1

Title

Public Wi-Fi and Risk: Are Individual Differences Associated with the Decision to Connect?

Angela Ryan

N00134834

Word Count: 7997

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

Signed Date

Thesis submitted as a requirement for the degree of MSc in Cyberpsychology, Dun Laoghaire Institute of Art, Design and Technology, 2016.

Acknowledgements

My sincere thanks to the staff at IADT for facilitating this journey into the fascinating world of cyberpsychology, and in particular to my supervisor Dr. Grainne Kirwan whose guidance and encouragement helped me to develop this thesis and focus my efforts.

Many thanks also go to the friends I've made along the way particularly Clare O'Hara who started this journey with me on the cyberpsychology certificate course and whose support had been absolute and unwavering. To my friends and family my heartfelt appreciation for your encouragement and faith in me.

Table of Contents

List of Tables

List of Figures

Abstract

Public Wi-Fi is ubiquitous yet despite awareness campaigns highlighting risks associated with its use there is limited understanding as to whether individual differences explain the decision to connect. This study used an online survey (N=64) to explore whether impulsivity, privacy proclivity, technical expertise, and cyber-security knowledge correlate with public Wi-Fi usage. As predicted participants with high scores on general caution privacy behaviour, and those more knowledgable about cyber-security were less likely to use public Wi-Fi. Contrary to what was hypothesised impulsivity was not correlated with the decision to connect nor were privacy concerns or technical expertise. The implications of decision making with regards to risk are discussed, and suggestions made for future research which looks at the role of personal responsibility.

Public Wi-Fi and Risk: Are Individual Differences Associated with the Decision to Connect?

It is important to address why individuals continue to engage in insecure behaviours online. Using public Wi-Fi whilst commonplace is still unsafe. The design of information campaigns and training needs a greater understanding of the attitudes and behaviours that it seeks to change. Knowing whether users realise they are engaged in unsafe practices or have misjudged the likelihood that their unsafe behaviour will lead to negative consequences is essential in understanding the decisions they make. Given awareness of risk individuals may know well but not do well, be overly optimistic, or succumb to the temptations of the moment by trading security for convenience. This research examines if particular individual differences correlate with the decision to connect to public Wi-Fi by measuring participants' impulsivity, privacy proclivity, technical expertise, and cyber-security knowledge. Examining these variables is important given the dearth of research on individual differences in cyber-security behaviour, and the possibility of translating any insight into actions that encourages safe conduct online.

Introduction

Cyber-security, Cybercrime and the Individual

Cyber-security focusses mainly on technology yet factoring the human into the cyber-security equation is of fundamental importance in developing and maintaining secure systems (Wiederhold, 2014)□. Recognising how individuals differ in terms of security practices has implications for attempting to understand and/or change attitudes and behaviours (Dutton, 2014a)□. Educational campaigns that raise awareness of risky practices or promote internet safety could

benefit from knowing what type of individuals engage in problematic security behaviours (Halevi, Lewis, & Memon, 2013;Whitty, Doodson, Creese, & Hodges, 2015).

Law enforcement agencies are now presented with a major challenge in curtailing the incidence of cybercrime (Europol, 2014**)**. Given that individuals socialise, shop, and work online there is a fundamental need to protect personal information and prevent it from being stolen or misused. A greater reliance on technology equates with increased vulnerability in the form of bank fraud, identity theft, and cyber threats. Safe conduct online necessitates knowing about these threats and vulnerabilities, and acting to safeguard against them (US-Cert, n.d; National Cyber Security Alliance, n.d).

The Individual's Desire to be Constantly Connected

This reliance on technology means that ubiquitous computing and the desire to always be connected drives an insatiable demand for data (F-Secure, 2014). Similarly technological advances in mobile devices allow individuals the freedom to work remotely, and to browse and share on the go. The Global Mobile Consumer Survey (Deloitte, 2015) highlights not only growing device obsession with both smartphone and tablet ownership increasing but also that consumers are using their devices more whilst engaged in other activities such as shopping, dining out, and talking to friends.

To satisfy this desire for almost constant connection, businesses such as hotels, cafes and airports offer Wi-Fi. It is estimated that the Global public Wi-Fi network contains 98 million worldwide public hotspots, a 568% growth from 2013 (Ipass, n.d). In the pursuit of free bandwidth, individuals, who do not want (nor expect) to pay for broadband, often connect to Wi-Fi hotspots oblivious to or unconcerned about privacy and security risks (Simmons, 2014; Kando-Pineda, 2015).

Public Wi-Fi: The Security Risks

To understand how individuals perceive these risks it is important to understand what risks are inherent in the use of free Wi-Fi. According to Europol there has been 'an increase in the misuse of Wi-Fi in order to steal information, identity or passwords and money from the users who use public or insecure wi-fi connections' (Oerting as cited in Simmons, 2014). The broadcast nature of public Wi-Fi means that unencrypted data can be read and received as plain text thus making many communications visible and susceptible to misuse or abuse. Research into privacy leakage on public Wi-Fi networks has shown that network protocols broadcast device names and previous access points thus making it possible to identity and profile users via the aggregation of data (Cheng, Wang, Cheng, Mohapatra, & Seneviratne, 2013; Konings, Bachmaier, Schaub, & Weber, 2013).

Using unsecured Wi-Fi networks to access unencrypted websites enables those who want to exploit security vulnerabilities (via the use of packet sniffers such as Wireshark) to eavesdrop on other people's online activities, and to scan, collect and analyse traffic data sets. Spoof or rogue hotspots set up to mimic trusted services and steal data from unsuspecting users who log onto these networks also pose substantial risks, and studies have shown how susceptible some users are to trusting these services (Kindberg, O'Neill, Bevan, Kostakos, Stanton Fraser, & Jay, 2008; F-Secure, 2014). To safeguard against risk users of public Wi-Fi can take a number of precautions such as disabling the automatic connection to Wi-Fi on their device, and connecting to a Virtual Private Network (VPN) thereby ensuring data being sent and received is encrypted.

Public Wi-Fi: Why it is Important to Know Who is Connecting.

In order to promote these safer practices it is important to identify the type of individuals more likely to use public Wi-Fi. According to a recent study there is a 'dearth of research on the psychological characteristics of those who engage in risky cyber-security practice' (Whitty et al., 2015, p.6). Findings from that study suggested that some aspects of personality (lack of

perseverance, and self monitoring) predicted who was more likely to share passwords. There was however no correlation found between cyber-security knowledge and sharing/ not sharing passwords thus prompting the researchers to conclude that campaigns promoting safe online practice need to do more than simply present information if behaviours are to change.

Research has shown that many users do not understand how Wi-Fi actually works and this has implications for the threat models they develop regarding the risk associated with security and privacy. An exploratory study (Klasnja, Consolvo, Jung, Greenstein, LeGrand, Powledge and Wetherall (2009) looked at participant's awareness of risk, privacy and security concerns, and protective practices. Findings show that whilst individuals understood how to use Wi-Fi they had limited understanding of the technical aspects of how Wi-Fi works thus the possibility of connecting to malicious networks was rarely consciously considered or completely absent. A sense of security was provided by not being aware of risk and by the habit of engaging in a routine practice. Making users aware of what personal information had been broadcast had an effect on their intentions to adopt more privacy protective behaviours in the future. The researchers thus advocated the development and inclusion of end user awareness tools to help change user behaviours.

A study by Consolvo, Jung, Greenstein, Powledge, Maganis and Avrahami (2010) found that changing behaviour was possible by increasing awareness of the potential visibility of communications over public Wi-Fi via a demonstration. This was achieved by the inclusion of a browser tool that alerted users in real time to information at risk of being seen when using insecure connections. Kowitz and Cranor (2005) used a public display (in a research computer lab) of information leaked over Wi-Fi and showed that this awareness had an impact on decisions regarding technology use and thus allowed users the possibility of forming more accurate privacy expectations. Whilst these studies highlight the importance of communicating risk they do not include measurements of individual differences that could distinguish between the types of

individuals more likely to engage in risky behaviours.

In contrast to those public Wi-Fi users who lack awareness of risk others may hold inaccurate perceptions of risk attributable to optimism bias (Weinstein, 1980) thereby believing negative outcomes are more likely to happen to others and less likely to happen to them. A qualitative study (Swanson, Urner, & Lank, 2010) found that public Wi-Fi users do not develop a realistic view of the privacy and security implications of connecting to insecure networks. In this study a demonstration of how data can be captured did not result in intended behavioural change because individual's believed that negative outcomes would not happen to them. Participants also voiced their unwillingness to adopt any security tools that were costly both in monetary terms and in terms of convenience.

A study by Campbell, Greenauer, Macaluso and End (2007) assessing why individuals engage in risky online behaviours despite expressing concerns about privacy and security also looked to unrealistic optimism as a possible explanation. Findings suggested that participants (and in particular those who were experienced users of the internet) believed that negative outcomes were less likely to happen to them, and they were therefore less likely to adopt protective security behaviours. Continued use of the internet without experiencing undesirable outcomes reinforced these views and behaviours. Risky security behaviours can also be representative of an individual's decision to make a tradeoff between security/privacy and convenience (Taylor, 2003; Tam, Glassman, & Vandenwauver, 2010), and the immediate gratification that Wi-Fi provides can also mean lower risk being attributed to decisions regarding privacy (Acquisti, 2004).

Individuals More Likely to Use Public Wi-Fi

Despite the proliferation of public Wi-Fi hotspots and warnings associated with their use there has been limited exploration as to whether psychological factors correlate with the decision to

connect. This study aims to examine if there are types of individuals who are more likely to engage in risky cyber-security practices and focuses specifically on the types of individuals more likely to use public Wi-Fi. Whilst Whitty et al. 2015 addressed how individual differences impact on cyber-security via password sharing (as distinct from Wi-Fi use), the study did not measure whether participant's privacy concerns correlated with their security practices. This could be a significant factor given that privacy proclivity could inform attitudes and influence behaviour.

Although other studies have examined both the technical aspects of public Wi-Fi insecurity (Cheng et al., 2013) and the relationship between Wi-Fi, privacy, expertise and protection practices (Konings et al., 2013; Klasnja et al., 2009), this paper adds to the literature by focusing specifically on whether certain factors; impulsivity (instant gratification associated with demands to always be connected), privacy, technical expertise, and cyber-security knowledge are associated with the use of public Wi-Fi. Thus the research aims to contribute to the knowledge of problematic security behaviours by concentrating on the users of public Wi-Fi.

Impulsivity

It is important to look at the role impulsivity plays in decisions regarding risky online behaviours. From a conceptual perspective impulsivity relates to a range of "actions that are poorly conceived, prematurely expressed, unduly risky, or inappropriate to the situation and that often result in undesirable outcomes" (Evenden, 1999 p.348). There is lack of consensus from researchers as to what defines impulsivity, and as to what constitutes impulsive behaviour given that the behaviour may vary according to culture, era and the age of the person involved. Thus impulsivity is better understood as a classification of related behaviours rather than a single psychological construct (Whiteside, Lynam, Miller, & Reynolds, 2005).

Studies into personality traits support this view that impulsivity consists of various facets and should be regarded as an amalgam of factors however there is little agreement as to what these factors are. Dickman (1990) differentiated between acting with less forethought and thus getting into difficulty (dysfunctional impulsivity), and taking advantage of unexpected opportunities that need to be acted upon without delay (functional impulsivity), whilst Eysenck & Eysenck (1985 as cited in Whiteside et al., 2005) posited unconscious risk taking (impulsiveness) and conscious sensation seeking (venturesomeness) as varieties of impulsivity relating them to psychoticism and extraversion respectively.

The UPPS Impulsive Behaviour Scale (Whiteside & Lynam, 2001) delineates four facets of personality that, rather than being variations of impulsivity, are personality traits that result in impulsive-like behaviours thus inferring actions without forethought. According to research these four factors; urgency (a response to regulating negative emotions where resisting temptation is difficult), lack of premeditation (problems related to thinking about the negative consequences of actions, and the focus on small immediate rewards rather than more valuable delayed rewards), lack of perseverance (difficulty in focussing on tasks that may be boring or complicated), and sensation seeking (enjoyment of exciting activities and openness to new experiences that could be dangerous) 'appear to be core features of several forms of psychopathology thought to be associated with poor impulse control' (Whiteside et al., 2005 p.572).

With regard to the relationship between impulsivity and security/privacy behaviours online, research has shown an association between diminished impulse control and susceptibility to phishing scams. In two studies (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012; Mayhorna, Welka, Zielinska, & Murphy-Hill, 2015) participants who had lower scores on impulsivity measures were found to perform better at anti-phishing detection tasks than those who

were more impulsive. Thus decisions regarding risky practices were influenced by individuals differences in impulsivity.

Privacy and Risk

Given that the way individuals' manage their privacy has implications for the behaviours they engage it it is important to understand whether privacy proclivity can influence the use of public Wi-Fi. An individual's privacy or the 'ability to control and limit physical, interactional, psychological and informational access to the self or one's group' (Burgoon as cited in Joinson and Paine, 2007, p. 243) is a complex construct and has become even more so in the era of digital footprints, big data and ubiquitous computing (Joinson et al., 2007). Self disclosure online and the nature of connectivity to the internet increasingly result in personal information being intercepted, collected, analysed, and sold, and user's activities being tracked often without their knowledge or agreement (Buchanan, Paine, Joinson, & Reips, 2007).

Whilst the level of concern individuals have about their privacy is subjective (Harris & Westin, 1998), studies have shown that privacy related behaviours can also be situational in nature and not necessarily influenced by pre-held general attitudes to privacy (Joinson, Reips, Buchanan, & Schofield, 2010). Theorists have looked to behavioral economics to explain this disjunction between individuals' privacy disposition and their actual behaviour. Decision making, instead of being undertaken by rational agents who seek to maximise payoff, can instead be influenced by tradeoffs which are subject to personal judgements and uncertainty. Operating under conditions of bounded rationality, assessments about costs and benefits become distorted (Aytes & Connolly, 2005). Individuals are also subject to hyperbolic discounting such that lower value is assigned to long term risks and losses particularly when unrealistic optimism, and the lure of immediate gratification exert an influence (Acquisti, 2004; Acquisti & Grossklags, 2003). Thus even those

individuals who purport to be concerned about privacy may trade it for small rewards such as convenience (Spiekermann, Grossklags, & Berendt, 2001), and this trade-off infers that individuals believe risks are worth taking, or that awareness as to the true nature of a threat is lacking.

Whilst awareness of risk and the associated decisions and behaviours enacted to deal with that risk are important in explaining security behaviours, user omissive behaviour, or the gap between knowledge and what individuals do also explains why some individuals may engage in risky security behaviour (Cox, 2012; Aytes & Connolly, 2005). Workman, Bommer and Straub's (2008) study looked to the knowing-doing gap to explain why, given awareness of measures to counter security threats, they were not implemented. Findings suggested that the effect of convenience in terms of a cost benefit trade-off impacted on omissive security behaviours.

Communication Privacy Management (CPM) Theory

Inherent in the use of public Wi-Fi is the risk of disclosing personal information thus CPM theory (Petronio, 2002) can be used as a framework to conceptualise variations in disclosure and practices as they pertain to the behaviour of individuals online (Child & Petronio, 2011), and in particular to the use/non use of public Wi-Fi. CPM theory posits that individual's own their private information and retain control of it but once information is shared others become co-owners of it. Individuals have expectations of how others treat this information, and turbulence can ensue as a result of actions that violate privacy boundaries. It is these open or closed boundaries that signify a demarcation between what is public and what is private, although the influence of context sometimes means that privacy rules are changed to facilitate attaining certain goals. In the context of public Wi-Fi some individuals may engage in privacy protectionist behaviours by not connecting or by using a VPN, whilst others who normally regulate their privacy by restricting access to their personal information may trade-off privacy for the need to gain immediate access to the internet.

Technical Expertise

Individuals differ greatly in their technical proficiencies when it comes to computers and the internet, and can be categorised as novice, average, and expert users (Konings et al., 2013). Assessing users' familiarity with technology and their level of understanding of technical and computer related terminology pertaining to general use and to internet security and privacy (Hargittai & Hsieh, 2012) can have implications for understanding security related behaviours. Research has shown that those with greater levels of technical proficiency experience fewer negative privacy related outcomes online (Litt & Hargittai, 2014), and engage in less risky online behaviours. In Dinev and Hu's (2007) study familiarity with technology was found to correlate with protective behaviour regarding anti-spyware programs.

Boyd and Hargittai's (2010) study of young Facebook users found that greater familiarity with technology, as measured by frequency of use and levels of understanding of internet terms, correlated with increased privacy behaviours regarding adjustments made to Facebook privacy settings. Similarly in O'Connell and Kirwan's (2014) study measures for self perceived levels of technical competence (ratings of level of comfort with technological systems and tools) were also found to correlate with self-efficacy in individual's ability to protect their privacy and to deal with risks online.

Cyber-Security Knowledge

Whilst most users of the internet have some awareness of security, varying levels of knowledge may account for differences in risk awareness and consequent security behaviours (Bada & Sasse, 2014), in this instance whether individuals decide to use public Wi-Fi given knowledge of the true nature of the threat. To encourage a culture of cyber-responsibility users must be aware of risk, know how to use the internet safely and securely, and have both the time and inclination to

take the steps necessary to do so (Dutton, 2014b). Research has shown that limited understanding of the implications of threats to privacy/ security can inform online behaviours (Dinev & Hu, 2007). Thus individuals with a greater knowledge of cyber-security should be better equipped to identify and understand vulnerabilities and thus assess risk. According to Wiederhold (2014) □behavioural change facilitated by the adjustment of perceptions towards privacy can be achieved by increasing the public's awareness of cyber-security.

In contrast to those individuals who are technically proficient users of the internet, knowledge of cyber-security infers not only awareness of risk but also of taking personal responsibility and action to protect against risk (stopthinkconnect.org). Shillair, Cotten, Tsai, Alhabasha, LaRose, and Rifon's (2015)□ study for example assessd participants' knowledge of online safety as well as their technology awareness.

A Theoretical Framework of Risk: The Health Belief Perspective

Within the context of privacy and security it is important to assess whether an individual's awareness of risk predicts the intention to take preventative measures. Thus threat appraisal 'the process by which users assess threats towards themselves, including severity of threat and ones susceptibility to them' (LaRose, Rifon, & Enbody, 2008)□ is particularly relevant to online security behaviours. Behavioural models may explain that risks are not perceived as being severe, nor users perceiving themselves as vulnerable. Perceived self-efficacy in being able to protect the self from harm may also predict whether individuals engage in efforts/ intentions commensurate with secure online behaviour (Lee, Larose, & Rifon, 2008).

The Health Belief model (HBM) is a framework to understand health related behaviours and was developed in the 1950s to explain the lack of participation in preventative healthcare programmes (Rosenstock, 1974)□. It is applicable to addressing risky practices where behaviours

evoke concern. HBM posits that an individual's health related behaviours are dependent on the attitudes and beliefs of the individual with regards to the perceived susceptibility (an individual's belief regarding their chances are of becoming ill), perceived severity (the belief about how serious the illness is and its consequences), perceived benefits (the belief as to how efficacious taking an advised action is on reducing risk associated with illness), perceived barriers (beliefs about the cost of the advised action), cues to action (motivators/ triggers), and self-efficacy (how competent an individual believes he is in successfully taking action).

In assessing the effectiveness of the model Janz and Becker (1984) reviewed previous research and found methodological limitations associated with studies that had employed small convenience samples, used retrospective designs, and not included all dimensions of the HBM in their questionnaires. They also posited that certain behaviours were not necessarily explainable by decision making processes but were in fact influenced by other factors such as habit. Furthermore whilst the model may identify appropriate targets for intervention, the interventions themselves are not outlined. Thus an important component in testing whether causation exists between variables and changes to behaviour is absent.

Despite its limitations, a number of studies (Ng & Xu, 2007;Ng, Kankanhalli, & Xu, 2009; Davinson & Sillence, 2010; Williams, Wynn, Madupalli, Karahanna, & Duncan, 2014; Davinson & Sillence, 2014) have employed this model in researching problematic security behaviours. The model is **particularly useful when seeking to understand decisions taken in a context where no tangible benefits are perceived by the decision maker, and where instead decisions are predicated on taking protective actions to prevent a negative outcome (e.g. use of antivirus software or a VPN).**

The study undertaken by Davinson and Sillence (2014) used interviews to explore the role

of the user's perception and behaviour when conducting financial transactions using technology. This study situated the findings within the framework of the HBM as a way to consider factors associated with changing behaviours. The lack of perceived personal responsibility was said to account for some behaviours regarding perceived severity of fraud/ threat. Convenience was seen as a perceived cost/barrier to protective behaviours, and regular habits were seen as more convenient than having to consider the cost of acting more securely. The study also found that perceived benefits of protective actions were rarely considered.

Using the HBM to explain the risky practice of connecting to public Wi-Fi may also explain how assessments of threats are made, and how users manage risk. Given that barriers/costs are significantly related to outcomes then the inconvenience associated with not connecting to public Wi-Fi may explain why users fail to take preventative measures.

Research Question and Hypotheses

Are individual differences such as impulsivity, privacy proclivity, technical expertise, and cyber-security knowledge associated with the use of public Wi-Fi?

Individuals who are deemed to be more impulsive often do not consider the consequences of their behaviour, act rashly and without deliberation (Whiteside & Lynam, 2001) and seek immediate gratification rather than delayed reward. In this case immediate gratification seeking is fueled by devices and satisfied by public Wi-Fi. Individuals want to exchange information, receive feedback and connect with others in real time. The first hypothesis is:

H1: Individuals who use public Wi-Fi will score higher on measures of impulsivity than those who do not use public Wi-Fi.

Privacy concerned individuals want to protect personal information and take steps to safeguard this protection. Thus those individuals who manage their privacy by restricting access to their personal information and maintaining closed boundaries (Petronio, 2002) will engage less in risky online behaviours. The second hypothesis is:

H2: Individuals who use public Wi-Fi will score lower on privacy measures than those who do not use public Wi-Fi.

Technologically proficient individuals will be more familiar with privacy management online (Boyd & Hargittai, 2010) and are thus less likely to experience negative outcomes (Litt & Hargittai, 2014) The third hypothesis is:

H3: Individuals who use public Wi-Fi will score lower on technical expertise measures than those who do not use public Wi-Fi.

Knowledge of cyber-security has implications for threat/risk assessment and consequent online behaviours (Bada & Sasse, 2014). In the context of public Wi-Fi use those with cyber-security knowledge understand how technology works and are thus cognisant of the inherent risks to personal information. Thus the final hypothesis is:

H4: Individuals who use public Wi-Fi will have less cyber-security knowledge than those who do not use public Wi-Fi.

Method

Research Design

The aim of the research was to ascertain whether particular variables are associated with increased likelihood of use of public Wi-Fi thus the study was correlational in design to assess relationships between and among these variables. A quantitative approach designed to include a wide range of participants was adopted via the administration of self-report questionnaires which tested the hypotheses of predicted relationships outlined by this research. The inclusion of both single scale items and standardised questionnaires provided scores on each variable thereby allowing for predicted associations between the use of public Wi-Fi, and personality traits, technical expertise, and cyber-security knowledge to be tested.

Participants

Participants were recruited to take part in the study by email, via links shared on social media, and at the researcher's workplace (where free Wi-Fi is available to the public). A convenience sample was used. To ensure that cyber-security experts and non-experts were represented in the study a purposive sample of individuals proficient in digital forensics/cyber-security were also specifically invited to participate. A total of 64 survey responses were collected. Participant's mean age was 34.6 years (*SD* = 10.7; range 18-over 65 years). With regard to gender there was an equal number of male and female participants.

Materials

Data was collected using an anonymous questionnaire hosted on the online survey platform Survey Gizmo. Scales pertaining to the measurement of impulsivity, privacy, technical expertise, and cyber-security knowledge were included. Public Wi-Fi use was assessed using a yes/no question: 'Do you used public Wi-Fi on any device? To gauge the frequency of public Wi-Fi use participants were asked how often they used public Wi-Fi from several times per day through to not

at all. Questions pertaining to the reasons for using or for not using public Wi-Fi, location of use, and activities conducted whilst using public Wi-Fi were included (Appendix A).

Participants were also asked whether they understood the technical aspects of how Wi-Fi works, and whether they were concerned about the privacy and security of the information being transmitted over a public Wi-Fi network. Questions regarding awareness of negative outcomes, levels of concern, and responsibilities were also included. Participants were asked about their behaviours, and in particular whether they used VPNs. A question regarding where or from whom participants learned about security/privacy regarding online practices was also included (Appendix B).

To measure impulsivity, the 45 item UPPS scale (Whiteside & Lynam, 2001) was included (Appendix C). This scale assess the four different characteristics affiliated with impulsive behaviour: lack of premeditation, urgency, sensation seeking, and lack of perseverance. Questions in these sub scales were answered from 1 to 4 according to whether participants strongly agree with the statement (1) through to strongly disagreeing with the statement (4). As such, a low overall score in each category indicated low impulsivity for that particular element. Good reliability for these scales was demonstrated in Whiteside and Lynam's (2001) study where the scales were developed (Cronbach's alpha = 0.91, 0.86, 0.90, and 0.82 for lack of premeditation, urgency, sensation seeking, and lack of perseverance respectively). In the current study each of the subscales demonstrated good internal consistency (Cronbach's alpha= 0.87, 0.86, 0.89, and 0.87 for lack of premeditation, urgency, sensation seeking, and lack of perseverance respectively).

To measure privacy this study used the Online Privacy Concern and Protection Scale (Buchanan, Paine, Joinson, & Reips, 2007) which specifically looks at measuring privacy concern as it relates to the internet (Appendix D). That questionnaire uses two scales related to general and

online reported privacy behaviours: General caution (6 questions), and technical protection (6 questions). Participants were asked to answer each question via a 5 point scale. There was also one scale related to privacy attitude when online: Privacy concern (16 questions), and respondents used a 5 point scale to answer. In the 2007 study by Buchanan et al. (2007) where the scales were developed good reliability was demonstrated (Cronbach's alpha= 0.75, 0.74, and 0.93 for general caution, technical protection, and privacy concern respectively). In the current study each of the subscales demonstrated good internal consistency (Cronbach's alpha=0.80, 0.85, and 0.95 for general caution, technical protection, and privacy concern respectively).

Technological expertise was measured by a Web-Use skills instrument (Hargittai & Hsieh, 2012) which asked participants to rate their understanding of 15 internet/computer related terms on a 1 to 5 scale where 1 equates with a low level of understanding and 5 with a higher level of understanding (Appendix E). Overall participants had a good level of technical proficiency as measured by the Web-Use skills instrument (composite score= 3.566).Good reliability (Cronbach's alpha 0.90) was demonstrated for this scale in the study where it was developed (Hargittai & Hsieh, 2012). In the current study the scale demonstrated good internal consistency (Cronbach's alpha 0.97).

Measuring participants' knowledge of cyber-security asked participants to rate their knowledge of cyber -security on a 5 point scale from very knowledgable to very unknowledgeable (Whitty et al., 2015). Overall more than one third of participants rated themselves as knowledgable, just under one third rated themselves as average, and one third thought themselves unknowledgeable about cyber-security.

Procedure

Participating in the study required respondents to click a link that directed them to the

survey gizmo platform where the questionnaire was hosted. A short introduction outlined the purpose of the research, how the data would be used, and the contact details of the researcher and the researcher's supervisor (Appendix F). Participants were informed that the questionnaire results were anonymous and confidential. They then read a consent form (Appendix G) and indicated their consent to participate.

Participants were asked to complete demographic items, public Wi-Fi usage questions, and a question about their level of cyber security knowledge. They then completed the Web-Use skills measure, the UPPS impulsivity scales, and the Online Privacy Concern and Protection scales. Finally participants answered questions regarding their awareness, attitudes, levels of concern, and behaviour with regards to aspects of online privacy and security. Participants were made aware that they were able to withdraw at any stage and have their data removed from the study. On completion participants read a debrief form (Appendix H) which explained the purpose of the study, and included the contact details of the researcher and the researcher's supervisor to facilitate answering any questions about the study. Contact details for the Office of Internet Safety in Dublin were also provided for those participants who were interested in information about secure use of the internet. Finally participants were thanked for their contribution.

A pilot study involving three participants was undertaken to test that the layout of the questionnaire was clear and easy to navigate, and the questionnaire was of an appropriate length to avoid incomplete responses. The pilot study showed that the questionnaire layout on a mobile phone rendered some questions unclear. To rectify this changes were made to the formatting of certain text. A second pilot study was conducted to ensure there were no further ambiguities. The questionnaire did not seek any personal or intrusive details, and ethical approval was granted by the Department of Technology and Psychology Ethics Committee (DTPEC) to carry out this research.

Results

The study showed that the majority of participants (*n* = 49; 77 percent) used public Wi-Fi on any device. Of those over half were frequent users connecting at least once a week (*n*= 27; 55 percent), whilst the remainder were infrequent users connecting once a month or less (*n* = 22; 45 percent). Figure 1 overleaf shows a detailed breakdown of frequency of use.

Once a month or less	44.9%		22
Once a week	16.3%		8
Several times a week	28.6%		14
About once a day	4.1%		2
Several times a day	6.1%		3
		Total	49

Figure 1. Frequency of public Wi-Fi use

Figure 2 below shows the many places participants used public Wi-Fi with hotel/ hostel/ accommodation provider (*n* = 39; 80 percent), cafe/food establishment (*n* = 33; 67 percent), and airport (*n* = 32; 65 percent) being the most popular places to connect.

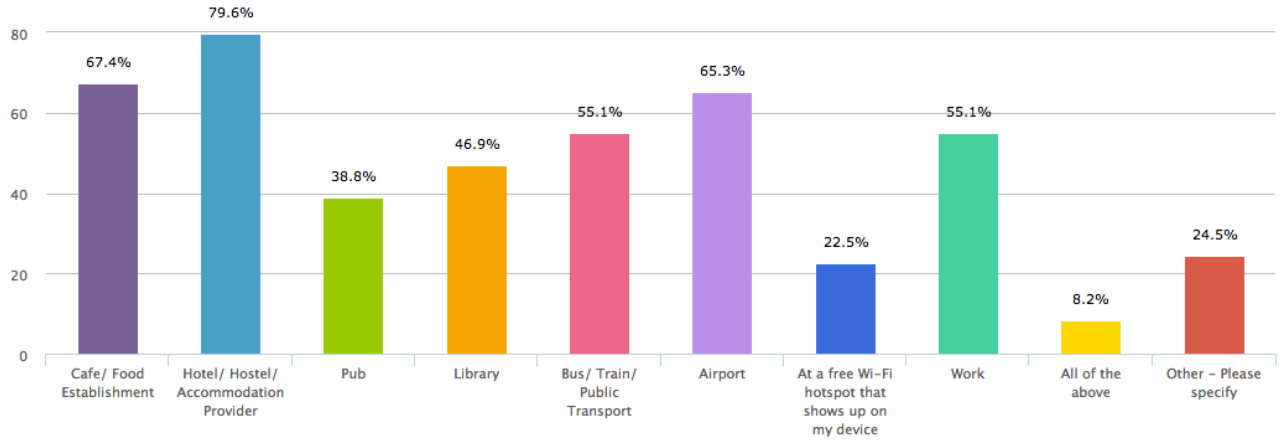


Figure 2. Use of public Wi-Fi at various locations

With regards to the reasons for using public Wi-Fi a majority of participants rated being able to use public Wi-Fi whilst abroad as important to very important (n = 38; 79 percent), and a majority also rated convenience as fairly important to very important (n = 40; 83 percent). Table 1 overleaf shows the level of importance participants ascribed to the various reasons for using free public Wi-Fi.

Table 1.

Reasons for using public W-Fi

	Not Important	Slightly Important	Fairly Important	Important	Very Important
	%	%	%	%	%
I use public Wi-Fi because it is free	16.3	16.3	18.4	32.7	16.3
I have run out of data on my smart phone	28.6	20.4	20.4	14.3	16.3
Because it gives me unlimited access to data	28.6	12.2	18.4	20.4	20.4
It is convenient	8.3	8.3	22.9	29.2	31.3
I can access the internet on the go	10.6	2.1	21.3	29.8	36.2
Roaming is expensive so I use public Wi-Fi	2.1	8.3	10.4	16.7	62.5
I always want to be connected	27.1	16.7	16.7	16.7	22.9

Figure 3 overleaf shows the activities participants engaged in when using public Wi-Fi. Browsing the internet (*n* = 41; 84 percent), using email (*n* = 38; 78 percent), and using social networks (*n* = 36; 74 percent) were the most common activities.

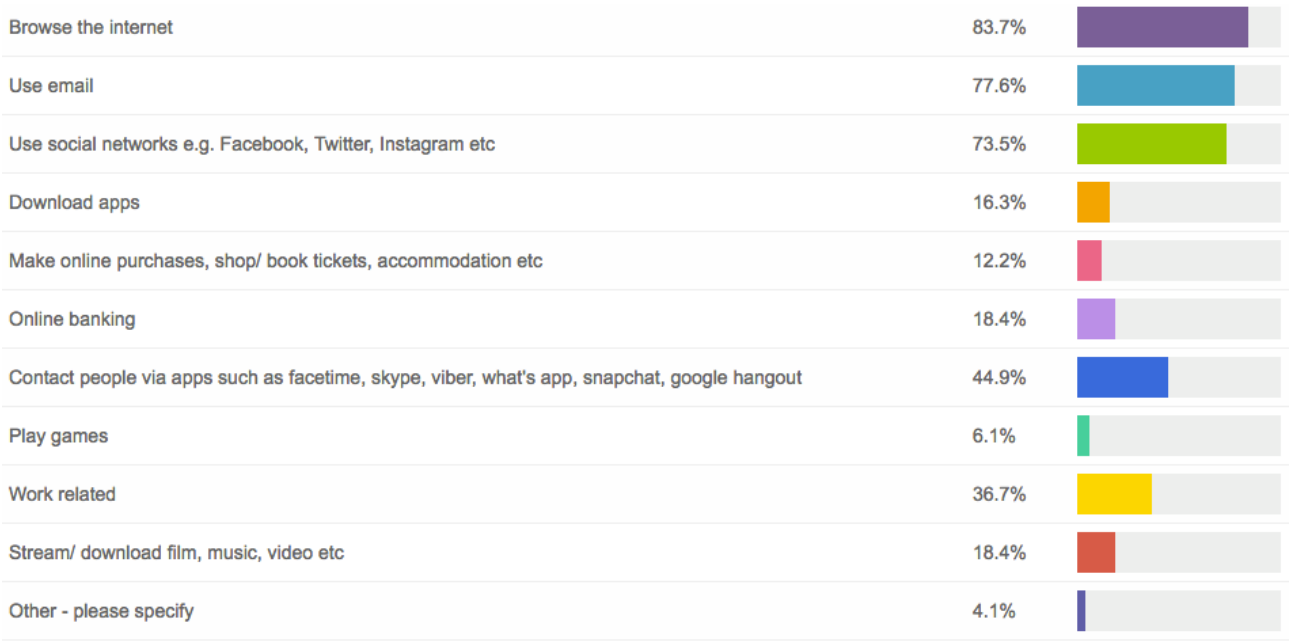


Figure 3. Activities participants engaged in when using public Wi-Fi

Of those participants who did not use public Wi-Fi (*n* = 15), eight (53 percent) cited issues regarding security as their reason not to connect, four (27 percent) said they only used their home Wi-Fi, two (13 percent) cited having unlimited phone data, and one participant (7 percent) cited not owning a smartphone as reasons they did not use public Wi-Fi. Table 2 (below) shows participants concerns about public Wi-Fi, and Table 3 (overleaf) shows their awareness and behaviours regarding public Wi-Fi use.

Table 2.

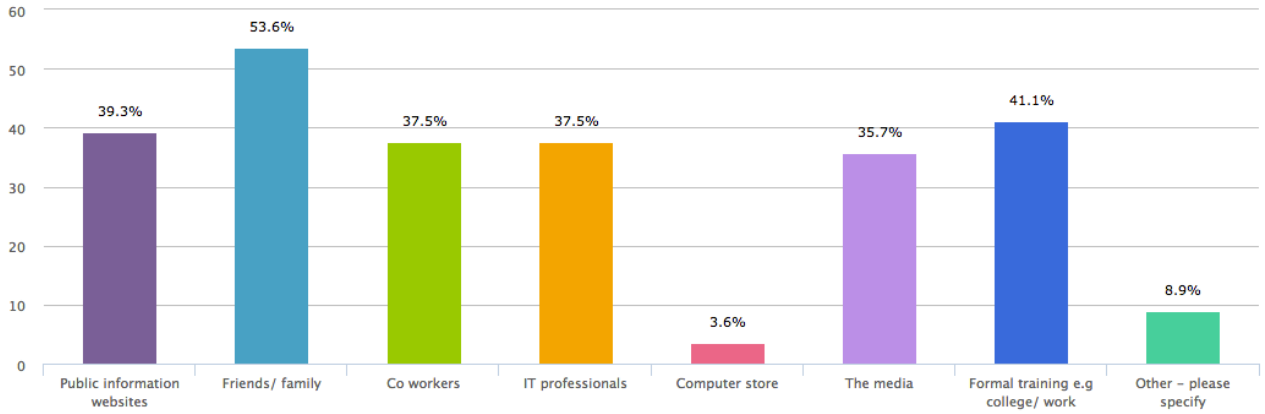
Participants' concerns about public Wi-Fi

When using public Wi-Fi I am concerned about:	Very concerned %	Some what concerned %	Neither concerned or unconcerned %	Not concerned %
The privacy/security of information transmitted	41	41	16	2
Device names being transmitted	43	47	5	5
Previous access points being transmitted	32	40	23	5

Table 3.
Participants' awareness, and behaviours regarding public Wi-Fi use

	Yes %	No %	Don't know %
I understand the technical aspects of how Wi-Fi works	61	39	-
Public Wi-Fi is less secure than home internet connection	88	5	7
Identity theft is a possible outcome	81	3	16
Hacked passwords are a possible outcome	84	5	11
Compromised bank accounts are a possible outcome	76	12	12
Public Wi-Fi network name could be spoofed and pose a security risk	88	9	3
Software tools are available that allow eavesdropping	82	9	9
Names given to devices can be transmitted over the network	91	9	-
Previous Wi-Fi access points can be transmitted over the network	70	30	-
Public Wi-Fi provider is responsible for keeping data secure/private	40	51	9
Password protected public Wi-Fi keeps data secure	14	58	28
I know there are ways to protect privacy when using public Wi-Fi	65	35	-
I name my device with full name	17	83	-
I switch off or disable auto-connectivity on mobile phone	60	28	12
I know what a Virtual Private Network is	59	41	-
I use a Virtual Private Network when using public Wi-Fi	20	80	-

Participants' main source of information about security and privacy issues relating to online practices was friends/ family (n = 30; 54 percent). Figure 4 below shows all sources of information



cited by participants.

Figure 4. Sources of information about security/privacy issues regarding online practices.

With regards to cyber-security knowledge over one third of participants rated themselves as somewhat knowledgeable to very knowledgeable (*n* = 24, 37 percent), one third as somewhat unknowledgeable to very unknowledgeable (*n* = *21*; 33 percent) and the remainder as having average knowledge (*n* = 19; 30 percent) about cyber-security.

With regards to measures for technical proficiency the composite score for Web-Use skills showed participants had a good understanding of computer and internet related terms (see Table 4 below).

Table 4.
Web-Use skills measures

Item	Mode	Mean	SD
Advanced search	4	3.719	1.147
Tagging	5	3.875	1.1339
Preference setting	5	3.578	1.319
PDF	5	4.063	1.097
Spyware	5	3.531	1.247
Tabbed browsing	5	3.203	1.535
Firewall	5	3.734	1.185
Wiki	5	3.571	1.411
JPG	5	3.797	1.405
Weblog	5	3.375	1.464

Podcasting	5	3.875	1.162
Cache	5	3.219	1.538
Malware	5	3.531	1.333
Phishing	5	3.578	1.378
RSS	1	2.844	1.664
Web-use skills (composite score)		3.566	1.335
N	63		
Scale	5-point		

Table 5 below summarises the descriptive statistics for means of the dependent variables broken down by those who had used and not used public Wi-Fi

Table 5.

Dependent variables for Wi-Fi Use

	Users of public Wi-Fi			Non users of public Wi-Fi			All participants	
	M	SD	Mean Rank	M	SD	Mean Rank	M	SD
Cyber-security Knowledge	2.79	1.27	30.23	3.47	1.06	39.90	2.95	1.25
Web-Use Skills	54.10	17.02	33.09	51.27	18.42	30.57	53.44	17.25
Lack of Premeditation	21.79	5.91	33.05	20.40	5.59	28.63	21.46	5.82
Urgency	27.35	7.16	32.01	27.40	6.88	31.97	27.37	7.04
Lack of Perseverance	19.15	6.07	32.70	18.07	4.37	29.77	18.88	5.69
Sensation Seeking	32.15	8.58	32.18	31.73	9.18	31.43	32.05	8.65
General Caution	17.02	4.69	27.04	21.00	5.11	40.87	18.02	5.07
Technical Protection	21.11	5.92	28.70	23.47	5.63	35.90	21.70	5.89
Privacy Concern	56.77	14.31	27.95	63.07	15.84	36.00	58.37	14.83

Impulsivity

The four sub scales; lack of premeditation, urgency, lack of perseverance, and sensation seeking were used to consider impulsivity. As the data was not normally distributed, Mann-Whitney tests were conducted to find out whether there was a statistically significant difference in the four facets of impulsivity between those who used public Wi-Fi and those who did not. No significant differences were found (see Table 6 overleaf) .Therefore H1 was not supported.

Table 6.

Mann-Whitney Test for Impulsivity and Public Wi-Fi Usage

	Lack of Premeditation	Urgency	Lack of Perseverance	Sensation Seeking
Mann-Whitney U	309.500	359.500	326.500	351.500
Wilcoxon W	429.500	479.500	446.500	471.500
Z	-.817	-.008	-.542	-.137
Exact Sig. (1-tailed)	.210	.498	.297	.447

To enable testing for differences regarding frequency of using public Wi-Fi, usage was collapsed from five groups; one a month or less (n = 22), once a week (n = 8), several times a week (n =14), about once a day (n = 2), and several times a day (n =3), into two groups; less frequently (once a month or less) and more frequently (from several times a day to several times a week). There was no statistically significant difference in the four facets of impulsivity for those who used public Wi-Fi less frequently and those who used public Wi-Fi more frequently (see Table 7 below).

Table 7.

Mann-Whitney Test for Impulsivity and Frequency of Public Wi-Fi Usage

	Lack of Premeditation	Urgency	Lack of Perseverance	Sensation Seeking
Mann-Whitney U	379.500	344.000	389.000	432.000
Wilcoxon W	610.500	575.000	620.000	1335.000
Z	-.899	-1.417	-.760	-.131

Exact Sig. (2-tailed)	.374*	.159*	.452*	.899

*Note *p<0.05* one-tailed

Privacy

Privacy was considered using the three sub scales. A Mann-Whitney test was performed to determine whether there was a statistically significant difference in general caution, and technical protection (privacy behaviours) and privacy concern (privacy attitude) between the participants who used public Wi-Fi and those who did not. It was found that the general caution privacy behaviour for the participants who used public Wi-Fi (Mean Rank = 27.04) was statistically significantly lower than the general caution privacy behaviour for the participants who did not use public Wi-Fi (Mean Rank = 40.87, U = 182.000, N_1 = 45, N_2 = *15*, p = .003, one-tailed). Thus H2 was partly confirmed. There was however no statistically significant differences in the other privacy subscales (see Table 8 below) or any difference for all privacy subscales regarding frequency of Wi-Fi use (Table 9 overleaf).

Table 8.

Mann-Whitney Test for Privacy and Public Wi-Fi Usage

	General Caution	Technical Protection	Privacy Concern
Mann-Whitney U	182.000	256.500	240.000
Wilcoxon W	1217.000	1291.500	1230.000
Z	-2.661	-1.386	-1.568
Exact Sig. (1-tailed)	.003	.084	.059

Table 9.

Mann-Whitney Test for Privacy and Frequency of Public Wi-Fi Usage

	General Caution	Technical Protection	Privacy Concern
Mann-Whitney U	346.000	391.000	335.000
Wilcoxon W	556.000	601.000	525.000
Z	-.849	-.142	-.730
Exact. Sig. (2-tailed)	.396	.887	.465

Technical Proficiency

The results of a Mann-Whitney test found that there was no significant statistical difference in technical proficiency between those who used public Wi-Fi and those who did not (U = 338.500, N_1 = 49 , N_2 = 15 , p = .645, two-tailed), or between those who used public Wi-Fi less frequently and those who used it more frequently (U = 397.000, N_1 = 22, N_2 = 42, p = .357, two-tailed), therefore H3 was not supported.

Cyber-security Knowledge

A Mann-Whitney test showed there was a statistically significance difference in cyber-security knowledge between those who used public Wi-Fi (Mean Rank = 30.23) and those who did not use public Wi-Fi (Mean Rank = 39.90, U = 256.500 , N_1 = 49, N_2 = 15, p = .035, one-tailed). Thus H4 was supported. There was no significant statistical difference between those who used public Wi-Fi less frequently and those who used it more frequently (U = 387.500, N_1 = 22, N_2 = 42, p = .278, two-tailed).

Discussion

In assessing whether there are particular individual differences that correlate with the decision to connect to public Wi-Fi this study measured participant's impulsivity, privacy proclivity, technical expertise, and cyber-security knowledge, and found that those who were generally cautious in their privacy behaviours, and those who had a greater knowledge of cyber-security were significantly less likely to be users of public Wi-Fi.

With regards to the first hypothesis participants who used public Wi-Fi were not found to be more impulsive than those who did not use public Wi-Fi. The presumption that those who acted without deliberation and made decisions on the spur of the moment, and whose poor impulse control would see them succumb to the immediate gratification provided by public Wi-Fi was not supported. Perhaps instead of impulsivity, those behaviors associated with acting without forethought may relate to habit and the routine nature of connecting to public Wi-Fi. Klasnja et al. (2009), for example, posited that the routine habit of connecting to free public Wi-Fi meant that risks were not consciously considered.

Those who already did more in general to protect their privacy by behaving cautiously were less inclined to be users of public Wi-Fi thus partially supporting the second hypothesis. It appears that other participants were willing to accept some loss of privacy as a cost of connecting to the network. This trade off between convenience and privacy/security predicates an awareness and assessment of the risks involved in using public Wi-Fi, and highlights a disjunction between attitudes and actual behaviour. The findings support previous research about privacy online whereby pre-existing attitudes/general privacy disposition were not found to mediate behaviour (Joinson et al., 2010).

Those who did not use public Wi-Fi were not found to be any more technically proficient according to Web-Use skills scores than those who used public Wi-Fi thus leading to the rejection of the third hypothesis. This is contrary to findings from other research (Boyd & Hargittai, 2010; Litt & Hargittai, 2014) where internet skills were deemed necessary for the successful management of online privacy and the minimisation of online turbulence (Petronio, 2002).The results of this study are however more in accordance with studies such as Campbell et al. (2007) that show that the more experienced users are the more they discount risks due to unrealistic optimism.

To explain these conflicting studies it is worth considering whether technical proficiency is more related to the successful management of privacy when disclosure of personal information is in the context of a perceived audience (such as on social networking sites) and can result in immediate, tangible negative outcomes. Thus being familiar with technology would help users navigate privacy settings successfully. In contrast, those situations were an audience is not perceived, when there is an estimation that there is a low probability of negative outcomes, and where there is no immediate feedback with regards to privacy violations (such as when using public Wi-Fi), more familiarity with the technology may not result in a better understanding of how to use it to protect privacy and remain secure.

Participants who had more knowledge of cyber-security were less likely to be users of public Wi-Fi thus confirming the fourth hypothesis. This disagrees with the findings of Whitty et al's. (2015) study where cyber-security knowledge did not distinguish between those who shared passwords and those who did not, but aligns with Dinev and Hu's (2007) contention that threat awareness is a strong predictor of engaging in protective security behaviours. Given that a purposive sample of individuals' formally trained in cyber-security/digital forensics were invited to participate in this study these results may be explained by it being normative/routine for them to

maintain jurisdiction over their information (Petronio 2002) given their knowledge of risk and their practical application of this knowledge.

Although studies (Klasnja et al., 2009; Swanson et al., 2010) have found that the threat models developed by users of public Wi-Fi emanate from their lack of understanding of how Wi-Fi actually works, participants in this study reported understanding the technical aspects of the workings of Wi-Fi. Thus given this awareness of risk use can be made of the HBM as a framework to guide the findings and to explain public Wi-Fi security behaviour in terms of threat severity, susceptibility, barriers and benefits.

In this study and in others (e.g.,Davinson & Sillence, 2014) it appears that whilst participants were aware of the risks associated with engaging in certain online behaviours the decision to engage implies that these threats were not considered to be severe or users susceptible to them. The longer users engaged in these behaviours (using public Wi-Fi) without experiencing negative outcomes (data breaches, turbulence) the more likely they were to believe that negative outcomes would not happen to them. Understanding the perceived barriers (such as convenience), and the intangible nature of the perceived benefits (protection of personal information or prevention of threats to privacy/security rather than an actual reward) together with how confidently individuals manage threats and what cues precipitate action can help to explain individuals' behaviour with regards to risk.

Practical and Theoretical Implications

The implications of these findings are that it is not enough to simply make individuals aware that there are security and privacy issues inherent in the decision to use public Wi-Fi. Even individuals who express concern about these insecurities and whose intention it is to protect their own information often trade privacy and security for convenience, are subject to optimism bias, or

know better but do differently. Hence any education or awareness initiatives need to find a way to not only inform but to translate this information into action to enact behavioural change.

Understanding users and the decisions they make regarding risk is the first step in this process. Instead of being purely rational decision makers, individuals are influenced by context/situation, past experiences, and automatic behaviours. Whilst these behaviours may not be attributable to acting on impulse they may perhaps be a product of the influence of habit and social norms. In this study those who decided not to use public Wi-Fi were those who were not only aware of risk but already practiced privacy and security cautious behaviours. Rather than only being concerned about security and privacy these individuals had made an assessment of risk based on knowledge and were behaving in ways commensurate with their security concerns and privacy proclivity.

Optimism bias (Weinstein,1980), and user omissive behaviour (Cox, 2012) may explain why despite reporting concerns about the privacy and security of personal information accessible over public Wi-Fi the majority of participants did not engage in selfprotective behaviours (such as not using public Wi-Fi or using a VPN to connect). Similar results were found by Swanson et al. (2010) where Wi-Fi users who were shown information that could be captured did not change their behaviour. Optimism bias means that individuals do not enact privacy protective behaviours and engage in more risky behaviours as negative outcomes are perceived to more be applicable to others than to themselves. Those participants who had the ability to protect themselves because of awareness and skill (those who scored highly on the Web-Use skills scale, and the technical protection privacy scale) may have experienced optimism bias as a result of familiarity of engaging in behaviours that up to that point had resulted in no negative outcomes thus allaying any concerns. According to Aytes and Connolly (2005)□ those engaged in risky behaviour are rewarded (in terms of convenience) each time they experience no negative outcomes.

According to CPM (Petronio, 2002)□ generally cautious individuals who did not use public Wi-Fi were likely to be those who already regulate/control their privacy by having closed privacy boundaries and who behave in ways that minimise the possibility of turbulence. For these individuals privacy rules are not influenced by context nor are trade-offs made to attain goals. In contrast individuals who scored highly on measurements of privacy concern, and on technical protection still used public Wi-Fi thus suggesting that their privacy boundaries allowed significant access to their private information or that the catalyst for changing their rules of privacy management was situation specific and contingent on decisions regarding risk versus benefit (Child & Petronio, 2011).

Limitations and Strengths of the Research

The methodological limitations of this study are the small sample size, and the possibility that some questions regarding knowledge of and concern about the risks associated with using public Wi-Fi may be biased by participants providing socially desirable responses. Furthermore given the dichotomy that often exists between attitude and behaviour, limitations exist for research that relies solely on self-report measures but does not test associated behaviours. Instead employing observational techniques in conjunction with surveys (as suggested by Joinson et al., 2010),□ or taking an experimental approach (as theorised by Acquisti et al., 2003)□ would help to distinguish between behavioural intention and actual behaviour.

According to Wiederhold (2014) 'understanding the behavioural economics governing people's perception of risk and reward...also identifying social situations in which individuals demonstrate a higher tendency to discount the risk of sharing private information' (p.131) helps to precipitate a move towards greater security conscious behaviour. Thus this study's strength is in identifying types of individuals more likely to engage in the risky behaviour of using public Wi-Fi and offering explanations as to why risk is discounted.

Future Research

Future research that attempts to understand why individuals engage in the insecure behaviour of using public Wi-Fi could look at the role of habitual behaviour and the influence of social norms to assess the extent to which connecting to public Wi-Fi using a VPN for example could be established as a social norm. Research could also assess whether personal responsibility plays a role in adopting protective security behaviours with regards to public Wi-Fi. Forty percent of this study's participants for example reported that the responsibility for protecting them whilst using public Wi-Fi was that of the network providers. Studies have shown that internet users abdicate personal responsibility with regards to internet safety (Larose & Riffon 2007; Lee & Kozar, 2008). Measuring participants locus of control (LOC) could help to explain the knowing-doing gap in terms of how responsible individuals feel for their actions regarding using public Wi-Fi. Those with external LOC may consider responsibility for security behaviours to rest with others.

Conclusion

This study looked at participants' behaviours regarding their use or non-use of public Wi-Fi to assess whether there were individual differences that correlated with the decision to connect. Those who were generally more cautious in their privacy behaviours, and those who had a better knowledge of cyber-security were found to be less likely to engage in risky behaviours. Findings also highlighted the dichotomy between users' concerns about privacy and security and their actual behaviours.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21–29). ACM. Retrieved from http://www.csl.mtu.edu/cs6461/www/Reading/Acquisti04.pdf

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3, pp. 1–27).

Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective. *Advanced Topics In End User Computing*, *4*, 257. Retrieved from http://www.researchgate.net/profile/Terry_Connolly/publication/220068606_Computer_Security_and_Risky_Computing_Practices_A_Rational_Choice_Perspective/links/0046352fd2529d65a6000000.pdf

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns Why do they fail to change behaviour? Global Cyber-security Capacity Centre: Draft working paper. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf

Boyd, Danah, & Hargittai, Eszter. (2010). Facebook privacy setting: who cares? *First Monday*, *15*. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. Retrieved from https://www.researchgate.net/profile/Ulf-Dietrich_Reips/publication/235767360_Development_of_measures_of_online_privacy_concer

n_and_protection_for_use_on_the_Internet/links/09e415092a686a1379000000.pdf

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284.

Cheng, N., Wang, X., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013). Characterizing privacy leakage of public wifi networks for users on travel. In *INFOCOM, 2013 Proceedings IEEE* (pp. 2769–2777). IEEE. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.384.7503&rep=rep1&type=pdf

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. *Computer-Mediated Communication in Personal Relationships*, 21–40. Retrieved from http://www.heinz.cmu.edu/~acquisti/SHB2015/Petronio.pdf

Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010). The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In *Proceedings of the 12th ACM international conference on Ubiquitous computing* (pp. 321–330). ACM.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. doi:10.1016/j.chb.2012.05.003

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747. doi:10.1016/j.chb.2010.06.023

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), 154–168.

Deloitte (2015). *Global Mobile Consumer Survey: US edition The Rise of the always connected*

consumer. Retrieved from http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html?id=us:

Dickman, S. J. (1990). Functional and dysfunctional impulsivity: personality and cognitive correlates. *Journal of Personality and Social Psychology*, *58*(1), 95.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies*. *Journal of the Association for Information Systems*, *8*(7), 386.

Dutton, W. H. (2014a). Fostering a Cyber-security Mindset. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CybersecurityMindsetDraftWorkingPaper.pdf

Dutton, W. H. (2014b). *Professor William Dutton - Cyber security, culture and attitudes within society.* Retrieved from https://www.sbs.ox.ac.uk/cyber-security-capacity/content/professor-william-dutton-cyber-security-culture-and-attitudes- within-society

Europol. (2014). *Cybercrime: A growing global problem.* Retrieved from (https://www.europol.europa.eu/ec/cybercrime-growing)

Evenden, J. L. (1999). Varieties of impulsivity. *Psychopharmacology*, *146*(4), 348–361. Retrieved from ftp://pop3.infomus.org/pub/CuesImpulsivita/Varieties_Evenden.pdf

F-Secure. (2104). *Tainted Love: How Wi-Fi betrays us.* Retrieved from https://fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f- secure.pdf

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on World Wide Web companion* (pp. 737–744). International World Wide Web Conferences Steering Committee.

Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science*

Computer Review, 30(1), 95–107.

Harris, L., & Westin, A. F. (1998). E-commerce and privacy: What net users want. *Privacy and American Business, Hackensack, NJ*.

Ipass. *Wi-Fi growth map.* Retrieved from http://www.ipass.com/Wi-Fi-growth-map/index.html

Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health Education & Behavior*, *11*(1), 1–47. Retrieved from http://deepblue.lib.umich.edu/bitstream/handle/2027.42/66877/10.1177_109019818401100101.pdf?sequence=2&isAllowed=y

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In Joinson, A. (Ed.), *Oxford Handbook of Internet Psychology* (pp.237-252). Oxford University Press.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1–24.

Kando-Pineda, C. (2015). *Hotel Wi-Fi weigh the risk. Retrieved* from http://www.consumer.ftc.gov/blog/hotel-wi-fi-weigh-risk

Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D., & Jay, T. (2008). Measuring trust in wi-fi hotspots. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 173–182). ACM.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1993–2002). ACM. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.147.6267&rep=rep1&type=pdf

Konings, B., Bachmaier, C., Schaub, F., & Weber, M. (2013). Device names in the wild: Investigating privacy risks of zero configuration networking. In *Mobile Data Management*

(MDM), 2013 IEEE 14th International Conference on (Vol. 2, pp. 51–56). IEEE. Retrieved from http://www.uni-ulm.de/fileadmin/website_uni_ulm/iui.inst.100/institut/Papers/Prof_Weber/2013-PriSMO-device-names-zeroconf.pdf

Kowitz, B., & Cranor, L. (2005). Peripheral privacy notifications for wireless networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 90–96). ACM. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1042&context=isr

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51LaRose*,(3), 71–76. Retrieved from http://www.researchgate.net/profile/Robert_Larose/publication/220420053_Promoting_personal_responsibility_for_internet_safety/links/02bfe512259767478e000000.pdf

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454.

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior*, *36*, 520–529. doi:10.1016/j.chb.2014.04.027

Mayhorna, C. B., Welka, A. K., Zielinska, O. A., & Murphy-Hill, E. (2015). Assessing Individual Differences in a Phishing Detection Task. In *Proceedings 19th Triennial Congress of the IEA* (Vol. 9, p. 14). Retrieved from http://ergonomics.uq.edu.au/iea/proceedings/Index_files/papers/230.pdf

National Cyber Security Alliance. (n.d.) *Stay Safe Online: Learn how to protect yourself, your family and your devices with these tips and resources.* Retrieved from https://www.staysafeonline.org/stay-safe-online/

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A

health belief perspective. *Decision Support Systems, 46*(4), 815–825. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.3377&rep=rep1&type=pdf

Ng, B.-Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 Proceedings*, 45. Retrieved from: http://beta.orionsshoulders.com/Resources/articles/26_18504_%20().PDF

O'Connell, R. & Kirwan, G. (2014). Protection motivation theory and online activities. In Power, A. & Kirwan, G. (Eds), *Cyberpsychology and New Media: A thematic Reader* (pp.139-148). Hove/New York: Psychology Press.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?.*Information Management & Computer Security*,*20*(1), 18-28.

Petronio, S. (2002). Boundaries of privacy. *State University of New York Press, Albany, NY*.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education & Behavior*, *2*(4), 328–335.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Simmons, D. (2014). *Free wi-fi hotspots pose data risk, Europol warns.* Retrieved from http://www.bbc.co.uk/news/technology-26469598

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38–47). ACM. Retrieved from http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf

Swanson, C., Urner, R., & Lank, E. (2010). Naïve Security in a Wi-Fi World. In *Trust Management*

IV (pp. 32–47). Springer. Retrieved from http://opendl.ifip-tc6.org/db/conf/ifiptm/ifiptm2010/SwansonUL10.pdf

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244.

Taylor, H. (2003). Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. *The Harris Poll, 17*(19), 44. Retrieved from: http://media.theharrispoll.com/documents/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf

US-Cert United States Computer Emergency Readiness Team. (n.d).*Tips.* Retrieved from https://www.us-cert.gov/ncas/tips

Whiteside, S. P., & Lynam, D. R. (2001). The five factor model and impulsivity: Using a structural model of personality to understand impulsivity. *Personality and Individual Differences*, *30*(4), 669–689.

Whiteside, S. P., Lynam, D. R., Miller, J. D., & Reynolds, S. K. (2005). Validation of the UPPS impulsive behaviour scale: a four- factor model of impulsivity. *European Journal of Personality*, *19*(7), 559–574.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(3), 131–132.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational and End*

User Computing (JOEUC), *26*(3), 23–46.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816.

Appendix A

Demographic and Public Wi-Fi Usage Questions

This part of the survey asks you to answer some general questions to do with you and your technology usage:

1. Please indicate what age you are:

- 18- 24
- 25-34
- 35-44
- 45-54
- 55-64
- Over 65

2.What is your Gender

- Male
- Female

3. Please answer the following question by choosing between 1 to 5

	Very unknowledgeable	Somewhat unknowledgeable	Average	Somewhat knowledgable	Very knowledgable
How would you rate your knowledge of cyber-security matters	1	2	3	4	5

4. Do you use Public Wi-Fi on any device (e.g. smart phone, laptop, tablet)?

☐ Yes

- No

5. If yes please indicate where you use Public Wi-Fi (select as many as are applicable)

☐ Cafe/ Food Establishment
- Hotel/ Hostel/Accommodation Provider
- Pub
- Library
- Bus/ Train

☐ Airport
☐ At a free Wi-Fi Hotspot that shows up my device
☐ Work
☐ Other. Please specify _____

6.How often do you use Public Wi-Fi?

- I don't use free public Wi-Fi.
- Once a month or less
- Once a week
- Several times a week
- About once per day
- Several times a day

7.Below are a number of statements describing reasons people may use public Wi-Fi.
For each statement please use the scale provided to indicate how important each reason is for you regarding your use of free public Wi-Fi

	Not Important	Slightly Important	Fairly Important	Important	Very Important
I use public Wi-Fi because it is free	1	2	3	4	5
I have run out of my data allowance on my smart phone	1	2	3	4	5
Because it gives me unlimited access to	1	2	3	4	5

data

It is convenient	1	2	3	4	5
I can access the internet on the go	1	2	3	4	5
When I'm in a different country roaming is expensive so I use public Wi-Fi	1	2	3	4	5
I always want to be connected	1	2	3	4	5

If there are other reasons you use free public Wi-Fi please outline them here

_____

8. If you don't use Public Wi-Fi which of the following best describes why?

- I don't have a smart phone
- I don't have a laptop/ tablet
- ☐ I have an unlimited data plan on my phone
- I use only my home Wi-Fi
- Issues regarding security
- ☐ Other _____

9. When connected to Public Wi-Fi which of the these activities describes what you do (select multiple if appropriate)

- Browse the internet
- Use Email
- Use Social Networks e.g. Facebook, Twitter, Instagram
- Download Apps
- ☐ Make inline purchases, shop/ Book tickets, accommodation etc
- Online Banking
- Contact people via apps such as Facetime, Skype, Viber, What's App, Snapchat
- Play Games
- Work related

- Stream/ Download film, tv, music, video

Appendix B

Awareness, Concerns, and Behaviours Regarding Public Wi-Fi Use

1.Would you say you understand the technical aspects of how Wi-Fi works?

- Yes
- No

2.Are you concerned about the privacy or security of the information being transmitted over a Public Wi-Fi network?

- Very Concerned
- Somewhat concerned
- Neither concerned nor unconcerned
- Not concerned

3.Please indicate whether you agree or disagree with the following statement:

Public Wi-Fi is less secure than my home internet connection

- Agree
- Disagree
- Don't Know

4. Please indicate if you think any of the following are possible outcomes of using Public Wi-Fi

(a) Identity theft

☐ Yes
☐ No
☐ Don't know

(b) Passwords being hacked

☐ Yes
☐ No
☐ Don't know

(c) Compromised bank accounts

☐ Yes
☐ No
☐ Don't know

5.Do you switch off or disable auto connectivity on your smart phone?

- Yes
- No
- I don't know what auto connectivity is
- I don't use a smart phone

6.Do you think that a Public Wi-Fi name (e.g. Central Cafe's Wi-Fi) could be spoofed and pose a security risk for you?

- Yes
- No
- I don't care

7. Do you think there are software tools available that allow other people to eavesdrop and intercept your data (e.g. log ins and passwords) when you are connected to Public Wi-Fi?

- Yes
- No

☐ I don't care

8. Do you name your device (e.g. your smart phone, tablet, laptop) with your full name? (e.g. John Citizen's iphone)

☐ Yes

- No

9. Do you think that this information could be transmitted over a Public Wi-Fi network?

- Yes
- No

10. How concerned would you be about this?

- Very Concerned
- Somewhat concerned
- Neither concerned nor unconcerned
- Not concerned

11. Do you think that a list of your previous Wi-Fi access point (e.g. Home, work, cafe, airport) could also be transmitted over a Public Wi-Fi network?

- Yes
- No

12. How concerned would you be about this?

- Very Concerned
- Somewhat concerned
- Neither concerned nor unconcerned
- Not concerned

13.Please indicate whether you agree/disagree with the following statements:

(a) It is the responsibility of the Public Wi-Fi provider to make sure I'm safe, my data is secure and remains private when I'm connected to the internet using their Wi-Fi

☐ Agree

- Disagree
- Don't know

(b) Accessing Public Wi-Fi that is password protected keeps my data secure

- Agree
- Disagree
- Don't Know

14. Do you think that there are ways to protect your privacy and security when using Public Wi-Fi?

- Yes
- No

15. Do you know what a Virtual Private Network (VPN) is?

- Yes
- No

16. Do you use a Virtual Private Network when connecting to the internet via Public Wi-Fi?

- Yes
- No

17. Where or from whom do you learn about security/privacy issues regarding online practices? (Select multiple if appropriate)

- Public Information websites
- Friends/ family
- Co workers

- IT Professionals
- Computer store
- The media
- Formal training e.g. work/college
- Other. Please specify _____

Appendix C

UPPS Impulsive Behaviour Scale

(Whiteside & Lynam, 2001)

The instructions accompanying the scales were '*Below are a number of statements that describe ways in which people act and think. For each statement, please indicate how much you agree or disagree with the statement. If you* ***Agree Strongly*** *circle* ***1****, if you* ***Agree Somewhat*** *circle* ***2****, if you* ***Disagree somewhat*** *circle* ***3****, and if you* ***Disagree Strongly*** *circle* ***4****. Be sure to indicate your agreement or disagreement for every statement below.'*

	Agree Strongly	Agree Some	Disagree Some	Disagree Strongly
1. I have a reserved and cautious attitude toward life	1	2	3	4
2. I have trouble controlling my impulses.	1	2	3	4
3. I generally seek new and exciting experiences and sensations.	1	2	3	4
4. I generally like to see things through to the end	1	2	3	4
5. My thinking is usually careful and purposeful.	1	2	3	4
6. I have trouble resisting my cravings (for food, cigarettes, etc.)	1	2	3	4
7. I'll try anything once.	1	2	3	4

8. I tend to give up easily	1	2	3	4
9. I am not one of those people who blurt out things without thinking.	1	2	3	4
10. I often get involved in things I later wish I could get out of.	1	2	3	4
11. I like sports and games in which you have to choose your next move very quickly.	1	2	3	4
12. Unfinished tasks really bother me.	1	2	3	4
13. I like to stop and think things over before I do them.	1	2	3	4
14. When I feel bad, I will often do things I later regret in order to make myself feel better now.	1	2	3	4
15. I would enjoy water skiing	1	2	3	4
16. Once I get going on something I hate to stop	1	2	3	4
17. I don't like to start a project until I know exactly how to proceed	1	2	3	4
18. Sometimes when I feel bad, I can’t seem to stop what I	1	2	3	4

am doing even though it is making me feel worse				
19. I quite enjoy taking risks	1	2	3	4
20. I concentrate easily.	1	2	3	4
21. I would enjoy parachute jumping	1	2	3	4
22. I finish what I start	1	2	3	4
23. I tend to value and follow a rational, “sensible” approach to things	1	2	3	4
24. When I am upset I often act without thinking	1	2	3	4
25. I welcome new and exciting experiences and sensations, even if they are a little frightening and unconventional.	1	2	3	4
26. I am able to pace myself so as to get things done on time.	1	2	3	4
27. I usually make up my mind through careful reasoning.	1	2	3	4
28. When I feel rejected, I will often say things that I later regret.	1	2	3	4
29. I would like to learn to fly an airplane.	1	2	3	4

30. I am a person who always gets the job done.	1	2	3	4
31. I am a cautious person.	1	2	3	4
32. It is hard for me to resist acting on my feelings.	1	2	3	4
33. I sometimes like doing things that are a bit frightening.	1	2	3	4
34. I almost always finish projects that I start.	1	2	3	4
35. Before I get into a new situation I like to find out what to expect from it.	1	2	3	4
36. I often make matters worse because I act without thinking when I am upset.	1	2	3	4
37. I would enjoy the sensation of skiing very fast down a high mountain slope.	1	2	3	4
38. Sometimes there are so many little things to be done that I just ignore them all.	1	2	3	4
39. I usually think carefully before doing anything.	1	2	3	4
40. Before making up my mind, I consider all the advantages and disadvantages	1	2	3	4

41. In the heat of the argument, I will often say things I later regret.	1	2	3	4
42. I would like to go scuba diving	1	2	3	4
43. I always keep my feelings under control	1	2	3	4
44. I would enjoy fast driving.	1	2	3	4
45. Sometimes I do impulsive things that I later regret.	1	2	3	4

Appendix D

Measures Of Online Privacy Concern And Protection

(Buchanan, Paine, Joinson, & Reips, 2007)

The instructions accompanying these scales were '*For this part of the survey, we are interested in your privacy related behavior in general and when online. Please answer every question using the full scale provided.'*

General Caution	Never	Rarely	Sometimes	Very Often	Always
1. Do you shred / burn your personal documents when you are disposing of them?	1	2	3	4	5
2. Do you hide your bank card PIN number when using cash machines / making purchases?	1	2	3	4	5
3. Do you only register for websites that have a privacy policy?	1	2	3	4	5
4. Do you read a website's privacy policy before you register your information?	1	2	3	4	5
5. Do you look for a privacy certification on a website before you register your information?	1	2	3	4	5
6. Do you read license agreements fully before you agree to them?	1	2	3	4	5
Technical Protection					
1. Do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in	1	2	3	4	5

or opt-out of certain offers)?

2. Do you remove cookies?	1	2	3	4	5
3. Do you use a pop up window blocker?	1	2	3	4	5
4. Do you check your computer for spy ware?	1	2	3	4	5
5. Do you clear your browser history regularly?	1	2	3	4	5
6. Do you block messages / emails from someone you do not want to hear from?	1	2	3	4	5

The instructions accompanying this scale were *'For this part of the survey, we are interested in any privacy concerns you might have when online. Please answer every question using the full scale provided.'*

Privacy Concern	Not at all	Slightly	Somewhat	Moderately	Very Much
1. In general, how concerned are you about your privacy while you are using the internet?	1	2	3	4	5
2. Are you concerned about online organisations not being who they claim they are?	1	2	3	4	5

3. Are you concerned that you are asked for too much personal information when you register or make online purchases?	1	2	3	4	5
4. Are you concerned about online identity theft?	1	2	3	4	5
5. Are you concerned about people online not being who they say they are?	1	2	3	4	5
6. Are you concerned that information about you could be found on an old computer?	1	2	3	4	5
7. Are you concerned who might access your medical records electronically?	1	2	3	4	5
8. Are you concerned about people you do not know obtaining personal information about you from your online activities?	1	2	3	4	5
9. Are you concerned that if you use your credit card to buy something on the internet your credit card number will obtained / intercepted by someone else?	1	2	3	4	5
10. Are you concerned that if you use your credit card to buy something on the internet your card will be mis charged?	1	2	3	4	5
11. Are you concerned that an email you send may be read by someone else besides the person you sent it to?	1	2	3	4	5
12. Are you concerned that an email you send someone may be inappropriately forwarded to others?	1	2	3	4	5
13. Are you concerned that an email you send someone					

may be printed out in a place where others could see it?	1	2	3	4	5
14. Are you concerned that a computer virus could send out emails in your name?	1	2	3	4	5
15. Are you concerned about emails you receive not being from whom they say they are?	1	2	3	4	5
16. Are you concerned that an email containing a seemingly legitimate internet address may be fraudulent?	1	2	3	4	5

Appendix E

WEB-USE SKILLS INSTRUMENT

(Hargittai & Hsieh, 2012)

How familiar are you with the following computer and internet-related terms?
Please choose a number between 1 and 5 where 1 represents “no understanding” and 5 represents “full understanding” of the item.

	Understanding Scale				
	None	Little	Some	Good	Full
Advanced search	1	2	3	4	5
Tagging	1	2	3	4	`5
Preference setting	1	2	3	4	5
PDF	1	2	3	4	5
Spyware	1	2	3	4	5
Tabbed browsing	1	2	3	4	5
Wiki	1	2	3	4	5
JPG	1	2	3	4	5
Weblog	1	2	3	4	5
Podcasting	1	2	3	4	5
Cache	1	2	3	4	5
Malware	1	2	3	4	5
Phishing	1	2	3	4	5
RSS	1	2	3	4	5

Appendix F

Information Sheet

Study Title:

Personality and Technology Use

Invitation

This study is part of the Masters in Cyberpsychology research project in the Department of Technology and Psychology, Faculty of Film, Art and Creative Technologies, Dun Laoghaire Institute of Art, Design and Technology (IADT). You are being invited to consider participating in this research study. This project is being conducted by Angela Ryan a Cyberpsychology Masters student.

Before you decide whether or not you wish to take part, it is important for you to understand why this research is being done and what it will involve. Please take time to read this information carefully and discuss it with friends and relatives if you wish. Ask if there is anything that is unclear or if you would like more information.

Purpose of the Research

This study seeks to examine the relationship between personality and the use of certain technologies.

Do I have to take part?

You are free to decide whether you wish to take part or not. If you do decide to take part you will be asked to sign a consent form. You are free to withdraw from this study at any time and without giving reasons. If you are a student the decision to take part or not take part will have no impact on

your marks, assessment or future studies.

If I take part, what do I have to do?

You will be asked to fill in a questionnaire as best you can.

The questionnaire is composed of 113 short questions and you respond by ticking a box or circling an answer. It should take less than 30 minutes to complete.

What are the risks/ benefits of taking part?

There are no conceivable physical or psychological risks associated with this study.

Your response will help to gain a better insight into personality and technology use.

How will information about me be used?

The data will be used in a final year Research thesis of a Master of Science in Cyberpsychology course. The data may also be published in an academic journal. Data will be retained for a period of 1 to 5 years depending on if the report is published in an academic journal.

Who will have access to information about me?

Data will be stored securely on a password protected laptop and all responses are confidential and will be anonymously reported.

What will happen to the results of the study?

As previously indicated, this research is being conducted as a final year major research project for a Masters in Cyberpsychology at Dun Laoghaire Institute of Art, Design and Technology. The results of this research will be available to IADT students and staff through the college library. The research may also potentially be published in an academic journal or book. Only the researcher and their supervisor will have access to data not included in the final report. The final printed report will

not include any data that is traceable to you. For a copy of the report please email Angela Ryan at N00134834@student.iadt.ie

Who has reviewed the study?

This study has been approved by the Department of Technology and Psychology Ethics Committee (DTPEC).

What if there is a problem?

If you have a concern about any aspect of this study, you may wish to speak to the researcher who will do their best to answer your questions. You should contact Angela Ryan or her supervisor via the contact information provided below.

Contact for further information

Please feel free to contact us if you have any queries whatsoever.

Researcher:	Supervisor
Angela Ryan Email N00134834@student.iadt.ie	Dr. Grainne Kirwan Email Grainne.Kirwan@iadt.ie
Phone 0851411197	

Thank you for taking the time to read this information sheet and consider taking part in this study.

Appendix G

Consent Form

CONSENT FORM

Personality and Technology Use.

Researcher: Angela Ryan

Consent to participate in study:

I have read the Information Sheet and I consent to take part in this study.

I understand that I can withdraw from the study at any time without giving a reason and that my data will be withdrawn also.

I can skip any question I do not wish to answer and that all information collected will be entirely anonymous and confidential.

I agree to allow the data to be used for future research projects.

Please indicate your consent to participate.

☐ **I agree**

Appendix H

Debrief Form

Thank you very much for taking part in this research study.

According to Europol there has been 'an increase in the misuse of Wi-Fi in order to steal information, identity or passwords and money from the users who use public or insecure wi-fi connections' (Oerting as cited in Simmons, 2014). Cybersecurity focusses mainly on technology yet factoring the human into the cybersecurity equation is of fundamental importance in developing and maintaining secure systems (Wiederhold, 2014).

The study in which you just participated was designed to investigate if there are certain kinds of people who are more likely to use Free Public Wi-Fi based on factors such as personality traits, privacy proclivity, technical proficiency, and cybersecurity knowledge. This could have implications for tailoring awareness and safety campaigns attempting to promote safer cybersecurity practices.

If you have questions about this study or you wish to have your data removed from the study, please contact me at the following e-mail address: N00134834@student.iadt.ie
Alternatively, you may contact my supervisor: Grainne.Kirwan@iadt.ie
If you have been affected by the content of this study in any way, the organisation below may be of assistance:

The Office Of Internet Safety	01 6028258
Department of Justice and Equality	internetsafety@justice.ie

We thank you sincerely for contributing and assure you that your data is confidential and anonymous, and if published the data will not be in any way identifiable as yours.