Online Identity Theft

An investigation of the differences between victims and non victims with regard to anxiety, precautions and uses of the internet

Researcher: Karen Reilly

Student #: 03475611

Supervisor: Dr. Gráinne Kirwan

Dissertation submitted as a requirement for the degree of MSc in Cyberpsychology,

Dun Laoghaire Institute of Art, Design and Technology, 2009.

Declaration

This Dissertation is entirely my own work, and has not been previously submitted to this or any other third level institution.

Signed: Ken Rutta. Date: 28/03/09

Acknowledgements

Thank you to my supervisor and lecturer Dr. Gráinne Kirwan. From our first developmental psychology lecture in 2nd year to our last Artificial Intelligence lecture in 6th year (ahhh), you have been supportive, knowledgeable and fun. Thank you for all your help this year with this project. I will miss you when I leave IADT once and for all!

Secondly, I would like to thank all the participants who took part in this study. I realise that it may have been difficult for victims of online identity theft to complete my online questionnaire but I am most grateful that you did. This study would be nothing without the victims' viewpoint.

Thank you ScamVictimsUnited for assisting me in finding participants.

Mammy and Daddy, thank you for always supporting me, believing in me and proofreading my thesis (and for the money, obviously!). Thank you Daddy for filling out my CAO form 6 years ago – I like where I've ended up! I love you both and I promise I will get sick of education at some point and will get a 'real' job!

Thank you Sarah for being a constant support in every aspect of my life. I'm so proud of you!

Thank you to my all my other friends; old and new! I couldn't have done this without all of you!

"It's the end of the world as we know it and I feel fine..."

Contents

List of Tables

List of Figures

1. Introduction

Online identity theft is a relatively new phenomenon and as a result the research is scarce and additional research is needed (Anderson, 2006). The main problem with online identity theft today is that people do not understand what an online identity is or how it can be used against them (OISR, 2005). According to Eisenstein (2008), because it can take months to recover from online identity theft the prevention of online identity theft is better than cure. Users should be educated as to how to prevent themselves from becoming a victim and should also be educated as to how and why victimisation occurs. The present study will examine the difference in precautions between victims of online identity theft and non-victims. The research will also identity whether victims of online identity theft experience higher levels of anxiety online.

This literature review will briefly discuss identity, identity theft, online identity theft, victims of online identity theft, availability of identity information and precautions. The present study and hypotheses will then be discussed.

1.1 What is identity?

Finch (2007) describes identity as "a multi faceted concept that is best understood by a division into three categories: personal, social and legal" (Finch, p. 29). Personal identity is characterised by a sense of continuity, an ability to know that we are different now than we were then and that life progresses (Locke, 1960). Social identity is the identity viewed by others in society (Burr, 2003). Social and personal identity can evolve and change over time. Legal identity relates to the way a group of information can distinguish one person from another – it answers the questions 'who is this person?' and 'is this the same person' (Torpey, 2000). Goffman (1968) describes legal identity as a sticky substance to which all biographical information and facts can be attached. Legal identity cannot be changed but more facts and information can be added to it.

With regards to identity theft, the legal aspect of identity is the most important factor of an individuals identity for many reasons. The purpose of legal identity is to create an unbreakable association between a collection of factual information and the individual to whom this relates.

Legal identity allows individuals to prove who they are at any point in time and it also has a cumulative element in that it provides a historical continuity of an individuals past for example, employment, education and credit. Legal identity becomes more comprehensive as an individual ages. (Torpey, 2000)

1.2 What is identity theft?

According to Felson (1998), identity theft is a product of the new age of information technology. It is the misuse of an individual's personal information (mainly legal identity such as date of birth, name, address) to commit fraud (Gonzales & Majoras, 2007). According to the Online Identity Security Report (OISR) (2006), obtaining an individual's information and creating fake bills and bank statements are not criminal offences' in Ireland and the United Kingdom (UK). It is only when someone attempts to use the stolen identity that it becomes an offence which is known as identity theft. Identity theft is rarely just one crime and it can be linked to a variety of crimes which are well known to most people. Identity theft is commonly associated with crimes such as; cheque and card fraud, various financial crimes, telemarketing and internet scams, theft aided by fraudulent documentation, counterfeiting and forgery and many more (Newman & Clarke, 2003; Maxfield & Clarke, 2004).

Identity theft is becoming one of the fastest growing crimes in the world (Smith & Lias, 2007) with one quarter of adults in the United Kingdom either having been a victim or knowing someone who has been a victim (OISR, 2006). According to the UK's Fraud Prevention Service; CIFAS (2008), there were 137,000 reported cases of identity theft in 2005 which was a 14% increase on 2004. CIFAS (2008) have dubbed identity theft of the deceased "Britain's largest growing identity theft related crime," which has grown from 5,000 cases in 2001, to16,000 in 2003, and an expected 20,000 in 2004.

In the United States alone, 27.3million people discovered that they had been victims of identity theft between the years of 2000-2005 (Synovate, 2005). 9.3million of these identity thefts occurred in 2004 (Better Business Bureau, 2005). Identity theft reportedly costs £1.7 billion per year (Home Office, 2006). These figures greatly exceed the estimates proposed in 2000 which

stated that identity theft would affect between 500,000 and 700,000 individuals per year (Givens, 2000). In 2003, the estimated loss to US banks and credit card issuers was $1.2 billion (Gartner Group, 2007). Credit card fraud remains the most common type of identity theft online and offline. The extent of credit card fraud on the internet has increased because of the opportunities provided by the internet environment (Newman & McNally, 2004).

The Internet has played a major role in distributing information about identity theft, both in terms of risks and information on how individuals may avoid victimisation. Ironically, it has also been identified as a major contributor to identity theft because of the environment of anonymity and the opportunities it provides offenders or would-be offenders to obtain basic components of other person's identities.

While identity theft has traditionally occurred through offline methods such as stealing credit and debit cards and household bills, online data collection of stolen identities can be easier and more efficient for thieves (Katyal 2001) because new approaches and scams can be created and implemented under the cloak of electronic anonymity (Milne, Rohm & Bahl, 2004).

1.3 Online identity theft

Online identities are made up of passwords, email addresses, social networking profiles, online banking and shopping accounts, and instant messaging (OISR, 2006).

Marshall and Tompsett (2005) describe online identity theft as "the acquisition of sufficient data for one individual to successfully impersonate another". Information can be stolen from victims by phishing (sending emails that direct the victim to a fake website), stealing software and hardware (laptops, discs) and by using malicious computer code (viruses that hack into the victims accounts and computer) (Gonzales & Majoras, 2007). Online identity thieves target many types of information such as user names, passwords, PPS numbers, credit card numbers, bank account numbers, birthdates, mother's maiden names and pet names. With this information, identity thieves can not only access an individual's account but can also create new accounts.

According to Newman & McNally (2004), there are three stages of identity theft. An identity theft crime can include all or just one of these stages. The first stage involves the acquisition of the identity through real world theft, computer hacking, fraud, trickery, force, re-directing or intercepting mail, or even by purchasing information on the internet. Stage two involves usage of the identity for financial gain, to hide one's own identity or to avoid arrest. As previously stated, identity theft involves a number of separate crimes and the usage of a person's identity can include crimes such as account takeover, opening of new accounts, debit or credit card use, sale of identity information, fraudulent licences, passport and visa acquisition, insurance fraud etc. The third stage of identity theft is discovery. Many crimes of identity theft are discovered quickly but for the most part, discovery of the crime can take victims from six months to several years.

1.4 Victims of Online Identity Theft

A crime victim is described as "a person who has suffered direct, or threatened, physical, emotional or pecuniary harm as a result of the commission of a crime". The study of victims first emerged in the 1940s and 1950s when Mendelsohn examined the interactions of victims and offenders and stressed the shared responsibility of crime. Mendelsohn's research (1963) found evidence to support that certain individuals who suffered damage and loss due to a crime may share some degree of responsibility with the offenders. Mendelsohn (1963) viewed the victim as one of many factors in any criminal case. This research led him to theorise that victims had an "unconscious aptitude for being victimised". For example, intoxicated customers in a bar may attract the attention of robbers, and more controversially, females are sometimes said to bear some responsibility for misunderstandings that evolved into sexual assaults (Encyclopædia Britannica, 2009).

Bryant and Peck (2007) state that victim blaming and shared responsibility of crimes is now affecting online identity theft victims. The amount and frequency of identity theft varies from region to region but research suggests that all people, regardless of social or economic background are potential victims of identity theft. Identity theft involves a minimum of two

victims; the individual whose identity has been stolen, and the financial institution that loses money due to the theft of the victim's identity (Sullivan, 2004; Foley, 2003).

As mentioned previously, it can take six months or more for victims to realize that the theft has occurred but according to Synovate (2003), even when the theft is known 38% of victims do not report the crime to the authorities. Victims who do report the identity theft do not always have their complaint recorded in official statistics especially when the crime is reported to the police (Federal Trade Commission (FTC) 2005; FTC 2004; FTC 2003; Synovate 2003; Foley 2003; Benner et al. 2000).

Benner et al. (2000) suggest that the reason victims do not always report the identity theft lies in the idea that individual's whose identity has been stolen are not always viewed as "victims". A victim of online identity theft states "they will lecture you, the victim, endlessly about how it's the fault of the credit card companies that you're in this position...that technically you're not the victim" (Benner et al., 2000).

According to Villiers (2009), the authorities will argue that victims of an online identity theft crime have only themselves to blame for being deceived and it is not the purpose of criminal law to protect people from their own foolery. Society views victims as responsible for their own fate as this allows non victims to maintain their own sense of invulnerability, safety and justice (Lerner, 1980).

1.5 Availability of identifiable information online

The internet provides numerous opportunities for identity theft to occur. Internet users can now shop, bank, network with friends and family and study/work online. In order to do any of these tasks, users must sign up to several websites and provide social and legal identity information. Social networking websites in particular have encouraged users to provide as much detailed personal information as possible.

1.5.1 Social Networking

Although the concept of online social networking dates back to the 1960s, it has only recently changed from niche phenomenon to mass adoption. The majority of social networking websites share common or core features such as a main profile (a representation of the user), social networks/groups, mail and comments. With over 66 million active users and a quarter million signing up every day, Facebook is one of the fastest growing social networking websites in the world. However, many of the characteristics that make Facebook so popular among social networkers also put Facebook users in danger of a variety of identity theft related crimes. (Next Advisor, 2009)

The amount and type of information people freely reveal on social networking websites is staggering (Gross & Acquisti, 2005). Internet users say and do things online that they would not ordinarily say or do in real life. Internet users sometimes feel more open, less restrained and are able to express themselves more freely (Suler, 2004). This is known as the online disinhibition effect. The information people provide on social networking websites can make stealing identities a much easier task. In a study of Facebook users in Carnegie Mellon University in Pittsburgh, Gross and Acquisti (2005) found that Facebook users provided a great amount of personal and legal identity information on their Facebook profiles. 90.8% of profiles contained a photograph of the users, 87.8% contained birth dates, 39.9% contained phone numbers and 50.8% included their current residence. The majority of users also displayed their sexuality, political and religious views, and various interests. 62.9% of users who displayed their current relationship status also identified their partner by name and/or link to their Facebook profile.

A study of Irish social networking users by AMAS (2008) revealed that 100% of Facebook users provided their full name and 62% provided full date of birth. AMAS (2008) also found that 83% of Facebook users display actual photographs of themselves on their profiles. Providing this amount of information on social networking websites puts users at risk of online identity theft. According to Sweeney (2004), people can be re-identified using a combination of a home address (ZIP code), gender, and date of birth. Therefore, a large proportion of Facebook users can be linked to outside data sources such as schools, universities, hospitals and banks.

1.5.2 Online Shopping

By shopping online, users are not only signing up to a service by inputting contact details, passwords and security questions but also have to use credit/debit cards or finance accounts such as paypal. Online shoppers are vulnerable to identity theft for three reasons: the data on any computer can be compromised when online, the data transfer to an online business can be compromised, and the data stored by businesses may be compromised. Increasingly, organizations and businesses are posting private customer/member information on websites.

Government agencies have posted public court records on the internet (Cohen, 2001). Churches and other social groups have posted private members information online (Hoy and Phelps, 2003). In 2002, JetBlue Airlines secretly provided the Transportation Security Administration with all travel records of its customers. This information was subsequently sold to an independent contractor who posted all of the records on the internet (Shenon, 2003). Online identity thieves can also hack directly into company databases and steal both personal and financial information such as PPS numbers and credit card details. Online consumers are very vulnerable targets of identity theft but are even more vulnerable when they also bank online.

1.5.3 Online banking

In 2006, 44million consumers used online banking in the United States. In the UK, online banking usage has grown by 50% since 2005. 85-90% of all banking in Finland is now done online. (Ireland statistic) In Ireland, online banking has become extremely common and is promoted by all major banks such as Allied Irish Bank (AIB), Bank of Ireland (BOI), Ulster Bank, and Permanent TSB. Although online banking is an efficient, useful and time saving service, the risks are numerous.

Rachwald (2008) has stated that the main risks of online banking are the following. With online banking, customer's information is accessible by anyone in the world, not just in the customer's physical area. Online security is a central concern when customers are choosing who to bank with. However for users who do not have much experience using the internet, it can be hard to differentiate between good and bad online security practices. With the rapid growth of online

banking systems, a lot of the common concerns have been alleviated. However, identity thieves have found new ways to resource information from customers – phishing attacks.

Phishing attacks involves a thief who attempts to fraudulently acquire sensitive information from a victim. The attacker generally impersonates a trustworthy third party such as a banking corporation or university. The attacker will send an email from the trusted third party stating that the victim should send information to the attacker. Sometimes, the attacker will add that there is a penalty if the information is not sent. The number of phishing attacks rose by 800% in 2005 (Rachwald, 2008). Gartner's (2003) research shows that 19% of people have clicked on a link in a phishing email and 3% have provided personal or financial information. 60% of banks report suffering from phishing attacks (Rachwald, 2008).

1.6 Anxiety Online

Anxiety is a psychological and physiological state which is characterised by cognitive, emotional, behavioural and somatic components. These components combine to create unpleasant feelings such as uneasiness, fear or worry (Seligman, Walker, & Rosenhan, 2001). Anxiety is associated with many emotional symptoms such as feelings of apprehension, dread, having trouble concentrating, feeling ill at ease or tense, anticipating the worst, restlessness and irritability. There can also be physical effects such as heart palpitations, difficulty breathing, fatigue, nausea, stomach aches and indigestion. (Smith, 2008)

Tyler and Rasinski (1984) found that victims of crime experienced anxiety about future victimisation which was associated with what the individuals learned from the experience of crime, for example, how much the victim learned about how to protect themselves, and also the emotional reactions experienced such as anger, shock, sadness and anxiety.

It is not only victims of crime that experience worry and anxiety. Non victims can experience worry when they can imagine themselves becoming victims. Victimisation has an indirect effect on anyone who has heard about a crime or knows others who have been victimised (Skogan & Maxfield, 1981).

Some research even suggests that indirect experiences of crime may cause more anxiety than the direct experience of being victimised (Hale, 1996). Indirect victimisation may account for the higher levels of fear with regard to a type of crime such as identity theft. This indirect victimisation can be caused by word of mouth and gossip which may inflate, deflate or garble the picture. It can also be caused by media influence (Skogan, 1986). According to Winkle and Vrij (1990), hearing about crime in the media can make victimisation imaginable especially when individuals can see themselves in the same situation as the crime occurred. The same crime can have different physical and emotional effects from one individual to another (Gabriel & Greve, 2003).

Two key features of fear of crime are sensitivity to the impact of victimisation and control over its occurrence (Tulloch, 2003; Ferraro, 1995). There is a difference in the amount of fear and anxiety that males and females experience regarding victimisation. Females are generally more worried and concerned about becoming victims because females feel less able to control the victimisation and anticipate more severe consequences. Females also believe that the risk of victimisation is more likely to happen to them and to females in general. (Farrell, Gray & Jackson, 2007)

In a study by RSA Security Inc (2003), the researchers found that identity theft was second only to terrorist attacks in terms of its impact on consumer awareness of security issues on and offline. 22% of consumers feel threatened by identity thieves. Whitson (2005) suggests that online crimes such as identity theft have become a locus for insecurity and anxiety. Kilner (2007) found that 90% of people consider online banks, retailers and auction sites to be less than completely secure and 46% of people fear that banks and retailers are not doing enough to keep users information safe. Victims of online identity theft may experience higher levels of anxiety on and offline as it can take months and even years to regain financial control and restore their good credit history after the theft occurs (Hammond, 2003).

1.7 Precautions

There is research to suggest that individuals who are most worried and anxious about crime take more precautions to make themselves feel less at risk and safer (Jackson & Gray, 2008). This is known as functional fear and when it does not affect the individual's quality of life it can be beneficial to internet users (Farrall, S. & Murray, L., 2008). There are precautions to combat online identity theft. According to the OISR (2005), the most important thing that users can do is to be aware of what they are doing online and be aware of the threats of online identity theft. Internet users should treat their online experience as they would an offline experience, taking necessary precautions when spending money online etc. Milne (2003) suggests that users should be educated in the importance of deleting documents containing personal information, using firewalls, virus scanners, spyware detection and controlling access to personal information. Internet users should always question why they are being asked for information. On receipt of an email from an online bank or online shop requesting updated details, users should always log into the website, rather than clicking on any links in the email.

1.8 The Present Study

Although there is some research to support that people around the world are fearful of online identity theft and experience some anxiety because of this fear, there is no research to highlight the anxiety experienced by actual victims of online identity theft. This may be due to victim blaming (Bryant & Peck, 2007; Villiers, 2009) and the fact that many victims of online identity theft never report the theft. The present study will address this issue by focusing on two groups of individuals; online identity theft victims and non victims and the anxiety that both groups experience online.

There are ways in which individuals can reduce the risk of becoming online identity theft victims. However, according to the RSA (2003), 40% of individuals have not implemented these common forms of security protection. The present study will determine whether previous victims of online identity theft take stronger precautions and security measures when shopping and banking online. The present study will also reveal whether there is a difference in the amount of information that victims of online identity theft and non victims provide online.

Research by AMAS (2008) and Gross and Acquisti (2005) suggest that the vast amount of information individuals provide on social networking websites can make them vulnerable to online identity theft. This study will examine the amount of information Irish individuals provide on these websites to identify how vulnerable the Irish social networking community is to online identity theft.

1.9 Research Question and Hypotheses

Do social networking users provide sufficient information on profiles to make it possible to identify the individuals concerned?

The primary hypothesis states that victims of online identity theft will experience higher levels of anxiety than non victims when shopping/banking online.

The secondary hypothesis states that victims of online identity theft take stronger precautions/measures when shopping and banking online.

A further hypothesis states that there is a difference between the amount of information provided by victims and non victims online.

2. Methodology

In order to test the three hypotheses of this study, the researcher conducted a content analysis of profiles on the social networking website; www.facebook.com and carried out an online survey to gauge participants knowledge of online identity theft and the difference in precautions and anxiety levels of victims and non victims.

2.1 Participants

2.1.1 Phase 1 –Social networking websites

60 participants took part in phase 1 of this study. The participants were required to have an account on facebook.com to take part in the study. 30 female participants and 30 male participants took part in this study. All participants were aged between 18-34 with a mean age of 26. Convenience sampling was used in order to select the participants.

2.1.2 Phase 2 – Online Identity Theft Questionnaire

85 participants completed phase 2 of the present study. All participants were above the age of 18 and were required to currently either shop or bank online. Figure 1 below shows the number of participants in each age group. 33 (39%) participants were in the 18-25 age group, 23 (27%) participants were in the 26-35 age group, 10 (12%) participants were in the 36-45 age group, 11 (13%) participants were aged between 46-55 and 5 (6%) participants were in the 56+ age group. Figure 2 shows the gender breakdown of participants who took part in this study. 46 (52%) female participants took part in the study along with 39 (48%) male participants. Convenience sampling was used in order to select the participants.

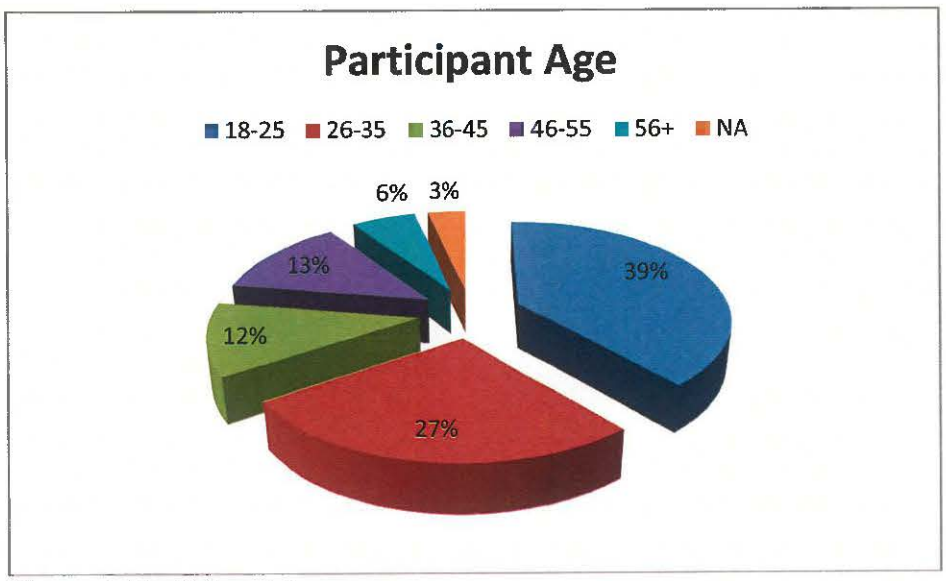

Figure 1. Participant Age

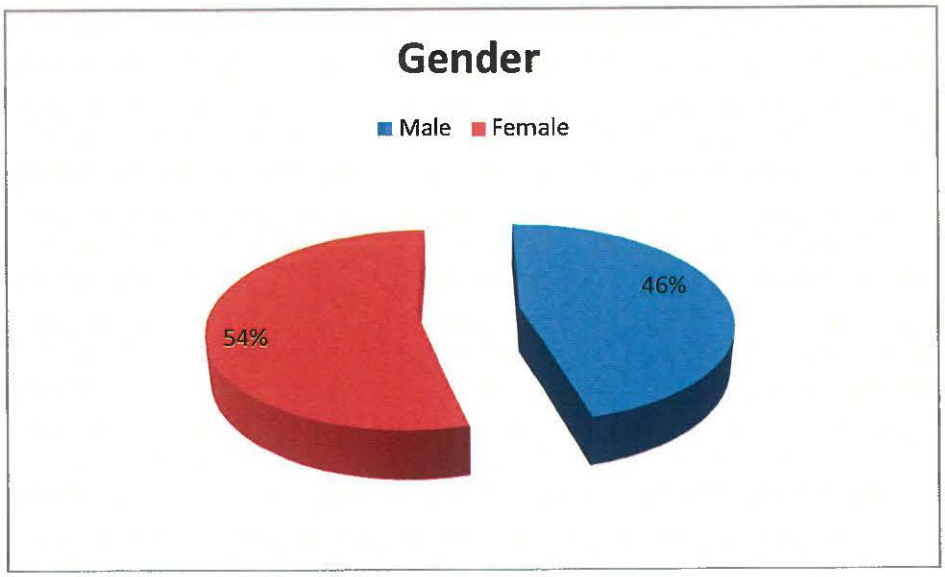

Figure 2. Participant Gender

2.2 Materials

The research study completed consisted of a questionnaire study and a content analysis of facebook.com profiles. A semi-flexible design was employed. The questionnaires were

administered in an online setting. The data collected from the 2 studies provided both qualitative and quantitative data.

For phase 1 of the study, the researcher devised a list of 16 codes for the content analysis of the Facebook profiles (Appendix A). The coding scheme was developed from creating a new Facebook profile and determining the information that was required and the information that was optional.

The researcher used previous research and documentation to aid in creating the Online Identity Theft questionnaire (Appendix B). The online survey scripts consisted of questions relating to online identity, attitudes and knowledge. Beck's Anxiety Inventory (BAI) was also used to analyse the amount of anxiety experienced by different levels of computer users, online identity theft victims and non victims. The BAI was developed to address the need for a scientific scale that would discriminate anxiety from depression. The inventory consists of 21 items that each describes a common symptom of anxiety such as nervousness, shaky, scared, or faint. The participant must rate how much they have been bothered by each symptom over the past week on a 4-point scale. The BAI is a reliable and valid scale for measuring anxiety (reliability - .60, validity - .48).

2.3 Procedure

2.3.1 Phase 1. Facebook.com Content Analysis

Pilot Study

A pilot study was completed in order to identity any unforeseen complications or difficulties within the research. Another further purpose of the pilot study was to identify problems with the data collection and analysis such as coding errors. The researcher analysed content from 3 facebook.com profiles. The study was modified based on the recommendations of the reviewer to account for any misunderstandings and suggestions for enhancement.

Main Study

Each participant consented to take part in study prior to participating in the present study. The participants were fully briefed on the purpose of the study, and how the study would be conducted before the study began (Appendix C). The researcher stated that withdrawal from the study was permitted at any stage during the study by completing the Revocation of consent form (Appendix E). Once all participants had provided consent, the researcher began a content analysis of the participant's profiles. When the content analysis was completed, the participants were debriefed.

2.3.2 Phase 2 – Online survey

Pilot Study

A pilot study was completed in order to identity any unforeseen complications or difficulties within the research. The pilot study was also used to find the amount of time required for participants to complete the survey. Another further purpose of the pilot study was to identity problems with the data collection.

Ten participants completed the online survey which studied people's attitudes and knowledge of online identity theft. The study was modified based on the recommendations of the participants to account for any misunderstandings and participants suggestions for enhancement.

Main Study

Each participant consented to take part in the online study by selecting "I have read and understand the information provided by the researcher. I hereby acknowledge the above information and give my voluntary consent to participate in this study. I understand that I may revoke my consent from the study at any time" prior to participating in the present study. The participants were fully briefed on the purpose of the study, and how the study would be conducted before the study began (Appendix D).

The participants were informed that the study would take about 10-15 minutes to complete but participants had an unlimited amount of time to complete the online survey. Participants were

informed that withdrawal from the study was approved at any stage by completing the Revocation of consent form (Appendix E). The participants were requested to answer all questions openly and honestly but all participants had the right to refuse to answer any question that made them uncomfortable. Help was provided by the researcher for any problems with the questionnaire that may have arisen during the study. When the participant completed the survey, the debriefing process began.

Data collection began when the study was completed.

2.4 Ethics

Before data collection commenced, a research proposal was put before the IADT Department of Learning Sciences Ethics Committee. Any concerns raised were examined and rectified and approval was granted. Only participants who gave consent were allowed to partake in the study. Those who did not give consent were directed to the last page of the study and asked to exit the survey. The online survey ensured anonymity and confidentiality of participants during and after the data collection process. There were no known risks to participants. A brief and debrief were presented to participants before and after the study.

3. Results

After data collection, raw scores were inputted into SPSS for statistical analysis. Statistics such as independent t-tests and chi squares were used to test the three hypotheses.

3.1 Facebook Analysis

60 Facebook profiles were analysed to determine the type and quantity of information that participants openly and freely displayed on social networking websites in particular www.facebook.com.

The content analysis revealed that no participants provided all 16 items from the coding sheet (Appendix B) on their Facebook profiles. However, 42 participants revealed more than half of the 16 items on Facebook with an average of 8.8 items per participant.

The items that appeared most often on the participants Facebook profiles were Email (100%), School/University (95%), Gender (80%), Date of Birth (80%), Relationship Status (75%), Hometown (70%) and Favourite Things (70%).

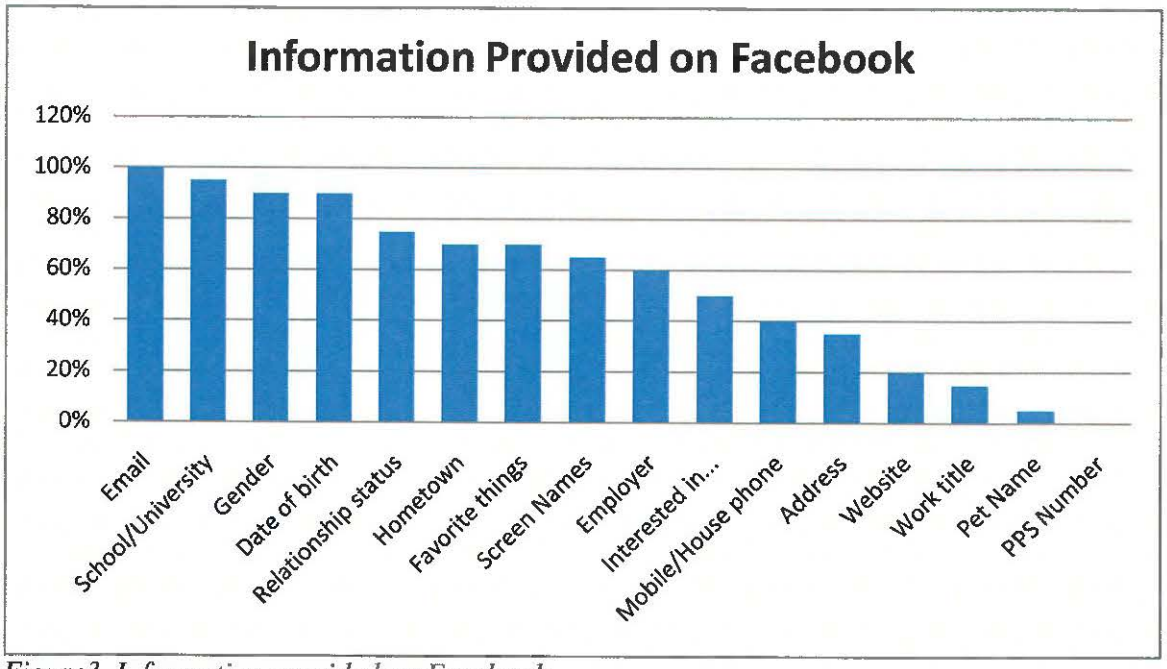

Figure3. Information provided on Facebook

3.2 Computer Experience

Figure 4 below shows that 32 (38%) participants were Beginner or Intermediate computer users and the remaining 53 (62%) participants were advanced computer users.

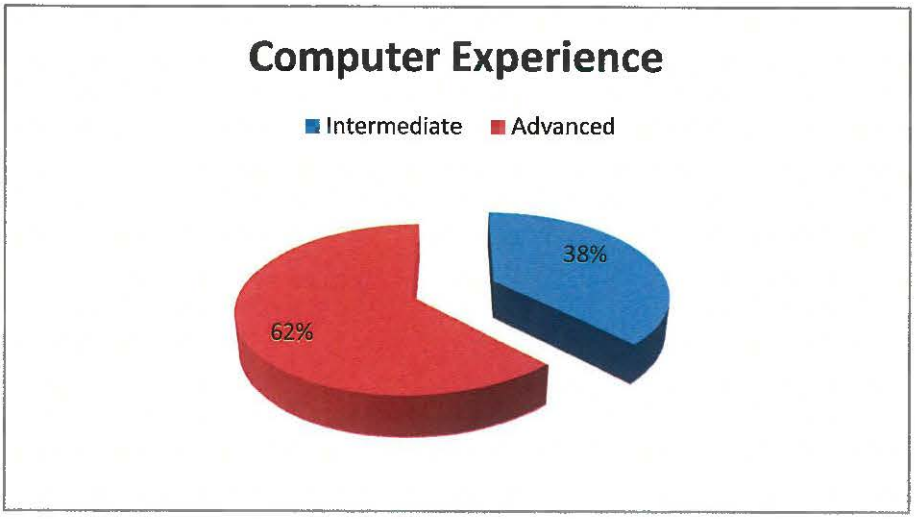

Figure 4. Participant's computer Experience

3.3 What is Identity Theft

Figure 5 reports that 88% participants reported that they understood what the term "Identity Theft" meant. 12% of participants revealed that they somewhat understood the term "identity theft".

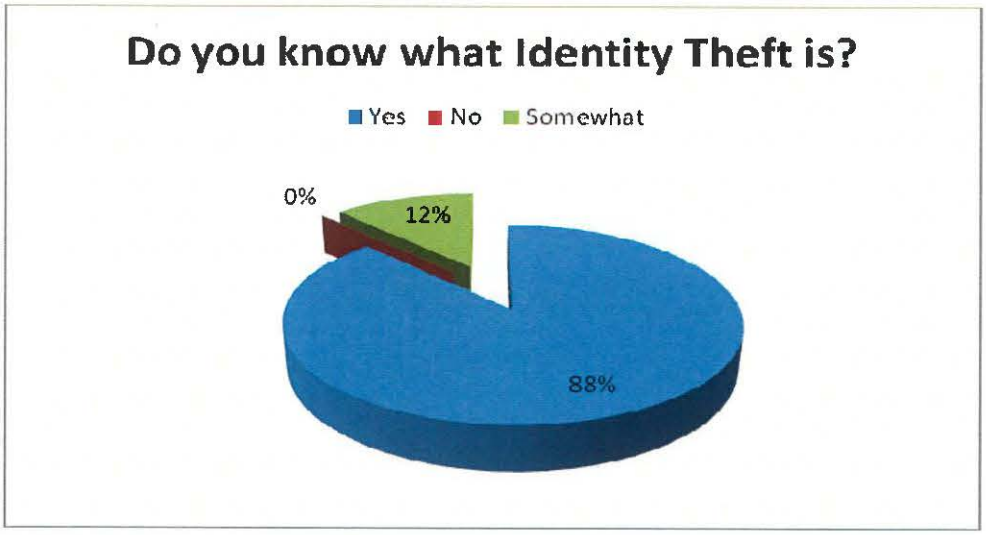

Figure 5. Knowledge of Identity Theft

3.4 Precautions and Measures Online

3.4.1 Ordered copy of Credit Report in last year

Figure 6 shows that 60 (71%) participants reported that they had not ordered a copy of their credit report in the last year. 22 (26%) participants had ordered a copy of their credit report in the last year.

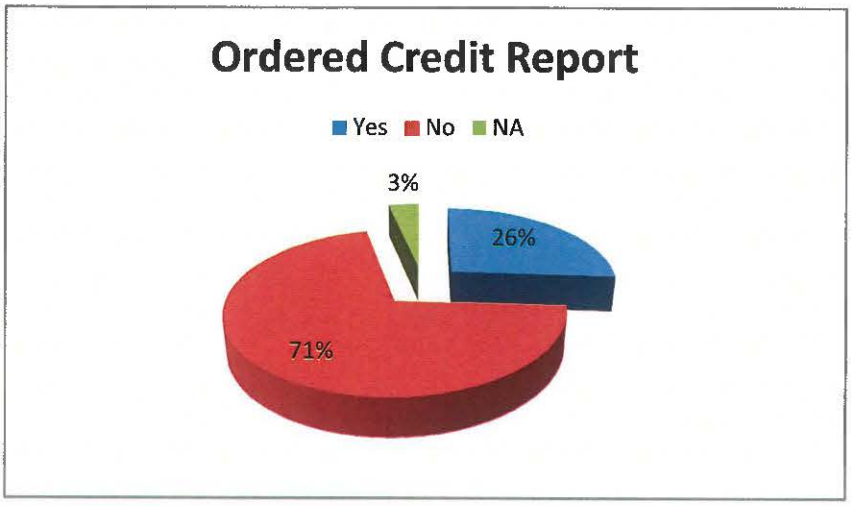

Figure 6. Ordered Credit Report

3.4.2 Used personal information when creating passwords

Figure 7 below shows that 36 (43%) participants had used personal information such as mother's maiden name, date of birth when creating online passwords.

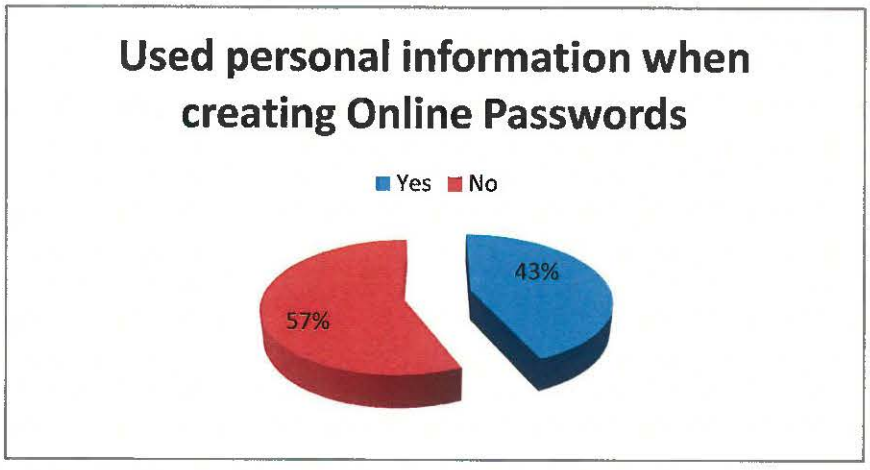

Figure 7. Online Passwords

3.4.3 Before providing information online, I find out what it is going to be used for.

55 (65%) of participants in this study find out what their personal information is going to be used for before providing information online. 30 (35%) do not check what their information is going to be used for.

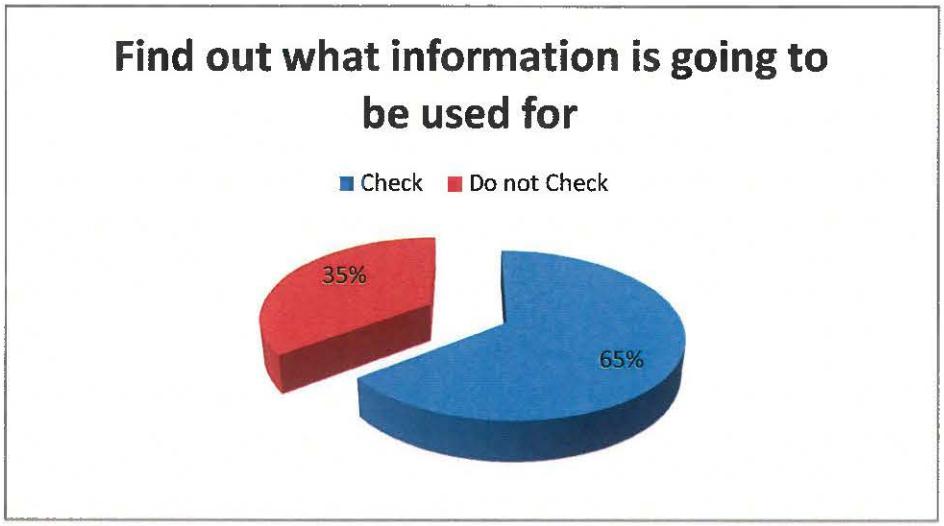

Figure 8. Find out what information is going to be used for

3.4.4 Check Billing Statements

Figure 9 below illustrates that 42 (51%) of participants never check billing statements for mistakes. Only 15 (18%) participants always check billing statements for mistakes and 25 (31%) participants sometimes check.

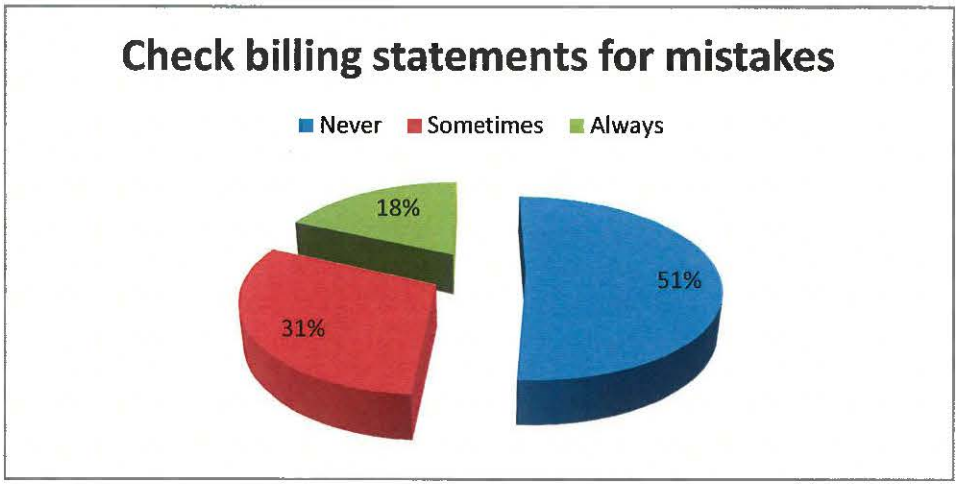

Figure 9. Check billing statements for mistakes

3.4.5 Provided PPS Number online

49 (61%) participants have never provided their PPS number online. 31 (39%) have at some point provided their PPS number online.

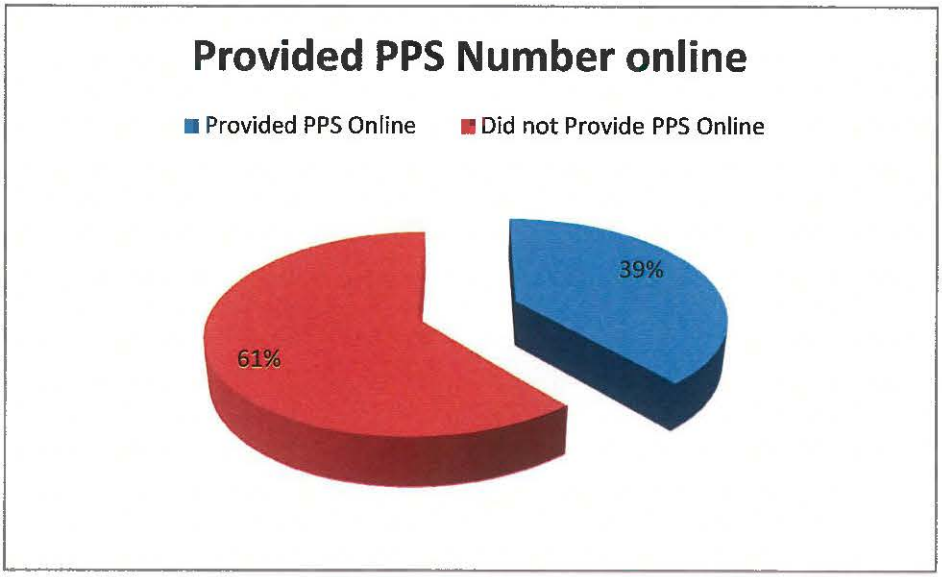

Figure 10. Provided PPS Number online

3.5 Providing information Online

Table 1 below shows the ways in which participants provide information online. 68 (87.2%) participants shop online using credit cards and 40 (51.3%) participants shop online using debit cards. 52 (66.7%) participants use online bill payment services and 34 (43.6%) participants provide information on social networking websites.

Table 1: Participants use of the internet

% Of Participants	Uses of the Internet
87.2%	Shop Online Using Credit Card
51.3%	Shop online using debit card
66.7%	Use online bill payment services
43.6%	Provide information on social networking websites

3.6 Experiences of Identity Theft

Table 2 depicts participant's experiences of identity theft. 17 (21%) participants had personal identity information stolen or used. 18(22%) participants had credit or debit cards stolen. 1(2%) participant had their PPS number stolen and 22 (26.7%) participants found unauthorised charges on bank statements.

Table 2: Experiences of Identity Theft

Percentage Of Participants	Experiences of Identity Theft
21%	Personal Identity Information stolen or used
22.2%	Credit Card/Debit Card stolen
1.2%	PPS # stolen
27.2%	Unauthorised charges on bank statements

3.7 Online Identity Theft and Anxiety Levels

3.7.1 Anxiety Score and Experienced Identity theft

Participants who had previously experienced one or more experiences of Identity theft described in Table 1 had higher anxiety scores ($M = 11.6$, $SD = 10.30$) than those participants who have never experienced any form of identity theft ($M = 4.1$, $SD = 2.21$). This result was found to be significant ($t = 4.929$, $df = 83$, $p < 0.001$).

3.7.2 Anxiety Score and Experienced personal identity information theft

The 21% of Participants who had their personal identity information stolen had higher levels of anxiety ($M = 18$, $SD = 11.20$) than participants who experienced any of the other three types of identity theft and participants who did not experience any form of identity theft ($M = 5$, $SD = 3.46$). This result was found to be significant [$t = 8.234$, $df = 83$; $p < 0.001$].

3.7.3 Anxiety Score, age and computer experience

There was no significant difference [t = .033, df = 83; p = .213] between age ranges with regard to online anxiety; Under 45 years of age (M = 7.4, SD = 7.62), above 45 years of age (M = 7.4, SD = 8.98). There was also no significant difference in anxiety levels between Beginner/Intermediate (M = 8.0, SD = 9.13) and Advanced (M = 8.9, SD = 6.93) computer users [t = .664, df = 77; p = .189].

3.8 Precautions/Measures when shopping and banking online

3.8.1 Online Identity Theft and finding out what information will be used for online

A chi-square test of independence was performed to examine whether victims of online identity theft were more likely to find out what their information is going to be used for on the internet than non victims. No significant relationship was found between the variables $c^2(1, N = 85) = 1.545, p = .214$. Victims were no more likely to find out what their information was used for than were non victims.

3.8.2 Online Identity Theft and providing PPS number online

A chi-square test of independence was performed to examine whether victims of online identity theft were less likely to provide their PPS numbers online than non victims. No significant relationship was found between the variables $c^2(1, N = 80) = 1.852, p = .174$. Victims were no less likely to provide their PPS number online than were non victims.

3.8.3 Online Identity Theft and signing out of email accounts

A chi-square test of independence was performed to examine whether victims of online identity theft were more likely to sign out of their email accounts than non victims. No significant relationship was found between the variables $c^2(2, N = 81) = .295, p = .863$. Victims were no more likely to sign out of their email accounts than were non victims.

3.8.4 Online Identity Theft and checking billing statements

A chi-square test of independence was performed to examine whether victims of online identity theft were more likely to check their billing statements each month than non victims. No significant relationship was found between the variables c^2 (2, N = 82) = 2.366, $p = .306$. Victims were no more likely to check their billing statements frequently than were non victims.

3.8.5 Online Identity Theft and ordering credit reports

A chi-square test of independence was performed to examine whether victims of online identity theft were more likely to order yearly credit reports than non victims. No significant relationship was found between the variables c^2 (1, N = 82) = .109, $p = .741$. Victims were no more likely to order credit reports each year than were non victims.

3.8.6 Online Identity Theft and using personal information when creating online passwords

A chi-square test of independence was performed to examine whether victims of online identity theft were less likely to use personal information such as; pet names, mother's maiden name, date of birth, when creating online passwords than non victims. The relations between these variables was significant c^2(1, N = 83) = 5.793, $p = .016$. Victims were less likely to use this personal information when creating passwords than non victims were.

3.9 Uses of the internet

There was no significant difference between victims of credit card theft/debit card theft and non victims with regards to using credit cards;c^2(1,N=85)=.012,p = .913) or debit cards; c^2 (1,N=85)=.171,p = .679) to shop and bank online.

There was also no difference between victims of PPS number theft and non victims in providing PPS numbers online; c^2 (1,N=80)=1.852,p = .174). There was no difference in participants usage of online bill payment services c^2 (1, N = 85) = 1.855, p = .173) and there was no

significance in the amount of information participants provided on social networking websites c^2 (1, N = 85) = 1.156, p = .282).

However, a chi-square test of independence revealed that participants who had previously experienced personal identity information theft in particular were less likely to use credit cards to shop and bank online $c^2(1,N=85)=3.107,p = .078)$. There was no significant difference between victims of personal identity information theft and non victims with regards to using debit cards to shop and bank online $c^2(1,N=85)=2.656,p = .103)$.

A chi-square test of independence also showed that victims of personal identity information theft were less likely to provide PPS numbers online $c^2(1,N=80)=4.050,p = .044)$.

A chi-square test of independence revealed that participants who had previously experienced personal identity information theft in particular were less likely to use online bill payment services $c^2(1,N=85)=9.028,p = .003)$.

4. Discussion

4.1. Hypotheses

The purpose of the present study was three fold; to determine whether victims of online identity theft experience higher levels of anxiety online than non-victims, to reveal if there is a difference in the amount of information that victims and non victims provide online and to determine whether victims of online identity take stronger precautions when shopping and banking online. Through analysing 85 online questionnaire responses and conducting a content analysis of Facebook.com, the aims of the present study were accomplished and three hypotheses were investigated based on the findings.

The primary hypothesis which stated that victims of online identity theft would experience higher levels of anxiety than non victims when shopping and banking online sought to investigate whether there was a correlation between high anxiety levels and victims of online identity theft. There was a significant difference between victims and non victims levels of anxiety when shopping and banking online with victims experiencing higher levels of anxiety and thus the primary hypothesis of the present study was supported. This confirms Hammonds (2003) research that suggested that victims of online identity theft experience more anxiety online due to the tireless process of regaining financial control after becoming victims. The present study also revealed that anxiety levels were higher for those participants who had personal identity information stolen. This also supports the findings of Tyler and Rasinski (1984) who suggested that victims of crime experienced anxiety about future victimisation.

The secondary hypotheses which stated that victims of online identity theft would take stronger precautions and measures when shopping and banking online queried if victims would be less likely to provide certain types of information online and whether victims would be more likely to take precautions online such as sign out of email accounts. There was no significant difference found in victims and non victims precautions when shopping and banking online. Victims of online identity theft were no more likely to determine what personal information was going to be

used for online, to sign out of email accounts, to check billing statements or to order credit reports. Victims were also no less likely to provide their PPS number online. There was however a significant difference between victims and non victims usage of personal information when creating online passwords. Victims of online identity theft were less likely to use personal information such as pet's names, mother's maiden name, and date of birth when creating online passwords. Thus the secondary hypothesis was partially supported. These findings correspond with previous research by the RSA (2003) who discovered that although fear and anxiety were associated with online identity theft, 40% of individuals did not take any precautions to combat identity theft. The findings from the present study do not correspond with Jackson and Gray's (2008) finding that individuals who are most worried and anxious about crime take more precautions to protect them to make themselves feel less at risk and safer.

The third hypothesis stated that victims of online identity theft would provide less information when shopping and banking online than non victims. On examining the results of the amount of information victims and non victims provide online, no significant difference was found. Victims of online identity theft were no less likely to use credit and debit cards online. Victims were as likely to use online banking and online bill payment services. There was also no significant difference in the amount of information that victims and non victims provided on social networking websites.

Although there was no significant difference in the amount of information victims of online identity theft and non victims provide online, a significant difference was discovered between victims of personal identity information theft in particular and non victims/other online identity theft victimisation. Victims of personal identity information theft were less likely to use credit cards to shop online. Personal identity information theft victims were also less likely to provide PPS numbers online and were also less likely to use online bill payment services. Gabriel and Greve (2003) suggest that different crimes can have different emotional and physical effects from one individual to another. Personal identity information theft may cause more emotional

strain and anxiety than the other types of information theft such as credit/debit card theft and this may account for personal identity information victims providing less information online.

4.2 Research Question

The research question queried whether social networking users provided enough information on profiles to make it possible to identity the individuals concerned. The results of the content analysis of Facebook.com are adjacent to those of Gross and Acquisti (2005) who identified that the amount of information provided on social networking websites is staggering. The findings also correspond to the findings of AMAS (2008) who found that many of the social networking profiles examined provided sufficient information to identity the individuals. In the present study, the majority of participants provided email addresses, gender, date of birth, relationship status, hometown and school on the Facebook.com profiles. This also corresponds to Suler's (2004) online disinhibition effect.

4.3 Other Findings

4.3.1 Knowledge of Identity Theft

The researcher assumed that a high percentage of participants taking part in the present study would not fully understand what the term "Identity Theft" meant. However this was not the case with 88% of participants reporting to fully understand the term and 12% of participants somewhat understanding the term. This knowledge of identity theft may come from media coverage and as such this research may be influenced by this also (Skogan, 1986).

4.3.2 Precautions/Measures

Research suggests that online identity theft victims and perhaps those who have been indirectly victimised would take stronger precautions and measures when shopping and banking online. However, 71% of the total number of participants reported not having ordered a copy of their credit report in the last year. 43% of participants used personal information such as mother's maiden name and date of birth when creating online passwords. 35% of participants never find out what personal information is going to be used for online and only 18% of participants always

check billing statements for mistakes. 39% of participants have even provided their PPS number online. The lack of precautions that the participants take when shopping and banking online supports the findings of RSA (2003) who found that 40% of participants had not implemented common forms of security protection to guard against online identity theft and phishing scams.

4.3.3 Experiences of Identity Theft

A high proportion of participants had experienced some form of identity theft with 21% having personal identity information stolen or used. 24% of participants experienced having either a credit or debit card stolen and 26% found unauthorised charges on bank statements. These findings confirm that online and offline identity theft is becoming quite prevalent in Ireland which supports the findings of Smith and Lias (2007).

4.4 Implications of Results

The present study is the first to investigate online identity theft in an Irish audience and the psychological aspects of online identity theft victimisation. It is also the first study to determine the precautions and measures or lack thereof that Irish internet users take. The results form an additional step towards understanding and preventing online identity theft from occurring in an Irish context. The results also highlight the differences between online identity theft victims and non victims.

This study has implications for many sections of society. As technology progresses, online identity theft will and is becoming more prevalent each year. In this study alone, more than 70% of participants had experienced some form of identity theft. As a significant relationship was disclosed between victims of online identity theft and higher levels of anxiety, online banks, retailers, companies should acknowledge this problem and consider addressing this anxiety by creating safer websites and more visible security features and information.

The findings of the present study show that victims of online identity theft do not take stronger precautions when shopping and banking online. Not only was there no significant difference between the two groups, but a high number of participants used personal information to create

passwords with 31% of participants using their mother's maiden name in passwords. The majority of participants did not order credit reports or check billing statements. The lack of precautions taken by both victims and non victims on the internet may result in online identity theft becoming even more prevalent than it already is.

The results of the content analysis of Facebook.com illustrate how much information individuals provide to strangers online. Social networking websites have become major sources of information for identity thieves. Individuals who choose to join Social Networking websites should be made aware of what their information might be used for and also policies for adding and removing friends from your network.

4.5 Limitations of the study

As the survey was administered online, victims of online identity theft may not have been comfortable in taking part. As confirmed in the present study, victims of online identity theft do in fact have higher anxiety levels and therefore may not be very forthcoming with their responses in an online environment. This may account for the relatively low response rate, in particular, response from victims of online identity theft. A possible solution to this would have been to offer the survey as both an online survey and a paper survey.

Response rate from non victims was not as high as anticipated either. It was hoped to obtain response from 100 non victim participants. It is possible that the response rate would be higher if more time was allocated to the data collection process.

Within the sample that did partake in the online identity theft questionnaire, over half were under the age of 35, with only 6% of participants over 56 years old. A more even spread of age may have revealed different results to the present study.

Feedback from the pilot study revealed that some questions on the Beck's Anxiety Inventory did not fully make sense in the context of the Online Identity Theft questionnaire. It may have been better for the researcher to compile an anxiety scale specifically for the purpose of the present study.

4.6 Suggestions for future research

There are a number of different approaches that could have been taken when conducting this study. The researcher decided to investigate victims of all types of online identity theft. However, from the results of the present study, it may be interesting to focus on victims of personal identity information theft. Victims of this type of identity theft may experience more emotional and physical strain than victims of other types of identity theft. Thus this group are very important to study from a psychological perspective.

As mentioned previously, the ages of participants may have hindered the results of the present study in some ways. Future research could assess the difference between age groups and anxiety levels. For example, it could be investigated whether or not older people experience higher anxiety levels online.

The present study focused on an Irish population of online identity theft victims and non victims. There is a lot of research surrounding the topic of online identity theft in the UK and USA and thus, media influence may cause different levels of anxiety in these populations. It may be interesting to investigate differences between Irish internet users and the larger international online population.

To fully understand the psychological and emotional factors faced by online identity theft victims, detailed case studies of victims are required. It would be interesting to follow victims long term uses of the internet, precautions and the psychological problems that may be experienced.

A content analysis of sites such as BEBO.com, Friendster.com, Twitter.com, and Facebook.com, could explore the differences in amounts of information people offer in different online settings for example. It would also be very interesting and very valuable to society to determine how much information under 18 year olds provide on these websites. This is another worrying aspect of providing information online.

4.7 Conclusion

The overall aims of the present study were accomplished and a number of interesting findings were uncovered regarding online identity theft in Ireland. The main findings suggest that online identity theft victims have higher anxiety levels when shopping and banking online than non victims. Furthermore, online identity theft victims do not take stronger precautions or measures when shopping and banking online and there is no difference in the amount of information provided by victims and non victims online. An interesting finding of the present study revealed that victims of personal identity information theft did provide less information online than all of the other participants. The present study also discovered that age and gender did not have an effect on participant's anxiety levels while shopping and banking online.

The present study has highlighted some important aspects of online identity theft. It is the first research in Ireland to examine the psychological aspects of this topic. The fact that this research found that victims of online identity theft experience a high level of anxiety online makes this a very important topic to study in the future.

5. References

Benner,J., Mierzwinski, E. & Givens, B. (2000). Nowhere to turn: Victims speak out on identity theft. California Public Interest Research Group and the Privacy Rights Clearinghouse. Retrieved November 14, 2008 from http://www.calpirg.org/consumer/privacy/idtheft2000/idtheft2000.pdf

Encyclopædia Britannica (2009) Victimology. Retrieved March 23, 2009, from http://www.britannica.com/EBchecked/topic/1246187/victimology

Burr, V. (2003) *Social Constructionism.* Hove: Routledge.

CIFAS (2008) Victims of online identity theft speak out. Retrieved December 8, 2008 from http://www.cifas.org.uk/default.asp?edit_id=651-57

Cohen, A. (2001) Internet Insecurity. Retrieved October 1, 2008 from http://www.time.com/time/pacific/magazine/20010702/cover1.html

Farrall, S., Jackson, J., & Gray, E. (2007) Theorising the Fear of Crime: The Cultural and Social Significance of Insecurities about Crime. Retrieved March 1, 2009 from http://ssrn.com/abstract=1012393

Farrall, S. & Lee, M. (2008). *Fear of crime. Critical voices in an age of anxiety.* Oxford: Routledge.

Federal Trade Commission. (2003). Overview of the Identity Theft Program, October 1998-September 2003. Retrieved November 14, 2008 from http://www.ftc.gov/os/2003/09/timelinereport.pdf

Federal Trade Commission. (2004). National and state trends in fraud and identity theft, January-December 2003. Retrieved November 14, 2008 from http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

Federal Trade Commission. (2005). National and state trends in fraud and identity theft, January-December 2004. Retrieved November 14, 2008 from http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf

Felson, M. (1998). *Crime and Everyday Life* (2nd ed.). CA: Pine Forge Press.

Ferraro, K. F. (1995) *Fear of Crime: Interpreting Victimization Risk.* New York: Suny Press.

Finch, E. (2007) The problem of stolen identity and the internet. In Jewkes, Y. (Ed.), *Crime Online: Committing, Policing and Regulating Cybercrime.* UK: Willan Publishing.

Foley, L. (2003). *Identity theft: The aftermath.* Identity Theft Resource Center. Retrieved November 14, 2008 from http://www.idtheftcenter.org/idaftermath.pdf

Gabriel, U. & Greve, W. (2003). The psychology of fear of crime: Conceptual and methodological perspectives. *British Journal of Criminology, 43,* 600-614.

Gartner Inc. (2003). *Gartner says identity theft is up nearly 80 percent.* Retrieved November 14, 2008 from http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp

Givens, B. (2000). *Identity theft: The growing problem of wrongful criminal convictions.* Retrieved November 14, 2008 from http://www.privacyrights.org/ar/wcr.htm

Gonzales & Majoras (2007) *Identity Theft Task Force Comprehensive Strategic Plan.* Retrieved December 6, 2008 from http://www.usdoj.gov/archive/ag/speeches/2007/ag_speech_0704231.html

Gross, R. & Acquisti, A. (2005) Information Revelation and Privacy in Online Social Networks (The Facebook case) *Pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES).*

Hale, C. (1996), Fear of Crime: A Review of The Literature. *International Review of Victimology, 4,* 79-150.

Hammond, R., J. (2003) *Identity Theft: How to protect your most valuable asset.* USA: Bookmart Press.

Home Office (2004). *The British Crime Survey. Patterns of crime.* Retrieved November 14, 2008 from http://www.homeoffice.gov.uk/rds/patterns1.html.

Hoy, M. G., & Phelps, J. (2003). Consumer Privacy and Security Protection on Church Websites: Reasons for Concern. *Journal of Public Policy and Marketing, 22*(1), 58–70.

Kilner, R. (2007) *RSA research shows widespread identity fraud anxiety.* Retrieved March 1, 2009 from http://www.insurancedaily.co.uk/2008/10/06/rsa-research-shows-widespread-identity-fraud-anxiety/

Jackson, J. & Gray, E. (2008). Functional Fear: Adaptational features of worry about crime, Working Paper, London, LSE.

Lerner, M. J. (1980) *The belief in a just world: A fundamental delusion.* New York: Plenum.

Locke, J. (1690) *Essays on Human Understanding, Book II.* Retrieved October 9, 2008 from http://humanum.arts.cuhk.edu.hk/Philosophy/Locke/echu/

Maxfield, M., & Clarke, R. (eds.) (2004). Understanding and Preventing Auto Theft. Crime Prevention Studies. *Criminal Justice Press, 17.*

Mendelsohn, B. (1963) The Origin of the Doctrine of Victimology. *Excerpta Criminologica 3,* 30

Milne, G. R., Rohm, A. J., & Bahl, S. (2004) Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs, 38,* 2.

Newman, G., and R. Clarke (2003). *Superhighway Robbery: Preventing E-Commerce Crime.* London: Willan.

Next Advisor (2009) *Facebook Identity Theft Protection Guide.* Retrieved March 1, 2009 from http://www.nextadvisor.com/identity_theft_protection_services/facebook_identity_theft_protection_guide.php

Rachwald, R. (2008) Is banking online safer than banking on the corner? *Computer Fraud and Security,* 11-12.

Seligman, M.E.P., Walker, E.F. & Rosenhan, D.L. (2001). *Abnormal psychology, (4th ed.)* New York: W.W. Norton & Company.

Shenon, P. (2003). JetBlue Chef Was Not Told of Decision on Passenger Data. New York Times.

Smith, Melinda (2008). *Anxiety attacks and disorders: Guide to the signs, symptoms, and treatment options.* Retrieved March 3, 2009, from http://www.helpguide.org/mental/anxiety_types_symptoms_treatment.htm

Skogan, W. (1986) 'Fear of crime and neighborhood change'. *Crime and Justice, 8,* 203-229.

Skogan, W. & Maxfield, M. (1981) *Coping with Crime,* Beverly Hills: Sage

Suler, J. (2004) The online disinhibition effect. *Cyberpsychology and Behaviour. 7*(3).

Sweeney, L. (2004) Uniqueness of simple demographics in the U.S. population. Carnegie Mellon University: Laboratory for International Data Privacy.

Synovate. (2003). *Federal Trade Commission – Identity Theft Survey Report.* Retrieved November 14, 2008 from http://www.ftc.gov/os/2003/09/synovatereport.pdf

Tulloch, M. (2003). Combining classificatory and discursive methods: Consistency and variability in responses to the threat of crime. *British Journal of Social Psychology, 42*(3), 461-476.

Tyler, T. & Rasinski, K. (1984) Comparing psychological images of the social perceiver: Role of perceived informativeness, memorability, and affect in mediating the impact of crime victimisation. *Journal of Personality and Social Psychology, 46* (2): 308-329.

Torpey, J. (2000) *The Invention of the Passport: Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press.

Van Dyke, J. & Cherico, H. (2003). New research shows that identity theft is more prevalent offline with paper than online. Retrieved March 8, 2009, from http://www.bbbonline.org/idtheft/safetyQuiz.asp

Villiers, P. (2009). *Police and policing: and introduction.* UK: Waterside Press.

RSA (2003). *RSA Security Study Confirms Consumer Anxiety Over Threat of Identity Theft.* Retrieved October 1, 2008 from http://www.rsa.com/press_release.aspx?id=2468

Whitson, J. R. (2005) *Security and Technology: Identity Theft.* Retrieved October 19, 2008 from http://www.allacademic.com/meta/p42938_index.html

Winkel, F. W. & Vrij, A. (1990). Fear of crime and mass media crime reports: Testing similarity hypotheses. *International Review of Victimology, 1*, 251-265.

6. Appendices

Appendix A: Facebook Codes

Appendix B: Online Identity Theft questionnaire

Appendix C: Facebook Content Analysis Brief

Appendix D: Online Identity Theft Questionnaire Brief

Appendix E: Revocation of Consent

Appendix F: Debriefing

Appendix G: Statistical Analysis

Appendix A: Facebook content analysis codes

Code	Provided?
Gender	
Interested in...	
Hometown	
Date of birth	
PPS Number	
Email	
Mobile/House phone	
Address	
Website	
Relationship status	
School/University	
Employer	
Work title	
Screen Names	
Favourite things	
Pet Name	
Former addresses	

Appendix B: Online Identity Theft Questionnaire

Consent

1. I have read and understand the information provided by the researcher. I hereby acknowledge the above information and give my voluntary consent to participate in this study. I understand that I may revoke my consent from the study at any time.

- ☐ I consent to partake in this study
- ☐ I do not consent to partake in this study

Section1: Demographics

1. Gender

- ☐ Male
- ☐ Female

2. Age

- ☐ 18-25
- ☐ 26-35
- ☐ 36-45
- ☐ 46-55
- ☐ 56+

3. Internet User

- ☐ Beginner
- ☐ Intermediate
- ☐ Advanced

Section 2: Identity Theft

1. I understand the term "Identity theft"

- ☐ Yes
- ☐ No
- ☐ Somewhat

2. I have ordered a copy of my credit report within the last year

- ☐ Yes
- ☐ No

3. Have you ever used any of the following when creating online passwords?

- ☐ None
- ☐ Mother's maiden name
- ☐ Pet's name
- ☐ Date of Birth
- ☐ PPS number

4. Before I reveal any personal identifying information on the internet, I always find out what it is going to be used for

- ☐ Yes
- ☐ No

5. I carry more credit/debit cards than I need in my wallet

- ☐ Yes
- ☐ No

6. I check each item in my billing statements for mistakes and report these immediately

- ☐ Sometimes
- ☐ Always
- ☐ Never

7. I have provided my social security number (SSN) or PPS number online

- ☐ Yes
- ☐ No

8. I sign out of my email account

- ☐ Sometimes
- ☐ Always
- ☐ Never

9. I keep a copy of my Pin number and passwords in my wallet or on my computer in case I forget them

- ☐ Yes
- ☐ No

10. I carry my social security card with me in my wallet or purse

- ☐ Yes
- ☐ No
- ☐ Sometimes

11. I have used the online revenue service

- ☐ Yes
- ☐ No

12. Have you ever had the following happen to you?

- ☐ Personal Identity Information stolen or used
- ☐ Credit/Debit card stolen
- ☐ PPS number stolen
- ☐ Unauthorised charges on bank statements
- ☐ None of the above

13. Do you do any of the following?

- ☐ Shop online using my credit card
- ☐ Shop online using my debit card
- ☐ Use online bill payment services
- ☐ Provide information on social networking websites

Section 3: Anxiety

1. Below is a list of common symptoms of anxiety. Please carefully read each item in the list. Indicate how much you are bothered by each symptom when providing information on the internet.

Symptom	Not at all	Mildly	Moderate	Severely
Feeling Hot				
Unable to Relax				
Fear of the worst happening				
Dizzy or lightheaded				
Heart pounding or racing				
Unsteady				
Terrified				
Nervous				
Hands trembling				
Shaky				
Difficulty breathing				
Scared				
Faint				
Face flushed				
Sweating				
Indigestion				

Appendix C: Facebook Content Analysis Brief

Dear participant,

My name is Karen Reilly and I am a final year MSc in Cyberpsychology student in IADT, Dun Laoghaire . As part of my final year I must carry out a major research project in the area of Cyberpsychology.

The study I have chosen to carry out is entitled Online Identity Theft . The main aim of my study is to investigate the differences in the amount of information victims and non victims of online identity theft provide online. This study also aims to examine precautions people take when giving information on the internet.

I hope you will agree to participate in my study by allowing the researcher to analyse the information that you supply on your Facebook profiles. This study is entirely voluntary and participants may withdraw from this study at any stage if they so wish by submitting the withdrawal form. If there are any aspects of the profile that you do not wish to be analysed, please let the researcher know prior to the beginning of the study.

If you have any questions about the study please feel free to contact myself or my supervisor at the contact details below.

Thanking you in advance for taking the time to read this email and for considering to take part in my research study. I hope to hear from you soon.

Karen Reilly

Primary Researcher: Karen Reilly
Email: Karenreillyresearch@gmail.com
Phone: 0862126202

Supervisor: Dr. Gráinne Kirwan
Email: grainne.kirwan@iadt.ie

Appendix D: Online Identity Theft Questionnaire Brief

Dear participant,

Online identity theft is an increasing problem worldwide. This survey aims to gauge public awareness and knowledge of online identity theft in Ireland. The main aim of this study is to investigate the differences in the amount of information victims and non victims of online identity theft provide online, the differences in anxiety levels online and it will also examine precautions people take when giving information on the internet. This research has been approved by the IADT Ethics Committee. As a participant, you are asked to complete this survey as efficiently as is possible.

The results of this study will be kept strictly confidential. None of the data collected will be released without your prior written consent. The information you provide will only have your demographic information and not your name on it.

Participation is voluntary. There are no apparent risks to the participant from taking part in this study. Please let the researcher know if you experience any discomfort at any time or if you wish to revoke your consent to participate.

The information collected throughout this study may be used for scientific and educational purposes. It may be presented/published/reproduced in books and journal articles. However, anonymity of participants will remain.

Please click on the following link to enter the survey.

http://www.surveymonkey.com/s.aspx?sm=E9441okYNTUXCES_2bZsxleQ_3d_3d

Thank you,
Karen

Primary Researcher: Karen Reilly
Email: Karenreillyresearch@gmail.com
Phone: 0862126202

Supervisor: Dr. Gráinne Kirwan
Email: grainne.kirwan@iadt.ie

Appendix E: Revocation of Consent

I hereby wish to WITHDRAW my consent to participate in this research study and I understand that such withdrawal will not jeopardise any treatment, or my relationship, with the researchers or any other organisation.

Name:
Signature:
Date:

Appendix F: Debriefing

Dear Participant,

Thank you for agreeing to participate in this study. This survey aims to gauge public awareness and knowledge of online identity theft in Ireland. The main aim of this study is to investigate the differences in the amount of information victims and non victims of online identity theft provide online, the differences in anxiety levels online and it will also examine precautions people take when giving information on the internet.

If you have any questions about this study or your involvement in it, please feel free to contact the researchers at the contact details below.

A copy of the research project will be available upon request after June, 2009.
The researchers would like to ensure you that your involvement in this study is strictly confidential and anonymity is guaranteed. It is also still possible to withdraw your consent for participating in this study and to have the data you have provided destroyed. If you have any hesitations please contact the researchers.

Once again, thank you for participating in this study.

Yours sincerely,

Karen Reilly

Primary Researcher: Karen Reilly
Email: Karenreillyresearch@gmail.com
Phone: 0862126202

Supervisor: Dr. Gráinne Kirwan
Email: grainne.kirwan@iadt.ie

Appendix G: Statistical Analysis

3.7.1 Anxiety Score and Experienced Identity theft

Group Statistics

	Any Info Stolen	N	Mean	Std. Deviation	Std. Error Mean
Anxiety Score	Info Stolen	36	11.6111	10.30749	1.71792
	No info stolen	49	4.1429	2.21736	.31677

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Anxiety Score	Equal variances assumed	50.210	.000	4.929	83	.000	7.46825	1.51520	4.45458	10.48193
	Equal variances not assumed			4.275	37.389	.000	7.46825	1.74688	3.92999	11.00652

3.7.2 Anxiety Score and Experienced personal identity information theft

Group Statistics

	Identity Theft	N	Mean	Std. Deviation	Std. Error Mean
Anxiety Score	Identity Stolen	17	17.7059	11.20694	2.71808
	No info stolen	68	4.7059	3.46436	.42011

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Anxiety Score	Equal variances assumed	33.892	.000	8.234	83	.000	13.00000	1.57880	9.85984	16.14016
	Equal variances not assumed			4.727	16.771	.000	13.00000	2.75036	7.19122	18.80878

3.7.3 *Anxiety Score, age and computer experience*

Group Statistics

	Age	N	Mean	Std. Deviation	Std. Error Mean
Anxiety Score	Under 45	67	7.4478	7.62826	.93194
	Above 45	16	7.3750	8.98795	2.24699

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Anxiety Score	Equal variances assumed	1.575	.213	.033	81	.974	.07276	2.19758	-4.29973	4.44525
	Equal variances not assumed			.030	20.467	.976	.07276	2.43259	-4.99411	5.13964

Group Statistics

	Computer Experience	N	Mean	Std. Deviation	Std. Error Mean
Anxiety Score	Intermediate	32	8.0313	9.13160	1.61425
	Advanced	53	6.8679	6.93386	.95244

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Anxiety Score	Equal variances assumed	1.751	.189	.664	83	.509	1.16333	1.75229	-2.32190	4.64855
	Equal variances not assumed			.621	52.544	.537	1.16333	1.87429	-2.59678	4.92343

3.8.1 Online Identity Theft and finding out what information will be used for online

Information is used for * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Information is used for	Check	26	29	55
	Don't check	10	20	30
Total		36	49	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.545[a]	1	.214		
Continuity Correction[b]	1.027	1	.311		
Likelihood Ratio	1.566	1	.211		
Fisher's Exact Test				.255	.155
Linear-by-Linear Association	1.527	1	.217		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 12.71.

b. Computed only for a 2x2 table

3.8.2 Online Identity Theft and providing PPS number online

PPS Number * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
PPS Number	Provided PPS Online	11	20	31
	Didn't Provide PPS Online	25	24	49
Total		36	44	80

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.852[a]	1	.174		
Continuity Correction[b]	1.277	1	.258		
Likelihood Ratio	1.870	1	.171		
Fisher's Exact Test				.249	.129
Linear-by-Linear Association	1.829	1	.176		
N of Valid Cases	80				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 13.95.

b. Computed only for a 2x2 table

3.8.3 Online Identity Theft and signing out of email accounts

Sign Out of Email * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Sign Out of Email	Sometimes	10	15	25
	Always	21	24	45
	Never	5	6	11
Total		36	45	81

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.295[a]	2	.863
Likelihood Ratio	.296	2	.862
Linear-by-Linear Association	.178	1	.673
N of Valid Cases	81		

3.8.4 Online Identity Theft and checking billing statements

Check billing statements * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Check billing statements	Never	17	25	42
	Sometimes	14	11	25
	Always	5	10	15
Total		36	46	82

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.366[a]	2	.306
Likelihood Ratio	2.370	2	.306
Linear-by-Linear Association	.002	1	.966
N of Valid Cases	82		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.59.

3.8.5 Online Identity Theft and ordering credit reports

Ordered Credit Report * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		Total
		Info Stolen	No info stolen	
Ordered Credit Report	Yes	9	13	22
	No	27	33	60
Total		36	46	82

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.109[a]	1	.741		
Continuity Correction[b]	.006	1	.937		
Likelihood Ratio	.110	1	.740		
Fisher's Exact Test				.805	.470
Linear-by-Linear Association	.108	1	.742		
N of Valid Cases	82				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 9.66.

b. Computed only for a 2x2 table

3.8.6 Online Identity Theft and using personal information when creating online passwords

Online Passwords * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Online Passwords	Yes	21	15	36
	No	15	32	47
Total		36	47	83

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.793[a]	1	.016		
Continuity Correction[b]	4.767	1	.029		
Likelihood Ratio	5.833	1	.016		
Fisher's Exact Test				.025	.014
Linear-by-Linear Association	5.723	1	.017		
N of Valid Cases	83				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 15.61.

3.9 Uses of the internet

1. Credit and Debit cards

Credit Card Use * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Credit Card Use	Use Credit Card	29	39	68
	Don't use Credit Card	7	10	17
Total		36	49	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.012[a]	1	.913		
Continuity Correction[b]	.000	1	1.000		
Likelihood Ratio	.012	1	.913		
Fisher's Exact Test				1.000	.568
Linear-by-Linear Association	.012	1	.913		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 7.20.

b. Computed only for a 2x2 table

2. Debit Card

Debit Card Use * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Debit Card Use	Use Debit Card	16	24	40
	Don't use Debit Card	20	25	45
Total		36	49	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.171[a]	1	.679		
Continuity Correction[b]	.038	1	.846		
Likelihood Ratio	.171	1	.679		
Fisher's Exact Test				.826	.423
Linear-by-Linear Association	.169	1	.681		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 16.94.

b. Computed only for a 2x2 table

3. PPS number

PPS Number * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
PPS Number	Provided PPS Online	11	20	31
	Didn't Provide PPS Online	25	24	49
Total		36	44	80

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.852[a]	1	.174		
Continuity Correction[b]	1.277	1	.258		
Likelihood Ratio	1.870	1	.171		
Fisher's Exact Test				.249	.129
Linear-by-Linear Association	1.829	1	.176		
N of Valid Cases	80				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 13.95.

b. Computed only for a 2x2 table

4. Online Bill Payment

Billpay * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Billpay	Use Billpay	19	33	52
	Don't use Billpay	17	16	33
Total		36	49	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.855[a]	1	.173		
Continuity Correction[b]	1.292	1	.256		
Likelihood Ratio	1.850	1	.174		
Fisher's Exact Test				.186	.128
Linear-by-Linear Association	1.833	1	.176		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 13.98.

b. Computed only for a 2x2 table

5. Social Networking

Social Network * Any Info Stolen Crosstabulation

Count

		Any Info Stolen		
		Info Stolen	No info stolen	Total
Social Network	Use SN	12	22	34
	Don't use SN	24	27	51
Total		36	49	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.156[a]	1	.282		
Continuity Correction[b]	.725	1	.395		
Likelihood Ratio	1.166	1	.280		
Fisher's Exact Test				.371	.198
Linear-by-Linear Association	1.143	1	.285		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 14.40.

b. Computed only for a 2x2 table

6. Personal Identity Information and credit card usage

Credit Card Use * Identity Theft Crosstabulation

Count

		Identity Theft		
		Identity Stolen	No info stolen	Total
Credit Card Use	Use Credit Card	11	57	68
	Don't use Credit Card	6	11	17
Total		17	68	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3.107[a]	1	.078		
Continuity Correction[b]	2.027	1	.155		
Likelihood Ratio	2.802	1	.094		
Fisher's Exact Test				.096	.081
Linear-by-Linear Association	3.070	1	.080		
N of Valid Cases	85				

a. 1 cells (25.0%) have expected count less than 5. The minimum expected count is 3.40.

b. Computed only for a 2x2 table

7. Personal Identity Information and debit card usage

Debit Card Use * Identity Theft Crosstabulation

Count

		Identity Theft		
		Identity Stolen	No info stolen	Total
Debit Card Use	Use Debit Card	5	35	40
	Don't use Debit Card	12	33	45
Total		17	68	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.656[a]	1	.103		
Continuity Correction[b]	1.845	1	.174		
Likelihood Ratio	2.734	1	.098		
Fisher's Exact Test				.173	.086
Linear-by-Linear Association	2.625	1	.105		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8.00.

b. Computed only for a 2x2 table

8. Personal Identity Information and providing PPS Number online

PPS Number * Identity Theft Crosstabulation

Count

		Identity Theft		
		Identity Stolen	No info stolen	Total
PPS Number	Provided PPS Online	3	28	31
	Didn't Provide PPS Online	14	35	49
Total		17	63	80

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4.050[a]	1	.044		
Continuity Correction[b]	3.000	1	.083		
Likelihood Ratio	4.418	1	.036		
Fisher's Exact Test				.053	.038
Linear-by-Linear Association	4.000	1	.046		
N of Valid Cases	80				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.59.

b. Computed only for a 2x2 table

9. Personal Identity Information and billpay service

Billpay * Identity Theft Crosstabulation

Count

		Identity Theft		
		Identity Stolen	No info stolen	Total
Billpay	Use Billpay	5	47	52
	Don't use Billpay	12	21	33
Total		17	68	85

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	9.028[a]	1	.003		
Continuity Correction[b]	7.433	1	.006		
Likelihood Ratio	8.886	1	.003		
Fisher's Exact Test				.005	.003
Linear-by-Linear Association	8.921	1	.003		
N of Valid Cases	85				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.60.

b. Computed only for a 2x2 table