer the third research question, how does users' perception towards cybersecurity threats reflect their preparedness in mobile devices? various tests were performed for both mobile device's perception and preparedness and compared their scores to understand how different is perception and preparedness of users in mobile devices.

From table 8, 10 the items which are correlated for both mobile devices perception and preparedness were combined by taking the average of each item to form two variables, MD_Perception and MD_Preparedness.

Paired sample *t*-test (Student, Wilcoxon signed-rank test) was performed having MD_Perception as first variable pair and MD_Preparedness as the second and from table 49 we see that the variables are statistically significant and have a large effect size. Which gives an indication that people have higher perception combined with preparedness towards cybersecurity threats in mobile devices.

Paired Samples *t*-test

	Test	Statistic	df	p	Location Parameter	SE Difference	Effect Size
MD_Perception - MD_Preparedness	Student	28.686	514	< .001	1.568	0.055	1.789
	Wilcoxon	3699.500		< .001	1.557		0.943

Note. For the Student *t*-test, location parameter is given by mean difference *d* ; for the Wilcoxon test, effect size is given by the Hodges-Lehmann estimate.

Note. For the Student *t*-test, effect size is given by Cohen's *d* ; for the Wilcoxon test, effect size is given by the matched rank biserial correlation.

Table 49- Paired sample *t*-test (MD perception and preparedness)

Group 1 – Mobile devices perception

Group 2 – Mobile devices preparedness

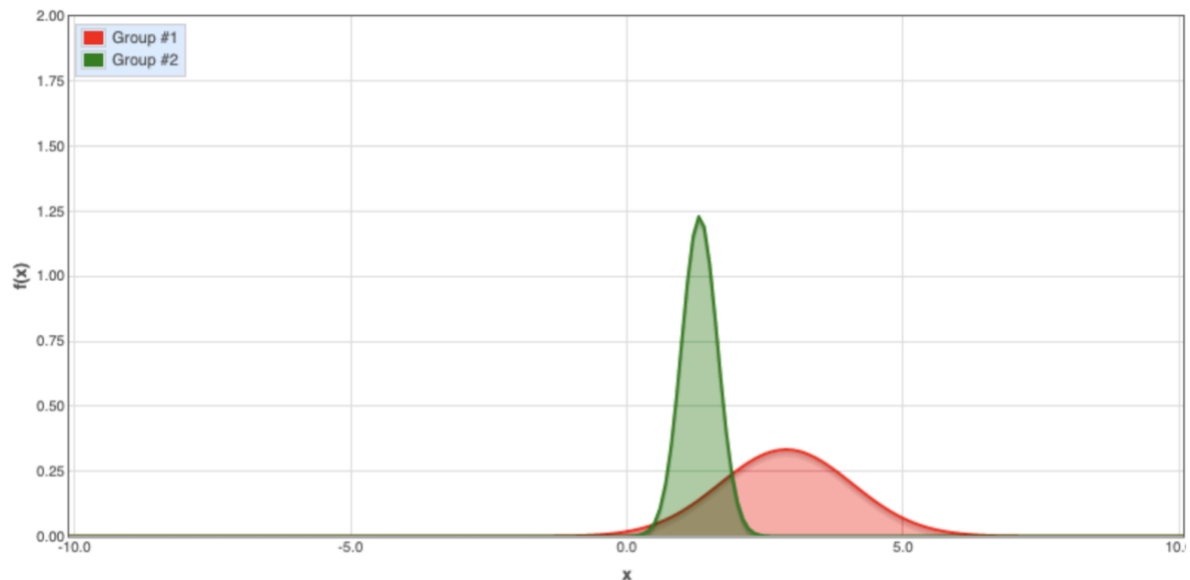


Figure 14- Effect size difference MD perception & preparedness

One sample *t*-test (Student, Wilcoxon signed-rank test) was performed for each variable mentioned above and from table 50 we see that both perception and preparedness are statistically significant $p < .05$ and have a large effect size.

One Sample *t*-test

	Test	Statistic	df	p	Location Parameter	Effect Size
MD_Perception	Student	92.306	514	< .001	1.318	4.067
	Wilcoxon	132870.000		< .001	1.306	1.000
MD_Preparedness	Student	54.735	514	< .001	2.885	2.412
	Wilcoxon	132870.000		< .001	2.835	1.000

Note. For the Student *t*-test, location parameter is given by mean difference *d* ; for the Wilcoxon test, location parameter is given by the Hodges-Lehmann estimate.

Note. For the Student *t*-test, effect size is given by Cohen's *d* ; for the Wilcoxon test, effect size is given by the matched rank biserial correlation.

Table 50- One sample *t*-test MD perception & preparedness

4.8 Analysis of IoT Devices Perception and Preparedness

To answer the fourth research question, how does users' perception towards cybersecurity threats reflect their preparedness in IoT devices? various tests were performed for both IoT device's perception and preparedness and compared their scores to understand how different is perception and preparedness of users in IoT devices.

From table 9,11 the items which are correlated for both IoT devices perception and preparedness were combined by taking the average of each item to form two variables, IoT_Perception and IoT_Preparedness.

Paired sample *t*-test (Student, Wilcoxon signed-rank test) was performed having IoT_Perception as first variable pair and IoT_Preparedness as the second and from table 51 we see that the variables are statistically significant and have a large effect size. Which gives an interpretation that people have good perception and preparedness towards cybersecurity threats in IoT devices.

Paired Samples *t*-test

	Test	Statistic	df	p	Location Parameter	SE Difference	Effect Size
IoT_Perception - IoT_Preparedness	Student	12.240	514	< .001	0.819	0.067	0.763
	Wilcoxon	10.340		< .001	0.850		0.559

Note. For the Student *t*-test, location parameter is given by mean difference *d* ; for the Wilcoxon test, effect size is given by the Hodges-Lehmann estimate.

Note. For the Student *t*-test, effect size is given by Cohen's *d* ; for the Wilcoxon test, effect size is given by the matched rank biserial correlation.

Table 51- Paired sample *t*-test (IoT perception and preparedness)

- Group 1 – IoT devices perception
- Group 2 – IoT devices preparedness

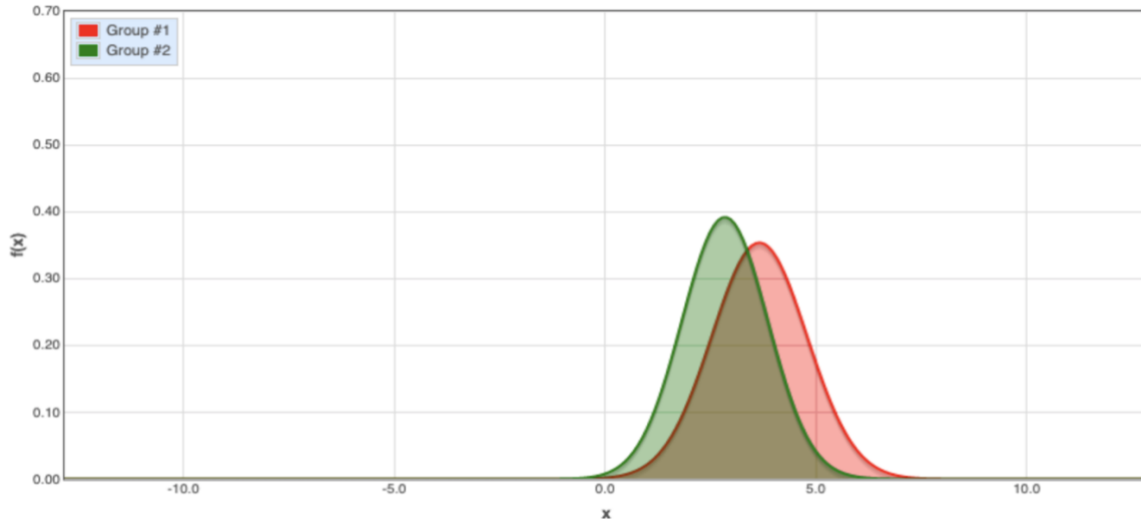


Figure 15- Effect size difference IoT perception & preparedness

One sample t -test (Student, Wilcoxon signed-rank test) was performed for each variable mentioned above and from table 52 we see that both perception and preparedness are statistically significant $p < .05$ and have a large effect size.

One Sample t -test

	Test	Statistic	df	p	Location Parameter	Effect Size
IoT_Perception	Student	73.715	514	< .001	3.663	3.248
	Wilcoxon	132870.000		< .001	3.625	1.000
IoT_Preparedness	Student	63.412	514	< .001	2.844	2.794
	Wilcoxon	132870.000		< .001	2.800	1.000

Note. For the Student t -test, location parameter is given by mean difference d ; for the Wilcoxon test, location parameter is given by the Hodges-Lehmann estimate.

Note. For the Student t -test, effect size is given by Cohen's d ; for the Wilcoxon test, effect size is given by the matched rank biserial correlation.

Table 52- One sample t -test (IoT perception and preparedness)

5 Discussion

5.1 Research Implications

The study used quantitative statistical analysis to examine data derived from online surveys. This study examined the hypothetical relationships between perception and preparedness of a user towards cybersecurity threats in mobile and IoT devices, drawing from the literature review. It also sheds light on previously unexplored relationships between perception and preparedness of users towards various cybersecurity threats. Four objectives are discussed using the statistical results listed in Chapter 4.

Objective 1: Whether the user's perception towards cybersecurity threats for older mobile devices differ when compared to newer IoT devices?

As we have seen in the section 2.3 individuals play an important role in cybersecurity. The perception on mobile and IoT devices are measured as the extent to which a person has heard about past incidents, increases the identification of various vulnerabilities inherent to those devices and the day-to-day activities the user perform in those devices. Unless cybersecurity perception comes with a strong understanding of and commitment to security, it does not gain the required psychological attention to security issues.

Analysis of section 4.5 we see how the perception of users towards cybersecurity threats varies between mobile and IoT devices. From table 39, it is evident that the perception of IoT device threats is higher than that of the mobile devices as it depends upon the knowledge about the security implications in those devices. The analysis of variance helped to identify notable groups of people who are between 25-34 age groups with a master's or Ph.D. level of education have a more substantial perception of security in mobile devices. In contrast, users with an 18-24 age group with a bachelor's degree have a good understanding of security in IoT devices. This shows that the difference in age groups and education level have a significant factor in adapting to the latest technology and methods. This is the clear indication that user's perceptive changes based on the culture and education [24]. From table 40, we see that individually the perception score of knowledge of cybersecurity risks changes and has a considerable effect when considering the perception of the user separately for IoT and mobile.

Objective 2: Whether the user's preparedness towards cybersecurity threats for older mobile devices differ when compared to newer IoT devices?

From in section 4.6, we see that the preparedness of users towards cybersecurity threats varies between mobile and IoT devices. The exponential growth of the IoT has led to greater security and privacy risks, which makes the preparedness of these devices more complex and advanced compared to that of the mobile devices. From table 47, it's evident that user's preparedness to cybersecurity threats in mobile devices is higher than that of IoT devices. Due to the complexity of the IoT devices, it makes it more expensive and challenging to devise and apply appropriate measures. From table 48, 51 we can see that preparedness of user's with IT background with regards to security in mobile devices is slightly better that IoT devices.

Objective 3: Whether the user's perception towards cybersecurity threats in mobile devices is associated with preparedness?

Analysing furthermore on the concept of user's perception and preparedness, we look into the case on how the knowledge of users towards cybersecurity threats reflects their readiness in mobile devices. From section 4.7, we see a strong link between the perception and preparedness of cybersecurity threats in mobile devices. Since people are more familiar with the use of mobile devices it increases their perception and preparedness due to experiences in encountering various risks while using them. For example, People tend to avoid downloading applications from third-party websites even though some of the apps shared by such repositories are passed through strict controls as it doesn't provide any guarantee that the app is secure enough to be used. Being more aware helps a user to be more ready to control the threats on their devices.

Objective 4: Whether the user's perception towards cybersecurity threats in IoT devices is associated with preparedness?

After looking into the analysis of how perception and preparedness are linked in mobile devices, we now see how the knowledge of users towards cybersecurity threats reflects their readiness in IoT devices. From section 4.8, we can infer that perception has an effect on preparedness towards cybersecurity threats in IoT devices. But comparing the result of Objective 3, section 4.7 it is clear that the link between perception and preparedness in mobile devices is almost double that of what we see in IoT devices. On the contrary, the perception of security threats in IoT devices is higher compared to that in mobile devices, although the difference is not substantial.

5.2 Practical Implications

The theoretical findings of this study offer policy implications for cybersecurity practitioners and policymakers. This study discusses how the perception of users reflects in preparedness in their day-to-day usage of IoT and mobile devices. Significantly, this comparison is done considering dimensions like education, work background and age group. This study provides statistical evidence that preparation to cybersecurity should be responsively tailored to the needs of the users especially considering the psychological divides arising from demographic conditions. The above implications can be considered as an indication that practitioners and policymakers can better reach the end-users if they consider demographic dimensions and tailor their policies and awareness trainings accordingly. For example, demographic controls such as age, exhibited a significant influence as seen from table 3. This finding reveals that age group of above 35, experience more gap of perception compared to the lower age groups. This is also an indication that sensitivity of perception and psychological reactions to technological threats vary across generations. These psychological observations should be the main focus for practitioners and policymakers when creating new policies. Practitioners cannot directly influence personal practices and awareness of cybersecurity breaches. However, practitioners could make long-term commitments to building confidence in multidimensional trust using the link between the perception and preparedness towards privacy and security in day-to-day activities. Also, strategies for attitudinal shifts are essential, particularly to more technologically advanced countries that are more exposed to cyberattacks against critical infrastructures.

In an organization, a single device which gets infected has a way of infecting other devices, and compromised systems can make everyone vulnerable. However, organizations must further enhance their efforts by strengthening awareness training and security behavior education.

User's perception analysis outcomes are vital for designing user awareness programs [80]. Universities and organizations have various options available to teach students and other mobile or IoT device users about risks and educate them about the merit of precautionary behaviors. This study offers different user dimensions and would help designers to develop user awareness programs more accurately. For teachers, this study can be used as a starting point of discussion in various lectures and other educational purposes or as a start to a more extensive study on user's perception of cybersecurity threats.

5.3 Limitations

There are several limitations to the study that could not be controlled. The results of the study express the views of users, covering a total sample size of 515 participants. Due to the limitation of time, an extensive survey could not be performed to sample a broader range of users. Without the time limitation we could increase the density of samples under each demographic considered. For example in age demographic, there were no respondents to the survey who were below 18 years of age and the sample size of respondents above 35 years of age was not significant. The accuracy of quantitative research can be increased with larger sample sizes. Quantitative research methods usually comprise of a structured questionnaire with close-ended questions. This can produce responses from random guessers and potentially induces some errors in the data, and accurate opinions may be obscured. Also, the respondents have limited options of reactions, based on the selection made by the researcher.

5.4 Future Work

Various questions surfaced during the research, and the following points would be a continuation of this study:

1. It will also be interesting to perform a comparative analysis between users from different countries to understand how societal, governmental, or educational environments can affect the perception and preparedness in mobile and IoT devices.
2. Future research could be performed using a similar structured sample, with a consideration of a larger population, so it would reduce the influence the sample data can have on the outcomes.
3. It will also be valuable to create a model to predict the preparedness scores using the perception as input data and compare it with the statistical method outcome to see how the results vary between the different approaches.
4. More analysis on discovering gaps in why different age-groups do not have an understanding of various security concerns in mobile and IoT devices.
5. Stalking or tracking in IoT devices is one of the most frequent human attacks that has been recorded in 2019 [65]. Exploring the user's perspective and readiness to these types of attacks will help in mitigating the threats posted on those devices.

6 Conclusion

The objective of this study was to examine the user's understanding of cybersecurity threats and how prepared they are in IoT and mobile devices. In the literature review, various studies related to IoT device vulnerabilities, finding the weakest actors in specific critical threat scenarios, and many proposals of cyber exercises, awareness training, policy creations were mainly focusing on understanding the security vectors. However, it has failed to address the gap between perception and preparedness towards different cybersecurity threats in mobile and IoT devices. The study used quantitative statistical analysis to examine data derived from online surveys. Various parametric and non-parametric tests are conducted to answer the research questions presented in this study.

The sample results and analysis highlight how factors like education level, age, IT-background, have an effect on the user's knowledge and readiness towards cybersecurity threats in IoT, and mobile devices. The study also discovers how the difference in age group and education level affects user's perception scores. The analysis shows a strong link between perception and preparedness in terms of cybersecurity. This is a clear indication that understanding and bridging this gap in perception among users should be a priority for cybersecurity practitioners in all public and business entities. The conclusions from this study can be utilized as a primary discussion point by various parties, such as schools, universities, parents, and teachers, to educate and develop personalized user perception and preparedness comparisons. This study also motivates further research on how the type and extent of the gap between the perception of and preparedness for cybersecurity in IoT and mobile devices change over time, taking into consideration the ever-changing nature of cyberspace.

References

- [1] Committed to connecting the world(2019), Statistics, [Online], Available: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> [Accessed 15 April 2020].
- [2] SonicWall (2019), Ransomware Attacks, Malware Volume Drop But More Targeted, Nefarious, [Online], Available: <https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/> [Accessed 14 April 2020].
- [3] Security Boulevard (2019), 20 Surprising IoT Statistics You Don't Already Know, [Online], Available: <https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/> [Accessed 14 April 2020].
- [4] Enterprise Verizon (2017), Data Breach Investigations Report, [Online], Available: https://enterprise.verizon.com/resources/reports/2017_dbir.pdf [Accessed 14 April 2020].
- [5] Hicham, Hammouchi, Othmane, Cherqi. (2019), Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time, *Procedia Computer Science* v 151, 2019, Pages 1004-1009.
- [6] Roberto, O, Andrade, Sang, Guun, Yoo, (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity, *Journal of Information Security and Applications*, v 48.
- [7] R. Breton, R. Rousseau. (2018). THE C-OODA: A Cognitive Version of the OODA loop to represent C2 activities Topic.
- [8] J. Timonen. (2015). Improving situational awareness of cyber-physical systems based on operator's goal, *International conference on cyber situational awareness, data analytics and assessment (CyberSA)*, London, pp. 1-6.
- [9] Ling, Li, Wu, He, Li, Xu, Ivan, Ash, Mohd, Anwar, Xiaohong, Yuanb. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour, *International Journal of Information Management*, v 45, pp. 13-24.
- [10] T. Herath, H.R. Rao. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness *Decision Support Systems*, v 47(2). pp. 154-165.
- [11] .K.C. Park, D.-H. Shin. (2016). Security assessment framework for IoT service *Telecommun. Syst.*, pp. 1-17.
- [12] A. Gendron Cyber threats and multiplier effects: Canada at risk *Can. Foreign Policy J.*, 19 (2) (2013), pp. 178-198
- [13] C. Griffy-Brown, D. Lazarikos, M. Chun How do you secure an environment without a perimeter? Using emerging technology processes to support information security efforts in an agile data center *J. Appl. Bus. Econom.*, 18 (1) (2016), pp. 90-102

- [14] H. Miller, C. Griffy-Brown Developing a framework and methodology for assessing cyber risk for business leaders *J. Appl. Bus. Econom.*, 20 (3) (2018), pp. 34-50
- [15] G. Weimann Cyberterrorism: the sum of all fears? *Stud. Conflict Terrorism*, 28 (2) (2005), pp. 129-149
- [16] B. Hoffman *Inside Terrorism* Columbia University Press, New York (1998)
- [17] N. Ben-Asher, C. Gonzalez Effects of cyber security knowledge on attack detection *Comput. Hum. Behav.*, 48 (2015), pp. 51-61
- [18] The recent study of Hewlett Packard, Hewlett Packard Internet of Things Research Study, 2015 Report (2015), v 3.
- [19] Christopher J. Rezendes & W. David Stephenson, (2013) *Cybersecurity on the Internet of Things*.
- [20] Pratyusa K. Manadhata & Jeannette M. Wing, (2010). *An Attack Surface Metric*, IEEE Transactions on Software Engineering, pp. 4.
- [21] Groopman, J., Etlinger, S. (2015). *Consumer Perceptions of Privacy in the Internet of Things*. Altimeter, Atlanta.
- [22] P. Kumaraguru and N. Sachdeva. (2012). *Privacy in India: Attitudes and Awareness V 2.0*, Indraprastha Institute of Information Technology, New Delhi.
- [23] P. Kumaraguru and L. Cranor. (2005). *Privacy in India: Attitudes and Awareness*, Carnegie Mellon University, Pittsburgh.
- [24] Frank, Breitingea., Ryan, Tully-Doyle., Courtney, Hassenfeldt. (2019), A survey on smartphone user's security choices, awareness and education, *Computers & Security*, v 88.
- [25] The recent study of Hewlett Packard, Hewlett Packard Internet of Things Research Study, 2015 Report (2015), v 3.
- [26] Dan, Goodin. (2019), *Alexa and Google Home abused to eavesdrop and phish passwords*, Arstechnica.
- [27] Tom, Spring. (2019), *DEF CON 2019: Researchers Demo Hacking Google Home for RCE*, Threat post.
- [28] InformationWeek IT networks. (2019). *IoT Attacks Up Significantly in the First Half of 2019*, Dark Reading.
- [29] Melissa, Michael. (2019). *Attack Landscape H1 2019: IoT, SMB traffic abounds*. F-secure blog.
- [30] Scott, Shackelford., Anjanette, Raymond., Rakshana, Balakrishnan., Prakhar, Dixit., Julianna, Gjonaj., Rachith, Kavi, (2016) *When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things*, Kelley School of Business Research Paper No. 16-6.

- [31] Massimo, Ficco., Francesco, Palmieri. (2019). An open-source cybersecurity training platform for realistic edge-IoT scenarios, *Journal of Systems Architecture*, 97, P. 107-129.
- [32] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi J. (2017) *Netw. Comput. Appl.*, 88 (15), pp. 10-28.
- [33] Harley, D., Morgan, J., & Frith, H. (2018). *Cyberpsychology as everyday digital experience across the lifespan*. Springer.
- [34] Young, K. S., & Rogers, R. C. (1998). The relationship between depression and Internet addiction. *Cyberpsychology & behaviour*, v 1(1), pp. 25-28.
- [35] Connolly, I., Palmer, M., Barton, H., & Kirwan, G. (Eds.). (2016). *An introduction to cyberpsychology*. Routledge.
- [36] Ethan, Sprissler., Zheng, Yan., Thomas, Robertson., River, Yan., Sung, Yong, Park., Samantha, Bordoff., Quan, Chen. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment. *Computers in human behaviour*, v 84, pp. 375-382.
- [37] Taewoo, Nam. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society*, v 58.
- [38] Karen, Renaudb., Verena, Zimmermann. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, v 131, pp. 169-187.
- [39] Statistics Canada (2010), *Survey Methods and Practises*, Ottawa: National Library of Canada..
- [40] G. Peersman, (2014), *Overview: Data Collection and Analysis Methods in Impact Evaluation*, Florence: UNICEF Office of Research.
- [41] E. Heiervang and R. Goodman, (2011), "Advantages and limitations of web-based surveys: evidence from a child mental health survey.," *Soc Psychiatry Psychiatr Epidemiol*, vol. 46, no. 1, pp. 69-76.
- [42] Dzofo Azmi, (2019), *Clear Gap Between Perceived And Actual Preparedness In SME Cybersecurity*. [Online]. Available: <https://www.digitalnewsasia.com/business/chubb-clear-gap-between-perceived-and-actual-preparedness%E2%80%9D-sme-cyber-security>. [Accessed 14 May 2020].
- [43] L. Hansen, H. Nissenbaum *Digital disaster, cybersecurity, and the Copenhagen School* *Int. Stud. Q.*, 53 (4) (2009), pp. 1155-1175.
- [44] Hadi Hosn, (2018), *Cybersecurity Perception vs Reality: Is Your Organisation Actually Secure?* [Online]. Available: <https://www.secureworks.com/blog/cybersecurity-perception-vs-reality-is-your-organization-actually-secure>. [Accessed 14 May 2020].

- [45] CJ Schmit, [2020], Cyber Security Risk: Perception vs. Reality in Corporate America. [Online]. Available: <https://www.wired.com/insights/2014/03/cyber-security-risk-perception-vs-reality-corporate-america/>. [Accessed 14 May 2020].
- [46] H. Nissenbaum Where computer security meets national security *Ethics Inf. Technol.*, 7 (2) (2005), pp. 61-73.
- [47] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, B. Combs How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits *Policy Sciences*, 9 (2) (1978), pp. 127-152
- [48] S. Hansche Designing a security awareness program: Part I *Inf. Syst. Secur.*, 10 (1) (2008), pp. 14-22
- [49] S.M. Furnell, P.N. Gaunt, R.F. Holben, P.W. Sanders, C.T. Stockel, M.J. Warren (1996), Assessing staff attitudes towards information security in a European healthcare establishment *Med. Informat.*, 21 (2), pp. 105-112
- [50] Y. Chen, F.M. Zahedi (2016), Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China *MIS Quarterly*, 40 (1), pp. 205-222
- [51] A.C. Johnston, M. Warkentin, (2010), Fear appeals and information security behaviors: An empirical study *MIS Quarterly*, 34 (3) , pp. 549-566
- [52] Norton, (2020), What is cyber security? What you need to know, [online]. Available: <https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html> [Accessed 14 May 2020].
- [53] Larry Magid (2014), Why Cyber Security Matters To Everyone. [Online]. Available: <https://www.forbes.com/sites/larrymagid/2014/10/01/why-cyber-security-matters-to-everyone/#711170de5a71> [Accessed 14 May 2020].
- [54] Tier1Cyber, (2019), Cybersecurity Preparedness perception vs reality. [Online] Available: <https://static1.squarespace.com/static/5cd06b029d142c000160a5cc/t/5e261d36166a41157ca57d96/1579556158972/Report-Tier1Cyber.pdf> [Accessed 14 May 2020].
- [55] Sassan S. Hejazi, (2017), Cyber Security Readiness: Perception vs. Reality. [Online]. Available: <https://www.kmco.com/resource-center/article/looking-forward/cyber-security-readiness-perception-vs-reality/> [Accessed 13 May 2020].
- [56] Kritzinger vonSolms, (2010), E.Kritzinger,S.H.vonSolms Cyber security for home users: a new way of protection through awareness enforcement *Comput. Secur.*, 29 (8), pp. 840-847.
- [57] Statistics Canada (2010), Survey Methods and Practises, Ottawa: National Library of Canada..
- [58] G. Peersman, (2014), Overview: Data Collection and Analysis Methods in Impact Evaluation, Florence: UNICEF Office of Research.

- [59] E. Heiervang and R. Goodman, (2011), "Advantages and limitations of web-based surveys: evidence from a child mental health survey.," *Soc Psychiatry Psychiatr Epidemiol*, vol. 46, no. 1, pp. 69-76.
- [60] M. v. Gelder, R. W. Bretveld and N. Roeleveld, (2010), "Web-based Questionnaires: The Future in Epidemiology," *American Journal of Epidemiology*, vol. 172, no. 11, p. 1292–1298.
- [61] S. Rice, S. R. Winter, S. Doherty and M. Milner, (2017), "Advantages and Disadvantages of Using Internet-Based Survey Methods in Aviation-Related Research," *Journal of Aviation Technology and Engineering*, vol. 7, no. 1, p. 58–65.
- [62] C. Greenlaw and S. Brown-Welty, (2009), "A Comparison of Web-Based and Paper-Based Survey Methods," *Evaluation Review* , vol. 33, no. 5, pp. 464 - 480.
- [63] Z. RUHANYA, (2015) "Attitudes toward, and awareness of, online privacy and security: a quantitative comparison of East Africa and U.S. internet users," Kansas State University, Manhattan.
- [64] The JASP Team (2018). JASP (Version 0.12.1)[Computer software]. Available: <https://jasp-stats.org/>
- [65] A.G. Yong, S. Pearce, (2013) "A Beginner's guide to factor analysis: Focusing on EFA" *Tutorials in Quantitative Methods for Psychology*, Vol. 9(2), p. 79-94.
- [66] Clark and Watson, (2017), "Creation and Initial Validation of the Physical Educator Efficacy Scale for Teaching Lifetime Physical Activities", *Journal of Physical Activity Research.*, Vol. 2 No. 1, 7-14.
- [67] Yale University, (1997), "Tests of Significance," Yale University. [Online]. Available: <http://www.stat.yale.edu/Courses/1997-98/101/sigtest.htm>. [Accessed 2 April 2020].
- [68] Abebe, Daniels and McKean, (2001), *Statistics and Data Analysis*, Kalamazoo: Western Michigan University.
- [69] E. Martz, (2013), "Bewildering Things Statisticians Say: "Failure to Reject the Null Hypothesis".
- [70] Laerd Statistics, (2013), "Pearson Product-Moment Correlation" Laerd Statistics.
- [71] D. Denis, (2012) "Understanding Cohen's d" [Online] http://www.bwgriffin.com/gsu/courses/edur9131/content/cohen_d_Denis.pdf [Accessed 5 April 2020].
- [72] D. Groppe, "How to compute p-values and Cohen's d for z-tests" [Online] http://www.cogsci.ucsd.edu/~dgroppe/STATZ/ztest_pvalue_d.pdf. [Accessed 5 April 2020].
- [73] J. Cohen, (1977), "Statistical power analysis for the behavioral sciences," Hillsdale.
- [74] *Fundamentals of Statistics*, (2012), "Two-Sample F-Test,". [Online]. Available: http://www.statistics4u.com/fundstat_eng/cc_test_2sample_ftest.html. [Accessed 5 April 2020].

- [75] Kruskal; Wallis (1952). "Use of ranks in one-criterion variance analysis". *Journal of the American Statistical Association*. 47 (260).
- [76] Corder, Gregory W.; Foreman, Dale I. (2009). "Nonparametric Statistics for Non-Statisticians". Hoboken: John Wiley & Sons. pp. 99–105.
- [77] Daniel, Wayne W. (1990). "Spearman rank correlation coefficient". *Applied Nonparametric Statistics* (2nd ed.). Boston: PWS-Kent. pp. 358–365.
- [78] Mann, Henry B.; Whitney, Donald R. (1947). "On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other". *Annals of Mathematical Statistics*. 18 (1): 50–60.
- [79] Susanne, Furman., Mary, Frances, Theofanos., Yee-Yin, Choong., Brian, Stanton. (2012). "Basing Cybersecurity Training on User Perceptions". *IEEE Security and Privacy Magazine* 10(2):40-49.
- [80] Technology Safety, (2019). "Evidence Collection Series: Internet of Things (IoT)". [Online]. Available: <https://www.techsafety.org/iot-evidence> [Accessed 22 April 2020].
- [81] Oztuna D, Elhan AH, Tuccar E. (2006) Investigation of four different normality tests in terms of type 1 error rate and power under different distributions. *Turkish Journal of Medical Sciences*, 36(3):171–6.
- [82] Altman DG, Bland JM. (1996) Detecting skewness from summary information. *Bmj.*, 313(7066):1200.

Appendix 1 – Survey Consent Form

Survey: Perception and preparedness of a user towards cybersecurity threats in IoT and mobile devices

* Required

Thank you for participating in this survey. The purpose of this study is to understand the perception and preparedness of a user towards cybersecurity threats in IoT and mobile devices.

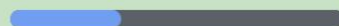
The entire survey should take at most 5 minutes. Participation in this study is purely voluntary, and you can also skip questions that you do not feel comfortable answering. The survey is entirely anonymous. Your personal information is not stored, and you cannot be identified from the results of the study in any way.

If you have any questions or concerns about this study, please contact the investigator, Rishikesh Ram Shankaran at rishan@taltech.ee

Consent *

I acknowledge that I have read this consent form and I freely consent to participate in this survey.

Next



Page 1 of 3

Appendix 2 – Questionnaire

Please select your age group

- <18
- 18 - 24
- 25-34
- 35-50
- 50+

Please select your gender

- Female
- Male
- Prefer not to say

Select your current level of education

- Less than a high school diploma
- High school degree or equivalent
- Bachelors degree
- Masters degree
- PhD or higher

Are you working in an IT-related field?

Yes

No

Perception of a user towards cybersecurity threats in IoT and mobile devices

Mobile Devices

Portable computing devices such as a smartphone, laptops or tablet computer.

Please rate how familiar you are in using the following mobile devices such as laptops and smartphones?

Least familiar 1 2 3 4 5 6 More familiar

Please rate how much do you know about the threats in mobile devices such as Laptops and smartphones?

Less often 1 2 3 4 5 6 More often

Please rate how safe it is to use public/open wifi's which are not password-protected and are available in places like airports or hotels?

Less safe 1 2 3 4 5 6 More safe

Please rate how safe it is to allow applications to access location while using a mobile device (Laptops, smartphones, tablets, etc.)

	1	2	3	4	5	6	
Less safe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	More safe

Please rate how safe it is to save credit/ debit card information on third-party websites or applications?

	1	2	3	4	5	6	
Less safe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	More safe

IoT devices

The Internet of Things (IoT) devices are things that sense and collect data and send it to the internet. Examples: Google Homes, Amazon Echo, smartwatches, smart locks, smart Tv.

Please rate how safe do you feel about private data such as location, health readings, etc. being stored in an IoT device?

	1	2	3	4	5	6	
Less safe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	More safe

Please rate how comfortable are you with an IoT device recording the following data.

	Very uncomfortable	Uncomfortable	Slightly uncomfortable	Slightly comfortable	Comfortable
Sound	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Video/Pictures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health readings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Smart TVs commonly keep track of your watching routine like duration of channels/programmes the user watches. This information can be used to create and display relevant ads. Please rate the following statements:

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
I am aware of this functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am comfortable with data being collected	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Privacy concerns stop me from purchasing or using this type of device	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Smart home devices such as Google homes, Amazon Echo, etc. record audio for each voice command. For example, Amazon Echo that responds to the user's questions saves these audio logs online. Please rate the following statements:

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
I am aware of this functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am comfortable with data being collected	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Privacy concerns stop me from purchasing or using this type of device	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Preparedness of a user towards cybersecurity threats in IoT and mobile devices

Mobile Devices

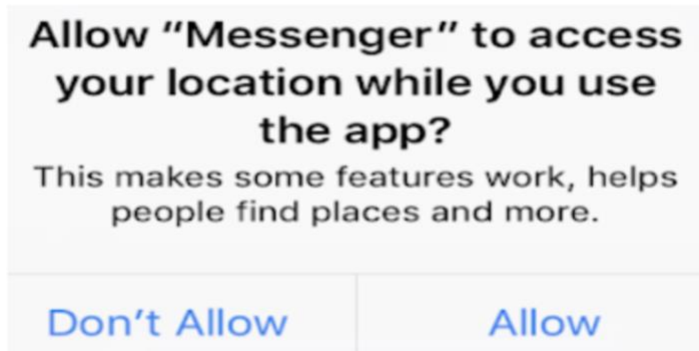
Portable computing devices such as a smartphone, laptops or tablet computer.

“A VPN encrypts data so that a hacker cannot identify what a person is doing online. VPNs can be used on any mobile device, including laptops, smartphones, and tablets.” Please rate how often do you use a VPN while using a public/open wifi which is not password-protected and is available in places like airports or hotels in your mobile devices such as Laptops and smartphones?

1 2 3 4 5 6

Less often More often

Please rate how often do you check the permissions required to access the installing application to read data from your mobile devices? For example, please see the image below.



1 2 3 4 5 6

Less often More often

Please rate how frequently do you download third-party (Apps which are not from play store) apps in your smartphones?

1 2 3 4 5 6

Less frequent More frequent

Please rate how often do you read the application provider's privacy and policy terms and conditions for saving the user data while accessing the application? For example, please see the image below.

Terms of Use

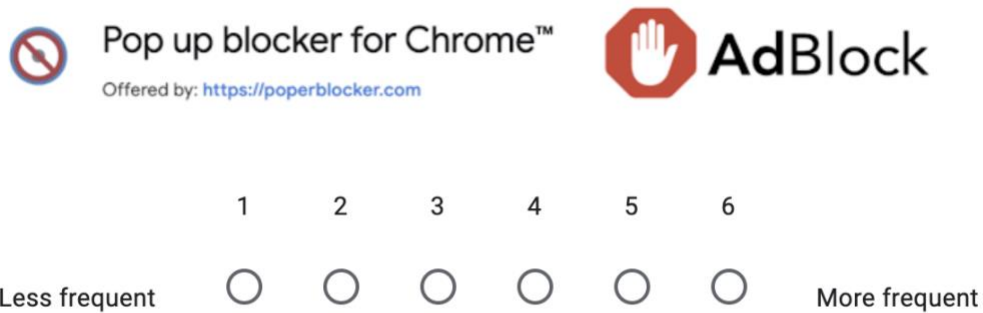
I accept and agree to the [Terms of Use](#).

CONTINUE

1 2 3 4 5 6

Less often More often

Please rate how frequently do you use an ad blocker and pop-up blocker while using your web browser? For example, please see the image below.

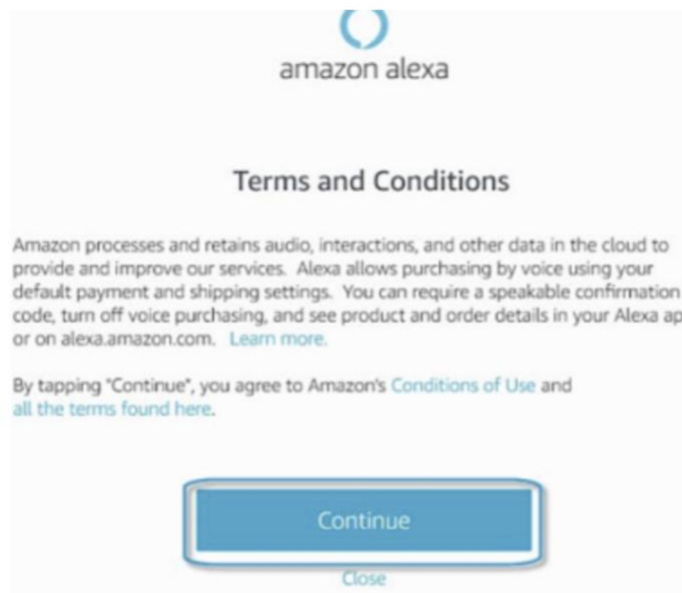


The image shows a notification for 'Pop up blocker for Chrome' and 'AdBlock'. The notification includes the logos for both, with 'AdBlock' in a red octagon. Below the logos is a rating scale from 1 to 6, with 'Less frequent' on the left and 'More frequent' on the right. All six radio buttons are currently unselected.

IoT devices

The Internet of Things (IoT) devices are things that sense and collect data and send it to the internet. Examples: Google Homes, Amazon Echo, smartwatches, smart locks, smart Tv.

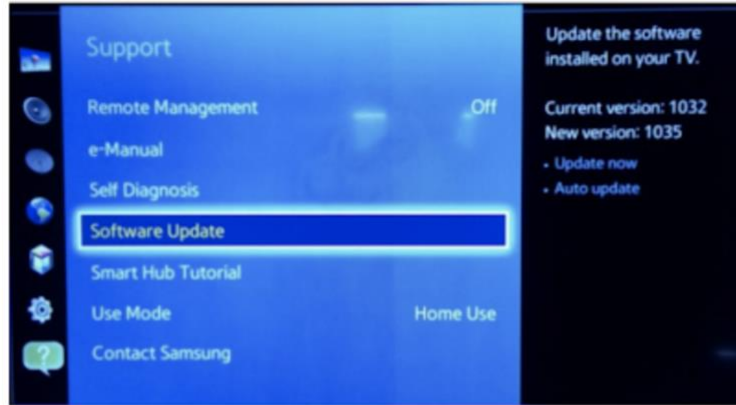
How often do you read terms and conditions to understand what data is being collected while using the application? For example, please see the below image.



1 2 3 4 5 6

Less often More often

How frequently do you update the software of the IoT devices? For example, a software update on smart tv, please see the below image.



1 2 3 4 5 6

Less frequent More frequent

Please rate how often do you download third-party (Apps which are not from store) apps/ software for your IoT devices?

1 2 3 4 5 6

Less often More often

Please rate how often do you connect an external device such as External hard drives, USB sticks to your smartTV, or any other IoT Device?

1 2 3 4 5 6

Less often More often

Please rate how frequently do you change the password of connected IoT devices?

	1	2	3	4	5	6	
Less frequent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	More frequent

Back

Submit

Page 3 of 3