Journal of Global Information Management
Volume 27 • Issue 3 • July-September 2019

Do We Trust the Internet?

Ignorance and Overconfidence in Downloading and Installing Potentially Spyware-Infected Software

Kenneth Howah, Central Queensland University, Melbourne, Australia
Ritesh Chugh, Central Queensland University, Melbourne, Australia

ABSTRACT

The threat profile of spyware is increasing rapidly when we consider the pervasiveness of computing in everyday life. The surreptitious nature of spyware can lead to information mining, data theft and exploitation of stolen data. This article aims to explore the relationship between trust in the Internet and neglecting risks in downloading and installing free potentially spyware-infected software. This study found that trust can be viewed as an indirect function of ignorance and overconfidence through the mechanism of the calculated probability of risk. An enhanced model of trust, based on Li and Betts' trust model has been proposed with two additional vectors. The inference drawn from the study is that in most users' minds, the calculated or perceived risk is substantially less than the anticipated benefit of the software. The analysis shows that users trust the Internet when it comes to downloading and installing potentially spyware-infected software, although such nonchalant trust appears to be based on ignorance and over-confidence.

KEYWORDS

Australia, Ignorance, Install, Internet, Malicious Software, Over-Confidence, Spyware, Trust

INTRODUCTION

Malware ('mal', a Latin root meaning 'bad') is a generic term for any software created with malicious intentions, including spying. Views vary about what types of software are included under the umbrella term 'spyware'. The term 'spyware' includes adware, key loggers, trojans, hijackers, dialers and malware (Garrie, Griver & Joller, 2010; Stafford & Urbaczewski, 2004). In contrast, it is not uncommon to find discussions treating adware and spyware as separate terms (Chien, 2005). While these terms refer to software with quite specific functions, other terms such as 'malware' are more generic and refer to any malicious software including viruses and worms, and these are usually treated as a separate category to spyware (Australian Government, 2006). The review of literature showed that most authors concur with this view. In short, viruses and worms are about causing destruction, damage or inconvenience to their victims, while spyware is about surreptitious information mining, data theft and exploitation of stolen data. This is the general distinction that will be utilised in this paper.

DOI: 10.4018/JGIM.2019070105

Spyware works by existing in background processes from which they perform their designed 'mal' functions. A variety of 'mal' functions exist, but in general, all engage in user or system monitoring, data gathering, and secret communications with a third party over the victim's Internet connection. Software that is, or that contains, spyware is acquired in many ways, and the significant growth of public use of the Internet since the early 2000s has meant that increasingly, spyware can be acquired through users simply clicking on links found in websites, in emails (Sophos, 2013) and on social networking platforms (Wüest, 2010). Spyware has evolved over time into increasing levels of sophistication and consequent hazard to the victims.

Whilst computers and the Internet have reached widespread popularity only in recent decades, there appears to have been no substantial or significant breakthrough in human factors studies within this context since the Theory of Reasoned Action (TRA) in 1967, or the Technology Acceptance Model (TAM) in 1986. As a result, much of the scholastic literature concerning user motivations and technology use that rely on these models is not specific to addressing spyware proliferation (Boldt, 2007) and academic research has been parsimonious. In the already established Theory of Planned Behaviour (TPB) model, a factor called 'perceived behaviour control' is shown to be capable not only of influencing behavioural intentions, but also capable of directly influencing usage behaviour, that is, conscious intention is bypassed. It is important to recognise that what is being studied in this paper is fundamentally a facet of human behaviour around technology. A study of this nature may lead to the lowering of spyware proliferation globally by assisting both users and organisations alike. Current defences against spyware include user avoidance actions such as refraining from downloading free software, and installing antispyware detection and removal software. However, what needs to be explored are contributory factors to users' calculation of risk probability that ultimately lead to the action of downloading and installing potentially spyware-infected software.

A useful synthesis of various concepts of trust relevant to this paper conceptualises trust as a construct involving conscious choice or decisions that are "preceded by expectations and followed by behavioral intent and action" (Li & Betts, 2004, p.2). Applying this to the context of this paper would imply an expectation of the free software to perform an intended task for the user and the subsequent action of downloading and installing free software. The action of downloading and installing free potentially spyware-infected software can also be hypothesised as an action that indicates a level of trust, with a degree of deliberation whether the intended task would actually be accomplished without an infectious software being installed. The context of this paper is based on the premise that trust is an issue only when risk exists (Conklin, 2006 p. 69). Where there is zero risk, "trust plays no part in the decision to proceed" (Li & Betts, 2004, p.6), referring to actions following behavioural intent. Similarly, where there is zero trust, risk actions are avoided, that is, the actions are not undertaken (Li & Betts, 2004). It is hypothesised that then ignorance and over-confidence also come in to the scenario. If calculated trust is a belief of probable occurrence of the perceived risk, it is synonymous to confidence. Thus, overconfidence may well be viewed as a strong trusting belief that the risk will not occur and may be seen as a point on the trust continuum.

The intent (malafide or altruistic) of the other party (the potentially spyware-infected software creator) on the Internet is also questionable, especially as the creator of the software being anonymous. Also, the propensity to take risk, the urgency of access, ability to bear possible loss from a malware inserted in the downloaded software and the lack of financial ability to procure the software, could all influence behaviour. Hence, it becomes important to look at over-confidence and ignorance in user behaviour.

Downloading software, while technically a separate action from installation, does not generally lead to a different decision to installation, resulting in installation almost always following download. This meant that most factors influencing the decision to download would be nearly identical to the factors influencing the decision to install. A study to understand the relationship between trust in the Internet, and neglecting risks in downloading and installing free software containing spyware is essential given the cost and pervasiveness of spyware and the associated threats to privacy and security.

This work fits in the context of information systems security, systems administration, computer user behaviour, and more broadly, online consumer behaviour. These areas of scholarship often rely on the same theoretical models as studied in technology-related consumer behaviour (Cheung et al., 2003). This research contributes to a better understanding of these factors, increasing the potential for advocating effective user behaviour on the spread of spyware and possibly reducing spyware proliferation universally.

The remaining part of the paper is organised as follows. The next section provides a review of the literature. This is followed by the research method. The subsequent section outlines the results and discusses them in light of other related studies. Finally, in the conclusion section, key premises of the study have been highlighted along with an outlook for further work.

LITERATURE REVIEW

Spyware as a general class of invasive software was first named by Steve Gibson in 2003 (Stafford & Urbaczewski, 2004). In its 2006 second quarter report, Webroot clarified that the company considered a wide range of malicious software to be part of 'spyware', including adware and Trojan horses, key loggers and installers (Webroot, 2006). Spyware can be used to monitor communications, perform clandestine tracking of users' actions, gather personal information and report it back to the spyware creator (Garrie, Griver & Joller, 2010).

One of the best-known methods for spyware to gather data is by raiding cookies, which are small text files planted in a user's computer by a visited website and used to store data about the target computer such as operating system, plug-ins installed, DNS information and websites visited (McCardle, 2003). On the user's next visit, the cookies can be retrieved by its owner website and the data can be utilised for various purposes such as customer recognition, storage of passwords, and targeted marketing.

The legitimate use of cookies to facilitate routine interactions between organisations and end-users is well-established, and it is both more accurate and useful to view cookies as a technology that is capable of being misused, rather than classing all cookies as inherently malicious technology. For this reason, a distinction is drawn between ordinary cookies used for legitimate purposes and cookies used for nefarious purposes, the latter being qualified as 'spyware cookies' (Dick, 2007).

A particularly dangerous trend appears to be the growing ability of spyware to embed themselves into the core of desktop operating systems like Windows, effectively hijacking parts of the operating system, and thus evading detection and removal by conventional means. This type of spyware exploits a component of operating systems called 'rootkits' (Hoglund & Butler, 2005). Complicating the situation is that rootkits are a legitimate part of the operating system and their functions are by design not always visible to end users, for example, the function in Windows allowing users to hide certain types of files from being visible in File Explorer. This means that removal of rootkit spyware, even when detected, may require technical expertise to determine its true origin and function since accidental removal of legitimate rootkit components could cause damage to the system.

A class of malware called Trojan Horses (or just Trojans) is frequently responsible for spyware penetrating computer systems. Trojan Horses gain entry by offering a bait of some kind (Greitzer et al., 2014) such as a pop-up advertisement or in other cases, an enticing on-stream video. Users clicking on the link are then advised that to watch the video they need an update to their media player, and are given a link to click. Once clicked, Trojan horse software is downloaded which is capable in turn, of downloading other spyware programs (Webroot, 2006).

A security intrusion could lead to not only data losses but reputational damage and monetary losses too (Li, Huang, Luftman & Sha, 2010). The prevailing motivation of malware authors has shifted from the desire to do damage for the sake of it through releasing viruses, to the desire to gain financially by writing spyware designed to steal valuable data (Sophos, 2014). One of the most frequently mentioned threats is the violation of privacy inherent in spyware operation (Phillips & Ryan, 2014;

Stafford & Urbaczewski, 2004). This is a wide-ranging issue that includes unintended disclosure of personal information to third parties, and the theft of personal information with consequences such as financial loss and identity theft, now recognised as a separate and growing category of cyber-crime (Arief, Adzmi & Gross, 2015).

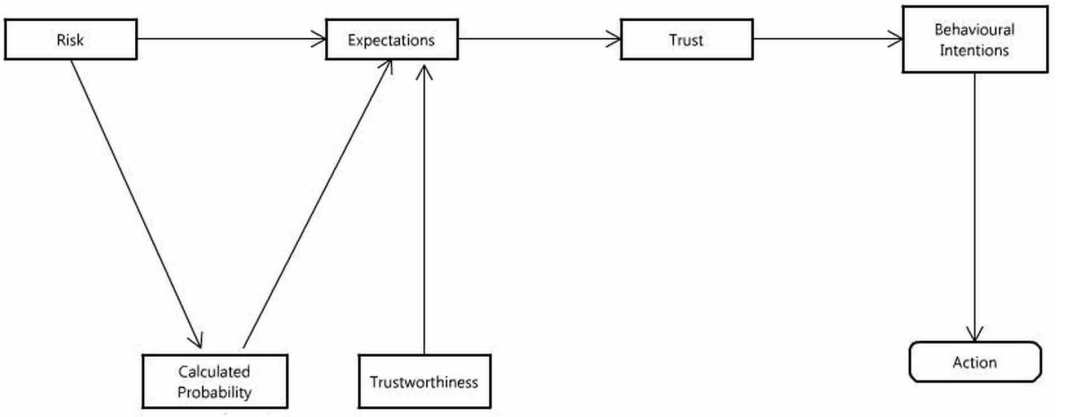
Trust is defined as a psychological state that indicates the willingness to accept vulnerability based on positive expectations of other people and/or actions, often indicating reliance (Dzindolet et al., 2003; Mayer, Davis, & Schoorman, 1995; Rousseau, Sitkin, Burt, & Camerer, 1998). Trust can be categorised according to the source of trust, for example, calculus-based trust, deterrence-based trust, knowledge-based trust, identification-based trust, institution-based trust and others (Li & Betts, 2004). Trust involves the tendency on the part of individuals to take risks according to the level of trust, called calculated-probability-based trust (Li & Betts, 2004). This means that the more we trust something or someone, the more risk we would be willing to bear with that entity. At the extreme, "when trust is absent, risk is avoided" (Li & Betts, 2004, p.8). Applied to the act of downloading software that may contain spyware, this means that the act would not be taken at all if the user had a zero level of trust in the particular website. Trust and ignorance are not simple components.

Proctor (2008) defines ignorance as a native state that arises due to the non-existence of knowledge. Most people are aware of the existence of spyware threats, however, most people do not know enough about the details, for example, the types of threats, why they exist, who is vulnerable, how it is caught, and damages done – the lack of detailed knowledge can be characterised by the word "ignorance", the word is here used strictly in the descriptive (lack of detailed knowledge) sense, and not in any pejorative sense. Thus, user responses to threats may be inadequate. The stark contrast between a general knowledge of the threat environment, and consistent risk-taking action shows there is a strong expectation that there will be no negative consequence arising from the action. The level of knowledge of those threats is not high, and the extent of the nature of the spyware threat is not understood by most users (Zhang, 2005). Ignorance leads people to make mistaken conclusions (Congleton, 2001). In order to alleviate malware threats, it is important to raise its awareness universally (Schmidt et al., 2008).

Among users there is high confidence associated with increasing use and knowledge of the Internet and computers as well as of specific threats such as spyware infection, but relatively low knowledge of the technical details of technology and associated threats. Over-confidence is defined as an overestimation of aptitude, performance, level of control, or chance of success (Moore & Healy, 2008). "Confidence" is closely associated with another concept, self-efficacy, which has been identified in various researches as a strong predictor of Internet usage including software usage (Conklin 2006; Sriramachandramurthy, Balasubramanian & Hodis, 2009). Defined as self-belief in one's ability to take action and solve problems, self-efficacy in effect may make users braver or more confident than they should be given the threat environment (Sriramachandramurthy, Balasubramanian & Hodis, 2009). Overconfidence leads people to overestimate their capability to perform an activity (Moores and Chang, 2009). Overconfidence of knowledge can be harmful as it may lead to wrong choices and it is vital to recognise one's ignorance (Son & Kornell, 2010), so potentially damaging situations can be avoided.

The model by Li and Betts (2004) in Figure 1 depicts behavioural intention (and hence action) as being preceded by trust, and shows that trust depends on positive expectations. The positive expectations are built on a combination of a calculated probability that the risks are acceptable, and belief in the trustworthiness of the other party. The model starts with perceived risk. Risk is knowing that some damage may occur when an action is taken. As with any action, the person taking the action makes a calculated probability with an expectation to achieve rewards although it may result in punitive results too. Trustworthiness refers to the characteristics of the trustee, based on their competence and reliability. The trustee could either be a person or a machine. The behavioural intentions and actions will be based upon the level of trust in a person or machine. Trust in the Internet is also considered an important mediating factor for user actions (Treiblmaier & Chong, 2011).

Figure 1. Li and Betts model of trust (Li & Betts, 2004)



The model is focused on the most basic level of trust, described as being the trust between an individual and another party (Li & Betts, 2004). This is therefore highly relevant to the inherent relationship between an end-user contemplating downloading and installing free software, and the providers of that software across the Internet. In effect, because most users are aware of the potential risk of spyware, the act of proceeding to downloading software may reasonably be viewed as an act of trust, in terms of this model.

A variety of literature is relevant to the topic of spyware proliferation, and generic theories are capable of providing suitable explanatory models of behaviour, but most relevant literature found was not written to directly address the spyware issue specifically in the context of trust. Howah and Chugh (2015) have called for studies that could look at trust issues in downloading and installing spyware infected software. There is a lack of research that studies the relationship between trust in computers and the Internet, and neglecting risks in downloading/installing free software. Hence, this research provides an analysis of trust.

METHOD

As this research is focused on human behaviour around the usage of technology, a quantitative approach was adopted to measure relevant aspects of trust. A quantitative method was used to discover statistically valid relationships between the likelihood of proceeding to download and installation of software containing spyware and trust.

Data was collected through a specifically tailored online questionnaire sent to a random sample population of a regional Australian university's registered alumni. Sampling based on alumni registration can be considered as random sampling since registration is open to all graduates from any past term of study. To the best of the researchers' knowledge, there were no existing questionnaires that were designed to elicit information specifically from the perspective of spyware proliferation. It was therefore decided to create a unique questionnaire, named the Spyware Survey, for this purpose. It was however found that several questionnaires encountered in the literature review validate the style and types of questions required for the kinds of data to be elicited (Conklin, 2006; Schmidt, Chen, Phan, & Arnett, 2009; Teo, Lim & Lai, 1999).

Questionnaires are an efficient data collection mechanism when the researcher knows exactly what is required and how to measure the variables of interest (Cavana, Delahaye & Sekaran, 2003). Questionnaires are also economical to administer, cater for a rapid turnaround in data collection and allow the collection of views from a larger population (Babbie, 1990). The Spyware Survey consisted

of a total of 31 questions (demographic questions, exploratory questions and direct measures of the dependent variable). However, for the purpose of this paper, we have only focussed on questions pertaining to the experience and/or knowledge of spyware. The questionnaire was validated by pre-testing against two separate smaller groups – one of a group of students, the other of staff, to establish basic validity, that is, the questions measure the variable that was intended.

A basic test of internal consistency, the split-half method, was performed to establish reliability, using the Cronbach alpha coefficient executed in the SPSS statistical analysis software. Twenty-three variables were subjected to the test, selected based on having the same construct and scale (Trochim, 2006). According to Pallant (2001), a Cronbach alpha coefficient of above 0.7 would indicate internal consistency. As shown in Figure 2, in this case, the coefficient was 0.815.

The online survey was e-mailed to 10,029 registered alumni for voluntary completion, with a response of 281 or 2.8% completed surveys within an approximately three-week period. Data for this study was analysed quantitatively, consistent with the post-positivist paradigm that underpins the approach to acquiring knowledge. The data was cleaned and transformed, and then imported directly into the SPSS program for analysis. Data cleaning involved identifying records with missing values, invalid or unusable records. The process of converting text responses into corresponding numerals was accomplished by using the search-replace function in Excel, applied to each data element one column at a time. The use of electronic forms and spreadsheets from point of collection through to SPSS-formatted data eliminated data transfer errors such as manual transcribing or human reading errors at the early stages of data processing.

FINDINGS AND DISCUSSION

The resulting non-discriminatory random sample represented a broad spectrum of computer users with a wide variety of demographic characteristics, but it necessarily excluded those with no experience of tertiary education. Tertiary education in itself is not critical to the factors being investigated, but it does mean that the impact of educational levels on the research problem cannot be fully addressed in this study. The population sample consisted of 57% males and 43% females. The largest age groups were those in the ranges 31 – 40 (25.7%), followed by 41 – 50 (24.3%) and then 21 – 30 (23.2%). The majority of respondents graduated with a bachelor's degree (57.7%). More than a third (35.6%) indicated that they had some degree of professional I.T. experience.

Figure 2. Cronbach Alpha (SPSS)

Case Processing Summary

		N	%
Cases	Valid	226	80.7
	Excluded[a]	54	19.3
	Total	280	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.815	23

Frequency analysis was used to derive statistical conclusions about the relationship between trust in the Internet, and neglecting risks in downloading and installing free potentially spyware-infected software. In respect to the potential for contracting spyware, the data from this study shows that most participants were aware of spyware and potential exposure to risk, yet most have admitted to downloading and installing software from the Internet. The survey data showed the following descriptive statistics:

- 63% agreed or strongly agreed that they "enjoyed trying out new software" (Figure 3);
- 77% were generally aware, including 30% who were acutely aware, "of the possibility of spyware being present in their computers" (Figure 4);
- 84% were generally aware, including 45% being very aware, "of the potential for spyware to be present in software being downloaded" (Figure 5);
- 86% were generally aware, including 43% who were acutely aware, "of the potential threat of spyware" (Figure 6);
- By contrast, only 9% of participants claimed to have "never downloaded" free software from the Internet (Figure 7), and only 8% claimed to have "never installed" such free software (Figure 8).

Figure 3. Enjoyed trying out new software

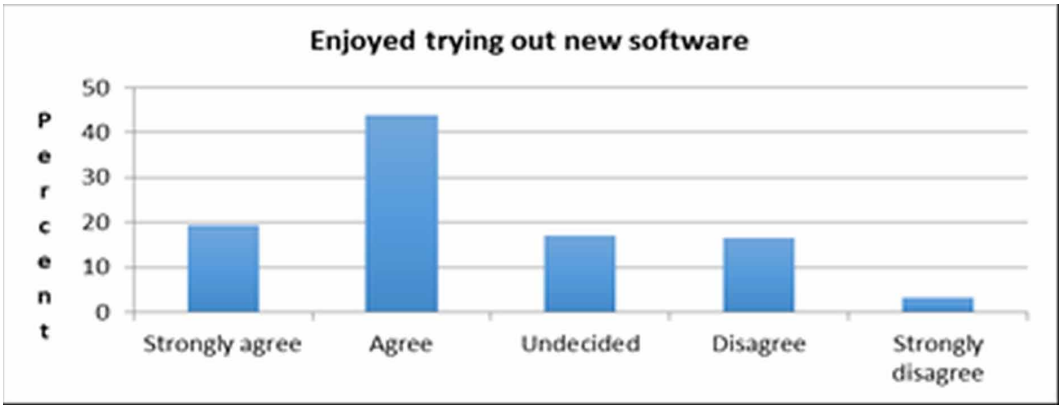


Figure 4. Conscious of possibility of spyware being present in users' computers

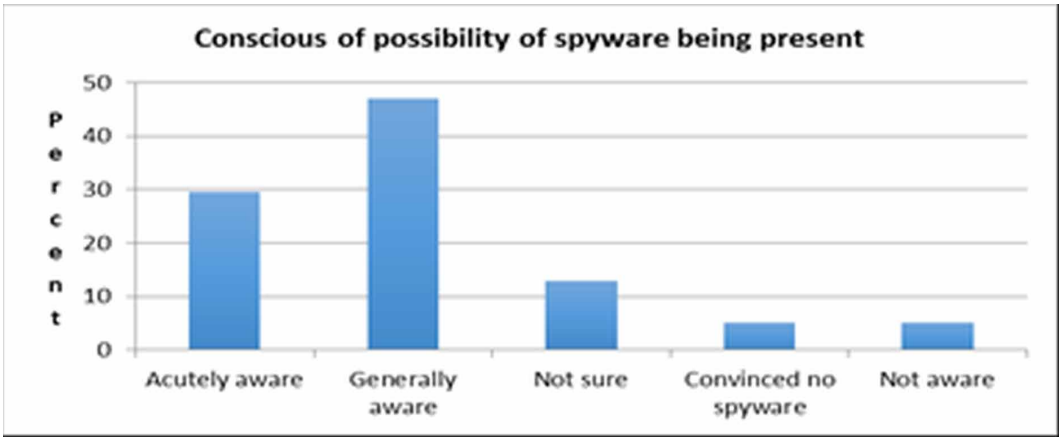


Figure 5. Aware that spyware is potentially present in software being downloading

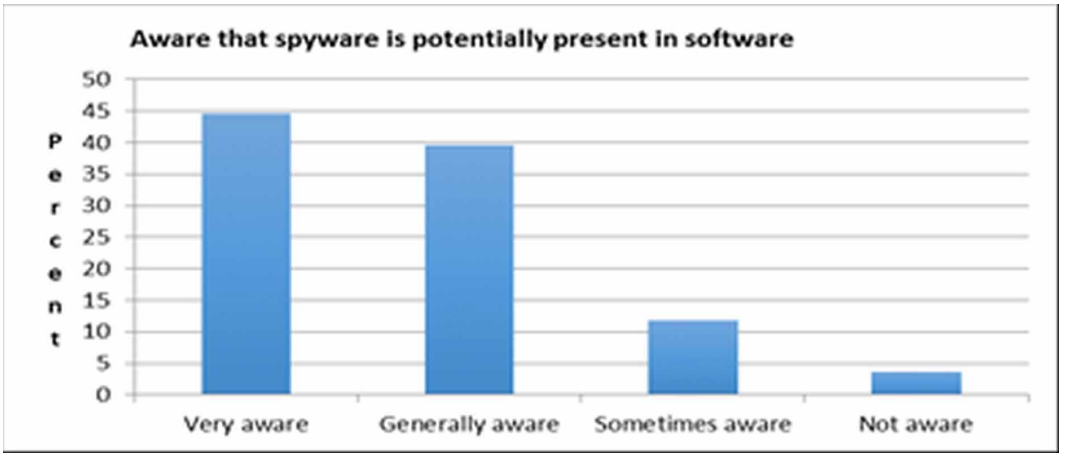
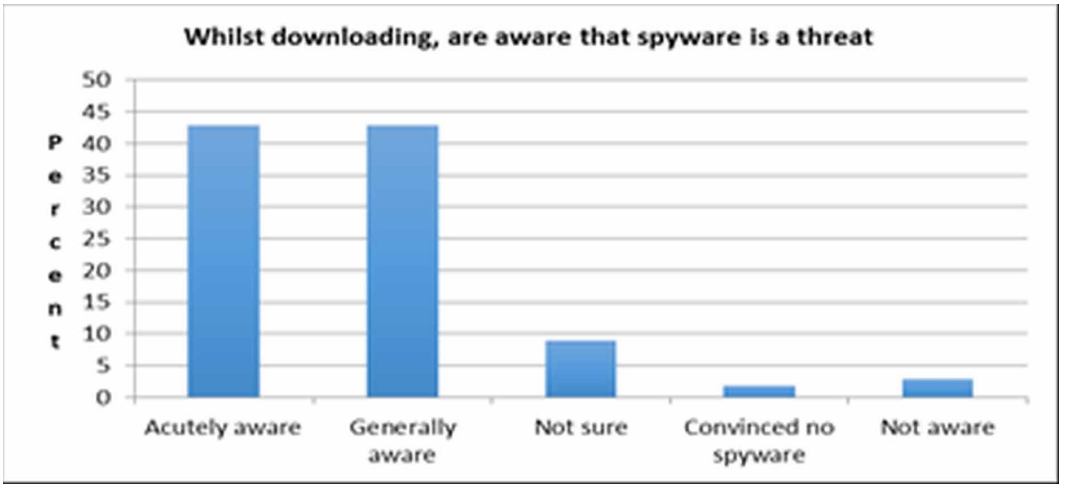


Figure 6. Whilst downloading, are aware that spyware is a threat



The inference drawn from the frequencies of variables (refer to Figures 3-8) is that in most users' minds, the calculated or perceived risk is substantially less than the anticipated benefit of the software. This idea is captured within the model of trust developed by Li and Betts (2004) – refer to Figure 1, which proposed that trust is an antecedent to behavioral intention and action, including actions that may involve known or calculated risks (Li & Betts, 2004). Another way of putting it is that, in the researchers' view, the concept of trust accounts for the contrasts shown in the data and literature between general awareness and knowledge of threats on one hand, but persistent risk behaviour on the other.

The high incidence of downloading coupled with a high degree of knowledge and awareness of potential threat indicates that the majority of Internet users have a high degree of trust in the Internet, whether that trust is warranted or not, and that this high level of trust is a major factor leading many users into high-risk downloads despite general knowledge of such risks.

This issue was based on the observation that an equally large proportion of users are aware of the potential threats posed by malware and spyware in particular, as they engage in downloading free

Figure 7. Have never downloaded free software from the Internet

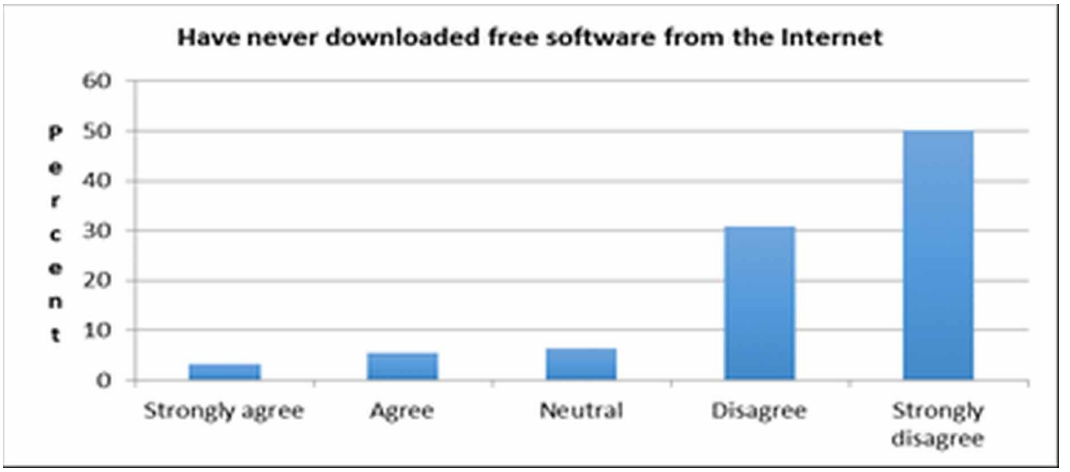
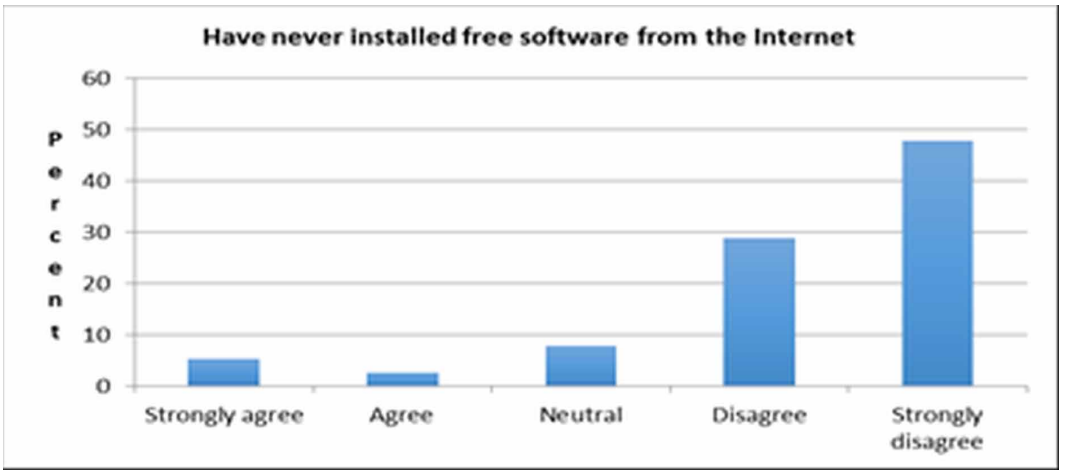


Figure 8. Have never installed free software from the Internet



software from the Internet. This behaviour pattern has been explained in different ways in the literature, for example, as apathy (Stafford, 2005) or in terms of users not having adequate understanding of the threats (Zhang, 2005), or in reduced concern for privacy among those with more skill and experience (Dinev & Hart, 2004) or in terms of an increased sense of self-efficacy (Sriramachandramurthy, Balasubramanian & Hodis, 2009). The nature of "apathy" was not defined and therefore remains a vague concept, while users with inadequate understanding of threat or reduced awareness of privacy can easily fit into the construct of "trust" developed by Li and Betts (2004), in terms of a user's calculation of the probability of risk. In this case, our contribution to the model adds the vectors of "ignorance" plus "over-confidence" arising from experience in successful use of the Internet as factors that feed into that calculation of risk, leading to trust. Judgements based on ignorance and over-confidence could be damaging.

The combination of confidence and ignorance affecting risk and trust is consistent with the finding of a negative relationship between Internet technical literacy and Internet privacy concerns (Dinev & Hart, 2004, p.4). The converse of that relationship suggests that the higher a user's level

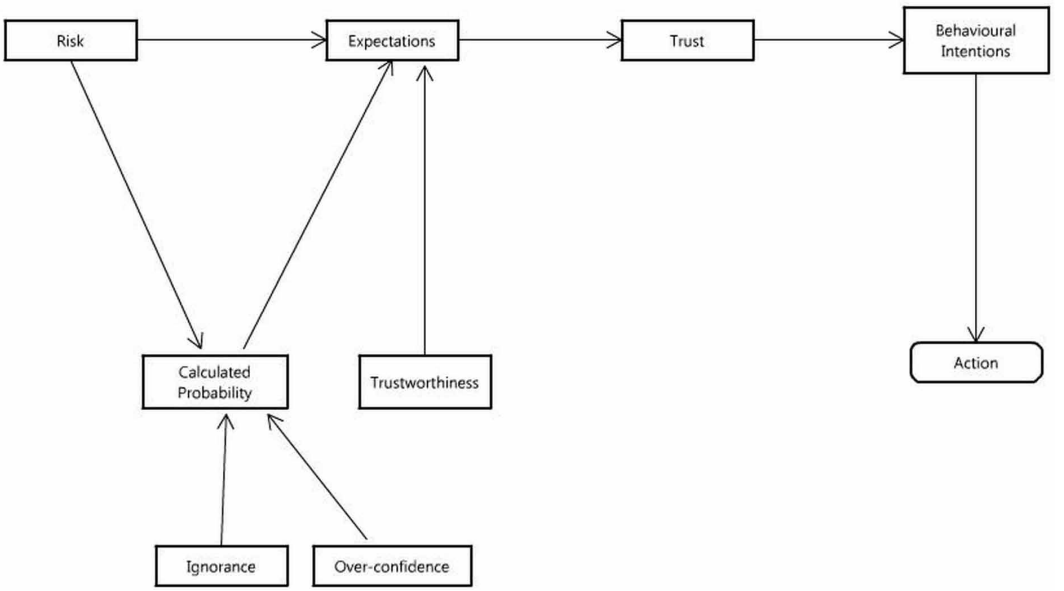
of internet technical literacy, the lower will be their concern about privacy issues, that is, they would have a reduced concern for the invasive potential of spyware. This does not suggest that those with high technical literacy take no defensive measures; it simply implies that due to higher levels of knowledge and self-efficacy, there is an over-confidence as noted, leading to an underestimation of the actual risk level. This phenomenon was also noted in the Schmidt et al. (2009) study which found that although "heavy users" (more than 15 hours per week) of the Internet showed greater awareness of malware threats, paradoxically, it was the "light users" who scored higher in terms of password practices. In some sense then, trust can be viewed as an indirect function of ignorance (as defined above) and overconfidence through the mechanism of the calculated probability of risk and this can be readily incorporated into the Li and Betts model as shown in the enhanced model of trust (Figure 9).

The 'Ignorance' and 'Over-confidence' vectors feed into Calculated Probability rather than directly into Perceived Risk as this reflects that users are not necessarily aware of the extent of their lack of knowledge or of their over-confidence, therefore these do not form part of their perceived risk environment, rather they affect the way the user assesses the overall risk probabilities and hence, their expectations. This suggests that what Stafford described as "apathy" (Stafford, 2005) might be more accurately viewed in the light of "trust." A further study is needed to pursue the full implications of these additions to the enhanced model of trust.

In summary, what various researchers have seen as user apathy, disinterest in personal privacy or security, can actually be viewed as reflections of an entrenched public trust in the Internet. Such trust is often based on ignorance of the dimensions of the spyware threat rather than on extensive knowledge, and on over-confidence in personal skills and self-efficacy rather than on an educated caution. Overconfidence is related to self-efficacy and could have a debilitating effect on performance (Moores and Chang, 2009). Over-confidence in personal skills arises from the increasing frequency of relatively successful usage of the Internet by individuals and the experienced usefulness of downloaded software, which is a key factor in motivating users to download and install free software.

The insights derived from this study should lead to a more informed calculation of risks, more generally-aware users and lowered unnecessary overconfidence. From a global perspective, these findings can help to reduce the risks in downloading and installing free potentially spyware-infected

Figure 9. Enhanced model of trust



software. It is imperative for users to beware of overconfidence. Apart from an individualistic user perspective, organisations that develop anti-spyware software can utilise these findings to educate their users to make more informed decisions when downloading and installing software over the Internet.

CONCLUSION

The study contributes to the field by finding that users have a high degree of trust in the Internet and the concept of trust can capture the discrepancies noted in literature between knowledge of threats and persistent risk behaviour. Internet users in general trust the Internet, often nonchalantly. Although there has been much media coverage of the multitude of scams, malware, privacy breaches through spyware, and other cybercrime including cyber warfare activities occurring across the Internet, this has in no way diminished the high level of user interaction with the Internet, including the downloading of potentially spyware-infected software. In effect, users are making risk calculations and are consistently concluding that the benefits substantially outweigh the risks.

It is evident that there are a very limited number of articles about ignorance and confidence, with nothing specifically about downloading and installing potentially spyware-infected software. This paper fills in that gap. The key contribution of this paper has been the identification of the concepts of ignorance and overconfidence as contributory factors to users' calculation of risk probability leading to trust as an antecedent to action as shown in the enhanced model of trust. The enhanced model of trust constructed in this study, fits as a drill-down model to provide more explicit explanatory power to future research globally. Specifically, the problem of high-risk Internet interaction arises from uninformed or uneducated trust. Put another way, people are consistently miscalculating their current level of knowledge of the threats, as well as their current level of knowledge of computers and the Internet, and therefore, their interactions with the Internet are largely based on trust rather than knowledge.

In terms of generalisability, the response rate of 2.8% is low despite the useful sample size and cannot be statistically established as being representative of the population under study. The conclusions can therefore only apply to the response group at best. A usable sample size of 280 has provided sufficient cases to allow significant data analysis to be performed, although frequency analysis is not devoid of its own inherent limitations. The data in this study was skewed toward males (57%) and toward those with some degree of IT professional experience (35.6%). All conclusions or generalisations arising from this research should be viewed in the light of these demographic characteristics. As with any research, this study also has other inherent limitations. The sample frame was restricted to graduates of a regional Australian university and excluded the non-tertiary educated population. In addition, it is reasonable to assume that a degree of response bias exists, as 35.6% respondents indicated that they had had some degree of professional I.T. experience. Future studies could look at computer literacy in terms of trust in computers and the Internet. The effect of different education levels on spyware proliferation may be investigated in further studies. Empirical research could also be carried out to validate the enhanced model of trust and its propositions.

Existing studies on this topic, including this study, tend to be spot analyses only, that is, taking measurements and analysing only small snapshot sub-sections of society as a whole. Yet spyware and other malware problems are recognised as having universal scope in the computing world. The researchers believe that there is a danger that the wider impacts of the problem may be systematically overlooked due to the limited generalisability of all extant studies. There is therefore, a gap in scholarly research on a national and international scale to assess the problem of spyware from much broader perspectives.

In conclusion, there is an increasing level of general public knowledge and involvement in online activities, including social networking and solution seeking behaviours. This in no way implies that policy should be directed at reducing public trust in the Internet, but rather, that trust as a concept must be better understood by the computing public. Indications are not that people should not trust the Internet, but that a requisite degree of knowledge and caution is essential in interacting with it to maintain cyber safety.

REFERENCES

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding Cybercrime from its Stakeholders' Perspectives: Part 1—Attackers. *IEEE Security and Privacy*, *13*(1), 71–76. doi:10.1109/MSP.2015.19

Australian Government. (2006). More Malware – Adware, Spyware, Spam and Spim. *Australian Institute of Criminology*, *11*, 1–2.

Babbie, E. (1990). *Survey Research Methods* (2nd ed.). Belmont: Wadsworth.

Boldt, M. (2007). Privacy-invasive Software [Dissertation thesis]. Blekinge Institute of Technology, Karlskrona, Sweden.

Cavana, R. Y., Delahaye, B. L., & Sekaran, U. (2003). *Applied Business Research: Qualitative and Quantitative Methods*. Milton, Queensland: John Wiley & Sons.

Cheung, C. M. K., Zhu, L., Kwong, T., Chan, G. W. W., & Limayem, M. (2003). Online Consumer Behavior: A Review and Agenda for Future Research. In *Proceedings of the 16th Bled eCommerce Conference*, Bled, Slovenia, June 9-11.

Chien, E. (2005). Techniques of Adware And Spyware. *Symantec*. Retrieved March 26, 2016, from http://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf

Congleton, R. D. (2001). In Defense of Ignorance: On the Significance of a Neglected Form of Incomplete Information. *Eastern Economic Journal*, *27*, 391–408.

Conklin, W. A. (2006). Computer Security Behaviors of Home PC Users: A Diffusion of Innovation Approach [Doctor of Philosophy thesis]. University of Texas, San Antonio.

Dick, J. (2007). *What Makes a Cookie a Spyware Cookie?* Ezine @rticles. Retrieved March 13, 2016 from http://ezinearticles.com/?What-Makes-a-Cookie-a-Spyware-Cookie?&id=716437

Dinev, T., & Hart, P. (2004). Internet Privacy, Social Awareness, and Internet Technical Literacy - an Exploratory Investigation. In *Proceedings of the 17th Bled eCommerce Conference*, Bled, Slovenia, June 21-23.

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The Role of Trust in Automation Reliance. *International Journal of Human-Computer Studies*, *58*(6), 697–718. doi:10.1016/S1071-5819(03)00038-7

Garrie, D. B., Griver, Y., & Joller, M. (2010). Regulating Spyware: Challenges and Solutions. *Journal of Internet Law*, *13*(8), 3–13.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In IEEE Security and Privacy Workshops (SPW), May 17-18 (pp. 236-250). doi:10.1109/SPW.2014.39

Hoglund, G., & Butler, J. (2005). *Rootkits: Subverting the Windows Kernel*. Massachusetts: Pearson Education.

Howah, K., & Chugh, R. (2015). Perceived Utility as a Motivational Factor in Affecting Users' Decisions to Download and Install Potentially Spyware-Infected Software. In *Proceedings of the Twenty-first Americas Conference on Information Systems (AMCIS)*, Puerto Rico, August 13-15 (pp. 1-8).

Li, D., Huang, W. W., Luftman, J., & Sha, W. (2010). Key Issues in Information Systems Management: An Empirical Investigation from a Developing Country's Perspective. *Journal of Global Information Management*, *18*(4), 19–35. doi:10.4018/jgim.2010100102

Li, F., & Betts, S. C. (2004). Between Expectation and Behavioral Intent: A Model of Trust. *Journal of Organizational Culture*. *Communications and Conflict*, *8*(2), 1–11.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, *20*(3), 709–734.

McCardle, M. (2003). How Spyware Fits into Defense in Depth. *Sans*. Retrieved March 1, 2016, from https://www.sans.org/reading-room/whitepapers/malicious/spyware-fits-defense-in-depth-905

Moore, D. A., & Healy, P. J. (2008). The Trouble with Overconfidence. *Psychological Review*, *115*(2), 502–517. doi:10.1037/0033-295X.115.2.502 PMID:18426301

Moores, T. T., & Chang, J. C. J. (2009). Self-Efficacy, Overconfidence, and the Negative Effect on Subsequent Performance: A Field Study. *Information & Management*, *46*(2), 69–76. doi:10.1016/j.im.2008.11.006

OnguardOnline. (2014). Malware. Retrieved March 1, 2016, from http://www.onguardonline.gov/topics/spyware.aspx

Pallant, J. (2001). *SPSS Survival Manual*. Chicago: Allen & Unwin.

Phillips, J., & Ryan, M. D. (2014). A Future for Privacy. In S. Stalla-Bourdillon, P. Joshua, & M. D. Ryan (Eds.), *Privacy vs. Security* (pp. 91–115). London: Springer.

Proctor, R. (2008). Agnotology: A Missing Term to Describe the Cultural Production of Ignorance. In R. Proctor & L. Schiebinger (Eds.), *Agnotology: The Making and Unmaking of Ignorance* (1st ed., pp. 1–36). Stanford, California: Stanford University Press.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, *23*(3), 393–404. doi:10.5465/AMR.1998.926617

Schmidt, M. B., Chen, J. Q., Phan, D. D., & Arnett, K. P. (2009). Security Perceptions of E-Commerce Users. *Journal of Internet Commerce*, *8*(1-2), 44–57. doi:10.1080/15332860903341307

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A Cross-Cultural Comparison of US and Chinese Computer Security Awareness. *Journal of Global Information Management*, *16*(2), 91–103. doi:10.4018/jgim.2008040106

Son, L. K., & Kornell, N. (2010). The Virtues of Ignorance. *Behavioural Processes*, *83*(2), 207–212. doi:10.1016/j.beproc.2009.12.005 PMID:20006687

Sophos. (2013). *Security Threat Report 2013.* Retrieved March 1, 2016, from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

Sophos. (2014). *Security Threat Report 2014: Smarter, Shadier, Stealthier Malware*, 1-34, Retrieved March 1, 2016, from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

Sriramachandramurthy, R., Balasubramanian, S. K., & Hodis, M. A. (2009). Spyware and Adware: How Do Internet Users Defend Themselves? *American Journal of Business*, *24*(2), 41–52. doi:10.1108/19355181200900010

Stafford, T. F. (2005). Consumer Apathy and the Emerging Revenue Model of the Internet: The Economic Case for Spyware. *Journal of Electronic Commerce in Organizations*, *3*(4), 1–4.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *Communications of the Association for Information*, *14*, 291–306.

Teo, T. S. H., Lim, V. K. G., & Lai, R. Y. C. (1999). Intrinsic and Extrinsic Motivation in Internet Usage. *International Journal of Management Sciences*, *27*, 25–37.

Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure: results from three countries. *Journal of Global Information Management*, *19*(4), 76–94. doi:10.4018/jgim.2011100104

Trochim, W. M. K. (2006). Types of Reliability. *Social research methods*. Retrieved February 12, 2016, from http://www.socialresearchmethods.net/kb/reltypes.php

Webroot. (2006). *State of Spyware Q2 2006*. Retrieved February 19, 2016, from http://www.webroot.com/pdf/2006-q2-sos-US.pdf

Wüest, C. (2010). The Risks of Social Networking. *Symantec*. Retrieved February 19, 2016, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

Zhang, X. (2005). What Do Consumers Really Know About Spyware? *Communications of the ACM*, *48*(8), 44–48. doi:10.1145/1076211.1076238

Kenneth Howah has worked in the university sector since 2002. He holds two master's degrees in information systems (one by research) and lectures in networking technologies at CQUniversity. He is currently interested in researching in authenticity in higher education assessment.

Ritesh Chugh lectures in the School of Engineering and Technology. He teaches to both undergraduate and graduate students in the fields of Information Systems (IS) Management, Analysis and Design, and IS Project Management. Ritesh is an enthusiastic and committed educator who has been awarded many teaching awards over the past few years to recognise his teaching excellence and commitment to improved student outcomes. Ritesh is an active researcher and has published many articles in international refereed journals and contributed to several book chapters. He has presented and published papers in many peer reviewed international conferences too. His publications demonstrate varied research interests. He has also been a peer reviewer, program committee member and session chair for multiple international refereed conferences. Ritesh is also the co-recipient of two learning and teaching grants. He has been interviewed multiple times on radio talk back shows and has written articles for many major Australian newspapers too. His range of interests include social media, knowledge management, information systems management and theory, project management, electronic commerce and developing varied teaching and learning practices on a formal note and philately and numismatics on a more casual note. Ritesh is a senior member of IEEE and the Australian Computer Society. He holds a membership of IEEE Computer Society and the IEEE Green ICT Community too. Ritesh also contributes to social goodness via volunteering