Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Master's Thesis

User perception's and behavioral intentions towards privacy and information security

Md Sahadat Hossain Sagor

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Md Sahadat Hossain Sagor

Informatics

Thesis title

User perception's and behavioral intentions towards privacy and information security

---

Objectives of thesis

The main objective of this thesis is to compare user's perceptions and behavioral intentions towards privacy and information security between graduate students and junior employees.

The partial goals of this thesis are as follows:

- To review existing models of privacy and information security.
- To prepare and conduct a survey among users.
- To run statistical analysis, evaluate results and interpret findings.

Methodology

The methodology of the theoretical part of the thesis will be based on the literature overview of scientific sources regarding privacy, information security, user perception, user behavior, and existing models of privacy and information security. In the practical part, a survey will be prepared and conducted among the selected target users regarding privacy and information security. Statistical analysis will be conducted after collecting the data from the survey. Conclusion and recommendations will be formulated based on the synthesis of the literature review and the outcome from the practical part.

The proposed extent of the thesis

80 pages

Keywords

privacy, information security, user perceptions, user behavior evaluation, statistical analysis

---

Recommended information sources

Ayalon O., and Toch E. (2019). Evaluating Users' Perceptions about a System's Privacy: Differentiating Social and Institutional Aspects. Fifteenth Symposium on Usable Privacy and Security. August 12–13, 2019 • Santa Clara, CA, USA. ISBN 978-1-939133-05-

Flinn, S. and Lumsden, J., (2005). User perceptions of privacy and security on the web. Url-https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9160&rep=rep1&type=pdf

Mekovec, Renata & Hutinski, Zeljko. (2012). The role of perceived privacy and perceived security in online market. 1549-1554.

M. Williams, J. R. C. Nurse and S. Creese, (2017) ."Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things," 2017 15th Annual Conference on Privacy, Security and Trust (PST), 2017, pp. 181-18109, doi: 10.1109/PST.2017.00029.

Zhuang, M., Toms, E. and Demartini, G. (2016) The Relationship between User Perception and User Behaviour in Interactive Information Retrieval Evaluation. In: Advances in Information Retrieval. 38th European Conference on Information Retrieval, 20 -23 Mar 2016, Padua, Italy. Lecture Notes in Computer Science . Springer International Publishing , pp. 293-305.

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 21. 02. 2023

Declaration

I declare that I have worked on my master's thesis titled "User perception's and behavioural intentions towards privacy and information security" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 31/03/2023 _____

Acknowledgement

I would like to thank my respected supervisor Ing. Miloš Ulman, Ph.D. for all his positive suggestions and valuable comments during the whole period of my thesis. I am grateful to my supervisor for his active kind support and friendly cooperation to overcome all the obstacles throughout the thesis work. Thank you very much Nayeem Al-Tamzid Bhuiyan for his support during my tough time because I lost my most important person, my dearest mother when I was writing my thesis. I also thank Arpana Shanta for her great support.

Finally, I would like to thank my family and the Almighty for allowing me to complete my degree and achieve my dream. I am dedicating this thesis to my mother. My love is always with her. I am grateful to her for sacrificing her whole life to give us the best life.

User perception's and behavioral intentions towards privacy and information security

Abstract

The increasing use of technology and online platforms has led to growing concerns about privacy and information security. This thesis explores users' perceptions and behavioral intentions towards this privacy and information security. The study aims to investigate the comparison between graduate students and junior employees to see their awareness of privacy and information security and also see the significant differences. The literature review provides an in-depth analysis of various aspects related to user perceptions, behavior intention, privacy, and information security. It covers different measures of user perception and user perceptions of privacy, along with the relationship between user perception and behavior. Through a statistical method approach, the study analyzed collected from a survey. The findings provide insights into users perceptions and behavioral intentions towards privacy and information security, highlighting the responds of individual groups. The study's contributions to see the significant differences between graduate and junior employees towards privacy and information security. It also provides a better understanding of the awareness of these group and recommendation has been provided to increase their knowledge of privacy and information security to reduce security issues.

Keywords: privacy, information security, user perceptions, user behaviour
evaluation, statistical analysis

Záměry vnímání a chování uživatelů vůči soukromí a bezpečnosti informací

Abstrakt

Rostoucí používání technologií a online platforem vedlo k rostoucím obavám o soukromí a bezpečnost informací. Tato práce zkoumá vnímání a chování uživatelů vůči tomuto soukromí a bezpečnosti informací. Cílem studie je prozkoumat srovnání mezi postgraduálními studenty a mladšími zaměstnanci, aby bylo vidět jejich povědomí o soukromí a bezpečnosti informací a také významné rozdíly. Přehled literatury poskytuje hloubkovou analýzu různých aspektů souvisejících s vnímáním uživatelů, záměrem chování, soukromím a bezpečností informací. Zahrnuje různá měřítka uživatelského vnímání a uživatelského vnímání soukromí spolu se vztahem mezi uživatelským vnímáním a chováním. Prostřednictvím přístupu statistické metody byla analyzována studie získaná z průzkumu. Zjištění poskytují vhled do vnímání uživatelů a jejich záměrů v oblasti ochrany soukromí a bezpečnosti informací a zdůrazňují reakce jednotlivých skupin. Příspěvky studie k poznání významných rozdílů mezi absolventy a mladšími zaměstnanci v oblasti soukromí a bezpečnosti informací. Poskytuje také lepší pochopení povědomí těchto skupin a bylo poskytnuto doporučení, jak zvýšit jejich znalosti o soukromí a zabezpečení informací, aby se snížily bezpečnostní problémy.

Klíčová slova: soukromí, informační bezpečnost, uživatelské vnímání, uživatelské chování hodnocení, statistická analýza

Table of content

1. Introduction

The progression of the industrial revolution refers to technology increasing exponentially. The Fourth Industrial Revolution(4IR) in terms of the cyber-physical system, is also at its peak. Compared to the past decades, people's daily lifestyles have changed unimaginatively. To be a part of the modern world, people are getting increasingly involved in this electronic media, and they are more likely to employ electronic media because of their simple usability and availability. According to(Statista, 2022) report on the global digital population, there are 5.03 billion internet users and 4.7 billion social media users. People are using social media in different sectors like communications, data storing, data sharing, etc with the help of the internet. To use online media, user information, and other private information are needed to be kept online. Although many companies and well-known sites require users' personal information for their business growth or to analyze user data. Which is moreover can be unreliable or unfaithful. Data sometimes gets stolen, and the user's personal information gets leaked to the public which can be unpleasant to that user. Data piracy has become a major threat. A lot of data is getting leaked due to lower privacy and security policies. Moreover, people are not as aware of it. The average data breach cost increased by 2.6% in comparison from 4.24 million dollars in 2021 to 4.35 million dollars in 2022. Average costs are up 12.7% from 3.86 million dollars in the 2020 report (IBM, 2022). Compromised or Stolen credentials were responsible for 19% of breaches conducted from data breaches. 16% of the time it is said that the responsible item was Phishing. 15% of breaches are done by Cloud misconfiguration. Phishing occurs when the security of the information lacks to protect it. Stolen data or personal information can be used by criminals to do any bad occurrences. They will hide under the shadow and make innocent guilty.

The main concerns of the users while using the internet are to secure their data and the privacy of the data. Usual policy on information security does not reflect actual user behavior or some policies exploit users by ignoring their privacy control. Individuals experience a loss of control when it becomes more difficult to manage their online personal data. Furthermore, recurrent consumer data breaches have given customers a sense of futility, eventually leaving them tired of worrying about internet privacy which can be called “Privacy Fatigue”. To maintain privacy and mitigate security issues, illegal access, and unwanted interruption, numerous security policies were introduced by researchers. Researchers are also working on it to improve the

terms privacy and information security of users. But there are a lot of issues that are making it tough to interpret. Privacy and securities are complex terms. It should be monitored otherwise it also gets vulnerable and can be easily stolen. As, information security policies do not reflect the actual user behavior; or some policies exploit users, neglecting their privacy control (e.g., complicated privacy settings of online platforms that rely on users fatigue, etc.)

2. Objectives and Methodology

2.1 Objectives

The main objective of this thesis was to compare user's perceptions and behavioral intentions toward privacy and information security between graduate students and junior employees. The partial goals of this thesis are as follows:

- To review existing models of privacy and information security.
- To prepare and conduct a survey among users.
- To run statistical analysis, evaluate results and interpret findings.

2.2 Methodology

The methodology of the theoretical part of the thesis was based on the literature overview of scientific sources regarding privacy, information security, user perception, user behavior, and existing models of privacy and information security. In the practical part, a survey was prepared and conducted among the selected target users regarding privacy and information security. The survey was created on google forms. Statistical analysis T-Test was conducted after collecting the data from the survey. The analysis has been conducted on Microsoft Excel. Conclusion and recommendations were formulated based on the synthesis of the literature review and the outcome from the practical part.

3. Literature Review

Nowadays, the privacy of user information and data has become the main concern for individual internet users. To maintain the privacy of data, data, and information must be secured. Researchers proposed many methods to summarize the perceptions and behavioral intentions of the user regarding privacy and information security. Though the terms privacy is not familiar to users. Sometimes they get confused over privacy policies and make their information vulnerable unwillingly.

3.1 User Perceptions

User perception is a viewpoint that has developed through time because of direct or indirect user contact. Additionally, perception may include both objective and qualitative information, and it may be influenced by a variety of factors such as features, policies, other service practices, etc. The measurements of perceived usability relate to user perception (Zhuang, 2016). Understanding how users perceive activity is a crucial first step in identifying data access that goes against user expectations(Nguyen, 2021)

The final multidimensional User Engagement Scale (UES) evaluates six aspects in terms of the user experience:

a. Aesthetic Appeal,

b. Novelty,

c. Focused Attention,

d. Felt Involvement,

e. Perceived Usability and

f. Endurability

3.1.1 Multiple measures of user perception

User-perceived measures are more likely combined with the measurement of perceived usability. An example might be “Satisfaction”, it has been rewritten from usability research along with tends to be implemented regularly across studies of IIR. The User Engagement Scale (UES), a modern multi-dimensional metric, identifies six aspects of user experience: Novelty, Focused Attention, Perceived Engagement, Likely Perceived use, and Durability are all important design elements.

3.1.2 User Perceptions of Privacy

Furini proposed the analysis of user attitudes about privacy in terms of using applications with smartphones and categorized two different hypotheses(Furini, 2020). In this research, they developed a questionnaire for privacy perception where the controlled variable is the information about the possible misuse of user data. The analysis shows that 80% of adults believe that Americans should be concerned about the government listening in on their phone and internet conversations. Many say that key communication channels like phone and email aren't secure enough. Meanwhile, 91% of American adults say consumers no longer have control over how businesses collect and use their personal information. WASHINGTON (November 12, 2014) – As concerns about government surveillance and commercial use of personal information grow, perceptions of privacy vary across the United States, according to new research from the Pew Research Centre. A new poll by Pew Research shows that the majority of adults feel threatened in key areas such as personal information security and privacy. These are part of a new national representative given the ongoing public discussion about the US government's surveillance program, a poll of 607 people was conducted to examine public perceptions and attitudes regarding privacy in the public debate about govt. surveillance program.

3.2 User Behaviour Intention

The connection between privacy concerns, trust, and behavioral intentions has not received much empirical study(Liu, 2005). The primary purpose of their study's objective was to put out and experiment with a hypothetical model that purported to clarify how trust influences the user's behavioral intention towards transactions online and the privacy influences trust.

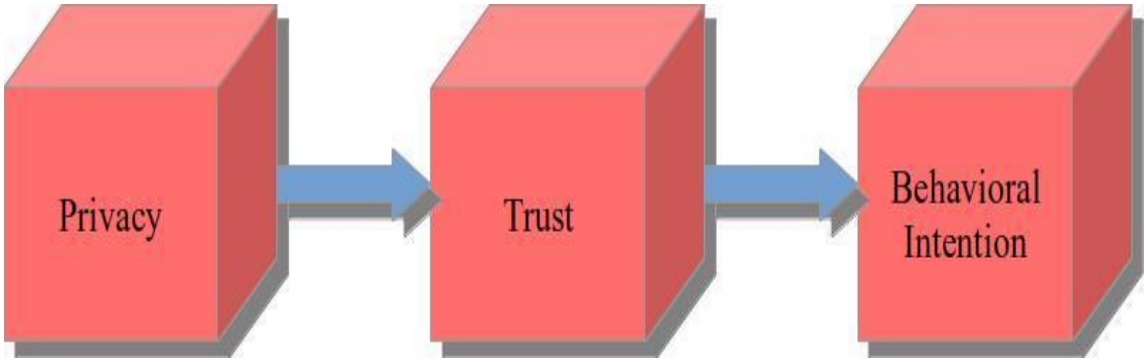

Figure 1: Model relating Privacy,trust & Behavioural intention).(Liu, 2005)

Where the dimensions of Privacy, Trust, and Behavioural Intentions are mentioned in table 1.

Table 1: Dimensions for Privacy, Trust, and Behavioural intentions

Dimensions		
Privacy	**Trust**	**Behavioural Intention**
Noticing	Degree of trust	Repeating
Accessing		Revisiting
Choosing		Recommending to others
Security		Positive Remarking

Expanding on this privacy-trust-behavioral intention model, (Wang, 2019) proposed that, improving the efficacy of privacy management might boost customers' confidence in e-commerce sites and, as a result, their behavioral intentions, and actual actions. However, they investigated how institutional privacy assurance affects consumers' trust toward s-commerce (social commerce) sites, and how much trust facilitates pre-purchase activities and purchase intentions, increasing the likelihood of actual purchase. Because young customers make up the large majority of the s-commerce audience, this study focused on millennial behavior. The following contributions are intended by this study:

1. It broadens privacy-trust research in the context of s-commerce.
2. It takes a comprehensive view of social interactions by investigating not only the valence and content of words but also the passive observation of learning encounters.
3. It broadens the Privacy-Confidence-Behavior paradigm by investigating how institutional privacy guarantee boosts users' trust in s-commerce websites, which in turn boosts social interactions and, as a result, users' buy intention and actual purchase behavior.

4. Rather than focusing on consumers' behavioral intentions, the research looks at their actual buying behavior. This gives further information about the customer decision-making process on s-commerce sites.

Although this model has been proven in e-commerce environments where it indicates that lowering consumers' privacy concerns may increase their trust in online transactions, hence raising behavioral intention to purchase a product.

Additionally, as suggested by (Zeithaml, 1996) the variables regarding the behavioral intention of the customers are the finest predictors of the satisfaction of the customer and the business service quality in online shopping. These variables include:

- Repetition call to the website.
- Refer other people to the website.
- Positive comments or remarks on the website; and
- Snap up again from the same.

They discovered that the desire to pay more is positively correlated with service quality. Customers are prepared to pay extra for higher service quality. Hypotheses are put out in light of the research that has been reported which says Perceived quality influences behavioural intentions admiringly. Following this research (Hu, 2009) proposed a hypothesized model with parameter estimates that confirm that high service quality leads to higher perceived value, customer satisfaction, and positive corporate image perceptions Customers' perceived value was also found to affect customer satisfaction, the image of the hotel, and customers' likelihood to prefer and recommend the organization to others. Furthermore, it was discovered that customer satisfaction has a positive impact on corporate image. Furthermore, the analysis shows that behavioral intentions were influenced not only by perceived value but also by the firm's image. A positive image can influence repeat business. A Research (Rita, 2019) focuses on the four e-service quality model dimensions that better predict consumer behavior. The study investigates the effect of customer satisfaction on consumer behavior such as repurchase intent, word-of-mouth, and site revisit. It also examines the effect of consumer trust. According to the study, the outcome is predicted to broaden understanding of diverse national cultures and the various importance of e-service quality qualities.

3.3 User Perception and User behaviour's relation

According to (Zhuang, 2016) there is little evidence about which measurements are reliable and robust. Therefore, correlation values greater than 0.35 should be considered as a first step in testing the relationship between perceptual and Behavioural measures. They measured the correlation between user behavior and perception, and the results were not what they expected. The user behavior does not appear to be strongly associated with user perceptions of aesthetics and perceptions of usability. It concerns the users' expectations of aesthetics and usability and limits the degree of inter-individual variability. This indicates that individual exploratory behavior could not fully contribute to their user engagement calculations. However, common behaviors related to coping with outcomes were moderately correlated with attentional focus, perceived engagement, and novelty. They were joined to form one factor in the UES analysis. This suggests that system data indicative of general user behavior may contribute to these current subscales of user engagement. According to the type of experiment, various user behavior variables can be extracted from log files. The model was further developed when (Zhuang, 2017)examined the association between a limited number of behavioral traits and perceived engagement during an aimless browsing activity. This research proposed to answer three main research questions on user-perceived engagement, behavioural signals, and engagement prediction performance. Another study was conducted (Azizan, 2022) to solve the existing model limitations. In this research, they proposed a theoretical framework combining TTF (Task-Technology Fit) and UTAUT. Overall, the research claims the respondents' positive attitudes and acknowledgment of flexibility, suitability, and several aspects of usefulness in support of the suitability of TTF and UTAUT models.

In the paper (Zhuang, 2016) they showed a relationship between the 3-user behavior and the 6-user Engagement Scale (UES) sub-scales. The UES scale is a multi-dimensional measure. In this research, the scale contained 31 items, where the items are presented as scale as "strongly agreed" to "strongly disagreed". Aesthetics and perceived usability do not connect with user behavior characteristics. Relationships with Endurability, Focused Attention, and Novelty of the other components were equally insignificant., as were their connections with the factors affecting browsing and searching behavior. General behavior was the only factor that moderately correlated with focused attention, felt involvement, and novelty. In this research, they tested the hypothesis on 157 participants by isolating measures of user behaviour as represented by actions in log files and examining the association with user perception of their experience as measured by the UES.

Table 2: Interdependence of User's -UES sub-scales and behaviour factors (Zhuang, 2016)

	Searching	**Browsing**	**General**
Aesthetics	0.05	0.09	0.09
Endurability	0.16	0.17	0.27
Felt Involvement	0.23	0.22	0.38
Focused Attention	0.14	0.23	0.35
Novelty	0.27	0.23	0.39
Perceived Usability	0.04	0.10	0.07

There are few clues as to whether the measurements are reliable. Therefore, correlation values greater than 0.35 should be considered as a first step in examining associations between cognitive and behavioral measures. Their measurement of the relationship between user behaviour and user perception was surprising. User perceptions of perceived aesthetics and usability do not appear to be strongly correlated with user behavior.

However, they confirm that high service quality leads to higher perceived value, customer satisfaction, and positive corporate image perceptions Customers' perceived value was also found to affect customer satisfaction, the image of the hotel, and customers' likelihood to prefer and recommend the organization to others. Furthermore, it was discovered that customer satisfaction has a positive impact on corporate image. Although, the analysis shows that behavioral intentions were influenced not only by perceived value but also by the firm's image. A positive image can influence repeat business.

There is another term called privacy paradox. According to (Barth, 2017) privacy paradox is a mismatch between user behavior and privacy. That is determined by well-calculated circumstances for systems for online profiling and contexts of social media.

3.4 Privacy

Privacy refers to the protection of private information. Authors have defined privacy in many ways. (Roger, 1997) defined information privacy as, “The interest a private has in controlling, or a minimum of significantly influencing, the handling of knowledge about themselves”. in line with Olga Sushko,” Online privacy, also called internet privacy or digital privacy, refers to what proportion of your personal, financial, and browsing data remains private when you're online.” (Sushko, 2021) in an exceedingly legal setting, the "right to be left alone" additionally because the right to privacy is closely connected (Warren, 1890). Others contend that proper privacy merely entails the power to prevent others from learning personal information about you (Westin, 1968). The privacy theories proposed by Westin (1967) and Altman (1975) stand noteworthy within the psychological literature. the quantity of daily internet users is rising drastically. Lack of security can make the privacy of the user invaded. Moreover, the behavior of the net user will be tracked. In keeping with (Williams, 2018), more often than not, privacy is seen as being compromised for entertainment purposes over its necessity. We, humans, are highly concerned about our privacy in the real world. we do not want people to hinder our freedom and interfere in our lives quite we allow them to. Virtual life puts our privacy at great risk.

According to opinion surveys, the overall public values privacy, 86% of respondents from the US said they took action to safeguard themselves (Lee, 2013) and 88% from the United Kingdom claimed to value the principle (Truste, 2015).

3.4.1 The dimension and categories of privacy

According to Burgoon, 4 dimensions of privacy have been defined in their study. They also defined these dimensions as ‘‘The ability to control the access and bound the physical, interactional, psychological and informational access to the self or one’s group’’ (Burgoon, 1989). DeCew also exhibits the complex aspect of privacy in her writing. A definition with the following three components: the informational dimension, the expressive dimension, and the accessibility dimension.

Based on previous research many researchers have defined privacy individuals in many groups. (Hann, 2007) has defined privacy as:

1. Guardians of privacy.
2. Sellers of the information.

3. Seekers of any convenience.

In this research (Friedewald, 2013) the author has categorized privacy into 7 different types.

1. Person's Privacy: To maintain the privacy of bodily processes and bodily information (such as genetic composition and biometrics).

2. behaviour and privacy actions: To keep habits and other activities like political, social, and religious practices private.

3. Communication privacy: To avoid communication interception, such as email interception, bugs, microphones, telephone or radio interception or recording, and email message access.

4. Privacy of the images and data: To keep personal data such as emails, videos, etc private.

5. Thoughts and feelings privacy; To keep their ideas or feelings private or to have those thoughts or feelings unrevealed.

6. Location and space privacy: To keep the location private in public domains.

7. Association (including group privacy) privacy: To keep the association whomever someone wishes without being monitored.

According to operations performed on data, the data of online privacy can be categorized (Mascarenhas, 2003):

1. Collection of data

2. Usage of data.

There are 4 categories into which the data collection process can be divided:

1. Public usable volunteered data,

2. Private usable volunteer data.

3. Noticed Un-volunteered data gathering and

4. Unnoticed un-volunteered data gathering.

The following data can be identified as categories of online voluntary data sampling for public use:

1. Registering data.

2. Administration.

3. Facilitated data.

Besides this for private use volunteered data collection includes

1. Online survey data

2. Online purchaser data

Categories of involuntary but informed collection of data include online transactional data collected via online interactive shopping or online postal catalogues.

3.4.2 Privacy Policies

Privacy policies help to protect sensitive information collected by the site. A security policy cannot by itself be post-collection protection, but it can ensure that the webmaster will take additional steps to protect the data. The answer to this question depends on the choice of respondents. They are not always conscientious about reading the privacy rules and terms of service that they frequently encounter. The Privacy Policy is a brief statement of how the website operator treats information collected from us and how it is obligated to protect that information.

In a study on "User Perceptions of Internet Privacy and Security" (Scott, 2005), users may confuse browser cookies with other types of data and draw false conclusions. Respondents strongly felt they were sceptical of privacy regulations but believed that websites could comply with their stated policies.

The privacy boundary management model proposed and tested by (Chang, 2018) shows how users define and maintain their privacy border. Additionally, it examines how the 5 privacy policies affect the creation of privacy boundaries and determines how users relate these components to the efficiency of privacy policies. 363 users who have been using online banking services for at least six months provided the survey data. The study's model clarifies a significant portion of the variance in perceived privacy, according to partial least squares results. Four elements of the Fair Information Practice Principles substantially impact how well a privacy policy is perceived:

1. Accessing.
2. Noticing.
3. Securities.
4. Enforcement.

Perceived efficacy greatly impacts how much privacy control and risk are valued. Trust and perceived privacy concerns both have a big impact on perceived privacy.

3.4.3 Privacy Concerns and privacy actions

In (Goswami, 2020), according to 'Internet Society and Consumers International', concerns regarding the way that personal data is gathered by mobile applications are held by 69% of customers. That's a massive leap when differentiated to his consumers about 0.01%, opting out of Lotus databases. The main reason why privacy concerns are expanding is that customers are getting more informed about how businesses utilize their data. Consumers still don't completely understand how much personal information businesses gather.

Several measures have been developed over the years to address different aspects of privacy. But these scales were developed primarily to measure individual privacy preferences out of personal privacy concerns, not to assess systems. One of the most used scales named the 'Internet Users's Information Privacy Concerns (IUIPC)' scale was developed by(Malhotra, 2004). Their research focused on three different topics. First, they provided a theoretical framework for his IUIPC. Second, they attempted to operationalize his multidimensional conception of IUIPC using secondary structures, and finally, proposed and tested a causal model of the relationship between IUIPC and Behavioural intentions toward personal information.

A study (Martin, 2017) shows that consumers' attitudes toward personalized communication will be negative when they have strong privacy concerns. Because of the pervasiveness of online data-sharing, most research on privacy issues has tended to focus on consumers' perceptions of how firms and organizations obtain, keep, and use their personal information (Wang, 2019). As a result, significant safeguards, including laws, have been implemented to safeguard private information.

Privacy concern refers to people's level of apprehension about how a third party uses their information (Zeithaml, 1996). As may be observed, four different respondents kinds of exhibit "privacy concern-action." Most individuals who are worried about their privacy online take precautions to protect it. However, some respondents are worried about their privacy but do nothing about it. The most frequently cited excuse given by this set of individuals for not acting was a lack of knowledge. The respondents who claimed not to be concerned about privacy but yet took steps to safeguard it online did not provide a convincing justification for their actions.

According to (IGI, 2022) privacy concern is defined as:

1. Concern for the security and usage of private data given by businesses.

2. Anxiety or sensitivity associated with loss of personal intimacy.

3. Concerns about someone’s personal data being used by advertisers.

4. Concerns that someone's personal information may be utilized in unexpected ways by others.

The effect of privacy concerns on attitudes, actions, and perceptions of the hazards connected with social network use has been demonstrated in several research on this topic. (Malhotra, 2006) examined users' expectations for the security of their personal information while considering the collection of personal data. Following proposed the model, (Kuika, 2020) provided a new model, based on the literature, that considers both the management of information and the management of user interactions on social networks. This model enables us to recommend that:

H1a-H1c-H1d-H1e: Social media privacy problems are detrimental to trust, perceived utility, usability, and Behavioural control that is perceived.

H1b: Privacy concerns regarding security when utilizing social media strongly influence perceived risk.

Numerous studies consistently conclude that an overwhelming majority of people are "concerned" or "extremely concerned" about online privacy and to protect themselves from threats they are willing to take necessary steps. About threats to their privacy while users are online (FTC, 2002) reports that 70% of U.S online consumers are concerned about their privacy while (Harris, 1998) reported that 87% and 56% of Internet users were 'concerned' and ‘extremely concerned’ respectively. (epic, 2022) reports that 65% of his respondents said they refused to register on e-commerce sites for privacy reasons.

In (Paine, 2007) the author figured out that the greatest number of respondents, about 73%, answered that they take necessary steps to protect their privacy online. This technique was applied to men and women together. A proportion of men (75%) reported acting more than women (68%). There was no statistically significant difference between men and women. Based on their ages, the respondents were separated into four categories. Respondents are more engaged and took steps across all age groups than those who are not. The relationship between data protection measures and respondents' age was shown to be statistically insignificant.

3.4.4 Online Privacy and Security

More businesses are using the Internet. For a business as it becomes an integral part of people's life. Large amounts of data were transmitted as a result, and there is an increase in the capacity for data storage, retrieval, and monitoring. According to several studies, Internet users have major privacy and security concerns, and the expansion of e-commerce is largely due to their trust. Reference has investigated the significance of four trust indices that affect Internet user's willingness to share personal information and purchasing intentions. The included trust highlighted were:

(1) Privacy seals of the third party,

(2) Statement of privacy,

(3) Security seals of the third party, and

(4) Different security attributes.

The overall result is that respondents prioritize security aspects above anything else.

A study shows how users behave when they must protect their privacy while downloading apps from Google Play (Ullah, 2022). At First, two different Play Store accounts were used to develop and upload seven new applications, each with unnecessary permission requests. The apps had been in use for more than a year when data from the policy pages of the apps and Play Store analytics were gathered. According to the initial data analysis, just 20% of users voiced concerns about their privacy and security through email exchanges, platform comments, or other ways of engagement with the development team.

3.5 Information Security (IS)

Security is also a term that's familiar with defining the protection and reliability of user privacy. Information security means the privacy of the user's information. in step with (Mekovec, 2012), Information security is defined as a "Discipline that uses the concepts of confidentiality, integrity, and availability to answer the question of how data should be protected." Security also includes physical, logical, and procedural measures to remain data private. Privacy cannot be achieved without adhering to security protocols, and the employment of security equipment doesn't guarantee privacy protection. IS is also a serious worry for computer and Internet users due to the varied risks it faces. Every day, immeasurable

security events are caused by various threats to information security, including viruses, hackers, and spam (Berinato, 2005).

3.5.1 Policies of Information Security

An information security policy serves multiple purposes. Here's why we'd like an ISP:

- Establishing Repeatable and Consistent Information Management Processes.
- Document management to make sure individuals adhere to security measures.
- To Meet mission-critical compliance requirements.
- To develop policies to detect emerging threats and mitigate emerging risks.
- To increase consumer trust in the company's security measures
- To make sure that the acceptable personnel have access to the mandatory data and IT resources.
- To train staff on best practices and company security protocols.

(Dupuis, 2016) has presented three fundamental survey tools for human aspects of information security and privacy. The three instruments are.

- Computer performance degradation.
- Personal information leak.
- File and data loss.

To increase the arrogance of users in using online platforms and to mitigate the shortage of confidence in information security, providers of online services should have different formulas that control access to the information stored. However, Users on the web should have less control over their personal information. Online users should be ready to decide:

- Who sees their personal information?
- How it'll be employed in the long run. (Hann, 2007).

3.5.2 The importance of information security policies

According to(Exabeam, 2022) an information security policy provides organizations with the following benefits:

- Promoting integrity, availability, and confidentiality of data – The information security policies which are effective should lay out the rules and processes which protect against risks to the integrity, availability, and confidentiality of data.

- Protecting sensitive data - Protecting sensitive data, such as personally identifying information and intellectual property, is given high emphasis under information security regulations.
- Minimizing the risk of security incidents — An ISP aids a company in formulating the protocols for spotting and reducing risks and vulnerabilities. It also clarifies how anybody may act swiftly to reduce harm in the case of a security problem.
- Execution of Security programs at organizations — Form of the information security guidelines and operational framework for processes.
- Providing a clear security statement to third parties —ISP summarizes the organization's security posture and details how it safeguards its IT assets. They enable clients, partners, and auditors to respond quickly to information demands from other parties.
- Helps comply with regulatory requirements — Organizations might find security holes linked to regulatory requirements by developing and filling an information security policy.

3.5.3 Risk of Information Security

The reason for establishing information security is to protect and maintain integrity, information accessibility, and confidentiality. It also protects information by maintaining the authenticity and reliability of the knowledge.

Unpredicted events with adverse consequences for any organization are cited as threats, and data Security (IS) threats can occur both externally and internally (Cavusoglu et al., 2015) those who work for companies might pose insider risks since they have unrestricted access to knowledge about their operations and other procedures. External dangers originate from sources outside of a company. Human mistake incorporates a negative impact on ISP deployments (Jouini, 2014).

(ISO, 2022) defined risk because of the “effect of uncertainty on objectives”. ISO 31000 defined Information Security Risk (ISR) as “A combination of two factors:

a. probability and

b. consequences.

Information security risks often emerge because potential security threats are identified which may exploit vulnerabilities in an information asset or group of assets and thus cause harm to an organization”.

According to statistics (EY, 2014), respondent companies indicated that their investments in information security control were 46%, and their bank's business strategies were aligned with their corresponding information security strategies by 46%. In their firm, information security events have grown by a minimum of fifty during the last 12 months, per 31% of respondents.

3.5.4 Types of information security

The information gathered during online activities about online users is additionally arranged in three groups (Chellappa, 2005)

1. anonymous information,
2. non-identifying individuals and
3. personally identifiable information

Information is additionally secured by employing a kind of security measures. Confidentiality, integrity, and availability conjure the three main parts of the knowledge security concept referred to because of the CIA Triad. Each element stands for a fundamental information security objective. (ISO/IEC 27000, 2016) defines confidentiality, integrity, and availability as:

• Confidentiality: “Property that information isn't provided or disclosed to unapproved people, organizations, or procedures”.

• Integrity: “property of accuracy and completeness”.

•Availability: “Property of being available and useable to a certified organization upon request”.

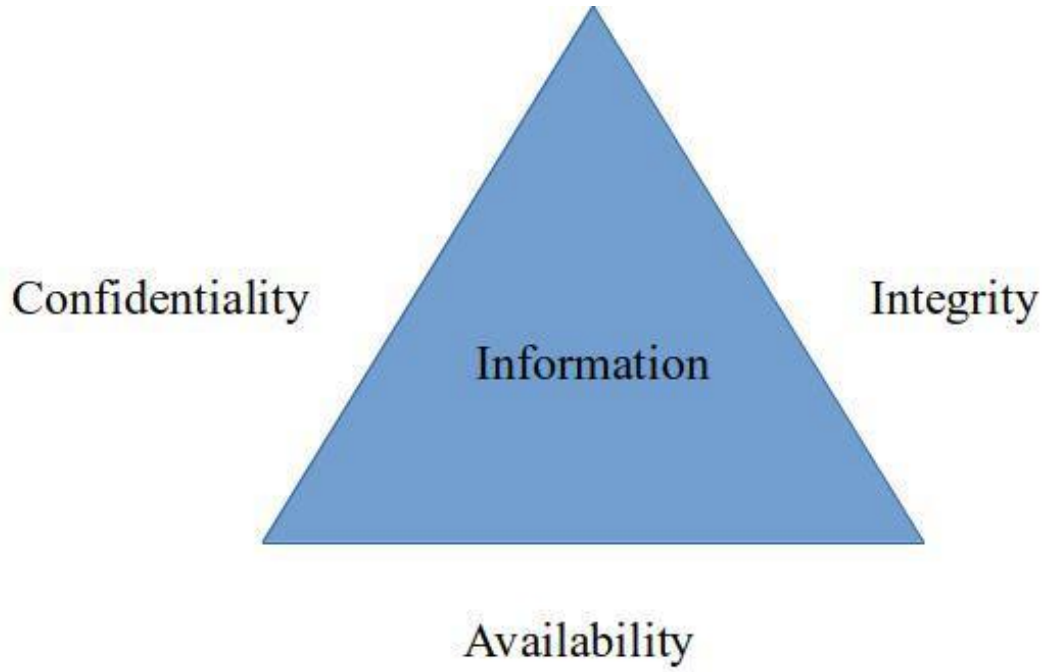

Figure 2: Usual CIA triad of Information Security. (Qadir, 2016)

3.5.5 Types of Information Security Behaviours in Organizations

There are three (3) types of behaviors of people in organizations towards information security which are deliberate risk averse, deliberate risk inclined, and naive and incidental behaviors (Pattinson, 2016). Naive and Accidental Behaviours Specifically explain the attitudes of computer users who are employees in the organizations. They leave the computer unattended, use social networking sites, open spontaneous email attachments, apply a guessable password that is easier for people to hack into, have no reports when there are security incidents, and get access to suspicious websites. Deliberate Risk-Averse Behaviours deliberate risk-averse behaviors are the type of behavior when people in the organization are aware of the information security deployment in protecting the information and privacy such as always logging off when the computers and desks, always making reports for any security threats and accidents, regularly change password, install antivirus, and block for spams. Deliberate Risk-Inclined Behaviour The other type is deliberate risk-inclined behavior in which this type of behavior intended to perform crimes and security threats to people and organizations that can cause many security issues and threats such as hacking into people's accounts and personal access, conducting crimes, and information security attacks, create spam emails, and give unauthorized access to unauthorized zones Employees behaviors are the most common obstacle associated with information security compliance. Employee behavior is related to actions taken upon performing job-related tasks. A good attitude and morale will lead

to better behavior while poor behavior will lead to inefficiency of work. Every single task related to the handling of data must be taken with security compliance. This is related to not exposing data to unauthorized persons, the secrecy of information, security measures in transferring information, and so on.

3.5.6 Information security and threats

Information security is threatened by a variety of factors. Anything representing a risk of information attack, destruction, or modification is considered a danger to information security (Musekura, 2004) Using common elements impacting the security of information systems for contemporary computer users, including businesses and people, a survey was done (Lubua, 2017) From this research they found 4 important factors those explains IS (Information system) security is still a problem to most of the organizations and individual users of modern technology too. The four factors are:

1. Human factor,
2. Unreliable information security policy,
3. Work environment and
4. Demographic factors

As the complexity of information systems grows over time, challenges of information security become increasingly critical for any firm. In this context, the study and evaluation of information security risks are emphasized as a crucial component of an integrated approach to information security.

3.6 Overview of studies on Privacy and Information Security

Table 3:Overview of studies on Privacy and Information Security

Author	Method	Participants	Key Findings
(Scott, 2005)	Anonymous online questionnaire	237 respondents (primarily Canadian, some from the UK and US)	Respondents have expressed skepticism about their privacy policy but feel they can trust the website to respect its policy. Confusion about cookies and locally stored data lead to inappropriate conclusions about risks.
(Williams, 2018)	Online surveys (N=170) and contextual interviews (N=40)	170 participants in online surveys, 40 participants in contextual interviews (60% male and 40% female)	The paradox of protective behavior being limited by IoT ratings is prevalent due to a lack of awareness. Confidentiality and data protection have a significant impact on customer's perception of IS in I-system (Internet Banking).
(Ayalon, 2019)	Three online experiments (N=1,313)	1,313 participants	User's perception of privacy in information systems consists of

			institutional, social, and risk aspects.
(Liu, 2005)	An online survey using two EC websites	Over 200 participants	Privacy elements of notice, access, choice, and security affect a person's perception of privacy.
(Paine, 2007)	Worldwide survey	1,261 internet users from 5 cities (Sydney, Singapore, Bangalore, Seoul, New York)	Demographic factors, internet-related experiences, and nationality and culture-related features affect online privacy concerns and self-protection behaviors.
(Wang, 1993)	In-depth interviews with university students	20 university students	The study takes into account the complex and multicultural nature of online behavior.
(Huang, 2010)	The comprehensive, open-ended questionnaire	20 university students	students Feedback on potential problems that might skew perceptions of information security was solicited.
(Malhotra, 2004)	Face-to-face and one-on-one interviews	742 household respondents	IUIPC-centered causal model fits data and accounts

			for significant variation in Behavioural intentions.
(David, 2017)	Experimental research	SurveyMonkey audience (Information Technology, Beginner, or Professional job status)	Association between Behavioural intentions and components from protective motivation and deterrent theories.

Several studies have been conducted on user perceptions of online privacy and information security. Scott's (2005) anonymous online questionnaire found that users express skepticism about privacy policies but still trust websites to respect them, often due to confusion about cookies and data storage. Williams (2018) found that a lack of awareness leads to the paradox of protective behavior being limited by IoT ratings, and confidentiality and data protection significantly impact customers' perceptions of IS in I-systems like internet banking. Ayalon's (2019) three online experiments discovered that users' perception of privacy involves institutional, social, and risk aspects. Other studies, such as Liu (2005), Paine (2007), Wang (1993), Huang (2010), Malhotra (2004), and David (2017), have also contributed to understanding users' perceptions of online privacy and security.

3.7 Reviewing existing models.

The dependent variable information security policy compliance Behavioural intention and the eight independent factors created from the theoretical framework are included in the variables reported by (David, 2017). The remaining 4 independent variables are as follows:

1. formal sanction certainty.
2. formal sanction severity.
3. informal sanction certainty.
4. informal sanction severity.

are constructs from deterrence theory. The first 4 independent variables are:

1. perceived threat vulnerability.

2. perceived threat severity.
3. response efficacy.
4. Self-efficacy.

are constructs from the protection motivation theory. Their research process is depicted in the picture below.

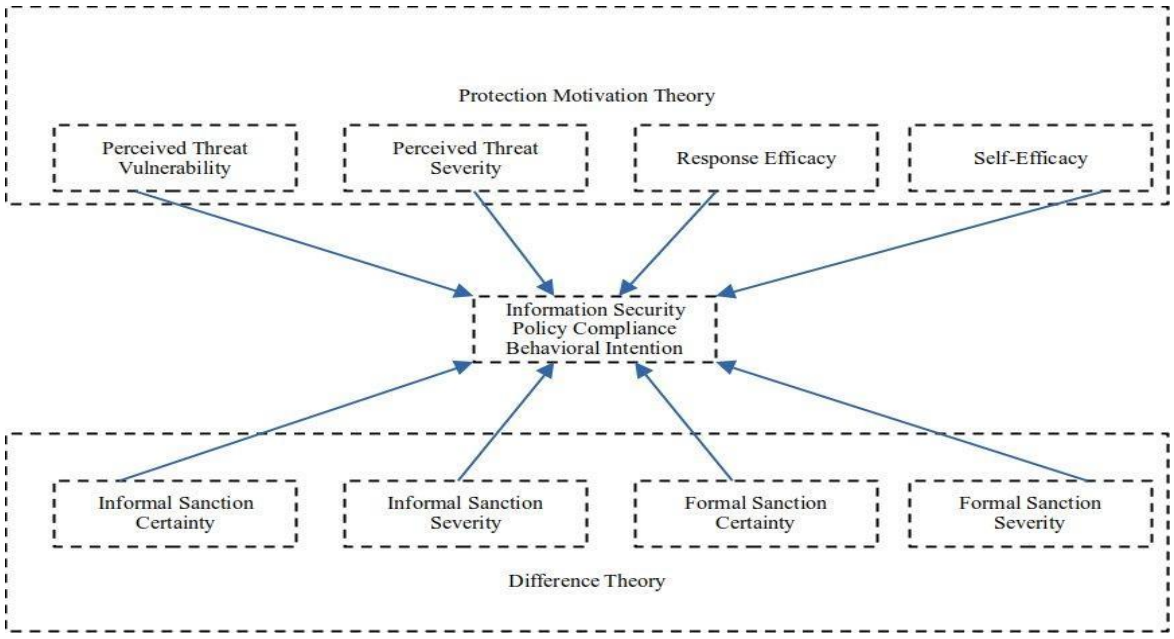

Figure 3: Research Methodology(David, 2017)

The procedure outlined by (Hair, 2012) for doing a partial least squares-structural equation modeling analysis, steps of this method were used to create the structural model, define the measurement model, gather data, estimate the model, evaluate the measurement model, and evaluate the findings. The technique was repeated twice, and there were two groups in the study.

1. Replies of the control group.
2. Replies of the experimental group.

To use all partial least squares-structural equations they have used the 'SmartPLS(v3.0)' software package modeling calculations.

In this research (David, 2017), Technology Acceptance Model (TAM) was used as a baseline model for the verification of a series of hypothesized relationships that are particular to the e-library usage context. TAM is based on two specific beliefs in adopting information

technology. Utility is defined as an individual's belief that using a particular technique will improve performance. Certain technologies make life easier(Fortes, 2016).

Seven independent variables, two belief variables, and one dependent variable make up the model that is suggested here. Three groups comprise the seven independent variables:

1. Separate differences,
2. Attributes of the interface and
3. Attributes of the system.

Individual variations include both computer self-efficacy and search domain knowledge. The terms "interface characteristics" ."screen design" and "navigation" come to mind. Relevance and system quality are examples of system attributes. The two belief criteria that were used in this investigation were perceived usefulness and perceived usability. The dependent variable is the desire to use an electronic library(Kuika, 2020) has put out a model that illustrates social media's impact on people's privacy. The fundamental inspiration for the construction of this model came from a variety of ideas, including TAM, TPB, privacy concerns, and perceived risk. A clearer understanding of social media's grip on privacy will result from the synthesis of these many theories and approaches. Both quantitative and qualitative research methods are used. An alternative method of evaluating the accuracy of models in IS research is to use surveys for study. Since it is especially appropriate for explanatory models where occurrences must be analyzed in light of their natural environment(Pinsonneault, 2015).

(Norberg, 2007)has proposed a conceptual model that reflects how risk and trust influence both actual and intentional behaviour toward privacy.

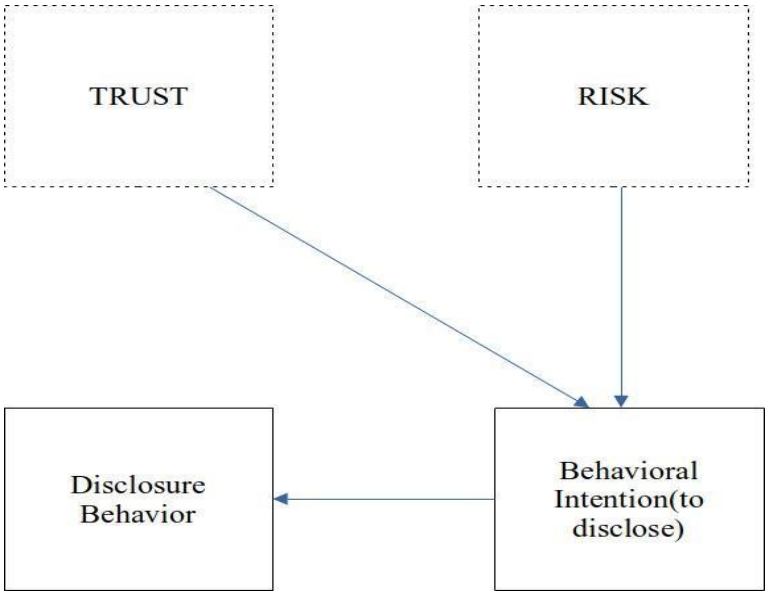

Figure 4: Conceptual model of disclosure (Norberg, 2007)

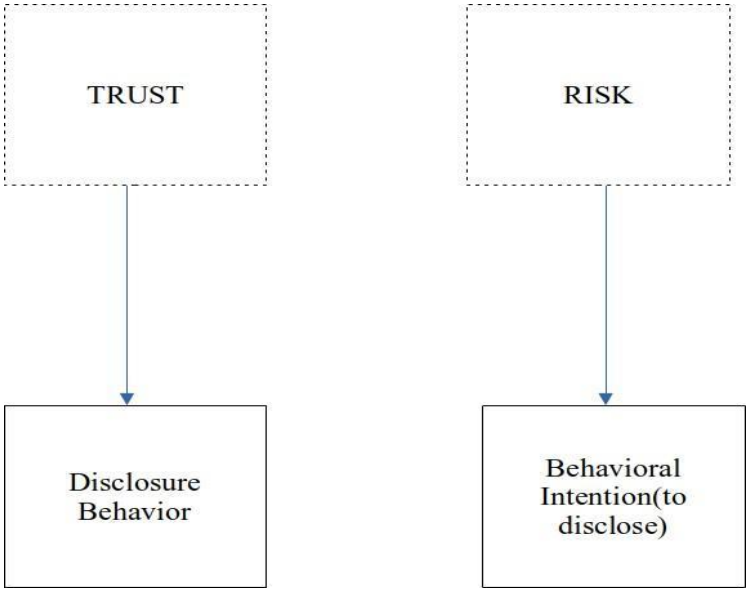

Figure 5: Conceptual model of privacy paradox (Norberg, 2007)

Figure 5 shows a conceptual model that reflects how they believe that risk and trust work according to actual behaviour and intentions.

The Unified Theory of Acceptance and Use of Technology (UTAUT) model has similarly done away with the importance of attitudes, claiming that the inclusion of performance and effort expectation components in the model prevents attitudes from directly impacting intention. 51 of the 188 academic publications (Auwal, 2015) found identified dealing with the issue of accepting electronic payments were empirical studies. UTAUT was recognized as the preeminent research model among them. The UTAUT model has the advantage that, in its simplest version, it takes into account the majority of the elements stated above that may function as barriers to the adoption of electronic payments, including performance expectations, effort expectations, and social impact. The fundamental model is also easily enhanced by new variables. (Tomić, 2022) used the UTAUT model to explain Serbia's acceptance of electronic payment systems. Along with the fundamental UTAUT predictors, they utilized an expanded model that considers several external factors, including perceived security, trust, privacy, convertibility, and financial expenses. In his research, a new research model is an extension to the basic UTAUT model, with additional

variables and research hypotheses. Hence, this model is based on the literature that he reviewed.

In this model, user behavior depends on privacy, behavioral intention, convertibility, and financial costs. However, behavioral intention depends on

1. Performance expectancy,
2. Effort Expectancy,
3. Perceived Security,
4. Trust and
5. Social influence.

Another study conducted (Maita, 2018) used the modified UTAUT for user behavior analysis in academic information systems. The model represents 11 hypotheses that find the empirical evidence of the four constructs of UTAUT moderated by gender and age variables. Though in (Negahban, 2014) among many other things Despite its success, UTAUT had its limitations because the concept was based solely on organizational settings rather than individual consumers. To address the UTAUT's limitations, the consumer context must be integrated (Merhi, 2019) the result was UTAUT2. The addition of hedonic motivation as a new construct is regarded as a powerful predictor that emphasizes utility, which was lacking in the initial UTAUT. The UTAUT2 model outperformed the others in predicting technology acceptance by explaining more of the variance in intention and use of technology. While the UTAUT2 has been validated in a variety of industries and research settings, it falls short of constructs that have become relevant in the use of technology, particularly in the banking sector, where risk is a major consideration.

Our goal is to study the association between privacy concerns and behavior intention toward privacy and information security. Hence, some questionnaires of the measured characteristics of user behavior that are related to such engagement of user perceptions will be asked to clarify.

The research questions are:

RQ1: Which group of people are more aware of perceptions and behavioral intentions toward privacy and information security?

RQ2: What are the differences between junior employees and graduate students concerning user perceptions and behavioral intention toward privacy and information security?

4. Practical Part

In order to evaluate the user perceptions and behavioral intention towards privacy and information security, the author surveyed junior employees and graduate students. The survey aimed to identify the level of their awareness regards of privacy and information security. The survey results provided valuable insights into areas that require improvement and enhance overall security awareness. This section explains how the survey was created, how it was disseminated, how the data was gathered, and how it was analyzed.

4.1 Survey creation

The survey has been created using Google Forms and has 3 sections including demographic data, Perceptions, and Behavioral intention. The demographic data section includes 3 questions where the most important question was student or employee and education/working field. The author made the weight scale from 1 (I disagree) to 5 (I fully agree). Perceptions and Behavioral intention both have 2 sub-sections named Privacy and Information security. Each privacy section includes 7 questions and Information Security contains 6 questions. So, in total there were 29 questions including the demographic data section.

Perception section is more about understanding people's understanding of Privacy and Information security whereas the Behaviour intention section is to understand their actions towards privacy and Information security.

4.2 Data Collection

The author has sent the survey link to over 200 people from many student groups including Graduate and Undergraduate students. He has also shared the survey link on Facebook, Whatsapp, Linkedin, and telegram channel to collect the response as many as possible. He also has used many groups of higher study aspirants, Job searching aspirants, CSE employees groups, etc, and asked his own working company to respond to the survey. The author has been collecting the data for 1 month and got responses from 102 people including 49 responses from Junior Employees, 33 responses from Graduates, and 20 from Undergraduate students.

4.3 Data Analysis

The author has analyzed each question by using Microsoft Excel do the analysis.

Table 4: Analysis of demographic data

Are you a Graduate Student or Junior Employee?	Graduate Student	32.4% (33)
	Undergraduate Student	19.6% (20)
	Junior Employee	48% (49)
Education or Working field?	Business	40.2% (41)
	Technical	59.8% (61)
Age of respondents in years.	18-25	38.2% (39)
	26-35	57.8% (59)
	36-45	2.9% (3)
	45+	1% (1)

The table presents data related to the demographic characteristics of the survey respondents. Out of the total respondents, 32.4% were graduate students, 19.6% were undergraduate students, and 48% were junior employees. In terms of education or working field, 40.2% of the respondents were from the business field, while 59.8% were from the technical field. When it comes to age, the majority of the respondents fell within the 18-35 age range, with 38.2% being 18-25 and 57.8% being 26-35. The remaining 4% were 36 years or older. These demographic characteristics provide insight into the sample population of the survey and can aid in the interpretation of the results.

The main objective was to check the differences between graduate students and junior employees. Hence, the author made all the undergraduate students in to graduate variables and conduct the rest of the analysis.

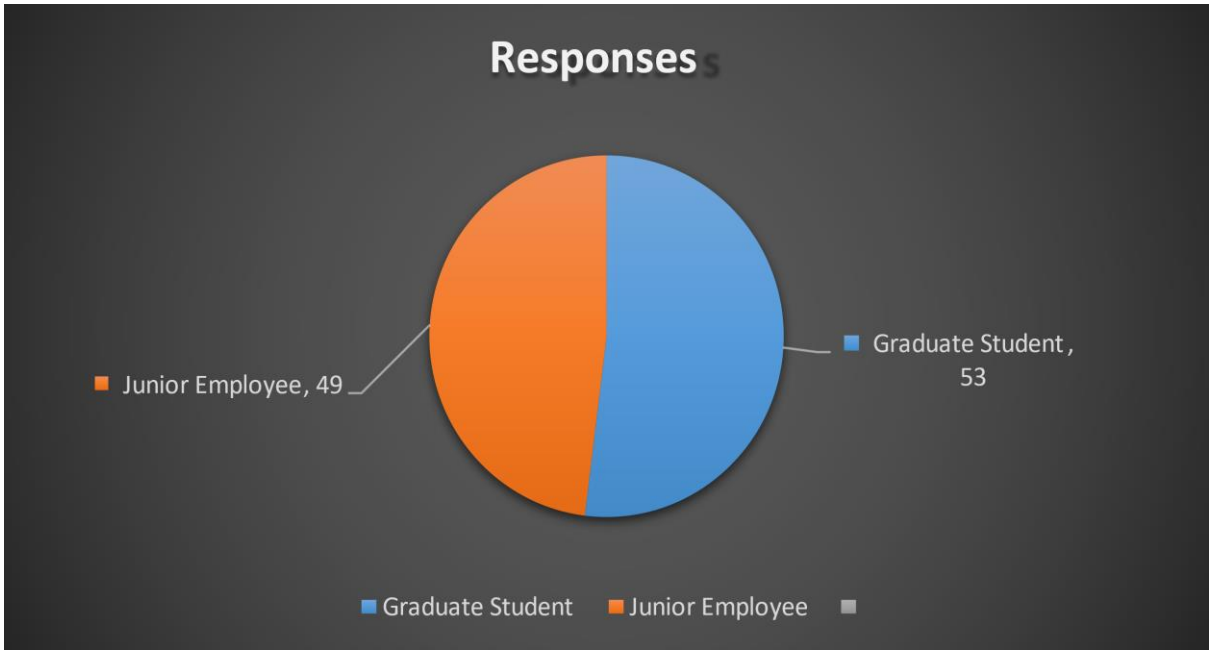

Figure 6: Pie chart of responds

All the responds from undergraduates have been renamed to graduate and figure out that 53 responds from Graduate students and 49 responds from Junior employees.

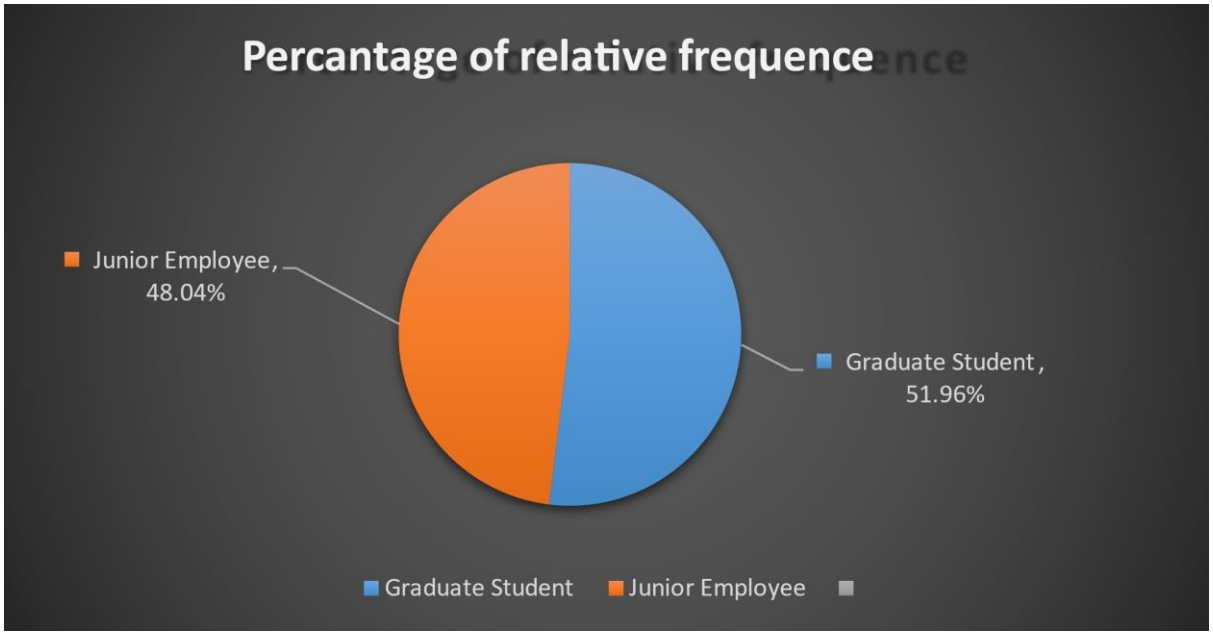

Figure 7: Pie chart of the percentage of relative frequence

5. Results and Discussion

The author has chosen an Independent Sample t-test to do the hypotheses testing because an Independent Samples t-test is used to check the difference between two independent groups. The author has decided to conduct this statistical method for found the best method to fulfil the thesis objective of comparing the user perceptions and behavioral intentions toward privacy and information security between Graduate students and Junior employees.

In the T-Test, the author has set one dependent and two independent variables. The test has been conducted 4 different times because of comparing the users perceptions of privacy, users perceptions of information security, users behavioral intention of privacy, and users behavioral intention of information security.

One dependent variable has been chosen for 4 different types for each test and these are respectively- users perceptions of privacy, users perceptions of information security, users behavioral intention of privacy, and users behavioral intention of information security.
Two independent variables are Graduate students and Junior employees for all tests.

Hypotheses have been decided as follows:

Null (H0): There is no significant difference between graduate students and junior employees mean users perceptions of privacy/ users perceptions of information security/ users behavioral intention of privacy/ users behavioral intention of information security.

Alternative (H1): There is a significant difference between graduate students and junior employees mean users perceptions of privacy/ users perceptions of information security/ users behavioral intention of privacy/ users behavioral intention of information security.

The significance level has been set for $p = 0.05$; Two-tailed.

The decision has been set by Rejecting the null hypothesis if $p < 0.05$ and failing to reject the null hypothesis.

p > 0.05. t-Test: Two-Sample Assuming Equal Variances has been conducted in Microsoft Excel for all the tests.

5.1 Data analysis of both group

This section describes the total response from both groups of people and their overall respond to each question.

0 – 1.75 = I disagree, 1.76 – 2.75 = I partly disagree, 2.76 – 3.75 = I am not sure, 3.76 – 4.75 = I partly agree, 4.76- I fully agree.

Table 5: Analysis of perceptions of privacy overall

Questions	Mean
I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to a mobile operator to register a new SIM card.	**3.08 (I am not sure)**
I do not mind speaking about my personal matters or habits with my friends in person.	**2.70 (I partly disagree)**
I do not mind if my private conversation can be overheard in public.	**1.70 (I disagree)**
I like to keep the privacy option private on social media for sharing my family photos.	**3.71 (I am not sure)**
I feel comfortable sharing my innovative ideas or business plans with my friends.	**3.38 (I am not sure)**
I feel comfortable sharing my innovative ideas or business plans with my friends.	**2.13 (I partly disagree)**
I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to access my PC, laptop, or smartphone	**3.60 (I am not sure)**

The data represent responses to a series of questions related to personal privacy and comfort level with sharing personal information. The responses are on a scale of 1 to 5, where 1 represents disagreement and 5 represents full agreement. The first question, which asks about providing biometric information to a mobile operator, received an average response of 3.08, indicating uncertainty among the respondents. The second and third questions, which ask about comfort level with discussing personal matters and being overheard in public, received average responses of 2.70 and 1.70, respectively, indicating partial disagreement. The remaining questions all received average responses indicating uncertainty, with values ranging from 2.13 to 3.71. Overall, the data suggest that respondents are not entirely comfortable with sharing personal information or biometric data.

Table 6: Analysis of perceptions of information security overall

Questions	Mean
I understand what information is considered as 'personal data'.	**4.10 (I partly agree)**
I know how to protect myself against - 'social engineering', 'phishing' and 'cybercrime'.	**3.82 (Consider as I partly agree)**
I know how to recognize a trusted website before I access it.	**3.60 (I am not sure)**
I consider saving passwords on the browser or in a password manager is a good practice.	**3.46 (I am not sure)**
I consider regular backups of data as important.	**3.94 (Consider as I partly agree)**
I am familiar with the consequences of a ransomware attack.	**3.41 (I am not sure)**

The data represent responses to questions related to perceptions of information security. The respondents were asked to rate their level of agreement with various statements. The overall average response for the statement "I understand what information is considered as 'personal data'" was 4.10, indicating partial agreement. The statement "I know how to protect myself against - 'social engineering', 'phishing' and 'cybercrime'" had an overall average response of 3.82, which can also be considered partial agreement. For the statement "I know how to recognize a trusted website before I access it," the average response was 3.60, indicating that the respondents were not entirely sure. The statement "I consider saving passwords on the browser or in a password manager is a good practice" had an overall average response of 3.46, indicating a lack of clarity. The statement "I consider regular backups of data as important" received an average response of 3.94, indicating partial agreement. Finally, the statement "I am familiar with the consequences of a ransomware attack" received an average response of 3.41, indicating that the respondents were not entirely sure.

Table 7: Analysis of behavioral intentions of privacy overall

Questions	Mean
If a mobile operator requests my biometric information to register a new SIM card (e.g., fingerprint), I provide it.	**3.52 (I am not sure)**
I sometimes speak about my personal matters or habits with my friends.	**3.06 (I am not sure)**
I sometimes lead personal conversations in public that can be overheard.	**2.05 (I partly disagree)**
I let my family photos be visible to the public on the Internet.	**2.35 (I partly disagree)**
I discuss innovative ideas or business plans with my friends.	**3.25 (I am not sure)**

I sometimes use someone else's contact number or email for my parcel delivery.	**2.04 (I partly disagree)**
I use a biometric option (fingerprint, face recognition, retina scan) to use my laptop PC, or smartphone.	**3.90 (Consider as I partly agree)**

The data represents responses related to the behavioral intentions of privacy for different scenarios. The respondents were asked about their likelihood of performing certain actions related to their personal information and privacy. The overall average response for each question is provided on a scale ranging from 1 to 5, with 1 indicating disagreement and 5 indicating agreement.

The data indicates that the respondents are not entirely sure about providing their biometric information to register a new SIM card, with an average response of 3.52. They are also unsure about discussing personal matters or habits with friends (average response of 3.06) and sharing innovative ideas or business plans (average response of 3.25) with them.

On the other hand, respondents disagree with leading personal conversations in public (average response of 2.05) and letting their family photos be visible to the public on the internet (average response of 2.35). The data also shows that respondents have a moderate inclination towards using a biometric option to access their devices (average response of 3.90).

Table 8: Analysis of behavioral intentions of information security overall

Questions	Mean
I usually post or upload personal data (e.g., address, phone number, email address, birth date) on social media sites or 3rd party cloud storage services.	**2.52 (I partly disagree)**
If I receive a request for an action (e.g., to log in, confirm some information, etc.) from a familiar email ID, I comply with it without a doubt.	**2.26 (I partly disagree)**
I usually check whether the website is secure to access.	**3.55 (I am not sure)**
I regularly keep my passwords saved in a browser or a password manager.	**3.52 (I am not sure)**
I regularly keep my passwords saved in a browser or a password manager.	**3.53 (I am not sure)**
I do download software from the first place where I find it.	**2.78 (Consider as I am not sure)**

This data is about the Behavioral Intentions of Information Security. The questions asked about the respondents' intentions and habits related to protecting their personal information and data. The responses were given on a scale of 1 to 5, with 1 indicating strong disagreement and 5 indicating strong agreement. The overall responses show that most of the respondents partly disagreed or were not sure about posting personal data on social media or cloud storage services, complying with requests from familiar email IDs, and downloading software from the first place they find it. The respondents were also not sure about regularly keeping their passwords saved in a browser or a password manager and checking whether a website is secure before accessing it.

5.2 Data analysis of individual group

Table 9: Analysis of perceptions of privacy individual group

Users Perceptions of Privacy		
Questions	**Graduate Mean**	**Junior employee Mean**
I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to a mobile operator to register a new SIM card.	**3.19 (I am not sure)**	**2.96 (I am not sure)**
I do not mind speaking about my personal matters or habits with my friends in person.	**2.85 (I am not sure)**	**2.53 (I partly disagree)**
I do not mind if my private conversation can be overheard in public.	**1.83 (I partly disagree)**	**1.55 (I disagree)**
I like to keep the privacy option private on social media for sharing my family photos.	**3.58 (I am not sure)**	**3.84 (I partly agree)**
I feel comfortable sharing my innovative ideas or business plans with my friends	**3.57 (I am not sure)**	**3.18 (I am not sure)**
I do not mind using someone's else's contact number or email for my parcel delivery.	**2.48 (I partly disagree)**	**1.76 (I partly disagree)**

I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to access my PC, laptop, or smartphone	**3.47 (I am not sure)**	**3.73 (I am not sure)**

The data compares the responses of graduate and junior employees regarding their perceptions of privacy. Overall, both groups are not entirely sure or comfortable about providing their biometric information to a mobile operator for a new SIM card or using biometric information to access their devices. However, junior employees are more likely to disagree with sharing personal matters or habits with friends in person, being overheard in public conversations, and using someone else's contact information for parcel delivery. On the other hand, graduate employees are more likely to consider keeping their privacy options private on social media for sharing family photos.

Table 10: Analysis of perceptions of information security individual group

Users Perceptions of Information Security		
Questions	**Graduate Mean**	**Junior employee Mean**
I understand what information is considered as 'personal data'.	**3.87 (I partly agree)**	**4.34 (I partly agree)**
I know how to protect myself against - 'social engineering', 'phishing' and 'cybercrime'.	**3.47 (I am not sure)**	**4.28 (I partly agree)**
I know how to recognize a trusted website before I access it.	**3.34 (I am not sure)**	**3.90 (I partly agree)**

I consider saving passwords on the browser or in a password a good practice.	**3.21 (I am not sure)**	**3.73 (I am not sure)**
I consider regular backups of data as important.	**3.80 (I partly agree)**	**4.10 (I partly agree)**
I am familiar with the consequences of a ransomware attack.	**3.06 (I am not sure)**	**3.80 (I partly agree)**

The data shows the comparison of responses between graduate and junior employees regarding their perceptions of information security. Overall, junior employees seem to have a stronger understanding and awareness of information security than graduate students. Junior employees gave higher ratings on their knowledge of personal data, protecting themselves against social engineering, phishing, and cybercrime, recognizing trusted websites, and the importance of backups. However, both groups were unsure about the benefits of saving passwords on a browser or password manager and the consequences of a ransomware attack.

Table 11: Analysis of behavioral intention of privacy individual group

Users Behavioral Intention of Privacy		
Questions	**Graduate Mean**	**Junior employee Mean**
If a mobile operator requests my biometric information to register a new SIM card (e.g., fingerprint), I provide it.	**3.91 (I partly agree)**	**3.10 (I am not sure)**
I sometimes speak about my personal matters or habits with my friends.	**3.58 (I am not sure)**	**2.45 (I partly disagree)**
I sometimes lead personal conversations in public that can be overheard.	**2.28 (I partly disagree)**	**1.80 (I partly disagree)**
I let my family photos be visible to the public on the Internet.	**2.55 (I partly disagree)**	**2.14 (I partly disagree)**
I discuss innovative ideas or business plans with my friends.	**3.51 (I am not sure)**	**2.96 (I am not sure)**
I sometimes use someone else's contact number or email for my parcel delivery.	**2.40 (I partly disagree)**	**1.65 (I disagree)**
I use a biometric option (fingerprint, face recognition, retina scan) to use my laptop PC, or smartphone.	**4.04 (I partly agree)**	**3.73 (I am not sure)**

The comparison of data shows the differences in the behavioral intentions of privacy between graduate and junior employee respondents. Overall, graduate respondents have a higher tendency to protect their privacy compared to junior employee respondents. Graduate respondents are more likely to provide their biometric information to register a new SIM card, keep personal matters private, not have personal conversations in public, not let their family photos be visible to the public, discuss innovative ideas or business plans with friends, and use a biometric option to use their devices. Junior employee respondents, on the other hand, have a lower tendency to protect their privacy and are more likely to be unsure about their intentions regarding privacy.

Table 12: Analysis of behavioral intention of information security individual group

Users Behavioral Intention of Information security		
Questions	**Graduate Mean**	**Junior employee Mean**
I usually post or upload personal data (e.g., address, phone number, email address, birth date) on social media sites or 3rd party cloud storage services.	**3.04 (I am not sure)**	**1.96 (I partly disagree)**
If I receive a request for an action (e.g., to log in, confirm some information, etc.) from a familiar email ID, I comply with it without a doubt.	**2.68 (I partly disagree)**	**1.82 (I partly disagree)**
I usually check whether the website is secure to access.	**3.30 (I am not sure)**	**3.10 (I am not sure)**
I regularly keep my passwords saved in a browser or a password manager.	**3.28 (I am not sure)**	**3.77 (I partly agree)**

I regularly backup my data.	**3.38 (I am not sure)**	**3.69 (I am not sure)**
I do download software from the first place where I find it.	**3.43 (I am not sure)**	**2.16 (I partly disagree)**

The table compares the behavioral intentions of information security between graduate and junior employees. The ratings are based on a scale of 1 to 5, where 1 indicates strong disagreement and 5 indicates strong agreement. Overall, the graduate responses suggest a higher level of caution and awareness regarding information security than the junior employees. The graduate respondents are more likely to avoid posting personal data on social media and to question the authenticity of requests for action from familiar email IDs. However, both groups demonstrate a lack of certainty when it comes to regularly backing up data, checking website security, and downloading software from trustworthy sources.

5.3 Hypothesis testing

The author has conducted the test for 4 times because there are 4 different hypotheses to test and compare the differences to do the research in depth. The comparison has been described separately for each section and also do the hypothesis testing separately to get the data more accurately.

5.3.1 users perceptions of privacy

7 questions have been asked in the user perceptions of privacy so the n = 7 for this section.

t-Test: Two-Sample Assuming Equal Variances

Table 13: t-test for users perceptions of privacy

	Graduate	*Junior Employee*
Mean	**3.00**	**2.79**
Variance	0.43	0.81
Observations	7.00	7.00
Pooled Variance	0.62	
Hypothesized Mean Difference	0.00	
df	**12.00**	
t Stat	**0.48**	
P(T<=t) one-tail	0.32	
t Critical one-tail	1.78	
P(T<=t) two-tail	**0.64**	
t Critical two-tail	2.18	

The given hypothesis testing is comparing the means of two populations, Graduate and Junior Employees, based on a two-tailed test for users perceptions of privacy The null hypothesis states that there is no significant difference between the mean scores of the two populations, while the alternative hypothesis states that there is a significant difference.

The test is performed using a significance level (α) of 0.05, which means that if the p-value is less than 0.05, we reject the null hypothesis, and if the p-value is greater than 0.05, we fail to reject the null hypothesis.

The mean score of the Graduate population is 3.00, and the mean score of the Junior Employee population is 2.79. The variance of the Graduate population is 0.43, and the variance of the Junior Employee population is 0.81. The sample size for both populations is 7.

Using the pooled variance method, the pooled variance is calculated as 0.62. The hypothesized mean difference is 0.00, indicating that there is no significant difference between the mean scores of the two populations.

The t-statistic is calculated as 0.48, and the degree of freedom (df) is 12. The p-value for a one-tailed test is 0.32, and the critical t-value for a one-tailed test with 12 degrees of freedom and a significance level of 0.05 is 1.78.

The p-value for a two-tailed test is 0.64, and the critical t-value for a two-tailed test with 12 degrees of freedom and a significance level of 0.05 is 2.18.

Since the p-value (0.64) is greater than the significance level (0.05), we fail to reject the null hypothesis. Thus, we can conclude that there is no significant difference between the mean scores of the Graduate and Junior Employee populations at a significance level of 0.05.

5.3.2 users perceptions of information security

6 questions have been asked in the user perceptions of information security so the n = 6 for this section.

t-Test: Two-Sample Assuming Equal Variances

Table 14: t-Test for user perceptions of information security

	Graduate	*Junior Employee*
Mean	**3.46**	**4.03**
Variance	0.10	0.06
Observations	6.00	6.00
Pooled Variance	0.08	
Hypothesized Mean Difference	0.00	
df	**10.00**	
t Stat	**-3.38**	
P(T<=t) one-tail	0.00	
t Critical one-tail	1.81	
P(T<=t) two-tail	**0.01**	
t Critical two-tail	2.23	

This test was conducted for the users perceptions of information security.
The mean score of the Graduate population is 3.46, and the mean score of the Junior Employee population is 4.03. The variance of the Graduate population is 0.10, and the variance of the Junior Employee population is 0.06. The sample size for both populations is 6.

Using the pooled variance method, the pooled variance is calculated as 0.08. The hypothesized mean difference is 0.00, indicating that there is no significant difference between the mean scores of the two populations.

The t-statistic is calculated as -3.38, and the degree of freedom (df) is 10. The p-value for a one-tailed test is 0.00, and the critical t-value for a one-tailed test with 10 degrees of freedom and a significance level of 0.05 is 1.81.

The p-value for a two-tailed test is 0.01, and the critical t-value for a two-tailed test with 10 degrees of freedom and a significance level of 0.05 is 2.23.

Since the p-value (0.01) is less than the significance level (0.05), we reject the null hypothesis. Thus, we can conclude that there is a significant difference between the mean scores of the Graduate and Junior Employee populations at a significance level of 0.05.

5.3.3 users behavioral intention of privacy

7 questions have been asked in the behavioral intention of privacy so the n = 7 for this section.

t-Test: Two-Sample Assuming Equal Variances

Table 15: t-Test for the behavioral intention of privacy

	Graduate	*Junior Employee*
Mean	**3.18**	**2.55**
Variance	0.56	0.57
Observations	7.00	7.00
Pooled Variance	0.56	
Hypothesized Mean Difference	0.00	
df	**12.00**	
t Stat	**1.58**	
P(T<=t) one-tail	0.07	
t Critical one-tail	1.78	
P(T<=t) two-tail	**0.14**	
t Critical two-tail	2.18	

This test was conducted for the users behavioral intention of privacy.

The mean score of the Graduate population is 3.18, and the mean score of the Junior Employee population is 2.55. The variance of the Graduate population is 0.56, and the variance of the Junior Employee population is 0.57. The sample size for both populations is 7.

Using the pooled variance method, the pooled variance is calculated as 0.56. The hypothesized mean difference is 0.00, indicating that there is no significant difference between the mean scores of the two populations.

The t-statistic is calculated as 1.58, and the degree of freedom (df) is 12. The p-value for a one-tailed test is 0.07, and the critical t-value for a one-tailed test with 12 degrees of freedom and a significance level of 0.05 is 1.78.

The p-value for a two-tailed test is 0.14, and the critical t-value for a two-tailed test with 12 degrees of freedom and a significance level of 0.05 is 2.18.

Since the p-value (0.14) is greater than the significance level (0.05), we fail to reject the null hypothesis. Thus, we can conclude that there is no significant difference between the mean scores of the Graduate and Junior Employee populations at a significance level of 0.05.

5.3.4 users behavioral intention of information security

6 questions have been asked in the behavioral intention of information security so the n = 6 for this section.

t-Test: Two-Sample Assuming Equal Variances

Table 16: t-Test for users behavioral intention of information security

	Graduate	*Junior Employee*
Mean	**3.19**	**2.75**
Variance	0.08	0.78
Observations	6.00	6.00
Pooled Variance	0.43	
Hypothesized Mean Difference	0.00	
df	**10.00**	
t Stat	**1.15**	
P(T<=t) one-tail	0.14	
t Critical one-tail	1.81	
P(T<=t) two-tail	**0.28**	

t Critical two-tail	2.23

This test was conducted for the users behavioral intention of information security.
Based on the given information, the means of the Graduate and Junior Employee groups are 3.19 and 2.75, respectively. The t-statistic is 1.15, and the degrees of freedom are 10.

The p-value for a two-tailed test is 0.28, which is greater than the significance level of 0.05. Therefore, we fail to reject the null hypothesis, and we conclude that there is not enough evidence to suggest that there is a significant difference between the means of the two groups.

The answers to the research questions are as follows-
RQ1: Which group of people are more aware of perceptions and behavioral intentions toward privacy and information security?

Ans- In the Users Perceptions of Privacy- Graduate Mean 3.00 (**I am not sure**) Junior Employee 2.79 (**I am not sure**)
Users Perceptions of Information Security- Graduate Mean 3.46 (**I am not sure.)** Junior Employee 4.03 (**I partly agree)**
Users Behavioral Intention of Privacy – Graduate Mean 3.18 (**I am not sure**) Junior Employee 2.55 (**I partly disagree)**
Users Behavioral Intention of Information security - Graduate Mean 3.19 (**I am not sure**) Junior Employee 2.75. (**I am not sure**).
Based on the responses, it is proved that not all groups of people are more aware of privacy and information security. However, junior employees respond and were found slightly more aware concerning Users Perceptions of Information Security and Users Behavioral Intention of Privacy.

RQ2: What are the differences between junior employees and graduate students regarding user perceptions and behavioral intention toward privacy and information security?

Ans- Based on all the tests, the author can conclude that there is no significant difference between the mean scores of the Graduate and Junior Employee populations for user perceptions of privacy and user behavioral intention of privacy at a significance level of 0.05. However,

there is a significant difference between the mean scores of the Graduate and Junior Employee populations for user perceptions of information security at a significance level of 0.05. For user behavioral intention of information security, there is not enough evidence to suggest that there is a significant difference between the means of the two groups at a significance level of 0.05.

5.4 Discussion

The author has described many previous studies on privacy and information security in section 3.6 and these studies have been done by some online questionnaires, and interviews. Two surveys, conducted by Scott (2005) and Williams (2018), focused on users' perceptions of privacy and security on the internet. Scott's survey focused on cookies, privacy policies, and trust marks, and found that users expressed skepticism about privacy policies but felt they could trust the website to respect its policy. Williams' survey focused on the Internet of Things (IoT) and found that a lack of awareness led to a paradox in which protective behavior was limited.

In this thesis, the author has surveyed graduate students and junior employees to understand the theory and practical awareness of user perceptions and behavioral intentions toward privacy and information security. This paper is more focused on finding out the awareness difference between both group and also help to get a better understanding of the awareness for the security of the people. The survey focuses on biometric information. Privacy, phishing, cybercrime, and ransomware attack focuses on understanding these and practical action on these topics so it provides the information more briefly and accurately.

This paper has carried out different information on user perceptions and behavioral intentions towards privacy and information security which will prove a different paradigm of security and help other authors to utilize the information from here to discover new findings.

5.5 Implications for theory and practice

The author has described the most important topics related to user perceptions, behavioral intentions, privacy, and information security in deeply to polish up the knowledge of these topics which are important to know. Many people are facing security issues every day and the number of incidents is increasing continuously. The contribution of the author in the literature

part will help people to understand these topics in a better way and can determine many of the security risks by themselves.

Recommendations- The result of the practical part comes out not so satisfied as the author found that most respond to some of the questions as **"I am not sure"** where the author believe they should at least know these security issues at the level of education or the level of working experience. As an IT graduate student, the author is very concerned to see the responses from both groups because the author found that, both groups have a lack of knowledge of privacy and information security which drag a line of worry. After all, the lack of knowledge in information security will harm society and the industry as well. They can easily fall into a trap where bad people can take advantage of them. The findings of the thesis can help to understand the awareness of information security of the graduate student and junior employees and universities should add more courses on privacy and information security for IT/Business students to increase the knowledge of security. Employers also should add mandatory training for their employees as not all employees are not technically sound.

5.6 Limitations of the study

Although the author has drawn depth attention to describing the literature part thoroughly and finding out the result by analyzing the data based on the response still there are few limitations of this study. The author believes the limitation of this study is a limited sample. The author had able to manage 102 responses to the survey but it could be more significant if the sample of respondents could reach more than 200. Also, the author could not do any face-to-face interviews which could also led the paper in more depth. There might be limited reliability in the data because sometimes many people may not respond to the survey with their full focus.

It might be positive to have a few limitations in research to use these resources for more research in the related topic to find out more important results to help society and industry.

6. Conclusion

The main aim of this thesis was to compare user's perceptions and behavioral intentions toward privacy and information security between graduate students and junior employees.

The literature review provides an in-depth analysis of various aspects related to user perceptions, behavior intention, privacy, and information security. It covers different measures of user perception and user perceptions of privacy, along with the relationship between user perception and behavior.

Moreover, the review analyzes information security policies, their significance, the risk involved in information security, different types of information security, and the types of behaviors related to information security in organizations. The final section of the literature review focuses on existing models related to privacy and information security. The review aims to provide a comprehensive overview of the current research on user perceptions, behavior, privacy, and information security.

The practical part of the study involves several steps, starting with the creation of a survey to collect data. The next step was to collect data from the survey, followed by the data analysis process. The results and discussion section of the study includes data analysis for both groups, as well as individual group analysis. The study also involves hypothesis testing, with specific sections dedicated to users' perceptions of privacy and information security, as well as their behavioral intentions related to these topics.

The study's implications for theory and practice are also discussed, along with the limitations of the study. Overall, the practical part of the study aims to provide a comprehensive analysis of user perceptions and behavior related to privacy and information security, using a variety of data analysis techniques to conclude and made recommendations for future research and practice.

7. References

Auwal Kabir, M., Zabedah Saidin, S., Ahmi, A., & Auwal Kabir, M. (2015). *Adoption of e-Payment Systems: A Review of Literature*. www.icoec.my

Ayalon, O., & Toch, E. (2019). *Evaluating Users' Perceptions about a System's Privacy: Differentiating Social and Institutional Aspects*. https://www.usenix.org/conference/soups2019/presentation/ayalon

Azizan, S. N., Lee, A. S. H., Crosling, G., Atherton, G., Arulanandam, B. V., Lee, C. E., & Rahim, R. B. A. (2022). Online Learning and COVID-19 in Higher Education: The Value of IT Models in Assessing Students' Satisfaction. *International Journal of Emerging Technologies in Learning*, *17*(3), 245–278. https://doi.org/10.3991/IJET.V17I03.24871

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/J.TELE.2017.04.013

Berinato, S. (2005). *The Global State of Information Security 2005 | CSO Online*. https://www.csoonline.com/article/2119435/the-global-state-of-information-security-2005.html

Burgoon, J. K., Parrott, R., le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*(2), 131–158. https://doi.org/10.1177/026540758900600201

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). *Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources*. https://doi.org/10.1016/j.im.2014.12.004

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445–459. https://doi.org/10.1016/J.GIQ.2018.04.002

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management 2005 6:2*, *6*(2), 181–202. https://doi.org/10.1007/S10799-005-5879-Y

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *Http://Dx.Doi.Org/10.1177/1461444808101618*, *11*(3), 395–416. https://doi.org/10.1177/1461444808101618

David A. Brown. (2017). *"Examining the Behavioral Intention of Individuals'' Compliance with Inf".''* https://scholarworks.waldenu.edu/dissertations/3750/

Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016). *Measuring the Human Factor in Information Security and Privacy*. https://doi.org/10.1109/HICSS.2016.459

epic.org. (2022). *EPIC - Public Opinion on Privacy*. https://archive.epic.org/privacy/survey/

Exabeam. (2022). *The 12 Elements of an Information Security Policy*. https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

EY. (2014). *Insights on governance, risk and compliance*.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*(3), 167–176. https://doi.org/10.1016/J.IEDEEN.2016.04.002

Friedewald, M., Finn, R., & Wright, D. (2013). *Seven Types of Privacy*. http://www.rogerclarke.com/DV/Intro.html.

FTC Headquarters. (2002). *Consumer Information Security Workshop | Federal Trade Commission*. https://www.ftc.gov/news-events/events/2002/05/consumer-information-security-workshop

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy Perception when Using Smartphone Applications. *Mobile Networks and Applications*, *25*(3), 1055–1061. https://doi.org/10.1007/S11036-020-01529-Z/TABLES/2

Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The Use of Partial Least Squares Structural Equation Modeling in Strategic Management Research: A Review of Past Practices and Recommendations for Future Applications. *Long Range Planning*, *45*(5–6), 320–340. https://doi.org/10.1016/J.LRP.2012.09.008

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. L. (2007). Analyzing Online Information Privacy Concerns: An Information Processing Theory Approach. *Undefined*. https://doi.org/10.1109/HICSS.2007.81

Harris, Associates Inc, & Westin. (1998, June). *E-commerce and privacy:What net users want. Privacy and American Business and Pricewater-house* . https://pandab.org/ecommercesurvey.html

Hu, H. H., Kandampully, J., & Juwaheer, D. D. (2009). Relationships and impacts of service quality, perceived value, customer satisfaction, and image: an empirical study. *Http://Dx.Doi.Org/10.1080/02642060802292932*, *29*(2), 111–125. https://doi.org/10.1080/02642060802292932

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour and Information Technology*, *29*(3), 221–232. https://doi.org/10.1080/01449290701679361

IBM. (2022). *Cost of a data breach*. https://www.ibm.com/reports/data-breach

IGI Global. (2022). *What is Privacy Concern*. https://www.igi-global.com/dictionary/privacy-concern/40729

ISO. (2022). *ISO 31000 — Risk management*. https://www.iso.org/iso-31000-risk-management.html

Jouini, M., Rabai, L. B. A., & Aissa, A. ben. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/J.PROCS.2014.05.452

Kuika Watat, J., & Mekonnen Jonathan, G. (2020). *The influence of Privacy Concerns on Intention to Use Social The influence of Privacy Concerns on Intention to Use Social Media Media*. https://aisel.aisnet.org/amcis2020

LEE, R., SARA, K., RUOGU, K., & MARY, M. (2013, September). *Anonymity, Privacy, and Security Online | Pew Research Center*. https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289–304. https://doi.org/10.1016/J.IM.2004.01.003

Lubua, E. W., Semlambo, A., & Pretorius, P. D. (2017). Factors affecting the use of social media in the learning process. *SA Journal of Information Management*, *19*(1). https://doi.org/10.4102/SAJIM.V19I1.764

Maita, I., Saide, Indrajit, R. E., & Irmayani, A. (2018). User behavior analysis in academic information system using unified theory of acceptance and use of technology (UTAUT). *ACM International Conference Proceeding Series*, 223–228. https://doi.org/10.1145/3230348.3230351

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/ISRE.1040.0032

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. *Https://Doi.Org/10.1287/Mnsc.1060.0597*, *52*(12), 1865–1883. https://doi.org/10.1287/MNSC.1060.0597

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Https://Doi.Org/10.1509/Jm.15.0497*, *81*(1), 36–58. https://doi.org/10.1509/JM.15.0497

Mascarenhas, O. A. J., Kesavan, R., & Bernacchi, M. D. (2003). Co-managing online privacy: A call for joint ownership. *Journal of Consumer Marketing*, *20*(7), 686–702. https://doi.org/10.1108/07363760310506201

Mekovec, R., & Hutinski, Ž. (2012). *The role of perceived privacy and perceived security in online market*.

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, *59*, 101151. https://doi.org/10.1016/J.TECHSOC.2019.101151

Musekura, J. B., & Ekh, R. (2004). *Information security issues – difference between perceptionand practice in organizations*.

Negahban, A., & Chung, C. H. (2014). Discovering determinants of users perception of mobile device functionality fit. *Computers in Human Behavior*, *35*, 75–84. https://doi.org/10.1016/J.CHB.2014.02.020

Nguyen, T., Nguyen, D. C., Schilling, M., Wang, G., & Backes, M. (2021). Measuring User Perception for Detecting Unexpected Access to Sensitive Resource in Mobile Apps. *ASIA CCS 2021 - Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 578–592. https://doi.org/10.1145/3433210.3437511

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/J.1745-6606.2006.00070.X

Olga, S. (2021). *What Is Online Privacy and Why Does It Matter? | Clario*. https://clario.co/blog/what-is-online-privacy/

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions.' *International Journal of Human-Computer Studies*, *65*(6), 526–536. https://doi.org/10.1016/J.IJHCS.2006.12.001

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security*, *24*(2), 228–240. https://doi.org/10.1108/ICS-01-2016-0009

Pinsonneault, A., & Kraemer, K. L. (2015). Survey Research Methodology in Management Information Systems: An Assessment. *Http://Dx.Doi.Org/10.1080/07421222.1993.11518001*, *10*(2), 75–105. https://doi.org/10.1080/07421222.1993.11518001

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/JIS.2016.73014

Rita, P., Oliveira, T., & Farisa, A. (2019). The impact of e-service quality and customer satisfaction on customer behavior in online shopping. *Heliyon*, *5*(10), e02690. https://doi.org/10.1016/J.HELIYON.2019.E02690

Roger, C. (1997). *Introduction to dataveillance and information privacy, and definitions of terms*. http://www.rogerclarke.com/DV/Intro.html

Scott, F., & Jo, L. (2005). *User Perceptions of Privacy and Security on the Web*. https://www.researchgate.net/publication/220919825_User_Perceptions_of_Privacy_and_Security_on_the_Web

Statista. (2022). *Internet and social media users in the world*. https://www.statista.com/statistics/617136/digital-population-worldwide/

Swish Goswami. (2020). *The Rising Concern Around Consumer Data And Privacy*. https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=3eecdd04487e

Tomić, N., Kalinić, Z., & Todorović, V. (2022). Using the UTAUT model to analyze user intention to accept electronic payment systems in Serbia. *Portuguese Economic Journal 2022*, 1–20. https://doi.org/10.1007/S10258-022-00210-5

Truste. (2015, January). *2015 TRUSTe UK consumer confidence index*. Http://Www.Truste.Com/Resources/ Privacy-Research/Uk-Consumer-Confidence-Index-2015/.

Ullah, S., Khan, M. S., Lee, C., & Hanif, M. (2022). Understanding Users’ Behavior towards Applications Privacy Policies. *Electronics 2022, Vol. 11, Page 246*, *11*(2), 246. https://doi.org/10.3390/ELECTRONICS11020246

Wang, P., & Petrison, L. A. (1993). Direct marketing activities and personal privacy. A consumer survey. *Journal of Direct Marketing*, *7*(1), 7–19. https://doi.org/10.1002/DIR.4000070104

Wang, Y., Genc, E., & Peng, G. (2019). Aiming the Mobile Targets in a Cross-Cultural Context: Effects of Trust, Privacy Concerns, and Attitude. *Https://Doi.Org/10.1080/10447318.2019.1625571*, *36*(3), 227–238. https://doi.org/10.1080/10447318.2019.1625571

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? *International Journal of Information Management*, *44*, 164–177. https://doi.org/10.1016/J.IJINFOMGT.2018.10.016

Warren, & Brandeis. (1890). *The Right to Privacy* (Vol. 4). Harvard Law Review. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Law Review*, *25*, 3–4. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

Williams, M., Nurse, J. R. C., & Creese, S. (2018). Privacy is the boring bit: User perceptions and behaviour in the internet-of-things. *Proceedings - 2017 15th Annual Conference on Privacy, Security and Trust, PST 2017*, 181–190. https://doi.org/10.1109/PST.2017.00029

Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1996). The behavioral consequences of service quality. *Journal of Marketing*, *60*(2), 31–46. https://doi.org/10.2307/1251929

Zhuang, M., Demartini, G., & Toms, E. G. (2017). Understanding engagement through search behaviour. *International Conference on Information and Knowledge Management, Proceedings*, *Part F131841*, 1957–1966. https://doi.org/10.1145/3132847.3132978

Zhuang, M., Toms, E. G., & Demartini, G. (2016). The Relationship between User Perception and User Behaviour in Interactive Information Retrieval Evaluation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence*

and Lecture Notes in Bioinformatics), *9626*, 293–305. https://doi.org/10.1007/978-3-319-30671-1_22

8. List 0f pictures, tables, graphs, and abbreviations

8.1 List of pictures

8.2 List of tables

Appendix

Demographic data

Are you a Graduate Student or Junior Employee:

- ○ Graduate Student
- ○ Undergraduate Student
- ○ Junior Employee

Education or Working field:

- ○ Business
- ○ Technical

Age of respondents in years:

- ○ 18-25
- ○ 26-35
- ○ 36-45
- ○ 45+

Scale

I disagree	I partly disagree	I am not sure	I partly agree	I fully agree
1	2	3	4	5

1. Perceptions

1.1 Privacy (*according to Chignell, (2003)*)

I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to a mobile operator to register a new SIM card.	1	2	3	4	5
I do not mind speaking about my personal matters or habits with my friends in person.	1	2	3	4	5
I do not mind if my private conversation can be overheard in public.	1	2	3	4	5
I like to keep the privacy option private on social media for sharing my family photos.	1	2	3	4	5
I feel comfortable sharing my innovative ideas or business plans with my friends.	1	2	3	4	5
I do not mind using someone’s else’s contact number or email for my parcel delivery.	1	2	3	4	5
I am comfortable providing my biometric information (e.g., retina scan, fingerprint, face recognition) to access my PC, laptop, or smartphone	1	2	3	4	5

1.2. Information Security (*according to authors' construct and Louisville University*)

I understand what information is considered as 'personal data'.	1	2	3	4	5
I know how to protect myself against - 'social engineering', 'phishing' and 'cybercrime'.	1	2	3	4	5
I know how to recognize a trusted website before I access it.	1	2	3	4	5
I consider saving passwords on the browser or in a password a good practice.	1	2	3	4	5

I consider regular backups of data as important.	1	2	3	4	5
I am familiar with the consequences of a ransomware attack.	1	2	3	4	5

2. Behavioral Intention

2.1 Privacy (authors' construct and Chignell, (2003)

If a mobile operator requests my biometric information to register a new SIM card (e.g., fingerprint), I provide it.	1	2	3	4	5
I sometimes speak about my personal matters or habits with my friends.	1	2	3	4	5
I sometimes lead personal conversations in public that can be overheard.	1	2	3	4	5
I let my family photos be visible to the public on the Internet.	1	2	3	4	5
I discuss innovative ideas or business plans with my friends.	1	2	3	4	5
I sometimes use someone else's contact number or email for my parcel delivery.	1	2	3	4	5
I use a biometric option (fingerprint, face recognition, retina scan) to use my laptop PC, or smartphone.	1	2	3	4	5

2.2 Information Security (*according to authors' construct and Louisville University*)

I usually post or upload personal data (e.g., address, phone number, email address, birth date) on social media sites or 3rd party cloud storage services.	1	2	3	4	5
If I receive a request for an action (e.g., to log in, confirm some information, etc.) from a familiar email ID, I comply with it without a doubt.	1	2	3	4	5
I usually check whether the website is secure to access.	1	2	3	4	5
I regularly keep my passwords saved in a browser or a password manager.	1	2	3	4	5
I regularly backup my data.	1	2	3	4	5
I do download software from the first place where I find it.	1	2	3	4	5

THANK YOU FOR COMPLETING THE QUESTIONNAIRE!