2021

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

THE DARK SIDE OF TRUST: IMPACTS OF USER BEHAVIORS, MISPLACED TRUST AND HABITUAL TRUST ON PERCEPTIONS OF ONLINE SECURITY AND PRIVACY

Cagatay Ozdinc

A Thesis Submitted to the
University of North Carolina Wilmington in Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science

Congdon School of Supply Chain, Business Analytics and Information Systems

University of North Carolina Wilmington

2021

Approved by

Advisory Committee

Devon Simmonds

Geoff Stoker

Jeff Cummings
Chair

Accepted By

Dean, Graduate School

TABLE OF CONTENTS

ABSTRACT

The internet is being used for almost everything nowadays, and life without the internet and applications would become harder for most of us. This reliance has increased even more as the recent pandemic has pushed many companies to rely on remote work, increasing online interactions. This situation makes trust an important factor for individuals who perform online activities. With the increased reliance on the internet and online interactions, an individual's security and privacy are at greater risk. Trust is essential for cybersecurity and privacy since the high trust of users will result in co-operation with systems features and methods to keep users safe. Trust is dependent on several factors, and these factors can change depending on individuals' behaviors and personalities. As trust is dependent on several factors, trust is also a significant force that shapes our behaviors in real life and the online environment. This thesis work aims to analyze specific user behavior values that are unique for each individual and find relations between certain types of trust. This thesis work also seeks to extend the research on relationships between mentioned types of trust and user perceptions about security and privacy. Research hypotheses mainly try to find a positive or negative relationship between three main variables of the thesis model mentioned above (user behaviors, types of trust, user perceptions). Most of the research variables are unique for each individual and reflect my thoughts on the most important aspects of individuals that can affect online trust. This uniqueness is also applicable for the trust variables, which reflect my ideas about the most critical types of trust that can affect individuals' perceptions of security and privacy online.

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Privacy and security of personal data have been issues since the early days of the internet. These problems have become more critical in the last few years as general internet usage continues to rise, even more so in the past year due to the pandemic forcing increased remote work. This increased use has not come without issues.

Individuals have the potential to become victims of illegal activities almost every day. In addition to individuals, companies can also be victims of cyberattacks impacting their security or violating their privacy (e.g., Facebook Scandal), resulting in loss of personal data. These recent incidents have had a significant impact on users' online behaviors regarding their privacy and security. However, what variables can impact these perceptions of security and privacy is still somewhat of an open question.

An individual's trust in online activity may have an impact on these perceptions. The concept of trust is an essential topic in cybersecurity. Trust shapes how users behave on a particular website or apply cybersecurity mechanics and use cybersecurity policies online. It has been a crucial factor in various studies within online environments, such as fostering successful relationships, reducing uncertainty and risk, and increasing willingness to purchase (Cho, 2006; Doney & Cannon, 1997; Grabner-Kräuter & Kaluscha, 2003; Jap & Anderson, 2003; Palmatier et al., 2006; Shankar et al., 2002). Also, since trust is based on different emotions, it may be influenced by how an individual behaves online (e.g., different levels of activity risk) (Tversky & Kahneman, 1986). Thus, online behaviors may indirectly impact perceptions of security and privacy by influencing trust online.

Trust, often perceived as a positive factor, can also negatively affect individuals called the dark side of trust. (Pienta, Sun, and Thatcher, 2016). These types of trust are often considered harmful for individuals and include both habitual and misplaced trust (Pienta, Sun, and Thatcher, 2016). Habitual trust is automatic and unconscious trust based on prior

positive outcomes with a system, often resulting from repeated satisfactory interaction (Pienta, Sun, and Thatcher, 2016). Misplaced trust is unknowingly extending trust to a malicious technology. This type of trust is common in individuals with low levels of cybersecurity knowledge (Pienta, Sun, Thatcher, 2016). However, little is known about how these types of trusts can be impacted by online behaviors or how they may impact perceptions of security and privacy.

This research aims to examine trust in the online environment and how trust can impact perceptions of security and privacy online. Additionally, individuals' behaviors (hedonic, utilitarian, risk avoidance – all are defined later) were examined to understand if those types of behavior impact trust. This research aims to answer the following questions:

1) Are there factors that influence habitual and misplaced trust, such as an individual's online behaviors?

2) Does habitual and misplaced trust impact an individual's perception of their security and privacy online?

CHAPTER 2: LITERATURE REVIEW

Trust and Trust Formation

Trust is commonly defined as “an individual's willingness to depend on another party because of the characteristics of that party” (Rousseau et al., 1998). The concept of trust can vary widely for each person and can change based on the type of studies such as psychology, sociology, economics, or social psychology. While trust can have different definitions based on the area of study, all those definitions have a common theme that trust can help to create successful relationships, reduce risk and uncertainty and increase willingness to do actions online such as shopping (Cho 2006; Doney & Cannon 1997; Grabner-Kräuter & Kaluscha, 2003; Jap & Anderson 2003; Palmatier et al. 2006; Shankar et al. 2002).

Based on personal interactions and experience, trust can be conceptualized in two different ways. The first definition focuses on the trust that is placed regarding an individual's behavior in return for something which can be called an expectation (Barber, 1983; Koller, 1988; Luhmann,1979; Rotter, 1967). The second definition is based on the individual's feeling of avoiding exposure to vulnerability (Doney, Cannon, & Mullen,1998; Mayer, Davis, & Schoorman, 1995; Rosseau et al., 1998; Zand, 1972). The individual's expectations and vulnerability may influence their overall security and privacy perception while performing online actions.

Expectation formation of trust relates to addressing a more social need than a psychological situation (Lewis & Weigert, 1985). Koller (1988) explains this bond between trust and expectation further. He defines trust as a trustor’s expectation that a trustee will willingly do as the trustor expects. In the expectation perspective of trust, showing trusting behaviors for individuals is essential to form a bond (Beldad et al., 2010). Those behaviors may be applied to the online environment and cybersecurity since users need a form of proof that what they are doing or what they are about to do is safe. One key form of proof is that

websites use certificates from third parties to prove their identity and legitimacy to users before users even interact with a website or application. This can help ensure a trusting environment between the trustor and trustee and increase the trustors' expectations of their trustees. Companies and individuals are mostly aware of this and use proof mechanisms mainly provided by third parties to prove their service is legitimate and safe. There are examples of this trust mechanism in lots of websites, such as verified accounts on YouTube or Twitter, to let ordinary users know that they are interacting with a trusted party or not.

As mentioned before, the second concept of trust is avoiding exposer to vulnerabilities. From this perspective, trusting someone is a form of accepting a particular type of risk. Uncertainty is a huge factor that influences the level of trust individuals give to the trusted party. Acceptance of risk differs from one individual to another, meaning an individuals' different levels of risk acceptance result in a change of degree of trust (Beldad et al., 2010). Luhmann (1979) explains trust in the context of vulnerability as a factor that reduces social complexity, as it simplifies making choices when taking a risk. Therefore, the act of trusting someone can be seen as a risk factor because while doing the act of trusting that person, an individual expects goodness and honesty from the trustor and wants to believe that way despite trustees' ability to betray that expectation or cheat the trustor (Elangovan, A.R., & Shapiro, D. 1998).

Apart from both concepts mentioned before, trust is a unique characteristic for each individual (Tyler & Kramer, 1996). This point of view sees trust as a factor that affects the capacity to assess the aimed parties' trustworthiness (Mayer et al., 1995). This explanation shows trust as a mirror that reflects the reliability of the trustee. Therefore, in online transactions and activities, applications and websites must prove reliable and trustable to gain an individual's trust. Giving trust also relies on good marketing and testing since these certificates that provide the feeling of safety have requirements that online parties need to comply with (Sztompka, 1999).

Again, in the concept of vulnerability for trust, trusting a website or application online also means exposure for the users. Users are exposing themselves to an unknown if they do not have any experience with the website or application they are using. They may use their similar experiences from other applications and websites to make assumptions about the safety level of action (Zand 1972). Thus, while trusting, users are increasing their vulnerability since their fate depends on the trustee. This willingness to trust can rely on the priority of certain actions or the importance of specific activities for users (Mayer et al., 1995). Different users can have different behaviors on the same website while doing the same action. A user's willingness is related to the importance given to particular action by that user. Doney et al. (1998) explain this as a relation between risk and vulnerability; they are related to the uncertainty of the result of the action, and it can be seen as the source of risk. Because of that, trust can also be explained as people's behavioral reliance on others on a condition of risk (Currall & Judge, 1995).

Trust is essential for the continuity of the transactions between users (Lewis & Weigert 1985), and this makes types of trust also essential for online systems as well for the same reason.

Trust in Technology

To understand trust in cybersecurity, one must first understand how the trust concept around technology is formed. Some researchers believe that humans cannot trust something that is not alive such as computers and systems. Schneiderman (2000) explains this situation as: “If users rely on a computer and it fails, they may get frustrated or vent their anger by smashing a keyboard, but there is no relationship of trust with a computer.” Other researchers also claim that humans cannot trust technology, as indicated by their statement: “People trust people, not technology” (Friedman et al., 2000). However, recent studies suggest that trust

can be a factor in influencing the acceptance of technologies such as recommendation agents, e-commerce systems, and knowledge management systems (Lankton et al., 2015).

Therefore, trust is crucial for online systems to work correctly (McKnight et al., 2009). All systems, including cybersecurity, rely on human trust to work appropriately (Pienta, Tams, and Thatcher, 2020). It is crucial to analyze what elements in technology are causing individuals to create a feeling of trust. Systems like password storage, data privacy, cloud system security, and two-factor authentication all require humans to trust that their information will be kept safe because trust values make individuals take specific actions online (Beldad et al. 2010). When trusting another person, these values are integrity, benevolence, and competence (Vance et al., 2008; Wang & Benbasat, 2005), but these values change to reliability, functionality, and helpfulness when it comes to trusting a technology (McKnight et al., 2011). Those values may have a massive effect on shaping the online consumer behavior and perceptions of users online. Perceptions related to security and privacy may also be affected by those values. Cybersecurity also depends on those values to work correctly, and because of that, cybersecurity systems are mainly designed to protect individuals' data as much as possible. (Pienta, Tams, and Thatcher, 2020).

Some researchers argue that when technology has human-like abilities such as voice recognition and answering ability, it can be misleading and cause individuals to evaluate systems integrity with human-like trust concepts (Lankton et al., 2015). This likeness of humanity can be misleading for individuals to choose the correct concept of trust values such as helpfulness, functionality, and reliability.

Helpfulness is the belief that a specific technology will provide ease and adequate help for users to make their actions much more straightforward than they used to be (McKnight et al., 2011). Applications and online platforms need to be aware of that to gain trust in individuals for their continuity since trust comes from experiences, and it is a thing

individuals tend to learn after experiences (Jones & George, 1998). The functionality aspect of the trust in technology is about if a specific technology or system has enough capacity to complete the desired action for individuals (McKnight et al., 2011). Another significant value is reliability which is about continuity and if a system or any technology can perform in a stable way (McKnight et al., 2011). These are essential concepts and can be helpful to understand trust in cybersecurity because cybersecurity is a system that relies on technology and human trust to work properly. Thus, understanding the relationship between trust and technology will also help us understand the relationship between trust and cybersecurity (Pienta, Tams, and Thatcher, 2020).

Cybersecurity and Trust

Cybersecurity's main objective is to protect individuals and organizations from malicious activities. Cybersecurity relies on individuals' trust in the technology and rules. The system, departments, and organizations create a trusting system that people rely on for their security. Individuals must trust all these parts of the cybersecurity system (Pienta, Tams, and Thatcher, 2020). Those cybersecurity agents also provide countermeasures that individuals can rely on and that can be used as a defense against cyber-attacks. For organizations, cybersecurity systems can produce legal strategies to discipline, educate, terminate, or maybe even prosecute using legal systems created within an organization to encourage individuals to comply with the cybersecurity policies (Pienta, Tams, and Thatcher, 2020).

In cybersecurity, trust is a highly compelling value that indicates user actions in times of uncertainty and vulnerability. Those situations that carry risk factors for individuals are crucial since they rely on cybersecurity agents to guide them on their behaviors if their knowledge is vast on a topic. (Pavlou, P.A., H. Liang, and Y. Xue, 2007). When individuals trust the system and rely on it with everything, but that system fails, the consequences can be

harsh. Therefore, trust can negatively affect situations because, after some point, users may automize the process of trusting the system and may reduce their attention. (Pienta, Tams, and Thatcher, 2020).

The function of cybersecurity is also crucial for individuals themselves because if individuals trust cybersecurity systems enough and comply with the methods that make cybersecurity work, users can educate themselves about identifying a cyber threat and how to protect against it. If a trusted system works correctly and according to plan, it can filter, identify, and even eliminate malicious and dangerous software and activities such as notifying emails to users that can cause potential harm. This effect of cybersecurity on individuals can also shape beliefs about trusting cybersecurity. Because of that multi-effect of trust in cybersecurity, it can be assumed that the trust concept in cybersecurity is a versatile and high-level phenomenon, including trust in the organization, trust in the function of cybersecurity, and the system of cybersecurity itself.

As mentioned, cybersecurity is a versatile high-level phenomenon created by several components (Pienta, Tams, and Thatcher, 2020), and this is particularly important for cybersecurity systems to work correctly. Trust must be created in several areas for this issue. Trust in cybersecurity function, trust in the organization, and trust in the cybersecurity system (McKnight et al., 2011). Trust in function consists of several values such as integrity of the system, competence of the system, and benevolence of the system (McKnight et al., 2011). Trust in the organization consists of values normality (situation plan) and assurance of the system's structure (McKnight et al., 2011). Lastly, trust in cybersecurity systems consists of values such as reliability, confidentiality, and accessibility (McKnight et al., 2011). These values are essential for conceptualizing trust in cybersecurity, and this conceptualizing can help create new values or develop new measures to help individuals trust cybersecurity systems more efficiently.

Apart from areas of cybersecurity where trust must be maintained among users to work cybersecurity systems properly, certain attributes are more personal and important for individuals for creating trust in a cybersecurity system. These system-like attributes for creating trust in cybersecurity are confidentiality, integrity, and availability, also known as the CIA triad (Pienta, Tams, and Thatcher, 2020). These values are essential for creating trust in cybersecurity systems. Confidentiality for trust in cybersecurity means restricting access to confidential information such as personal data and computing resources to only those who need to use it for protection activities. This value is essential for establishing trust in cybersecurity since the unauthorized entry into personal information may break the trust of individuals. (Pienta, Tams, and Thatcher, 2020).

The second significant value for trust in cybersecurity is availability, and this value represents the guarantee that individuals will be able to access crucial data or resources that helps to compute certain activities that will be available when it is necessary, which is guaranteed by authorized people (Pienta, Tams, and Thatcher, 2020). To be available to reach certain resources that may prevent cyberattacks and eliminate panic environments inside an organization. The last value which is essential for creating trust in cybersecurity is integrity. This backbone value represents the function and well-being of the system in times of crisis, and it also represents a stable working system (Pienta, Tams, and Thatcher, 2020).

Those concepts of trust for cybersecurity represent a mix of sociological and technical trust elements. For example, confidentiality represents the sociological side, while availability and integrity represent the technical side of this mix (Pienta, Tams, and Thatcher, 2020). These different types of trust can be used in different parts of organizations to create trust in cybersecurity for individuals and organizations.

Dark Side of the Trust

As stated before, trust is a form of action that gives privileges to the trustee until some level. This definition also means that the individual acknowledges risks and uncertainty, making him vulnerable to the trustee (Zand, 1972). According to the definitions above, individuals give a level of responsibility to the trustee that they can do what they want (Jones & George, 1998). This established relationship may help individuals in times of uncertainty and risk. Trust is a critical factor that reduces concerns in the context of privacy and shapes the behaviors of users in the area of privacy (Pavlou, P.A., H. Liang, and Y. Xue, 2007). In times of uncertainty and risk, feelings of individuals, such as concern and fear, can be eliminated with well-established trust (Gefen, D., E. Karahanna, and D.W. Straub, 2003). However, trust can negatively affect individuals since they may reduce their attention to detail and overlook some warnings, they usually are aware of.

To understand the effects of the dark side of trust on individuals further, the effects of trust on values that shape behaviors must also be examined. As mentioned, trust also affects values that shape behaviors such as information security and opportunism concerns in e-commerce (Pavlou, P.A., H. Liang, and Y. Xue, 2007). To further establish this relationship between trustor and trustee, signals of applications can be used to create a deeper trust relationship between a user and a trusted party. These signals can also keep users up to date with new security policies and teach them how to use certain technologies to enhance the trust between trustee and trustor (Pavlou, P.A., H. Liang, and Y. Xue, 2007). Trust function on cybersecurity also has an essential role in creating and implementing safe computing organization-wide policies, education of protective technologies, and the system of cybersecurity built on the bottom.

Arguably, the most significant vulnerability of cybersecurity is the human factor. Individuals have responsibilities, and they are bound to make essential decisions almost every

single day. They make these decisions by taking certain risks and sometimes even vulnerability to some extent in a malicious activity situation (Beldad et al., 2010). If an individual's trust is high enough in a cybersecurity system, that individual may not have certain feelings such as uncertainty, risk, and vulnerability compared to individuals who do not trust the system (Pavlou, P.A., H. Liang, and Y. Xue, 2007). Individuals trusting the system's capabilities and believing the system they have trusted will work adequately can be exposed to a specific form of vulnerability. For example, there are attacks designed to manipulate people to get inside of an organization or an individual's personal computer to extract personal information such as phishing, is designed to manipulate people with social engineering and gain advantage from their misplaced trust feelings (Pienta, Tams, and Thatcher, 2020). Individuals trust that the system will protect them, and they may not take extra protective measures to reduce the likelihood of exposing themselves.

When individuals encounter those threats online, they face certain decisions regarding the threat and the main factor that shapes that behavior/action is the level of trust in cybersecurity systems. (Pienta, Tams, and Thatcher, 2020). Individuals unconditionally trusting systems are inclined to trust systems without checking since they believe there will be no threats based on the overtrust placed in the system. Individuals may face the consequences of the dark side of trust since these individuals are abdicating the responsibility of filtering to the system, which is an agent of trust for cybersecurity. The dark side of trust can cause individuals to share their personal information or crucial information for access to personal data without even noticing that they are being hacked. They may download malicious files that can affect everybody in the organization or give hackers access to steal personal data.

Individuals need to be educated on when to trust a system and when not, face negative consequences. Negative consequences of trust on individuals are poor judgment,

relying on a system way too much, underperformance such as laziness, and overrelaxed management of systems (Gargiulo, M., and G. Ertug, 2006) (Yip, J.A., and M.E. Schweitzer, 2015).

Paying attention to details, notifications, and education about companies' policies can help individuals identify malicious activities. Paying more attention to detail has been proven to help individuals avoid malicious activities (Pienta, Tams, and Thatcher, 2020).
It can be said that companies and individuals should not rely on the system for their protection. They should also improve themselves to learn how to pay more attention to signs that can be malicious in emails or any activities. Proper security training and paying attention to details can help individuals avoid cyber threats. Research by ISec shows that individuals do not prioritize security while performing online activities (Herath, T., and H.R. Rao, 2009). This also shows that individuals are not aware of the latest cybersecurity developments or do not understand it all (Yip, J.A., and M.E. Schweitzer, 2015). Studies also showed that repeated warnings become habitual, and users fail to interact with those crucial warnings that can be considered the effects of the dark side of trust (Anderson, B., A. Vance, C.B. Kirwan, D. Eargle, and J.L. Jenkins, 2016).

Overall, the dark side of trust can have adverse effects on individuals and organizations alike. It can be prevented by not relying just on the system and improving the knowledge about cybersecurity and paying attention to details and warnings created by systems.

Habitual Trust

Habitual trust can be considered one of the dark sides of the trust mechanism. This type of trust can have negative consequences for both individuals and companies alike in terms of cybersecurity (Garguilo & Ertug 2006; Gambetta 1988). Arguably, the human factor in cybersecurity is considered the weakest chain in the link. Hackers aim to gain access to

personal data by using social engineering and human errors in cybersecurity, such as trusting a system habitually or unconsciously (McKnight et al., 2011). Habitual trust can be explained as unconscious and automatic trust based on the positive experiences of users on the system (Pienta, Sun, and Thatcher, 2016). The primary source of habitual trust is the user's belief about the system's robustness (Pienta, Sun, and Thatcher, 2016). This belief of users is formed with positive experiences and satisfactory interactions that happened in the past. This causes a form of excessive trust formed with repeated confirmation of the system's reliability and identifying malicious activities and threats (Bhattacherjee 2001; Bhattacherjee & Premkumar, 2004). These positive experiences may give users a feeling of safety and security that affects their perceptions. This repetition also leads to constant confirmation of the solidity of the system that it will always act in users' interests. (Kim et al. 2005; Limayem & Hirt, 2003). Continuity of usage is also an essential factor that creates habitual trust in users (Limayem et al., 2007). This type of trust can exist without any outside interference from hackers or other users, but this type of trust can also be analyzed and used by hackers to gain easy access (Gambetta, 1988; Shklar, 1984).

Misplaced Trust

Misplaced trust is also considered one of the dark sides of the trust mechanism like habitual trust. Hackers also use this trust type to gain access to the personal information of users and companies (Pienta, Sun, and Thatcher, 2016). In order to use this kind of trust, hackers need a more direct approach than habitual trust. Meaning that unknowingly extending users' trust to a malicious technology that can harm their data (Pienta, Sun, and Thatcher, 2016). Hackers can achieve this by giving users a false sense of trust in technology. If users have enough knowledge about cybersecurity and systems, prevention of this type of attack would be much easier since this kind of trust happens primarily because of a lack of knowledge. (Goel et al., 2005).

Studies showed that individuals with a lower level of technical knowledge about cybersecurity tend to rely on cues more than individuals with a higher level of knowledge (Hung et al., 2004). This means that individuals' low levels of knowledge lead to an inability to understand the information in front of them, whether it is real or not, and relies on cues to build a form of trust. Because of that, misplaced trust can have negative consequences for individuals and organizations alike.

This type of trust cannot exist without outside interferences, and those interferences are deception and betrayal. (Gambetta, 1988; Shklar, 1984). Hackers take advantage of users' trust to secure the compliance of users that are not aware of signs and notifications about the threat. (Pienta, Sun, and Thatcher, 2016). Hackers may try to deceive users with methods such as faking an installer for an application designed to make users believe it is a legitimate installer for applications. Imitation techniques of attackers are important to gain leverage of that kind of trust since details can give away the faked sources of creating compliance (Gambetta, 1988; Shklar, 1984).

CHAPTER 3: RESEARCH MODEL AND HYPOTHESES

As explained in the previous sections, this research aims to understand the relationships among online behavior, trust, and perceptions of security and privacy. The model consists of three main parts. First, the model introduces the impact of user behaviors on trusting intentions by evaluating how individuals prefer to use the internet in their daily lives and how much they avoid risky behaviors. These behaviors of individuals will be analyzed using the following online user behavior types: hedonic, utilitarian, and risk avoidance. The model will then evaluate the impacts of these online behaviors on two different types of trust: habitual and misplaced. Finally, the model evaluates the impact of these trusting behaviors on an individual's perception of privacy and security. Figure 1 presents the research model being evaluated.

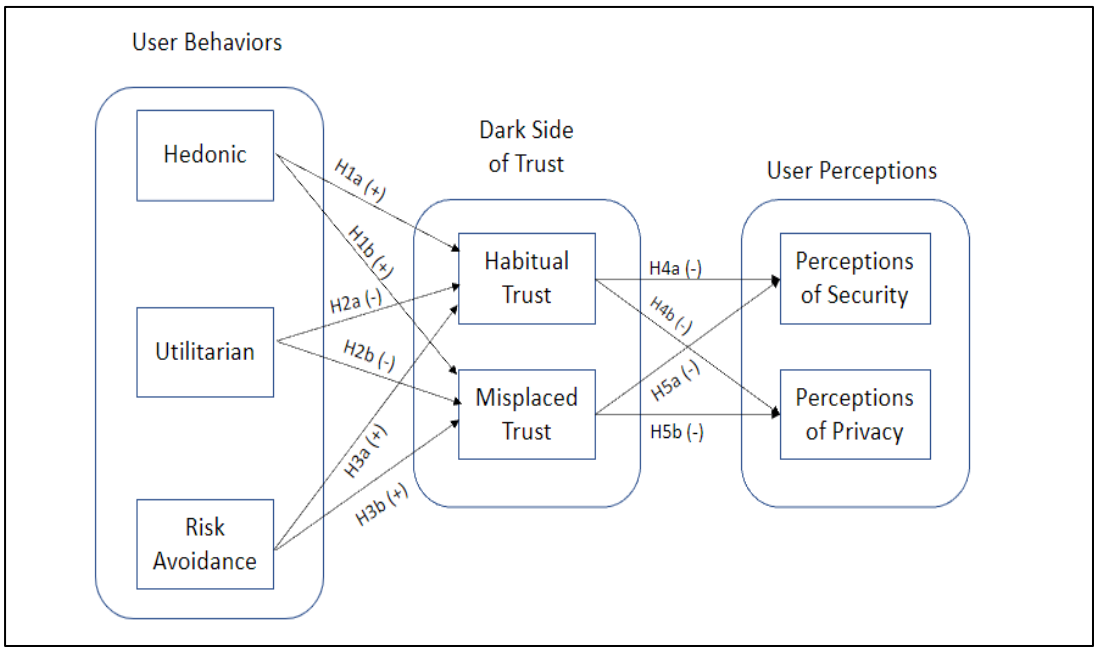

Figure 1. Research Model

In the following sections, each construct and relationship is evaluated as well as the development of hypotheses among these relationships.

Hedonic Use and Trust

Hedonic behavior focuses on the experienced pleasure or anticipated pleasure from actions made. More specifically, in the current research context, an individual's perception of using IT increases pleasure (Ja-Chul Gu et al., 2010). Hedonic behaviors focus on an individual's multisensory, fantastic, and emotive aspects of online behaviors (Hirschman & Holbrook, 1982). Hedonic aspects of behaviors are not limited to just positive feelings.

Hedonic values can also cover painful and displeasing feelings as well. Feelings considered hedonistic behaviors include love, hate, fear, joy, boredom, and generally liking or disliking something. For example, according to Arnold & Reynolds (2003), in shopping, six dimensions of hedonic shopping motivation are; adventure, social, gratification, idea, role, and value. These values of individuals are what shape their behaviors and can differ for everyone. These values can also be identified as desirable trans-situational goals that vary in importance according to individuals that serve as a guide not just in online platforms but also in real life (Schwartz, 1994). In an online environment, these values can be identified as motivational constructs that create standards and criteria for selecting activities and actions completed by users (Chiu et al., 2012).

This type of usage can be tied with the formation of habitual trust. As mentioned before, habitual trust occurs when a user unconsciously and automatically trusts the system based on positive experiences (Pienta, Sun, and Thatcher, 2016). The primary source of this unconscious trust is the belief that a system will always work like how it is supposed to work, and the system will not fail. This belief is formed with the help of a user's positive interactions with a system (Pienta, Sun, and Thatcher, 2016). This excessive trust caused by constant confirmation of services and systems may give users happiness and enjoyment. This repeated behavior of users may cause them to trust a system automatically. This repentance

leads to constant confirmation of the solidity of the system that it will always act in users' interests (Kim et al., 2005; Limayem & Hirt, 2003).

As previously mentioned, hedonic behaviors focus on using systems and technologies for pleasure rather than increasing their performance. (Ja-Chul Gu et al., 2010). An emotional approach may increase willingness to complete an action much more than a user who possesses utilitarian behaviors since the utilitarian aspect focuses on the usefulness value and being wise. (Holbrook and Hirschman 1982). Therefore,

H1a: Individuals with increased hedonic behaviors online will have increased habitual trust towards online systems.

Since hedonic user behavior focuses on the enjoyment of technology used to gain pleasure out of it, hackers may use the emotions of these types of individuals more easily since they may be willing to sacrifice much more than a user with utilitarian value to have that pleasure and happiness when they reach the aim of their behaviors since hedonic usefulness strongly influences intention to use technologies and systems (Ja-Chul Gu et al., 2010). This can result in a very bad scenario since attackers are unwillingly trying to extend an individual's trust. This outside interference of hackers may be much more effective on users who possess hedonic behavioral values since users with hedonic values focused on the thrill and excitement at the end of their transaction may miss interferences and details. This situation may lead to an extension of trust unwillingly. Thus,

H1b: Individuals with increased hedonic behaviors online will have increased misplaced trust towards online systems.

Utilitarian Use and Trust

A utilitarian approach of behavior online focuses on functionality and the ability to effectively fulfill duties (Ja-Chul Gu et al., 2010). Individuals focusing on utilitarian use are concerned with getting improved performance and effectiveness rather than enjoyment and

self-pleasure. Behaviors such as rational processing of the situation and environment are essential attributes of users exhibiting utilitarian use. (Holbrook & Moore 1981). Individuals possessing these attributes may be less likely to trust systems habitually since they may have the ability to analyze situations better than users with hedonic behaviors.

As stated before, individuals exhibiting utilitarian use online will be less focused on the enjoyment of using the system. They will be focused more on the benefits they have gained from a certain action. Because of that, those individuals may give more attention to detail, and building trust that surrounds the system may be much more challenging. Those individuals may think more rationally than users with hedonic behaviors and select different platforms that could accommodate the same task with better performance, making creating connections or forming bonds with a specific platform much harder.

We can make those assumptions because the technology acceptance model (TAM) supports the significant effect of the beliefs and values of perceived usefulness, and perceived ease of use is much more important for the utilitarian behavior context. (Wakefield & Whitten, 2006). The importance of rational thinking for those individuals may lead them to focus on the other alternatives while performing a certain action rather than focusing on the result of the action completely to get enjoyment and a feeling of happiness in the quickest way possible. This may lead users to search and read more to get the best value and performance out of a certain action. This kind of behavior is more relatable for users with utilitarian values such as being wise and efficient.

While searching for alternatives and improving themselves on a specific topic, individuals may also educate themselves and reduce the need to complete a certain action in just one way or platform. This process of education may increase their threshold of forming a trustworthy relationship with systems. Therefore,

H2a: Individuals with increased utilitarian behaviors online will experience decreased amounts of habitual trust towards online systems.

Multiple factors can impact misplaced trust. One of those factors is called "low level of knowledge," which is important in extending a users' trust unwillingly or without notice. Attackers always try to attack the weakest link of the chain, which is the human factor in cybersecurity. They are aware that deploying social engineering activities can be as effective as technical knowledge on systems. As stated before, this type of trust cannot be created without outside interference in the system. Studies also showed that individuals with a lower level of knowledge tend to rely on cues more than individuals with a higher level of knowledge (Hung et al., 2004). Meaning attackers can take privilege on the users with a lower level of knowledge and place fake cues to make users' jobs easier, preventing like helping them and may harm or steal their data through infected applications and software.

Again, users with utilitarian user behavior appreciate values like usefulness, increased performance, and ease of use since those values enhance users' attitudes more towards the utilitarian context of behaviors. (Davis, 1989; Mathieson, 1991; Szajna, 1996; Venkatesh, 1999). Perceived usefulness, an important aspect of utilitarian behavior, enhances job performance in a certain technological activity. This proves the usefulness is a major concept for utilitarian behaviors. The conclusion for utilitarian value is that it has a more rational behavioral attitude and is akin to a duty. (Babin et al., 1994). As studies state, consumption of utilitarian products is based on cognition and meets beneficial, target-oriented, functional, and practical functions (Dhar & Wertenbroch, 2000). This means that users with the utilitarian value are expected to search more for a specific activity and spend time getting information since getting the best value out of action is one of the main goals for those individuals. Utilitarian value for consumers and users is emphasized on objective and concrete qualities such as numbers and values (Chaudhuri & Holbrook, 2001).

With those factors stated above about utilitarian behavior and misplaced trust, users with utilitarian values in their behaviors may tend to search more for getting the most value out of action. This situation can also be related to the importance of performance-enhancing on utilitarian behaviors. Those said, searching for different alternatives for a specific action, importance on information and wise behaviors to gain the most value out of action, emphasizing on usefulness and easiness may lead the user to search more, gain more information about a specific topic which may lead to increase in the level of knowledge and attention to detail since users with those values expected to see different varieties of choices to achieve their goal. This positive effect on users can be helpful to not misplacing their trust in a system so easily since they may be more aware of their situation, and they may be more skeptical about following cues since they expected to see many alternatives because of their pursuit for getting the best value and performance out of action. Therefore,

H2b: Individuals with increased utilitarian behaviors online will experience decreased misplaced trust towards online systems.

Risk Avoidance and Trust

In online behaviors and activities, risk can be explained as potential negative outcomes resulting from a transaction or an activity. (Kim et al., 2008). When individuals face a negative consequence of a risky action, they expect to lose some values associated with actions, such as performance, time, psychological effect, financial harm, or shortfalls in privacy. (Grewal et al., 1994; Featherman & Pavlou, 2003). The importance of those attributes that are associated with risky action can differ from one individual to another. For example, financial risk and loss can be important for one person, but privacy and losing control over personal data can be much more important to another person. (Featherman & Pavlou, 2003). Some researchers also report that increased internet use causes individuals to perceive risk more while performing actions related to uncontrolled disclosure of personal

data. (Dinev & Hart, 2006). This means that individuals become more concerned about transactions they make when their level of expertise increases. This also affects users' priority of topics they care about when they perceive risk. As the level of expertise increases in online behaviors, individuals tend to care more about privacy over monetary losses. (Dinev & Hart, 2006). Such actions related to social security privacy may be considered more hazardous and riskier than other types of actions for different individuals (Keith et al., 2013).

Feeling of risk avoidance can increase when individuals encounter a potentially harmful activity that can result in financial loss and or loss of personal information. Research has shown that actions requiring the use of personal information increase the perception of risk and level of risk avoidance. These perceptions of risk play a huge factor in individuals' security and privacy perceptions (Dinev et al., 2015). Activities that are considered joyful and thrilling (feelings associated with positive experiences) are less risky (Finucane et al., 2000). Thus, it can be assumed, types of actions also affect individuals' level of risk avoidance. Different types of actions can create different risk avoidance measures, which can lead individuals to perform different types of online behaviors. In online activities related to privacy and security, some risks can be unknown because of values such as availability of the action, and the heuristic aspect of the action can be a blinding factor for individuals. (Paul van Schaik et al., 2018). Perception of risk increases with the desire for protection and security against actions considered to be risky (Floyd et al., 2000).

Voluntary actions are also considered a huge factor that affects risk avoidance for individuals and users. If users perceive exposure to hazards related to security and privacy more often involuntary, their perception of risk and level of avoidance of risk increases along with those values (Starr, 1969). This can be related to the use of social media because it can be assumed that using social media is not a required action for individuals and can be considered a voluntary action. This may cause individuals to perceive risk less while using

social media because their actions are not mandatory to complete certain behavior or aim. This can reduce the perception of risk and level of risk avoidance for individuals.

According to research, risk avoidance is one of the major factors that affects individuals' decisions about behaviors they are about to make that are considered risky. (Kahneman & Tversky, 1979). This means that individuals with a higher level of risk avoidance tend to avoid actions that can be considered risky or uncertain. This situation may make individuals more aware of their online environment while they perform a certain action online. Individuals with a higher level of risk avoidance may not perform those actions where they need to fulfill some requirements to complete the action itself. Because of the reasons mentioned above, users with a higher level of risk avoidance may choose the same trusted website or application repeatedly even that application or website does not give them the best value or performance out of a certain action. Positive experiences repeatedly from the same source may cause individuals to trust systems habitually since their avoidance of risk is high, they may not look for new sources or ways to complete their aims online. Thus,

H3a: Individuals with increased levels of risk avoidance behavior online will experience increased amounts of habitual trust towards online systems.

According to prior research, different individuals can perceive risk differently since risk sources for some actions can be unidentified. In this case, different mechanisms of behavior such as availability of the action or heuristic effect of action are considered for the continuity of that behavior (Keith et al., 2013). People with higher levels of risk avoidance may tend to approach unknown actions and behaviors more carefully and cautiously. According to models of human behavior, perceived risk increases willingness to protect against those risks, leading individuals to act more cautious when performing certain actions and behaviors online (Floyd et al., 2000). Evaluation of alternatives for individuals is also important to assess the actions that are going to be made. Prospect theory explains this

situation as, "People behave according to their evaluation of alternatives and their evaluations depend on outcomes and their attitudes of risk." (Kahneman & Tversky, 1979).

As mentioned before, individuals with the attitude of high-risk avoidance may tend to avoid actions that include uncertain risk factors. This may cause individuals to be more careful and be aware while performing certain actions, which may help users avoid placing their trust in a system easily. Even if users place their trust in a system, high levels of risk avoidance may help them avoid actions that they are not sure of or fully aware of the result of the action. Since risk in online behaviors is defined as uncertain and negative outcomes that can happen as a result of an action made by an individual, this concept of perceived risk can be identified by individuals as loss in performance, loss in a financial asset or can be a physiological loss as well as a loss in privacy and personal data (Featherman and Pavlou, 2003). This potential risk factor may create a feeling of uncertainty and fear in individuals. So, individuals with a high level of risk avoidance misplace their trust in a particular system to avoid such feelings and negative outcomes. Thus,

H3b: Individuals with increased levels of risk avoidance behavior online will experience increased amounts of misplaced trust towards online systems.

Habitual Trust and Security/Privacy

Perception of security can be defined as a situation that may result in a negative event such as loss in economic assets or loss in network and data resources of individuals in the ways of destruction, modification, disclosure of private data, denial of service, and abuse of personal information (Kalakota & Whinston, 1997). Online security aims to protect individuals from harmful activities with the methods like cryptography, digital signatures, certificates that are created with the purpose of protecting users from fraudulent activities online such as phishing or hacking. The presence of those methods in a system or an application affects individuals positively in terms of intention to perform activities/behaviors

(Ranganathan & Ganapathy, 2002; Yousafzai et al., 2003; Kim et al., 2008; Lian & Lin, 2008). Activities that require sharing personal information and financial information are some of the activities that users need to feel secure to complete a transaction (Mohammed A. Al-Sharafi et.al 2016).

Information security can be divided into three different areas. Those areas are confidentiality, integrity, and availability. Confidentiality means the protection of private data from unauthorized access and reading data without permission. Integrity is about the protection of data from unauthorized writing such as changing or adding new information to data. Availability is about the protection of data from unauthorized access by securing the access of the data for legitimate users as much as possible (Schneier,2015). Some studies show that perception of security is a much more important concern compared to the perception of privacy. An individual's security concerns may also shape the privacy concerns for a behavior/action. According to the researchers Flavia´n & Guinalı´u (2006), security perceptions affect the influence of trust in the handling of their personal information. We can also confirm that for individuals performing activities online their primary concern is still about security and handling of their personal data while performing activities and behaviors online (Luo, 2002; Lightner, 2003).

Trusting systems habitually occur when individuals have multiple positive experiences on a certain action leading to trusting the system based on these cues. Since users with a habitual trust may move with the mindset of the system will not fail me and individuals may trust the system close to a hundred percent, their perception of security on that system will be much less strict compared to individuals who do not trust systems habitually since they may be more skeptical and questioning about everything while performing a certain behavior or action. Therefore,

H4a: Individuals with increased habitual trust in online systems will have decreased amounts of concerns on perceptions of security towards online systems.

Perception of privacy can be defined as a regulatory process in which a person wants to make herself less accessible and open to others (Altman 1975). Individuals with strict perceptions of privacy tend to stay anonymous and want to stay "off the radar" with their internet activity (i.e., no one tracing of their internet activity). Individuals with strict perceptions of privacy want to maintain a higher level of privacy surrounding their tasks and behaviors online (Oldham, 1988; Rensel et al., 2006). The primary focus for the individuals is maintaining a certain level of discretion concerning their actions and behaviors such as communication of monetary topics or important personal data (Rensel et al., 2006).

An individual's perception of privacy can be affected by several events such as losing control over personal data, collection of that personal data, usage of the personal data without permission, location tracking of individual without permission, or usage of personal data for advertising services. Recent research shows that 74% of Americans believe it is important to maintain privacy in the online environment and their activities of life (Madden & Raine, 2015). This is a desire coming from their wish to stay private to a certain degree (Kang et al., 2013). Individuals care about anonymity and privacy because the action of staying anonymous and private give individuals a feeling of control and security over their important personal data (Rensel et al., 2006). Users with a high perception of privacy may want to keep their sense of privacy high to avoid interruptions and distractions from the outside environment that can harm their data or progress.

Three different variables related to perceptions of privacy have been announced by published (Westin, 1967; Zureik & Stalker, 2010). Those variables that are in close relationship with online privacy perceptions are informational privacy, social privacy, and personal privacy. Informational privacy is about transferring information online in a

controlled and safe manner. Social privacy concerns about other users online because of the distance toward others. Personal privacy concerns about control of emotions and cognitive outputs in online environments since uncontrolled emotions can result in the exposure of personal data. Those variables and concerns about privacy are important predictors of the individual's behaviors regarding their privacy online. Those variables may also affect individuals' attitudes and intentions about a certain activity or behavior online.

Studies show us values such as benefits of information sharing, experience, and size of social networks in social environments are important factors that affect personal information disclosure in a positive way (Beldad, 2015). As previously discussed, an important factor for habitual trust is the positive experiences of users in a certain action. It can be assumed that users who habitually trust systems because of their positive actions tend to have less strict privacy perceptions. For example, studies found that the effectiveness of a certain action in a social media platform are positive factors that affect the perception of privacy whereas experience was a negative predictor (Beldad 2016). Thus,

H4b: Individuals with increased habitual trust in online systems will have decreased amounts of concerns on perceptions of privacy towards online systems.

Misplaced Trust and Security/Privacy

An individual misplaces trust in a system when there is a lack of knowledge about the user's activity. Studies show that users with high levels of control over their personal information are less likely to be cyber-crime victims than users who perform increased activities in knowledge exchange (Saridakis et al., 2016). This shows us individuals who seek knowledge can be victims of cyber-attacks, and this also shows the importance of knowledge in cybersecurity and creating an accurate perception of security while performing online activities.

Identifying security features of the websites and systems, it is essential to avoid outside interferences on extending users' trust unwillingly to misplace their trust on a system.

Security features of systems if can be identified, are the key values of creating true trust and this trust in return positively affects customers' behavioral intentions. Users who tend to misplace trust in the system most likely will not be aware of the security features of systems. Therefore, their perceptions of security may be less strict since their knowledge of the topic is expected to be low compared to other users with experience. Thus,

H5a: Individuals with increased misplaced trust in online systems will have decreased amounts of concerns on perceptions of security towards online systems.

As stated, one of the main reasons for the misplaced trust happening is the lack of knowledge of a user on a specific topic. Hackers use this lack of knowledge to give a false feeling of security and privacy. Without enough knowledge, individuals also tend to follow cues that hackers left behind for users to give them a false sense of help and extend their trust unwillingly.

Users who misplace their trust in a system may have less strict privacy perceptions than those who do not misplace their trust in the system since users with a less misplaced trust may have enough knowledge on a specific topic to prevent the extension of trust unwillingly with the outside interference. This can mean that individuals who do not misplace their trust in a system may be aware of the topic before. That knowledge may be helpful to users for the prevention of misplaced trust since it will be much harder for hackers to convince a user of a falsely generated system. This may cause users with a higher level of knowledge to have many strict perceptions of privacy since they will be aware of the consequences and risks they face when performing online activities. This may lead those individuals to stay more anonymous and concealed in their online transactions than other users.

The privacy concept is mainly about concerns related to losing personal information, and users with a high level of knowledge will put much attention on that topic to avoid certain losses. They may make themselves much less accessible to others online to ensure there is enough privacy to complete their actions safe and private. This perception of anonymity can give users a sense of security and control in their transactions. Therefore,

H5b: Individuals with increased misplaced trust in online systems will have decreased amounts of concerns on perceptions of privacy towards online systems.

CHAPTER 4: METHODOLOGY

An online questionnaire was used to test the model. The survey questions were developed from prior research, and all use a 7-point Likert scale. The model is broken down into three areas: online behavior, trust, and perceptions of security/privacy. Individuals' level of risk avoidance and how they interact with sites online (hedonic/utilitarian) were evaluated for online behavior. To understand different trusting behaviors, both misplaced and habitual trust of users was analyzed to see what type of trust is triggered while they perform their online activities. Lastly, perceptions of privacy and security were measured to understand the impact of trust on overall user perceptions. For a complete list of questions used in the survey, see Appendix A.

Qualtrics software was used to create the survey and then it was distributed to participants through Amazon Mechanical Turk (MTurk). At first, the survey was tested with 15 participants before the pilot study for the quality measurement of the questions without using MTurk. Once the pilot study results were collected and evaluated, and Human Intelligence Task (HIT) was created within MTurk and released for participants to accept the HIT and answer the survey. After the first HIT, a second HIT was made to re-evaluate some questions that had lower outer loading levels. For the evaluation of the questions and relationships between model variables, SmartPLS was used. Final reports were created according to analysis that was made on SmartPLS again.

Why Amazon Mechanical Turk (MTurk)?

Amazon Turk is a crowdsourcing marketplace for tasks/work (also known as Human Intelligence Tasks or HITs) that require human intelligence. Amazon provides a system for distributing these tasks to workers, also known as “Turkers.” Businesses and individuals can use MTurk for various purposes, including sentiment rating, feedback collection, item categorization or, data cleaning (Ku, C. H., and Firoozi, M., 2019).

Crowdsourcing can be defined as outsourcing a function to a large, undefined group of people via an open call, with Amazon's Mechanical Turk being one of the many crowdsourcing resources that can be found online (Brabham, 2008). Compared to other systems, MTurk is more commonly used and has the most information for determining suitability for tasks/works. Della Mea, Maddalena, and Mizzaro (2015) conducted experiments on crowdsourcing platforms and found that Microworkers and ShortTask contain more spam tasks than MTurk.

Benefits of MTurk

Based on the task description and type of the work, MTurk can provide different benefits for users. One benefit is the low-cost rate compared to other crowdsourcing systems. For example, most other crowdsourcing websites using gift cards are much more expensive than MTurk, where a HIT can be done within the U.S. for $0.50 per worker (Berinsky, Huber & Lenz, 2012). This payment method is also reliable because all payments go through Amazon, where Amazon will hold payments until the task is complete. This also eliminates the necessity of individuals knowing each other, allowing users to stay anonymous to researchers (Mason, W., & Suri, S., 2012).

Another benefit of Amazon Turk is the wide variety of users. Compared to other crowdsourcing platforms, Amazon has a much larger user pool which allows researchers to recruit different sets of subjects from the pool. This also allows researchers to find multiple subjects who can participate in a HIT simultaneously, which can be useful for group tasks (Mason, W., & Suri, S., 2012).

Data Quality Control of MTurk

In MTurk, quality control is implemented in several ways. This includes qualification control and the ability for researchers to deny payment to participants of the HITs based on the quality of their responses. Amazon also gives incentives to users that provide accurate

and true information. Users with a "master" qualification can receive up to 5 percent in additional payments as a reward for providing accurate and quality information. Also, both U.S and non-U.S citizens are obligated to provide their valid taxpayer information in the registration section of the MTurk to comply with the Internal Revenue Service (Ku, C. H., and Firoozi, M., 2019).

From the beginning of the introduction of crowdsourcing websites on academic works, there have been questions and debates about the quality of data being collected through crowdsourcing and whether this impacts the quality of the results (Ku, C. H., and Firoozi, M., 2019). Berinsky, Huber, and Lenz (2012) and Paolacci, Chandler, and Ipeirotis (2010) conducted replication studies of prior research to determine the difference between the traditional method of data gathering and the online crowdsourcing method (e.g., MTurk). They collected data from three different participants areas, including MTurk, a midwestern U.S university, and online discussion boards. Results concluded that both MTurk workers and other traditional workers provide similar results and show similar decision-making and judgment behaviors (Paolacci et al., 2010). These results have been confirmed in other research areas containing psychological, economic, and behavioral studies, with all results showing similar outcomes, including little to no difference in users' behaviors and results of the answers (Chandler and Kapelner 2013).

Motivation and Payment Issues

In a study regarding worker motivation on MTurk, Kaufmann et al. (2011) created a model that separates five important motivation groups for workers. These are enjoyment-based motivation, community-based motivation, immediate payoffs, delayed payoffs, and social motivation. Compared with the current federal minimum wage of $7.25 hourly, in Amazon Turk, 39% of the workers earn between $5 and $7.99 while the remaining workers earn less than $5 per hour, according to a study conducted by (Hitlin 2016). Buhrmester,

Kwang, and Gosling (2011) investigate this issue further by asking if low payment compared to the minimum wage of $7.25 affects the quality of data provided by MTurk workers. According to the results, researchers found this relatively low pay compared to the minimum wage has little or no effect on the quality of data provided by workers in MTurk. However, they also found that Amazon's incentives to workers who regularly provide clean data to researchers are a really important factor in data quality. In his research about motivation on MTurk workers, Kaufmann et al. (2011) found that payment is the most important factor for workers that create motivation to finish work according to the rules, followed by several other factors related to enjoyment-based motivation. They also state that this importance can increase regarding the length and complexity of the work (Brandon et al., 2014). In summary, researchers should do a quality control check on the validity of the control quality mechanisms of each system before submitting a task or work.

Possible Solutions on Concerned Issues of MTurk

Some of the most important issues regarding MTurk are reliability (errors regarding responses of answers), internal validity (caused by biased responses), spamming, and external validity (issues regarding the generalizability of the answers). Possible solutions for the reliability issues are using multiple indicators per construct, prequalifying workers, replicating work, and using Amazon Mechanical Turk to validate responses. Solutions for the internal validity section can prevent and remove duplication among answers and consider the effect of monetary compensations on research questions. To prevent spamming workers, researchers can analyze the time taken for each task and look for patterns in responses to include checking survey questions to ensure workers are not spamming answers to gain time in surveys. External validity compared to traditional methods is not a perfect representation of internet users but compared to the alternatives it is not the worst. This issue can be reduced again by using multiple indicators per construct. This thesis will try to use most of these

methods on survey questions to get beneficial results from workers and minimize the issues regarding validity, reliability, and spamming (Crowston, K., 2012).

Survey Development

The survey consists of four main sections. First, demographics were collected including questions about age, gender, level of education. Then information about the level of usage, hours of usage, trust propensity, and activity importance was also collected. Next, online behaviors were assessed which included utilitarian behaviors, hedonic behaviors, and risk avoidance behaviors. The third section evaluated a participant's trust which measured both the habitual and misplaced trust variables, referred to as the dark side of trust in the thesis model. Finally, the participants' perceptions of security and privacy were assessed, and the survey was finished. Questions were selected from previously used measurements when available. Some variables in the model have not been quantified by prior research, thus these questions were created based on extensive research from multiple sources. For the control variable of trust propensity, a previously prepared questionnaire proved to be a valid measure.

For questions focused on online behaviors, existing measures were used within the survey. Questions for measuring hedonic behaviors and utilitarian behaviors are adapted from Davis et al. (1992) & Chiu, C. M. et al. (2014). To measure risk avoidance behaviors, questions were adapted from Kennison and Chan-Tin (2020) & Grable, J., & Lytton, R. H. (1999).

The questions focused on the dark side of trust (i.e., habitual and misplaced) have not been previously quantified in prior research. Since there were no previous studies or quantitative analyses regarding these variables, questions were created using the explanation of these variables from Pienta, Sun, and Thatcher (2016). Habitual trust questions were inspired by the general concept of habit in real life from an information systems perspective.

Questions related to habitual trust are more focused on individuals' actions related to their routines and habits. For the creation of the misplaced trust, questions focused on measuring a user's level of knowledge on information technologies.

Finally, the questions focused on the user perception variables were created based on prior studies. Perceptions of privacy questions focused on the users' view of what is considered private while performing certain actions online and how open users are while they perform activities under certain circumstances regarding their privacy and tries to measure their beliefs on privacy about systems. Likewise, perceptions of security questions try to answer the same questions and do the same measurements regarding the aspect of security instead of privacy. Questions for user perceptions of privacy were adapted from Kaleta, J. & Mahadevan, L. (2020). Questions for user perceptions of security were adapted from Van Schaik, P. et. al (2018).

All questions used related to these variables regarding perceptions of users, user behaviors, and the dark side of trust are included in Appendix A.

Pilot Study

The pilot study included two different phases. First, to test the overall completion time and relatability of the created questions, a group of 15 people was asked to take the survey before beginning the next phase of the pilot study. Participants indicated that the survey questions were clear and understandable, not complex, and arranged well according to feedback. They found that most of the questions were relatable to the model variables. Additionally, the average completion time for the survey was 4-6 minutes which matched the anticipated completion time for the overall survey.

To evaluate the variables further before the entire data collection, another phase of the pilot study was conducted with 50 participants. Participants were obtained from Amazon MTurk, and qualified workers were randomly selected for this assignment. After getting

results from the 50 participants, data were downloaded and cleaned. The cleaning process removed unnecessary columns and rows of data, eliminating data with N/A, converted Likert scale values to numbers for indicator analysis and renamed indicators with question export tags to see each question's effect on variables. Once the data was cleaned, a preliminary validity and reliability analysis was conducted to ensure the indicators were loading correctly (more detail of this process is included in the results section where the complete confirmatory factor analysis was conducted). Based on this analysis and participant suggestions, some of the questions were re-evaluated. The same questions were used for all the constructs except for habitual trust and hedonic behavior variables.

Once the pilot study was completed and changes were made, the survey was published through MTurk, and received a total of 319 responses. From these responses, six of them were incomplete. Additionally, this survey included attention checks through 3 questions that asked respondents to select a specific answer on a question. A total of 22 participants failed the attention checks (10 did not pass the first validity check, 8 did not pass the second, and 4 did not pass the third). This resulted in 28 additional responses being eliminated due to incomplete responses and attention check issues which left 291 remaining for the analysis.

CHAPTER 5: ANALYSIS

The analysis was conducted using Smart PLS 3, a variance-based structural equation modeling software that uses the partial least squares path modeling method (Ringle, Wende & Baker, 2015). For this thesis, the two-staged analytical procedures by Anderson and Gerbing (1998) were used. First, the validity and reliability (measurement model) of the measurements were tested for the model. In addition to validity and reliability, overall model fit was also evaluated before hypothesis testing. Next, the structural model examination to test the hypothesized relationships was conducted (Hair et al., 2017; Ramayah et al., 2011; 2013; Rahman et al., 2016). As part of this analysis, the significance of path coefficients and loadings were tested with the bootstrapping method on the SmartPLS with 5000 resamples.

Why use SmartPLS?

As previously mentioned, the Partial Least Squares (PLS) technique was used to evaluate the research model. Some papers argue that using the PLS technique is not suitable for analysis, and the software itself (i.e., SmartPLS) is not reliable to get solid analysis results (Petter, 2018). Because SmartPLS is easy to use and easy to understand, it sometimes gets misunderstood, and researchers claim that it is not suitable for all models due to its simple algorithms. Another claim about SmartPLS is that since it gives a result all the time, even with a small sample size (e.g., 30 or less), and when the model itself is incorrectly specified, it leads to incorrect results (Petter, 2018). As studies have shown, small-sized datasets are often associated with software's inability to detect the relationship within the model (Lee et al., 2011). This situation does not prove anything about flaws or errors of the PLS method, and it just proves how researchers use SmartPLS in the wrong way to justify their use of small-sized datasets (Petter, 2018). Another reason why the PLS technique got a bad reputation is using poor justifications for using SmartPLS. Some of the justifications used before recognized the PLS method as less important structural modeling compared to CB-

SEM based on previous norms set once. Hair et al. (2013) also state that some scholars falsely accuse and mislead users by taking advantage of the characteristics of the PLS algorithm to create solutions with extremely small-sized datasets even when a large-sized dataset can be acquired easily. Unfortunately, this practice hurts the reputation of the PLS method as the PLS method is a multivariate method that cannot turn flawed datasets into good ones (Marcoulides et al., 2009).

Many past studies claimed that PLS is used when the research was untested or exploratory, and the CB-SEM method is used for confirming the tested and explored models is a wrong statement (Petter, 2018). PLS method has also got its advantages compared to the CB-SEM method. Such as, PLS does not have the requirement of identification when specifying the measurement and structural model, which can make users much freer in lots of areas when analyzing their models (Petter, 2018). This requirement in the CB-SEM method often results in changing the model (such as adding new variables to the model) to get rid of the identification error, which messes the integrity of the model structure and creates the requirement of adding additional variables that do not have any place in the model in the first place. This situation limits the user when a model is defined by theory but not identified with measurement. Because of the limiting identification process in the CB-SEM method, users may need to change the model to fit the requirements of the software.

PLS algorithm uses raw data to generate estimates where the CB-SEM method is covariance-based, meaning there must be a covariance matrix to estimate the model meaning the main reason to use CB-SEM is to evaluate how a model fits into a specific dataset. This measurement is mainly applicable for just one specific dataset, which may not be so applicable for another different dataset (Petter, 2018). In SmartPLS, the algorithm uses regression and explained variance method. These methods are much more helpful in understanding relationships between the dataset and the model. This method's primary goal is

to identify parameter estimates essential to maximizing the amount of variation explained in the model. This is a very different approach compared to just focusing on the goodness of the fit (Petter, 2018).

Confirmatory Factor Analysis

As mentioned, two types of validity were examined in order to assess the model. The first validity measurement is convergent validity. After the assessment of the convergent validity, discriminant validity was examined.

Convergent Validity

Convergent validity explains the relationship between the variables and the scales of the model (Ramayah et al., 2017). It measures how these variables and other measures are closely related to the same construct. Construct should correlate with the related variables of the model, but at the same time, it should avoid correlating with unrelated variables in the model (Ramayah et al., 2017).

This measurement can be found with loading examination, looking at the average variance extracted values, or looking at the composite reliability values (Gholami et al., 2013; Rahman et al., 2015). Most of the loadings in the model were higher than the recommended value of 0.7, and the composite reliabilities of the loadings were higher than the recommended value of 0.7 as well. Also, the AVE of all loadings was higher than the recommended value of 0.5 (Gholami et al., 2013; Rahman et al., 2015).

Constructs	Items	Loadings	Cronbach	rhoA	CR	AVE
Hedonic Use	HED_1	0.813	0.789	1.000	1.000	1.000
	HED_2	0.786				
	HED_3	0.799				
	HED_4	0.730				
Utilitarian Use	UTL_1	0.740	0.737	0.743	0.834	0.558
	UTL_2	0.717				

	UTL_3	0.720				
	UTL_4	0.808				
Risk Avoidance	RISK_1	0.767	0.864	0.866	0.902	0.648
	RISK_2	0.825				
	RISK_3	0.805				
	RISK_4	0.782				
	RISK_5	0.844				
Habitual Trust	HBT_1	0.668	0.792	0.812	0.855	0.543
	HBT_2	0.700				
	HBT_3	0.720				
	HBT_4	0.795				
	HBT_5	0.793				
Misplaced Trust	MPT_1	0.875	0.849	0.851	0.909	0.768
	MPT_2	0.871				
	MPT_3	0.883				
Perceptions of Privacy	PRIV_1	0.883	0.832	0.834	0.899	0.749
	PRIV_2	0.841				
	PRIV_3	0.871				
Perceptions of Security	SEC_1	0.880	0.922	0.922	0.945	0.810
	SEC_2	0.900				
	SEC_3	0.911				
	SEC_4	0.908				
Trust Disposition (Trust Propensity)	TP_1	0.888	0.916	0.930	0.940	0.797
	TP_2	0.894				
	TP_3	0.865				
	TP_4	0.923				
Age	Age	1.000	1.000	1.000	1.000	1.000
Gender	Gender	1.000	1.000	1.000	1.000	1.000

Table 1. Convergent Validity

Discriminant Validity

Discriminant validity is concerned with ensuring that constructs that are not supposed to be related are found to be unrelated. To establish the discriminant validity in a model, proof of measurements about constructs must not be correlated in any way is necessary. While previous research suggests using the Fornell-Larckel (1981) criterion, recent research suggests this criterion lacks the reliability to detect the levels of discriminant validity in models. The argument also states that this situation happens in common research situations (Henseler et al., 2015). Another suggested method to calculate discriminant validity in literature is assessing the heterotrait-monotrait (HTMT) ratio of correlations using a multitrait-multimethod matrix. Henseler et al. (2015) proved this method's efficiency with the famous Monte Carlo simulation method. Results showed significant performance improvement with the usage of the HTMT method. Due to the improvements of the HTMT method, the model was tested with this new suggested method. Gold et al. (2001) states that HTMT values greater than 0.95 suggest an error in the model's discriminant validity. In this model, all values associated with every variable are below the suggested HTMT value.

	Habitual Trust	Hedonic Behavior	Misplaced Trust	Perceptions of Privacy	Perceptions of Security	Risk Avoidance Behavior	Utilitarian Behavior
Habitual Trust							
Hedonic Behavior	0.651						
Misplaced Trust	0.725	0.816					
Perceptions of Privacy	0.824	0.581	0.732				
Perceptions of Security	0.644	0.594	0.791	0.847			
Risk Avoidance Behavior	0.601	0.715	0.863	0.757	0.774		
Utilitarian Behavior	0.678	0.456	0.318	0.376	0.288	0.288	

Table 2. Discriminant Validity (HTMT Ratio)

Overall Model Fit

Model fit was tested by using three different fitting parameters. Model fit was evaluated using the suggestions from Ramayah et al. 2017. This includes evaluating the standardized root mean square residual (SMRS), the model fit using normed fit index (NFI), and a combination of two different values, which is the exact model fit, also called bootstrap-based statistical interference.

Standardized root means square residual is the difference between the model implied correlation matrix and the observed correlation (Hu & Bentler, 1998). This value allows the assessment of the model's average magnitude discrepancies between correlations of the model as a measurement of absolute of model fit variable. According to Henseler (2014), SRMR can be explained as a variable that explains the goodness of fit measure for PLS-SEM, and this method can be used to prevent model misspecifications. An SRMR value below 0.08 is considered a good fit (Hu & Bentler, 1998).

The second fit index used in this model is called normed fit index (NFI) and is a value that explains the incremental fit measure of the model by calculating the chi-square value of the model. After calculating the chi-square value of the model, PLS-SEM compares that value with a considerable benchmark (Bentler & Bonett, 1980). NFI in the formula version is defined as; 1 minus the Chi^2 value of the proposed model divided by the Chi^2 values of the null model. The result of this formula must be close to 1 to be considered a better fit for the model.

The last fit index used in this model is called exact model fit which is a measurement for explaining statistical interference of the discrepancy with testing method between matrices of empirical covariance and regular covariance matrix, which the composite factor model can explain. Two different measurement methods are suggested by Dijkstra and Henseler (2015a; 2015b) to compute the model discrepancy: calculating values of d_LS (the

squared Euclidian distance) and d_G (geodesic distance). According to these results, the difference between the tested correlation matrix explained by the model and the empirical correlation matrix should be non-significant (p>0.05).

The model's SRMR value is 0.069, which is below the suggested level of 0.08. Model's NFI value is 0.751 along with d_ULS 2.794 and d_G 0.968, which are not significant and bigger than p>0.05, proving model fit (see Table 3 for the full list of results).

	Saturated Model
SRMR	*0.069*
d_ULS	*2.794*
d_G	*0.968*
NFI	*0.751*
Chi-Square	*1667.505*

Table 3. Model Fit

Hypothesis Testing Results

Literature suggests checking beta (β) and the corresponding t-values by using the bootstrapping method with 5000 re-samples to assess the structural model (Hair et al., 2017). These values should be analyzed and reported to assess the model in detail. Providing a p-value is helpful to evaluate the existence of significant effects in the model, but only by itself, it will not show the size of that effect if there is one in the model. That is why when interpreting results, analyzing and explaining both effect size which is the substantive significance, and statistical significance, which is the p-value, is essential (Sullivan and Feinn, 2012). The results can be found in Figure 2.

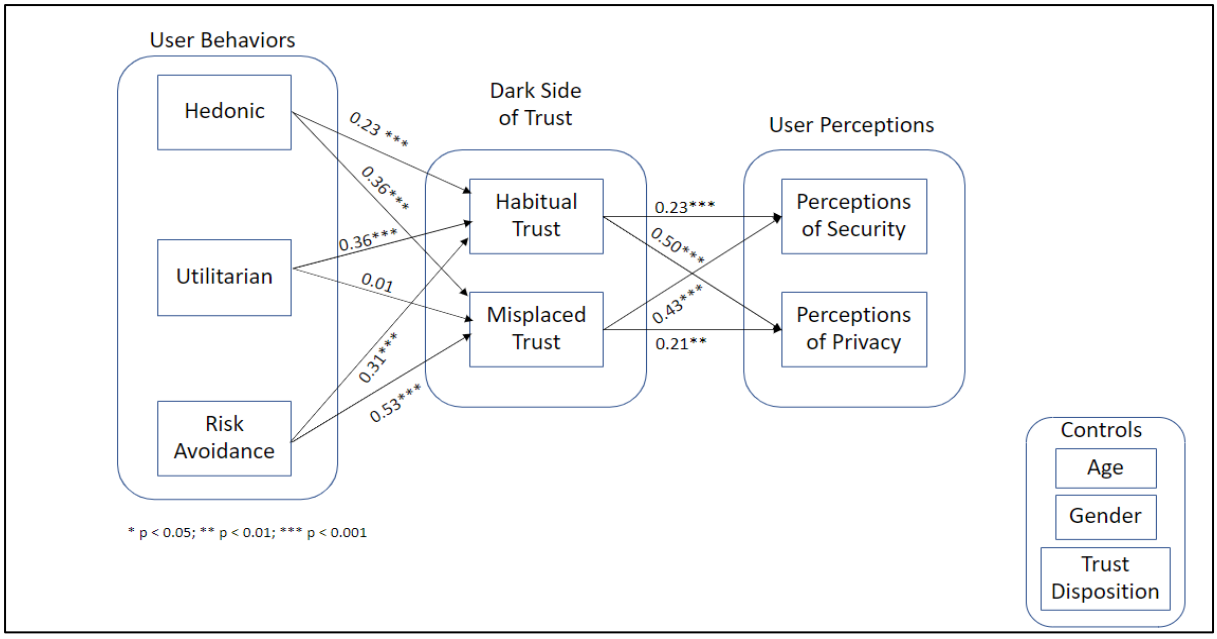

Figure 2. Research Model Results

To evaluate behavioral effects on habitual trust, the results found hedonic behavior ($\beta = 0.23$, $t = 3.464$, $p < 0.001$), utilitarian behavior ($\beta = 0.36$, $t = 6.155$, $p < 0.001$) and risk avoidance behavior ($\beta = 0.31$, $t = 4.553$, $p < 0.001$) to all be significant. While hypothesis 1a (hedonic behavior to habitual trust) and 1b (hedonic behavior to misplaced trust) was supported, hypothesis 2a (utilitarian behavior to habitual trust) and hypothesis 2b (utilitarian behavior to misplaced trust) were not supported and lastly hypotheses 3a (risk avoidance behavior to habitual trust) and 3b (risk avoidance behavior to misplaced trust) were also supported. The relationship between utilitarian behavior and habitual trust was a significant but not supported relationship. However, the relationship between utilitarian behavior and misplaced trust was not a significant relationship and it was not supported as well. This relationship between utilitarian behavior and misplaced trust was the only non-significant relationship in the dataset according to results.

Hedonic behavior ($\beta = 0.36$, $t = 6.202$, $p < 0.001$) and Risk avoidance behavior ($\beta = 0.53$, $t = 10.216$, $p < 0.001$) were both found to be significant predictors on a users' level of misplaced trust while utilitarian behavior ($\beta = 0.01$, $t = 0.268$, $p < 0.05$) was not a significant

predictor. This supports hypothesis 1b (Hedonic behavior to misplaced trust) but hypothesis 2b (utilitarian behavior to habitual trust) and 2b (utilitarian behavior to misplaced trust were not supported as the results indicated relationships in opposite way.

Next, the relationships between trust and perceptions were evaluated. Habitual trust ($\beta = 0.23$, $t = 3.436$, $p < 0.001$) and Misplaced trust ($\beta = 0.43$, $t = 5.546$, $p < 0.001$) were both found to be significant predictors on a user's perception of security. However, this was again a relationship opposite to hypothesized, resulting in no support for hypotheses 4a and 4b. For privacy, habitual trust ($\beta = 0.50$, $t = 7.262$, $p < 0.001$) and misplaced trust ($\beta = 0.21$, $t = 2.802$, $p < 0.01$) were both significant predictors on a user's perception of privacy. Hypothesis 5a and 5b stated a negative relationship with perceptions of privacy. Thus, both are not supported as results indicate that the relationships stated in hypotheses between these variables are in the opposite way.

	Relationship	**Std.Beta**	**t-value**	**p-value**	**Supported?**
H1a	Hedonic Behavior → Habitual Trust	0.23	3.464	0.00	Supported
H1b	Hedonic Behavior → Misplaced Trust	0.36	6.202	0.00	Supported
H2a	Utilitarian Behavior → Habitual Trust	0.36	6.155	0.00	Not Supported
H2b	Utilitarian Behavior → Misplaced Trust	0.01	0.268	0.79	Not Supported
H3a	Risk Avoidance Behavior → Habitual Trust	0.31	4.553	0.00	Supported
H3b	Risk Avoidance Behavior → Misplaced Trust	0.53	10.216	0.00	Supported
H4a	Habitual Trust → Perceptions of Security	0.23	3.464	0.00	Not Supported
H4b	Habitual Trust → Perceptions of Privacy	0.50	7.262	0.00	Not Supported
H5a	Misplaced Trust → Perceptions of Security	0.43	5.546	0.00	Not Supported
H5b	Misplaced Trust → Perceptions of Privacy	0.21	2.802	0.01	Not Supported

Table 4. Bootstrapping Results

CHAPTER 6: DISCUSSION

According to the results of our analysis, our research shows that all relationships but one inside the model are significant. These relationships proved to affect each other in a way, except for one relationship meaning there are some variables to be discussed in those relationships that affect each other positively or negatively. Our findings suggest that all user behavior variables (hedonic, utilitarian, and risk avoidance) are effective on the dark side of trust variables except one relationship, which happens to be the only relationship in the model that is not significant and does not prove any effect on the dark side of trust variable with the p-value of 0.79 which is the relationship between utilitarian behavior and misplaced trust. For our hypotheses, it was found that four of the significant relationships are supported, and the rest of the hypotheses are not supported, meaning after getting results, it was proved to be the relationships mentioned on the hypotheses, not in the direction that hypothesis stated. This will be discussed further in the following sections. Supported relationships which mean relationships mentioned in the hypotheses match the results and these relationships are all significant relationships that explain the direction of the relationship. Unsupported relationships in the model are also proved to be significant relationships, showing us these values indeed affect each other in a way but not in the way that hypothesis stated. Supported significant relationships in our model are hedonic behavior affecting habitual and misplaced trust and risk avoidance behavior affecting habitual and misplaced trust. Unsupported significant relationships in the model are utilitarian behavior affecting habitual trust, habitual trust affecting perceptions of security and privacy, and misplaced trust affecting perceptions of security and privacy. Lastly, one unsupported and not significant relationship between utilitarian behavior and misplaced trust proved that utilitarian behavior does not affect individuals' level of misplaced trust. Discussions will continue further in detail by analyzing

hypotheses and variables in the model individually and will provide insights into why those relationships affect each other in different ways.

Discussions About User Behavior

Hedonic Behavior

According to the results, the relationships mentioned in hypotheses H1a and H1b regarding the effect of hedonic user behavior on misplaced trust and habitual trust is significant. Meaning these variables in those relationships indeed affect each other, and these hypotheses are supported, which shows that the relationships mentioned in these hypotheses turned out to be as expected and match the hypotheses' description. The first hypothesis to be discussed is H1a which states that individuals with the hedonic behavior will have increased habitual trust towards online systems. This hypothesis is supported by the results of the analysis, meaning individuals who use the internet for pleasure tend to show higher habitual trust towards online systems. In literature, it is stated that users with hedonic behavior tend to focus on activities that bring them pleasure and joy rather than performance (Ja-Chul Gu et al., 2010). Also, according to the literature, habitual trust is generally formed with positive experiences related to users' actions (Pienta, Sun, and Thatcher, 2016). Results of our analysis support these statements that are in the literature. According to results and literature review about this topic, it can be said that when users with the hedonic type of behavior have a positive experience while performing their online activities, they want to live that happiness and joy out of their action again they are solely focusing on that part of actions which is getting happiness on results and not so much of the action or work itself. After a while, repeating those actions to get joy and excitement gives users a feeling of constant confirmation, which gives users more joy and happiness out of their actions. This constant repetition formed with positive feedback from systems causes users to trust systems excessively because they are primarily focusing on getting the joy and excitement out of

online activities as soon as possible. Again, as stated in the literature, repentance leads to constant confirmation of the solidity of the system that it will always act in users' interests (Kim et al., 2005; Limayem & Hirt, 2003). This is another proof of why users trust the system habitually more when they are primarily concerned with joy and happiness.

The second hypothesis to be discussed is H1b which states the relationship between hedonic behavior and misplaced trust. This hypothesis also supported, meaning the stated relationship in the hypothesis turned out to be as expected. According to the analysis results, it can be clearly said that individuals with the hedonic type of behavior, while they perform online activities, tend to misplace their trust in a system. As mentioned before, to misplace trust in a system, there must be an outside interference that causes users to unknowingly extend their trust to a fake system (Pienta, Sun, and Thatcher, 2016). Again, as mentioned above, since users with hedonic behaviors are about getting joy and excitement, outside interference becomes much easier on users who possess hedonic behaviors. This may happen because since they are focused on the emotional side of their actions, they may be manipulated much more easily. After all, they will mostly try to get to the result as soon as possible to get enjoyment and happiness. This willingness to sacrifice much more compared to a user that possesses utilitarian behaviors to have that pleasure makes them vulnerable targets and strongly influences intention to use technologies and systems (Ja-Chul Gu et al., 2010). This situation may make them pay much less attention to detail which can retain them to detect errors in a fake system only created for users to manipulate them.

Utilitarian Behavior

According to the results, the relationships mentioned in hypotheses H2a and H2b regarding utilitarian user behavior's effect on habitual trust are significant but not supported. In contrast, the relationship with misplaced trust is not significant, meaning these variables in this relationship does not affect each other. The first hypothesis to be discussed is H2a which

states that individuals with utilitarian behavior will have decreased habitual trust towards online systems. After the analysis, it can be said that this relationship proved to be otherwise but still a significant relationship meaning, users that possess the utilitarian type of behavior tend to habitually trust systems more. In literature, utilitarian value is task-oriented and cognitive. For example, from a shopping perspective, consumers usually achieve utilitarian value by getting products, which was the main reason to have the shopping trip in the first place (Irani and Hanzaee, 2011). Because the utilitarian approach is about fulfilling duties with effectiveness and focusing on functionality (Ja-Chul Gu et al., 2010). Utilitarian shoppers are motivated based on cognitive activities and goal-oriented tasks. Therefore, from a shopping experience perspective, it can be said that utilitarian purchasing behavior is more logical, rational, planned, part of daily routine, and always includes purchases (Hamzah 2013). This explanation in literature reflects the results of our analysis on this relationship much clearly. The relationship in hypothesis H2a is not supported because users with utilitarian behavior like activities planned and part of a routine. Liking routine is a perfect fit for trusting systems habitually because users with utilitarian value may want to keep the value they find in a system, and this may make them want to repeat that activity to get effectiveness in a quick way since being effective is one of the key values of utilitarian value and this may lead users to trust systems habitually without paying much attention thus there is a positive relationship between utilitarian behavior and habitual trust in our results.

The second hypothesis to be discussed is H2b which states the relationship between utilitarian behavior and misplaced trust. This relationship is not significant with a p-value of 0.79, meaning values in the corresponding relationship do not affect each other. The insignificant relationship between these variables also states that this type of behavior is strongly related to routines. As mentioned above, users with utilitarian behavior are about efficiency and completing tasks. Because of this, users may stick to doing the same activities

in a certain system if the result of their action is satisfactory and hold value. Users having such patterns in their activities online may be hard to misplace trust on systems because they may continue to perform that activity in the same system until it holds no value. Therefore, they may only misplace their trust in a very low probability system since they may not use much more alternatives.

Risk Avoidance Behavior

According to the results, the relationships mentioned in hypotheses H3a and H3b regarding the effect of risk avoidance behavior on misplaced trust and habitual trust is significant. Meaning these variables in both of those relationships indeed affect each other, and these hypotheses are supported, which shows that the relationships mentioned in these hypotheses turned out to be as expected and match the hypotheses' description. The first hypothesis to be discussed is H3a which is about the effects of risk avoidance behavior on users' levels of habitual trust. According to the results, users with higher risk avoidance will experience increased amounts of habitual trust towards online systems. According to the literature, risk avoidance is one of the major factors that affects individuals' decisions about behaviors they are about to make that are considered risky. (Kahneman & Tversky, 1979). This situation reflects on individuals' behaviors while performing online activities, such as avoiding risky transactions and activities. Because of this, individuals with high-risk avoidance behavior may not be able to perform all activities in their mind and may choose to go with the same trusted website and same trusted activity to minimize the risk-taking even that action does not give the best value for the user. Repeatedly positive experiences on the same activities in the same systems may form habitual trust towards a system since users will be so familiar with the system and the activity itself.

The second hypothesis to be discussed is H3b which states the relationship between risk avoidance behavior and misplaced trust. This hypothesis also supported, meaning the

stated relationship in the hypothesis turned out to be as expected. According to the results, as stated in the hypothesis, users with higher risk avoidance will experience increased amounts of misplaced trust towards online systems. According to the literature, different individuals can perceive risk differently since sources of risk cannot be identified (Keith et al., 2013). People with high-risk levels of risk avoidance tend to avoid unknown actions and perform actions much more cautiously, meaning higher levels of risk avoidance increases individuals' willingness to protect against those risks. This potential risk factor can create a feeling of uncertainty and fear in individuals (Floyd et al., 2000). Therefore, individuals under the effect of such feelings may choose to minimize their risk and do the same online activities through the same systems to minimize risk and uncertain factors of new actions or new systems. Since individuals with high levels of risk avoidance will perform activities in one system and only tend to trust one individual system, this will increase the possibility of misplacing their trust on one system and hardly even trusting other systems since they will probably be focused on one system where they got their positive experiences even if that system does not give them the best benefit.

Discussions About Dark Side of Trust

Habitual Trust

According to the results, the relationships mentioned in hypotheses H4a and H4b regarding the effect of habitual trust on perceptions of security and privacy is significant. Meaning these variables in those relationships indeed affect each other. These hypotheses are not supported, which shows that the relationships mentioned in these hypotheses did not turn out to be as expected and did not match the hypotheses' description. The first hypothesis to be discussed is H4a which states that individuals habitually trust systems will have decreased security concerns towards online systems. Again, this hypothesis is not supported by the results of the analysis, meaning individuals who habitually trust systems tend to have

increased levels of security concern about security towards online systems. One of the reasons this hypothesis is not supported may be that individuals do not even realize if they are habitually trusting systems. As mentioned, since habitual trust is formed with positive experiences and this repetitive positive feedback from the system, users can feel relaxed and confident about the system itself, resulting in a false sense of security. This false sense of security can be explained by increased concerns about security towards an online system. In this case, individuals probably trust the system itself, but they may still have concerns about whether their data is secure since they are not aware of their habitual trust. Likewise, the other hypothesis, H4b explaining the relationship between habitual trust and perceptions of privacy, is also not supported. According to results, users habitually trust systems tend to have increased concerns about perceptions of privacy towards online systems. This may happen because users are not aware when they are habitually trusted systems and get comfortable with the systems much more than necessary. This situation may lead to a false sense of privacy. This situation can be explained with the analysis result again since users tend to worry about their privacy more if they trust systems habitually. This habit-forming extends to privacy concerns and causes users to have increased levels of privacy concerns towards an online system even when they habitually trust that system.

Misplaced Trust

According to the results, the relationships mentioned in hypotheses H5a and H5b regarding the effect of misplaced trust on security and privacy perceptions is significant. Meaning these variables in those relationships indeed affect each other, but these hypotheses are not supported, which shows that the relationships mentioned in these hypotheses did not turn out to be as expected and did not match the hypotheses' description. The first hypothesis to be discussed is H5a which states that individuals who misplace their trust in online systems will have decreased security concerns towards online systems. Again, this hypothesis is not

supported by the analysis results, meaning individuals who misplace their trust in systems tend to have increased levels of security concern about security towards online systems. By looking at the analysis results, this can be also said for the effect of misplacing trust on concerns on privacy, which is hypothesis H5b. This hypothesis is also not supported, meaning individuals usually misplace their trust in systems that have increased concerns about perceptions of privacy through online systems. As for the habitual trust variable, the same reasoning may also be applicable for misplaced trust. People usually will not be aware of their misplaced trust in systems. Again, this false sense of security can affect individuals and their perceptions of privacy and security and make them much more concerned about their privacy and security than the website itself, which they are over-trusting without notice. Misplacing trust in systems happens with outside interference and mainly happens to individuals with low-level knowledge about systems. Individuals can have lower information about systems they are using online while doing activities online but can still be aware of the importance of security and privacy concerns, which are much more popular and easier concerns on the surface. Most people are already worried about their security and privacy.

Implications for Practice

Results found in this study have several implications for readers, general internet users, companies, and students. This information provided by the analysis of the results can be used in various areas, from individual purposes to company scale. Results of the study show that user behaviors affect the levels of performing dark side of the trust activities. These activities, as mentioned before, are trusting systems habitually or misplacing trust in a system. In connection with this information, according to results, this issue of users falsely trusting systems leads them to have false perceptions of security and privacy, meaning users trust systems falsely also process the information in the wrong way. This study addresses many issues regarding the use of trust and related with usage, addresses security and privacy

issues that come up with the effects of the dark side of the trust can also be stated as the wrong usage of trust in online systems. Again, research also mentions what types of user behavior can impact those wrong types of trust usage, can be used for individual purposes and educational purposes with various aims such as improving security and improving performance in the workplace.

From an individual's perspective, these studies can impact perceptions of security and privacy of users in a positive way and can make them aware of their misplaced or habitual trust issues happening in online systems. Fixing those issues will help individuals improve their level of technical expertise and knowledge, which can be helpful to avoid outside interferences that are necessary on the creation of the misplaced trust and improve their knowledge on the correct usage of the internet not habitually to trust systems. Users can also identify themselves by looking at the behavior types mentioned in this study and act accordingly during their online activities to prevent the misuse of the trust towards online systems. These implications can improve the ideas about perceptions of security and privacy of users while performing online activities and help them identify possible threats that are designed for their type of behavior.

From an organization's perspective, these studies can be useful to analyze workers' behaviors and take precautionary actions accordingly to those behaviors of workers since the study shows that users' behaviors are related to the wrong use of trust towards online systems. Again, the study also shows that this wrong use of trust towards online systems can cloud the perceptions of security and privacy towards online systems and results in false perceptions. This study can also be used to educate employees of organizations about threats of overused trust, and false perceptions can be helpful to prevent attacks on organizations through employees, such as using the misplaced trust of users to gain personal information. This awareness training can also be helpful to correct false perceptions of security and privacy and

help individuals do the right actions in the right place and right time by fixing their misuse of trust towards online systems according to their behavioral specifications.

Implications for Research

Variables inside the trust element's dark side, including misplaced trust and habitual trust, have not been the main topic of most studies regarding their effects on perceptions of privacy and security therefore, unlikely to be quantified in those studies for further research. According to our research, relationships between the dark side of the trust elements and perceptions of security and privacy are positively correlated, meaning users performing increased levels of the dark side of the trust in their activities have increased amounts of concerns about perceptions of security and privacy towards online systems unlike what is stated on the hypothesis that it would be a negative relationship. Since there are no quantitative evaluations about this topic in literature, it becomes much harder to comment because according to extensive research made, there were few closely related, or no example studies directly related, explaining this relationship between the dark side of trust in online systems and perceptions of security and privacy towards online systems. This negative relationship causes another problem in explaining the relationship between the dark side of trust and the perceptions of online systems since there are no quantitative evaluations about perceptions of security and privacy towards online systems. As mentioned, there is a positive relationship between the dark side of trust and increased concerns on perceptions of security and privacy towards online systems. Because of that, how individuals perceive perceptions needs further research since those relationships were not expected in our hypotheses.

Also, according to this research, user behaviors, including hedonic behavior, utilitarian behavior, and risk avoidance behavior, impact the dark side of trust. Unlike the relationship between the dark side of trust and perceptions of security and privacy, the number of studies about the variables consisting of hedonic behavior, utilitarian behavior, and

risk avoidance is much more common according to extensive research. The problem with these studies is that most of them mainly focus on those behavior types from a consumer perspective and focus on behaviors when performing real-life activities, unlike our thesis, which focuses on cybersecurity, information technologies, and online systems/activities. Based on similar research information available on those studies harmonized with information available in IT-related studies and with this research's results. As mentioned in our hypotheses, most of the results were expected, and relationship results came out. Effects of user behaviors on the dark side of trust is not the main topic of the studies mostly, regarding their effects on the variables of the da from an information technology perspective, and this research explaining significant results needs further research and commenting with additional studies in the future.

CHAPTER 7: LIMITATIONS AND FUTURE RESEARCH

Limitations

Generalizability is the main issue for this research since the main source used to get survey answers was the Amazon Turk (MTurk). Amazon Turk represents a specific part of the population. Even though age variety is enough to make assumptions on different ranges of ages, it can still be argued that it is not a representative sample for every part of the population. For example, results can differ for different purposes of use, such as a student population may differ from an organization population. Amazon Turk's wide range of age, education level, and gender make it hard to comment on specific areas. Further research may be needed to make more specific assumptions based on the area that researchers want to search, and they should pick their participant pool according to the research area on which they want to focus because again a wide range of age and education level makes it harder to represent every specific part of the population such as students, workers, daily users or informed experts and IT specialists. This research focuses on general daily users, so the initial thought was that Amazon Turk would be the best option to represent that part of the population since it is easier to get a wide range of age and education levels.

Future Research

Further research regarding the relationship between the dark side of trust and perceptions of security and privacy needs to be made to explain the positive relationship between trust elements' dark side and perceptions of users' security and privacy. This also shows us there needs to be a re-evaluation of how individuals perceive perceptions. Again, as mentioned, variables of habitual and misplaced trust have not been mentioned and quantified in most of the studies related to information technologies. These quantifications can answer how individuals perceive their perceptions about security and privacy when they are misplacing their trust or habitually trusting an online system. To make this research more

general to specific parts of the population, different population pools can be used based on the needs and questions of researchers. Expanding this research to different population sets can cause researchers to get different results compared to this research and can be useful for different aims such as education or awareness training. Another area where future research can be done is related to a control variable which is age. Age was a significant factor in our thesis that affects perceptions of privacy with a p-value of 0.04. This was also similar for perceptions of security, but it is not quite significant with a p-value of 0.06. This means that as individuals age increased, concerns about privacy about online systems decreased. This can also be said for security perceptions, but again, that relationship was not significant with a close value. Further research can be done on this are to examine the relationship between age and perceptions further. This further expansion of research can also be helpful to break down variables of this research based on age which makes generalizability much easier for the different parts of the population. The further expansion of this research can also be helpful to understand the positive relationship between the dark side of trust and perceptions by explaining how individuals perceive when they are habitually trusting a system or misplacing their trust on a system, so future research should focus on comprehension of perceptions and awareness of the dark side of trust. This can be done with a study that focuses on the quantification of misplaced and habitual trust.

CHAPTER 7: CONCLUSION

According to the results of this research, it can be clearly said that the vast majority of individuals engaging online interactions surrounding both privacy and security. Behaviors of individuals are also important factors that affect those online interactions and cause individuals to perform the dark side of the trust elements such as habitually trusting an online system or misplacing trust on an online system. Results show that variables belonging to the user behaviors section, such as hedonic behavior and risk avoidance behavior, significantly affect the dark trust individuals perform while interacting with online systems. These two variables also affect these trust types, but this cannot be said for the third variable, the utilitarian behavior.

When it comes to the types of dark trust, people are basing their perceptions since the relationship with the dark side of the trust is positive with users' perceptions. Again, these relationships are also significant, meaning variables on those relationships influence each other but in the opposite way. Therefore, it can be said that individuals are not aware of their misplaced or habitual trust when interacting the online systems and creating their perceptions for privacy and security elements towards online systems. Routine behavior causes individuals to trust systems habitually and misplace their trust much more easily, affecting the perceptions of security and privacy.

REFERENCES

Al-Sharafi, M. A., Arshah, R. A., Abo-Shanab, E. A., & Elayah, N. (2016). The effect of security and privacy perceptions on customers' trust to accept internet banking services: An extension of TAM. *Journal of Engineering and Applied sciences*, *11*(3), 545-552.

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, and crowding.

Arnold, M. J., & Reynolds, K. E. (2003). Hedonic shopping motivations. *Journal of retailing*, *79*(2), 77-95.

Babin, B. J., Darden, W. R., & Griffin, M. (1994). Work and/or fun: measuring hedonic and utilitarian shopping value. *Journal of consumer research*, *20*(4), 644-656.

Barber, B. (1983). The logic and limits of trust.

Beldad, A. (2016). Sealing one's online wall off from outsiders: Determinants of the use of Facebook's privacy settings among young Dutch users. *International Journal of Technology and Human Interaction (IJTHI)*, *12*(1), 21-34.

Beldad, A. D. (2015). Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International journal of web based communities*, *11*(3-4), 357-374.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behavior*, *26*(5), 857-869.

Benbasat, I., & Wang, W. (2005). Trust in and adoption of online recommendation agents. *Journal of the association for information systems*, *6*(3), 4.

Bentler, P. M., & Bonett, D. G. (1980). Significance Tests and Goodness-of-Fit in the Analysis of Covariance Structures. Psychological Bulletin, 88, 588-600.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating online labor markets for experimental research: Amazon. com's Mechanical Turk. Political analysis, 20(3), 351-368

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS quarterly*, 351-370.3

Bhattacherjee, A., & Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test. *MIS quarterly*, 229-254.

Brabham, D. C. (2008). Crowdsourcing as a model for problem solving: An introduction and cases. Convergence, 14(1), 75-90.

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2016). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality data?.

Chandler, D., & Kapelner, A. (2013). Breaking monotony with meaning: Motivation in crowdsourcing markets. Journal of Economic Behavior & Organization, 90, 123-133.

Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty. *Journal of marketing*, *65*(2), 81-93.

Chiu, C. M., Wang, E. T., Fang, Y. H., & Huang, H. Y. (2014). Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information Systems Journal*, *24*(1), 85-114

Cho, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. *Journal of retailing*, *82*(1), 25-35. consumer trust on intentions to transact with a web site: A trust building.

Currall, S. C., & Judge, T. A. (1995). Measuring trust between organizational boundary role persons. *Organizational behavior and Human Decision processes*, *64*(2), 151-170.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Crowston, K. (2012). Amazon mechanical turk: A research tool for organizations and information systems scholars. In Shaping the future of ict research. methods and approaches (pp. 210-221). Springer, Berlin, Heidelberg.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace 1. Journal of applied social psychology, 22(14), 1111-1132.

Dhar, R., & Wertenbroch, K. (2000). Consumer choice between hedonic and utilitarian goods. *Journal of marketing research*, *37*(1), 60-71.

Dinev, T., & Hart, P. (2006). Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *E-Service*, *4*(3), 25-60.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639-655.

Dijkstra, T. K., & Henseler, J. (2015a). Consistent and asymptotically normal PLS estimators for linear structural equations. Computational Statistics & Data Analysis, 81(1), 10-23.

Dijkstra, T. K., & Henseler, J. (2015b). Consistent partial least squares path modelling. MIS Quarterly, 39(2), 297-316.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of marketing*, *61*(2), 35-51.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of management review*, *23*(3), 601-620.

Elangovan, A. R., & Shapiro, D. L. (1998). Betrayal of trust in organizations. *Academy of management review*, *23*(3), 547-566.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies*, *59*(4), 451-474.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of behavioral decision making*, *13*(1), 1-17.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy. *Industrial management & data Systems*.,

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Friedman, B., Khan, P. H., Jr., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40.

Gambetta, D. (1988). Trust: Making and breaking cooperative relations.

Gargiulo, M., & Ertug, G. (2006). The dark side of trust. *Handbook of trust research*, *165*.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 51-90.

Gholami, R., Sulaiman, A. B., Ramayah, T., & Molla, A. (2013). Senior managers' perception on green information systems (IS) adoption and environmental performance: Results from a field survey. Information and Management, 50(7), 431-438.

Goel, S., Bell, G. G., & Pierce, J. L. (2005). The perils of Pollyanna: Development of the over-trust construct. *Journal of Business Ethics*, *58*(1), 203-218.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185–214.

Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International journal of human-computer studies*, *58*(6), 783-812.

Grable, J., & Lytton, R. H. (1999). Financial risk tolerance revisited: the development of a risk assessment instrument. Financial services review, 8(3), 163-181.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling. 2nd Edition. Thousand Oaks: Sage.

Hair, J.F., Ringle, C.M. and Sarstedt, M. (2013), "Partial least squares structural equation modeling: rigorous applications, better results and higher acceptance", Long Range Planning, Vol. 46 Nos 1/2, pp. 1-12.

Hamzah, M., & N. Hashim., & A. Othman., & A. Ahmad. 2013. The Relationship between Hedonic and Utilitarian Customer Experiences, Repurchase Intentions and Preferences among Shoppers. International Conference on Customer Service System and Management 2013 (ICCSSM 2013). www.elsevier.com/locate/procedia. Accessed on June 12th, 2015. Pp. 1-7.

Henseler, J., Dijkstra, T.K., Sarstedt, M., Ringle, C.M., Diamantopoulos, A., Straub, D.W., Ketchen, D.J.,Hair, J.F., Hult, G.T.M. and Calantone, R.J. (2014), "Common beliefs and reality about partial least squares: comments on Rönkkö and Evermann (2013)", Organizational Research Methods, Vol. 17 No. 2, pp. 182-209.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modelling. Journal of the Academy of Marketing Science, 43(1), 115-135.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hirschman, E. C., & Holbrook, M. B. (1982). Hedonic consumption: emerging concepts, methods and propositions. *Journal of marketing*, *46*(3), 92-101.

Hitlin, P. (2016). 4. Turkers in this canvassing: Young, well-educated and frequent users. Pew Research Center, 437.

Holbrook, M. B., & Moore, W. L. (1981). Feature interactions in consumer judgments of verbal versus pictorial presentations. *Journal of consumer research*, *8*(1), 103-113.

Hu, L.-T., & Bentler, P. M. (1998). Fit Indices in Covariance Structure Modeling: Sensitivity to Under parameterized Model Misspecification. Psychological Methods, 3(4), 424-453.

Hung, Y. T., Dennis, A. R., & Robert, L. (2004, January). Trust in virtual teams: Towards an integrative model of trust formation. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the* (pp. 11-pp). IEEE.

Irani, N., & Hanzaee, K. H. (2011). The effects of variety-seeking buying tendency and price sensitivity on utilitarian and hedonic value in apparel shopping satisfaction. International Journal of Marketing Studies, 3(3), 89.

Jap, S. D., & Anderson, E. (2003). Safeguarding interorganizational performance and continuity under ex post opportunism. *Management science*, *49*(12), 1684-1701.

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of management review*, *23*(3), 531-546.

Kalakota, R., & Whinston, A. B. (1997). *Electronic commerce: a manager's guide*. Addison-Wesley Professional.

Kang, R., Brown, S., & Kiesler, S. (2013, April). Why do people seek anonymity on the internet? Informing policy and design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2657-2666).

Kaufmann, N., Schulze, T., & Veit, D. (2011, August). More than fun and money. Worker Motivation in Crowdsourcing-A Study on Mechanical Turk. In Amcis (Vol. 11, No. 2011, pp. 1-11).

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, *71*(12), 1163-1173.

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontiers in Psychology, 11, 3030.

Kim, D. J., Steinfield, C., & Lai, Y. J. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems*, *44*(4), 1000-1015.

Kim, S. S., Malhotra, N. K., & Narasimhan, S. (2005). Research note—two competing perspectives on automatic use: A theoretical and empirical comparison. *Information systems research*, *16*(4), 418-432.

Koller, M. (1988). Risk as a determinant of trust. *Basic and Applied Social Psychology*, *9*(4), 265-276.

Ku, C. H., & Firoozi, M. (2019). The use of crowdsourcing and social media in accounting research. *Journal of Information Systems*, *33*(1), 85-111.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 1.

Lee, L., Petter, S., Fayard, D., & Robinson, S. (2011). On the use of partial least squares path modeling in accounting research. International Journal of Accounting Information Systems, 12(4), 305-328.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces*, *63*(4), 967-985.

Lian, J. W., & Lin, T. M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in human behavior*, *24*(1), 48-65.

Lightner, N. J. (2003). What users want in e-commerce design: effects of age, education and income. *Ergonomics*, *46*(1-3), 153-168.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*(1), 3.

Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS quarterly*, 705-737.

Luhmann, N. (1979). Trust and power.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, *31*(2), 111-118.

Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center.

Marcoulides, G.A., Chin, W.W. and Saunders, C. (2009), "Foreword: a critical look at partial least squares modeling", MIS Quarterly, Vol. 33 No. 1, pp. 171-175.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. Behavior research methods, 44(1), 1-23.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research*, *2*(3), 173-191.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on management information systems (TMIS)*, *2*(2), 1-25.

McKnight, D. H., Choudhoury, H., & Kacmar, C. (2002). The impact of initial

McKnight, H., Carter, M., & Clay, P. (2009). Trust in technology: development of a set of constructs and measures. *Digit 2009 proceedings*, 10.model. Journal of Strategic Information Systems, 11, 297–323.

Oldham, G. R. (1988). Effects of changes in workspace partitions and spatial density on employee reactions: A quasi-experiment. *Journal of applied psychology*, *73*(2), 253.

Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors influencing the effectiveness of relationship marketing: A meta-analysis. *Journal of marketing*, *70*(4), 136-153.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. Judgment and Decision making, 5(5), 411-419.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

Petter, S. (2018). " haters Gonna hate": PLS and information systems research. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(2), 10-13.

Pienta, D., Sun, H., & Thatcher, J. (2016). Habitual and Misplaced Trust: The Role of the Dark Side of Trust Between Individual Users and Cybersecurity Systems.

Pienta, D., Tams, S., & Thatcher, J. (2020, January). Can Trust be Trusted in Cybersecurity? In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Rahman, S. A., Amran, A., Ahmad, N. H., & Taghizadeh, S. K. (2015). Supporting entrepreneurial business success at the base of pyramid through entrepreneurial competencies. Management Decision, 53(6), 1203-1223.

Rahman, S. A., Amran, A., Ahmad, N. H., & Taghizadeh, S. K. (2016). Enhancing the wellbeing of base of the pyramid entrepreneurs through business success: the role of private organizations. Social Indicators Research, 127(1), 195-216.

Ramayah, T., Lee, J. W. C., Boey, J. C. I. (2011). Network collaboration and performance in the tourism sector. Service Business, 5(4), 411-428.

Ramayah, T., Yeap, J. A., Ahmad, N. H., Halim, H. A., & Rahman, S. A. (2017). Testing a confirmatory model of Facebook usage in SmartPLS using consistent PLS. *International Journal of Business and Innovation*, *3*(2), 1-14.

Ramayah, T.,Yeap, J. A. L., & Ignatius, J. (2013). An empirical inquiry on knowledge sharing among academicians in higher learning institutions. Minerva: A Review of Science, Learning and Policy, 51(2), 131-154.

Ranganathan, C., & Ganapathy, S. (2002). Key dimensions of business-to-consumer web sites. *Information & management*, *39*(6), 457-465.

Rensel, A. D., Abbas, J. M., & Rao, H. R. (2006). Private transactions in public places: an exploration of the impact of the computer environment on public transactional web site use. *Journal of the Association for Information Systems*, *7*(1), 2.

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. *Boenningstedt: SmartPLS GmbH*.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of personality*.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), 393-404.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330.

Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Schwartz, S. H. (1994). Are there universal aspects in the structure and contents of human values? *Journal of social issues*, *50*(4), 19-45.

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *The Journal of strategic information systems*, *11*(3-4), 325-344.

Shklar, J. N. (1984). *Ordinary vices*. Harvard University Press.

Shneiderman, B. (2000). Designing trust into online experiences. *Communications of the ACM*, *43*(12), 57-59.

Sullivan, G. M., & Feinn, R. (2012). Using Effect Size - or why the p Value is not enough. Journal of Graduate Medical Education, 4(3), 279–282.

Starr, C. (1969). Social benefit versus technological risk. *Science*, 1232-1238.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management science*, *42*(1), 85-92.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.

Tversky, A., & Kahneman, D. (1979). An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-292.

Tversky, A., & Kahneman, D. (1986). Rational Choice and the Framing of Decisions. *The Journal of Business*, *59*(4), S251-S278.

Tyler, T. R., & Kramer, R. M. (1996). Whither trust. *Trust in organizations: Frontiers of theory and research*, *1*, 15.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of management information systems*, *24*(4), 73-100.

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, *42*(2), 355-380.

Venkatesh, V. (1999). Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS quarterly*, 239-260.

Wakefield, R. L., & Whitten, D. (2006). Mobile computing: a user study on hedonic/utilitarian mobile device usage. *European Journal of Information Systems*, *15*(3), 292-300.

Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, *7*, 431-453.

Yip, J. A., & Schweitzer, M. E. (2015). Trust promotes unethical behavior: Excessive trust, opportunistic exploitation, and strategic exploitation. *Current Opinion in Psychology*, *6*, 216-220.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23*(11), 847-860.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative science quarterly*, 229-239.

Zureik, E., & Stalker, L. H. (2010). The cross-cultural study of privacy: Problems and prospects. *Surveillance, privacy, and the globalization of personal information: International comparisons*, 8-30.

APPENDIX. A CONSTRUCT MEASURES

APPENDIX A. CONSTRUCT MEASURES

Hedonic Use (Adapted from Davis et al., 1992) & (Adapted from Chiu, C. M. et al., 2014)

- I mostly care about having fun in my online activities (HED_1)
- I consider activities online worthless if it is not a joy to me (HED_2)
- If using a website or application is not enjoyable, I would consider it a waste of time. (HED_3)
- I value entertainment in my online activities, and I pursue entertaining activities online much more compared to other kind of activities (HED_4)

Utilitarian Use (Adapted from Mathwick et al., 2001) & (Adapted from Chiu, C. M. et al., 2014)

- I expect to get good values from my transactions and activities that I perform online. (UTL_1)
- When I visit a website, I want to make sure that I am not wasting my time and effort. (UTL_2)
- I enjoy more if an activity I performed online increase my performance in general. (UTL_3)
- When using the Internet, I am primarily concerned with how useful the website is and how easy it is to use. (UTL_4)

Risk Avoidance (Adapted from Kennison and Chan-Tin, 2020) & (Grable, J., & Lytton, R. H., 1999)

- I tend to use passwords that are not complex and easy to remember. (RISK_1)
- I would click on an unfamiliar URL if sender of the e mail seems reliable enough. (RISK_2)

- I love to use Wi-Fi freely in public places such as squares, cafes, lobbies etc. (RISK_3)
- I use same passwords for different accounts, devices, and applications. (RISK_4)
- It is okay for me to share my passwords with a person I trust in my workplace or in general. (RISK_5)

Habitual Trust (Adapted from Pienta, Sun and Thatcher, 2016)

- I tend to visit the same websites because I like routine and trust the site. (HBT_1)
- I find comfort in regularity which is why I visit the same websites again and again because I trust they have my best interests in mind. (HBT_2)
- I rely on the same websites rather than exploring something new sites because I trust them more. (HBT_3)
- I believe that companies like Google and Facebook will always maintain their systems and operations and my personal data will always be protected. (HBT_4)
- Regularly repeated positive experiences in my online activities makes me believe that the website will always act in my interest. (HBT_5)

Misplaced Trust (Adapted from Pienta, Sun and Thatcher, 2016)

- I trust whoever posts in online forums to gain knowledge about a certain action I need to do online. (MPT_1)
- I tend to trust the information provided by the website I am accessing even if I do not have any experience or knowledge about that action such as buying and selling bitcoins. (MPT_2)
- I trust the information a website is giving me if I do not know what I am doing or do not have any experience related to action I am performing online. (MPT_3)

Perceptions of Privacy (Adapted from Kaleta, J. P., and Mahadevan, L, 2020)

- I am confident that the private information I provide during my interactions online (e.g., transaction with mobile banking system) will only reach the site I am interacting with. (PRIV_1)
- I believe the information I provide during my interaction online will not be manipulated by inappropriate parties. (PRIV_2)
- I have confidence in the privacy of my online interactions. (PRIV_3)

Perceptions of Security (Adapted from Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., and Kusev P., 2018)

- I feel secure sending sensitive information across the Internet. (SEC_1)
- The Internet is a secure means through which to send sensitive information. (SEC_2)
- I would feel totally safe providing sensitive information about myself over the Internet. (SEC_3)
- Overall, the Internet is a safe place to transmit sensitive information. (SEC_4)