Edith Cowan University
Research Online

International Cyber Resilience conference | Security Research Institute Conferences

2011

Securing the Elderly: A Developmental Approach to Hypermedia Based Online Information Security for Senior Novice Computer Users

David M. Cook
Edith Cowan University

Patryck Szewczyk
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University

Originally published in the Proceedings of the 2nd International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 1st - 2nd August 2011
This Article is posted at Research Online.
http://ro.ecu.edu.au/icr/19

SECURING THE ELDERLY: A DEVELOPMENTAL APPROACH TO HYPERMEDIA-BASED ONLINE INFORMATION SECURITY FOR SENIOR NOVICE COMPUTER USERS

David M. Cook, Patryk Szewczyk, Krishnun Sansurooah
secau - Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia

d.cook@ecu.edu.au, p.szewczyk@ecu.edu.au, k.sansurooah@ecu.edu.au

Abstract

Whilst security threats to the general public continue to evolve, elderly computer users with limited skill and knowledge are left playing catch-up in an ever-widening gap in fundamental cyber-related comprehension. As a definable cohort, the elderly generally lack awareness of current security threats, and remain under-educated in terms of applying appropriate controls and safeguards to their computers and networking devices. This paper identifies that web-based computer security information sources do not adequately provide helpful information to senior citizen end-users in terms of both design and content. It subsequently demonstrates a solution designed with the elderly, yet novice, end-user in mind. This paper examines the need for practical computer-based instructions that have wide-ranging applications to a wide selection of under-informed internet consumers. As computer usage rapidly spreads towards total ubiquity across all generations and social levels, the need for web-based education resources to protect generationally differing internet users is urgently required.

Keywords

Security awareness, computer security, elderly, information security, online security, novice user, golden baby boomers.

INTRODUCTION

End-user cyber-knowledge, ICT education, technology, and awareness are ongoing issues in the context of computer security. For the broader cross section of internet end-users a comprehensive solution is yet to be developed to counteract this problem. Whilst there are glimpses of relief in a range of consumer-targeted anti-virus and security products, no single solution has emerged to offer consistent guidance for novice users, nor 'golden' baby boomers who present in novice form (Lusardi & Mitchell, 2007). In contrast, the sophistication of threats is continually developing. Senior citizens who are novice end-users are severely marginalised in terms of their access to information that translates generationally and makes sense to users with limited computing experience. There is a need for intelligible information for senior yet novice users to protect them from internet crime. From an end-users perspective, commercial convenience directs users to rely on computer retail outlets and Internet Service Providers as an information source. However, the source of the most reliable security information is a contested issue. Within the dynamic of a universal commercial imperative, it is important to acknowledge that retail outlets and service providers are not employed to provide computer security support or advice. It would also appear that in many instances, the individuals working in these environments lack the appropriate skill set and knowledge to provide accurate and supportive information to the novice end-user (Furnell, Shams, & Phippen, 2008).

The process of self efficacy is an ongoing dilemma for all end-users in the digital world (Dodge, Carver, & Ferguson, 2007). Individuals are often reluctant to apply appropriate safeguards to a computing device if they feel that they do not have the capacity to do so. As a result it is not surprising that end-users feel that they do not encompass the skill set to apply computer security safeguards. In numerous computer product manuals, critical security information is intentionally written for users with an intermediate to advanced skill set. In some cases the information is portrayed in such a manner as to confuse even computing experts who attempt to decipher the process of changing a password (Szewczyk & Valli, 2009).

The irony of education systems for computer security users of low computer literacy and poor understanding of security threats is that they are precisely the target audience of those engaged in phishing, social engineering, and spamming (Pfleeger and Pfleeger, 2007). A vicious circle of under-awareness and simplified pursuit therefore emerges. Computer literacy has settled into two main pathways. On the one hand, novice users rapidly acquire skills in the area of multimedia literacy and quickly become adept at navigating web-based media in both 1.0 and 2.0 forms. The popularity of social media and the inherent broad-based useability of internet possibilities attract large numbers of users. Novice users typically operate these web-based systems in a topical manner, barely scratching the surface of most multilayered software systems and focusing predominantly on

ease of use, rather than understanding (Ciampa, 2010). Novice users will frequently visit a site once and often leave without grasping the foundational system which operates within each program or application. Attackers will use social networking sites such as Facebook and MySpace to gain large amounts of information about specific people. End-users will give as much personal information as possible because that enables them to better enjoy the experience of social networking (Dhanjani, Rios & Hardin 2009, p13). In the case of elderly novice users, their grasp of ICT concepts is more fragile, whilst their understanding about what constitutes dangerous informational disclosure indicates significant ignorance and naivety.

On the other hand, literacy below the first layer of any operating system or program requires greater skills, deeper understanding, and a commitment to learning these fundamental aspects. Computer literacy in this area includes the essential security awareness to prepare and prevent the spread and effect of malware and their miscreant agents. Since novice users fall more readily into the first of these two broad categories, and since this area also appeals to popular internet usage that is tailored to entertain novice users, it is no surprise that novice users fall prey to a variety of security vulnerabilities (Gifford 2009, p29).

With limited options available for end-users to safeguard their computer, information, and network, the World Wide Web provides a possible answer to the problem of a novice user's security exposure. The only viable solution for end-users is to take responsibility and begin locating solutions for themselves and applying these with the skill set they encompass. The initial issue here is that the end-user must knowingly be aware of the issue; know how to circumvent the threat; and lastly understand the products or configuration settings that need to be applied. Additionally there isn't an overarching solution that can be applied to mitigate all security issues. As a result, end-users may often find themselves needing to seek numerous information sources to find an applicable solution. Elderly computer users are more likely to accept initial information at face value, without considering the need to corroborate computing information or to augment their learning by inquiring beyond a single source of facts.

Governments and security enthusiasts have begun developing information security portals. These are essentially web sites specifically designed with providing security information through a broad spectrum of areas. Unfortunately, many current computer security information portals are solely based on hypertext formats omitting hypermedia or multimedia site structures. Research suggests that hypermedia and multimedia web sites tend to result in end-users acquiring high levels of knowledge and being able to apply this to a real world (Shaw, Chen, Harris, & Huang, 2009). Alternatively hypertext web sites usually have the opposite affect and result in end-users not obtaining the skill set or knowledge to safeguard their computer effectively. Consequently, end-users are often deterred or reluctant to hunt for the correct information when it is concealed amongst text-based websites.

This paper demonstrates a proposed solution in aiding end-users to safeguard their computer. The subsequent sections are broken down into a review of two current and one obsolete Australian online information security portal and a respected portal from the United Kingdom. These portals were selected based on current media advertising by Australian Government agencies and those noted by respondents in previous security based questionnaires (Szewczyk & Furnell, 2009).

ACCEPTANCE AND FAMILIARITY WITH NEW TECHNOLOGY

The cohort of novice yet senior computer users exhibits a range of distinctive characteristics. Unlike other novice computer users, elderly users are in many cases required to turn to a web-based environment despite their desire to remain apart from it. Young novice users embrace ICT technology as normal and rise to new challenges with the expectation that each new task is anticipated and will lead to a better outcome. Elderly novice users have a different mindset, brought on by their enforced exposure to new norms such as internet banking, online health services, and online transport information (Ellis & Kurniawan 2000). Many information services that were previously available by phone or face to face delivery are now isolated to web-based information access portals. Bus timetables, product disclosures, and financial options now require senior citizens to embrace technology or ignore it at their own peril (McCloskey, 2006). In a physical sense, previous interactions with one's personal security needs were conducted in a face to face manner, with service providers such as policemen, postal workers, locksmiths and guards. In a cyber sense, personal security is now much more heavily reliant on self-awareness, personal comprehension of computing security issues, and individual cyber-security cognition (Dickinson, Newell, Smith, & Hill, 2005). What becomes second nature to young novice users, remains unnatural, and deliberate to the elderly (McCloskey, 2006).

EXISTING COMPUTER SECURITY PORTALS

As at December 2010, the Australian Government had released three information portals for consumers to utilise to safeguard their computers and enhance their online experience. The issue with many current security information portals is the overly professional (and potentially daunting) design of the navigation interface

coupled with confusing information, targeted at those with an intermediate to advanced skill set. In addition, previous studies have indicated that end-users have expressed the desire to locate information as promptly as possible, rather than rummaging through numerous web pages to reach the required information on the Australian Government security information portals (Szewczyk & Furnell, 2009).

Netalert (NetAlert, 2010) was designed to provide a free online content filter, to allow parents to control what their children are accessing on the Internet. Whilst the website was heavily marketed through various media channels, it is no longer accessible by end-users. More importantly, respondents from a previous study (Szewczyk & Furnell, 2009) reported that many were under the impression that it was in fact supposed to be a security information portal, although soon discovered that it provided very little useful information to effectively safeguard a computer, network, and information. As a result, the NetAlert information portal came to a close (due to a no longer freely available content filter), and the Australian Government subsequently released an updated information portal named the CyberSmart (CyberSmart, 2010).

The CyberSmart information portal is organised according to information for various age groups. The portal does not provide sufficient information to effectively guide an end-user through the steps required to secure any device. As per Figure 1, the website does encompass a section on installing a firewall. Unfortunately the portal provides no more than a glossary style definition of what a firewall is and its importance. Aside from the definition detailing what a firewall is, there is no further information relating to the process of installing an actual personal firewall coupled with the tedious configuration process that many end-users would face.

Figure 3 CyberSmart - Installing a firewall

To further aid end-users in safeguarding their computers, the Australian Government produced an information portal under the heading 'StaySmartOnline". According to the websites mission statement it is the intention of the portal to allow end-users to "understand cyber security risks and educate home and small business users on the simple steps they can take to protect their personal and financial information online" (StaySmartOnline, 2010).

As per Figure 2, the StaySmartOnline does not conform to its mission statement and as a result makes no real attempt to provide end-users with detailed step-by-step tutorials for installing, configuring and utilising personal firewalls effectively. In a similar fashion to the CyberSmart website, this particular information portal tends to provide a series of glossary style definitions rather than graphic based tutorials.

Home » Home Internet Users » Secure your computer » Install and use a firewall

Install and use a firewall

A firewall acts like a security guard at the door of your house; it checks who and what enters or leaves.

A firewall is a piece of software or hardware that sits between your computer and the outside world and acts as the gatekeeper for all incoming and outgoing traffic.

A correctly configured firewall will prompt you when it detects an unauthorised computer or program trying to access your computer or a software program is installed on your computer that tries to make an unauthorised outside connection.

If you are a home user, using a firewall and having it permanently turned on is the most effective and important first step you can take to help secure your computer. Always use a firewall, as well as anti-virus and anti-spyware software. The more lines of defence you have in place, the harder it is for hackers to get in.

Figure 4 StaySmartOnline - Installing a firewall

In contrast it is worth examining an information portal external to Australia, and this paper considers the relative worth of Get Safe Online (GetSafeOnline, 2011). In this instance, the information portal is a collaborative project amongst numerous computer security vendors, law enforcement, and Government agencies. Although external to Australia, it still suffers from the same issues as the StaySmartOnline and CyberSmart project. As demonstrated through Figure 3, the screen snap shot purports to explain the function of a firewall, together with installation and configuration information. In this instance, the StaySmartOnline portal falls short of its advertised and promoted intentions. The site ignores the need to provide step-by-step procedures into how to obtain, install and configure a personal firewall to be used effectively in a home or small business environment.

Although this paper does not attempt to provide an exhaustive analysis of security information portals, the sites considered in this paper are meant to provide an indicative sample of like portals in order to establish the context for novice senior users. This paper therefore assumes that security information portals are in the main deficient in terms of their efficacy, their language, and their logic. If most information portals preclude novice users from understanding their fundamental methods of use, then an extension of this logic suggests that senior novice users are at a significant disadvantage in relation to the access and deployment of information from online portals for the protection of web-based internet activity.

Home > Knowledgebase > Protect your PC > Use a firewall

Use a firewall

Firewalls keep out some viruses and hackers

A firewall acts as a barrier between the public internet and your private computer or network and blocks threats including some viruses.

Why install a firewall?

A firewall protects you against a number of different online threats:

- Hackers breaking into your computer.
- Some viruses, called "worms," that spread from computer to computer over the internet.
- Some firewalls block outgoing traffic that might originate from a virus infection.

How to configure a firewall

Most desktop firewalls require some training before they are fully configured. This is because they need to learn what programs you use and which ones connect to the internet. Windows Firewall pops up warnings when a program tries to connect to the internet for the first time. Other desktop firewalls work in a similar way but the information they give varies from product to product. The key thing is to pay attention to these messages and make sure that you only allow legitimate connections.

Figure 3 Get Safe Online - Using a firewall

SECURITY INFORMATION PORTAL SOLUTION

There are a variety of promising vectors which could be taken in designing a security information portal. Previous research suggests that the predominant factor is usability (Ciampa, 2010). In response to the dynamic nature of constantly morphing and innovating computer security threats, it is evident that consumers require a user-friendly portal by which to access accurate and unbiased information. Previous studies, in combination with an evaluation of current security information portals, revealed that one critical characteristic was repeatedly omitted. The need for graphical step-by-step procedures is therefore viewed as an essential component in order to solve the widening gap between computer-proficient and literate end-users at one extreme, and at the other extreme novice senior users. Furthermore scrutiny of existing portals identified that in the majority of cases the language has been highly formalised, and in some instances, inherently perplexing. Hence, three factors were deemed mandatory in the creation of a new security information portal. These features most closely resembled simple language, easy navigation, and useable procedural step-by-step tutorials.

A comprehensive process was used to determine the specific directions that the portal should encompass. On the one hand, there are a plethora of web portals that purport to instruct and inform ordinary users. Whilst these make a useful starting point, the great majority of samples are clearly not suitable for novice users. Many sites incorporated advertising that was misleading from the perspective of the novice users' needs. Many would offer multiple products with insufficient basic information for a novice user to be able to make an informed choice. Instead, advertising was 'salted' with high powered technical terminology that directed users to feel compelled to install (and possibly purchase) software-based security solutions. Many novice users are only motivated to look at web-portals on computer security if they have a problem (usually the suspicion that they are infected with a virus). These sites represent a highly opportunistic and predatory approach that relies on end-user urgency and helplessness rather than informed consumer judgement. Sites were generally classified according to how inappropriate they were to novice users rather than for their suitability.

An initial issue was the exposure and accessibility to information. One of the concerns was the ability for any and all users to be capable of accessing the portal from any computer, tablet, or mobile phone. This was raised from the assumption that the user may not have internet access on a specific device, or may not wish to connect a vulnerable device to the Internet without sufficient protection. Furthermore, new mobile forms of computing now place greater demand upon web development so that information can be found in a variety of formats and across a range of media products and platforms (Nielsen, 2009). As part of the detailed approach to web development, a cross platform review was conducted in order to determine the necessary design specifics for not only websites, but also mobile devices, smart-phones, touch-phones and tablets.

Ease of navigation was also addressed in the project. The need for an attractive layout, ease of use and access, and the use of eye catching graphics was deemed mandatory. A considerable amount of time was dedicated towards ensuring that the section labelled Frequently Asked Questions (FAQ) was accessible and searchable in a variety of ways. Since the website specifically targeted novice users, the FAQ section had a much greater likelihood of widespread access than in other web portals. It was also identified that the FAQ section should be populated through questions raised by those users seeking the answers. Hence, question raised by novice users from a previous study was utilised to formulate the FAQ (Szewczyk & Furnell, 2009). In addition to the overall layout the question of accessibility for seniors and those with disabilities imposed by age were also key elements. Seniors who are novice users are more deeply disadvantaged through a range of somewhat obvious issues such as font size, background colour, and language (Ball, 2008). The consideration here is not simply one of accessibility, but also one of language, context and environment.

The navigation for a proposed web portal to solve these generational differences was therefore designed to meet five fundamental criteria. Firstly, the navigation needed to ensure everything was very easy to find. Secondly, the site navigation needed to be consistent on each page and to offer a certain comfort and reliability in terms of browsing. Thirdly, each section of the site incorporated generationally clarity by means of obvious section names that enabled unambiguous navigation. Obscure words such as “resources” and “tools” were avoided and instead the site used obvious button names such as “news” and “podcasts”. The fourth characteristic for the navigation was to employ a strategy of “less is more”. This meant avoiding too many buttons, long lists of options, and the use of too many separate navigation bars. The last feature of the navigation was to remind the user where they were. This was achieved using a consistent method and by changing the colour of different sections so that a user could feel a difference in terms of each different environment.

EVALUATION AND PARTICIPATION

Having developed a prototype security information portal, it was deemed necessary to evaluate the research product against a pilot audience. The participants for this study came from a variety of informal sources through a snowball technique that identified respondents as Baby Boomers who did not have expert knowledge or experience with internet-based web portal usage. 29 participants who were not directly known to the researchers formed a pilot focus group assembled to assist the early directions of the research. Participants were invited to take part in the research as part of an informally promoted invitation to senior acquaintances of university staff and students. Respondents gave a broad range of comments and observations based upon their one-off first time interaction with a sample portal (Davies and Dodd 2002; Koro-Ljunberg 2008; Whyte 2001). Since in this instance the prototype portal required some base-line commentary to shape its critical effectiveness, it relied in this first instance upon a system of response that aimed to sit as an unobtrusive online exchange of ideas (Riva, 2001). Respondents noted areas of greatest frustration and areas that showed promise and were distinctively helpful. Based upon the responses the qualitative survey revealed that the need to address three main criteria. The researchers acknowledge the relatively small group of participants used in determining these early characteristics. The purpose of this pilot study was to determine that significant areas of concern existed, and that subsequently there was a need to address this in a more substantial and rigorous statistical analysis once a range of specific portal problems were identified.

Assurance and Acceptance

Elderly users were asked how much trust they placed in the sample portal compared to other online security information sources. Respondents mentioned uneasiness about the various assurances that were proffered in the portal (Table 1). Senior citizens begin from a base of scepticism in terms of technology, based on their perceptions of a widening gap of information, and also their fundamental understanding of the basic online security message. In the portal one clear message is that any new communication or program could be presumed malicious.

Since the prototype portal discusses many of the same themes that senior novice users will have heard of in passing, but not become fully aware of in expert terms, the starting point in terms of acceptance and assurance is always going to be biased towards an assumption of possible harmful intent. The objectives of any such portal might appear suspicious simply because of a lack of commercial imperative. In simple terms, “if the portal can be accessed for free, what is the catch?” The irony here is that a similarly presented portal that includes small charges requiring online payment (yet owned and operated by malfeasant actors) is more likely to gain a novice user’s acceptance than the portal which is the subject of this study, since this portal offers its information, guidelines and steps for free. Respondents to the survey commented that the portal wasn’t convincing in comparison to other portals. Many participants felt there were more reliable informational portals and at least some related price as a factor insomuch as there was uniformity of agreement about “free” portals being likely to conceal some form of financial misdirection.

Table 1. Acceptance of the information on the portal as reliable, believable and usable.

Assurance and Acceptance		
Accept advice at Face Value	Somewhat Sceptical	Sceptical and Don't Believe the information is free
14%	29%	57%

Step by Step Instructions

The second strong theme that the survey revealed was the manner by which participants could independently enact a solution. Respondents were asked to comment on whether they were reliant upon ordered instructions or whether they were confident to navigate on their own. By far the overwhelming acceptance centred on the key feature of step by step instructions, and on the basis of task-based interaction (Table 2). The important feature for novice users was the ability to carry through a single task rather than the multi-tasking options that most programs (including most security malware / antivirus programs) like to deploy. The irony of the saleability/viability of antivirus software to novice users is that the more options and functionality that is made available in a particular program, the less likely it is that a novice senior computer users will recommend the software.

Table 2. Respondents' reliance on Step by Step instructions for implementing security programs such as antivirus software.

Step by Step Instructions		
Always use Step by Step instructions	Prefer Step by Step Instructions	Confident to navigate freely
71%	29%	0%

Updates and Uninstalls

A third theme that emerged from the surveys was the issue of concrete guidelines in regards to uninstalling old and no longer used programs, whilst updating and improving the use of other programs (Tables 3 & 4). Respondents were asked to comment on how they coped with change in terms of program updates and changes. Many respondents were hesitant to remove old programs. Some remembered being asked a question about removal of certain files that the participant had no understanding of. Mid way through an uninstall, any question that posed a consequence (eg: "removing these files may affect the ability to ...in the future") were likely to cause a great deal of angst because senior novice users perceive the removal of a program in a physical context and worry that once removed the 'object' might not be able to be replaced. Other update and uninstall prompts carry equal concerns, as on each occasion the user feels unable to make an informed decision.

The single broad theme running through most of the respondents' comments all linked to an aversion to making uninformed decisions. At one level the need for unambiguous step by step instructions is seen as the most useful component of the portal. At the other end of interaction, uninstall activities that produce unforeseen 'prompt' questions are regarded with concern because the user is exercising what they perceive to be a dangerous guess rather than an activity that can be easily rectified.

Table 3. Level of confidence to uninstall a security-related program or execute a command that removed files.

Uninstalls		
Confident to execute an uninstall	Would proceed but with some caution	Not confident to proceed on their own
0%	14%	86%

Table 4. Level of confidence to update a security-related software program.

Updates		
Confident to execute an update	Would proceed but with some caution	Not confident to proceed on their own
14%	29%	57%

CONCLUSION

The creation of a computer security web portal that is designed specifically for elderly novice users illustrates a large gap in the market for web-based information. Senior novice users are highly vulnerable information seekers whose quest for a practical security solution brings to the fore difficulties with existing security web portals (Whitson, 2008). The research of existing security information portals makes it clear that security web portals in general are either designed for users with skills above the novice level, or otherwise are designed to take advantage of novice users. This project has deliberately circumvented the pattern of many other security web portals by avoiding the temptation to create a hybrid information platform that caters to both novice users and those with some skills. To the contrary, this project has demonstrated that hybrid models are unlikely to serve any useful purpose to novice users since the very act of using a web-portal must either start from a no-knowledge/ low knowledge position, or otherwise begin from a set of basic assumptions about exactly what a novice user might or might not know and understand. This paper highlights the need for further research into how best to educate senior novice computer users, and acknowledges the rapidly increasing demand for novice instruction that is commensurate with the increasing number of internet-connected computer users.

Based upon this initial pilot study, the next step proposed by the researchers is a more detailed and rigorous investigation into the three specific portal deficiencies of trust and financial confidence, navigational efficacy, and assurance in decision making. It is the intention of the researchers to develop the prototype portal more fully in order to embed solutions into its layout that would address these three deficiencies through the already identified conduits of language, accessibility, and hypermedia. This paper reveals some broad issues in relation to senior novice computer users. There is a need for a more detailed study of the various elements that differentiate senior novice computer users from mainstream first-time computer customers. This research is therefore presented as a progressive research endeavour that will more fully develop key differentiators for a hypermedia information portal that more clearly satisfies the needs of senior yet novice computer users.

REFERENCES

Ball, S. (2008) Design for all – how web accessibility affects different people. In Craven (Ed.) *Web accessibililty: practical advice for the library and information professional*. London: Facet publishing.

Ciampa, M. (2010) Security Awareness: Applying Practical Security in your world, Third Edition, Boston: Cengage

CyberSmart. (2010). CyberSmart - Internet and mobile safety advice and activities. Retrieved September 13, 2010, from http://www.cybersmart.gov.au/

Davies, D., and Dodd, J., (2002) Qualitative Research and the Question of Rigor, *Qualitative Health Research*, Vol 12, no.2. pp 279-289.

Dickinson, A., Newell, A.F., Smith,M.J., and Hill, R.L. (2005) Introducing the Internet to the over-60s: Developing an email system for older novice computer users, *Interacting with Computers*, Vol 17 Issue 6 pp 621-642.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Ellis, R. D., & Kurniawan, S.H. (2000) Increasing the Usability of Online Information for Older Users: A Case Study in Participatory Design, *International Journal of Human-Computer Interaction*, Vol 12 Issue 2, pp 263-276.

Furnell, S., Shams, R., & Phippen, A. (2008). Who guides the little guy? Exploring security advice and guidance from retailers and ISPs. *Computer Fraud & Security*(12), 6-10.

GetSafeOnline. (2011). Get Safe Online. Retrieved January 9, 2011, from http://www.getsafeonline.org/

Koro-Ljunberg, M. (2008) Validity and Validation in the Making in the Context of Qualitative Research, *Qualitative Health Research*, vol18, No.7. pp983-989.

Lusardi, A & Mitchell, O.S. (2007) Baby Boomer retirement security: The roles of planning, financial literacy, and housing wealth, Journal of Monetary Economics, Volume 54 Issue 1 pp205 - 224, Retrieved March 25th, 2011 from http://www.sciencedirect.com/science

McCloskey, D.W. (2006) The Importance of Ease of Use, Usefulness, and Trust to Online Consumers: An Examination of the Technology Acceptance Model with Older Consumers, *Journal of Organizational and End User Computing*, Vol 18 No.3

NetAlert. (2010). NetAlert - Protecting Australian Familes Online. Retrieved August 25, 2010, from http://www.netalert.gov.au/

Nielsen, J. (2009) Web Useability: Interview with Jakob Nielsen, Retrieved November 13, 2010 from

http://www.webdesignerdepot.com/2009/09/interview-with-web-usability-guru-jakob-nielsen/

Pfleeger, C. P. and Pfleeger, S. L. (2007) Security in Computing, Fourth Edition, Boston: Pearson, Prentice Hall

Riva, G. (2001) The Mind over the Web: The Quest for the Definition of a Method for Internet Research, *CyberPsychology and Behaviour*, vol4, No.1. pp7-16.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 51*(1), 92-100.

StaySmartOnline. (2010). Stay Smart Online - About. Retrieved October 12, 2010, from http://www.staysmartonline.gov.au/about

Szewczyk, P., & Furnell, S. (2009). *Assessing the online security awareness of Australian Internet users.* Paper presented at the 8th Annual Security Conference, Las Vegas, NV.

Szewczyk, P., & Valli, C. (2009). Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective. *Journal of Digital Forensics, Security and Law, 4*(3), 5-16.

Whitson, G. (2008) Security for Service Oriented Architectures, Journal of Computing Sciences in Colleges, Vol 23, Issue 4, Retrieved October 18, 2010, from http://portal.acm.org/citation.cfm?id=1352083

Whyte, W. (2001) *Research Methods for the Study of Conflict and Cooperation*, In Bryman (Ed), Ethnography,3 vols, Sage Publications: London.