THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 7 | Number 4 Article 3

2012

An Australian Perspective on the Challenges for Computer and Network Security for Novice Endusers

Patryk Szewczyk
Edith Cowan University

AN AUSTRALIAN PERSPECTIVE ON THE CHALLENGES FOR COMPUTER AND NETWORK SECURITY FOR NOVICE END-USERS

Patryk Szewczyk
Security Research Institute
Edith Cowan University
Perth, Western Australia

ABSTRACT

It is common for end-users to have difficulty in using computer or network security appropriately and thus have often been ridiculed when misinterpreting instructions or procedures. This discussion paper details the outcomes of research undertaken over the past six years on why security is overly complex for end-users. The results indicate that multiple issues may render end-users vulnerable to security threats and that there is no single solution to address these problems. Studies on a small group of senior citizens has shown that educational seminars can be beneficial in ensuring that simple security aspects are understood and used appropriately.

Keywords End-user, security usability, software usability, ADSL routers, Internet Service Providers, cyber security, cyber safety

1. INTRODUCTION

The Australian Bureau of Statistics (ABS) (ABS, 2012) reported continued growth of Internet subscribers, with almost twelve million active Internet connections in Australia as of December, 2011. This trend is expected to be extended through the Australian Government, National Broadband Network (NBN) initiative. Australian consumers will have access to a high-speed Internet connection, through either fibre optic cabling, or fixed wireless technologies (DBCDE, 2011). The incentives for adopting an Internet connection are varied. For the millennial generation social communication, gaming, and educational resources are typically sourced online while baby boomers and baby busters may have less of a need to access the Internet. However, live news, share trading, banking, online shopping discounts, medical advice, entertainment and travel resources provide significant incentives for all generations to have Internet access.

Unfortunately, the Internet has made it increasingly easy for individuals to use

this medium for profiteering scams, fraud and online attacks. Whilst operating system updates, anti-virus scanners, and personal firewalls reduce the probability of successful attacks, to be effectively protected end-users must recognise their importance, understand their functionality, and most importantly know how to optimize the protection mechanisms' potential. Moreover, sophisticated phishing scams, conflicting opinions on ideal security software, and technical cyber security jargon, have made it challenging for the average consumer to protect themselves online. Government departments have taken it upon themselves to create online portals (Get Safe Online, 2012; StaySmartOnline, 2010) with detailed information for protecting end-users online. However, the content tends to be limited, and does not address all aspects of online security in a rapidly changing environment.

Opinion is divided on who should be responsible for the online protection of novice end-users. Manufacturers continually enhance products and technologies to help protect end-users from online threats; however some manufacturers, professionals and academics believe that cyber security responsibility lies with the individual (Phippen & Furnell, 2007). End-users must be well aware of the risks and the potential outcomes, if sufficient cyber security is to be applied. Secondly, the user must have the appropriate supporting information to guide them through the implementation of the security process. Individuals are generally aware that their home premises could be physically broken into, and as a result consider a house alarm as one method of protection. Television, print and online media promote the simplicity of how a wireless network could be broken into and used to access or steal data (Seymour, 2010). However, simply highlighting the online risks, without providing solutions, may not result in effective actions by the end-user to secure a wireless network.

The paper presents six years of accumulated research into identifying the misconceptions and challenges that end-users face when attempting to utilise security effectively. The research began with an attempt to determine what prevents end-users from applying and using security. Figure 1 shows the progression of the research activity from an initial anonymous survey of novice end-users, which then lead to examining security manuals and undertaking personalised face-to-face interviews. The consumer interviews specifically identified that Internet Service Providers' (ISP) employees may be at fault, which initiated an ethics approved deceptive interview of ISP staff. The paper discusses the security information supplied by ISPs online and the usability of internet security software.

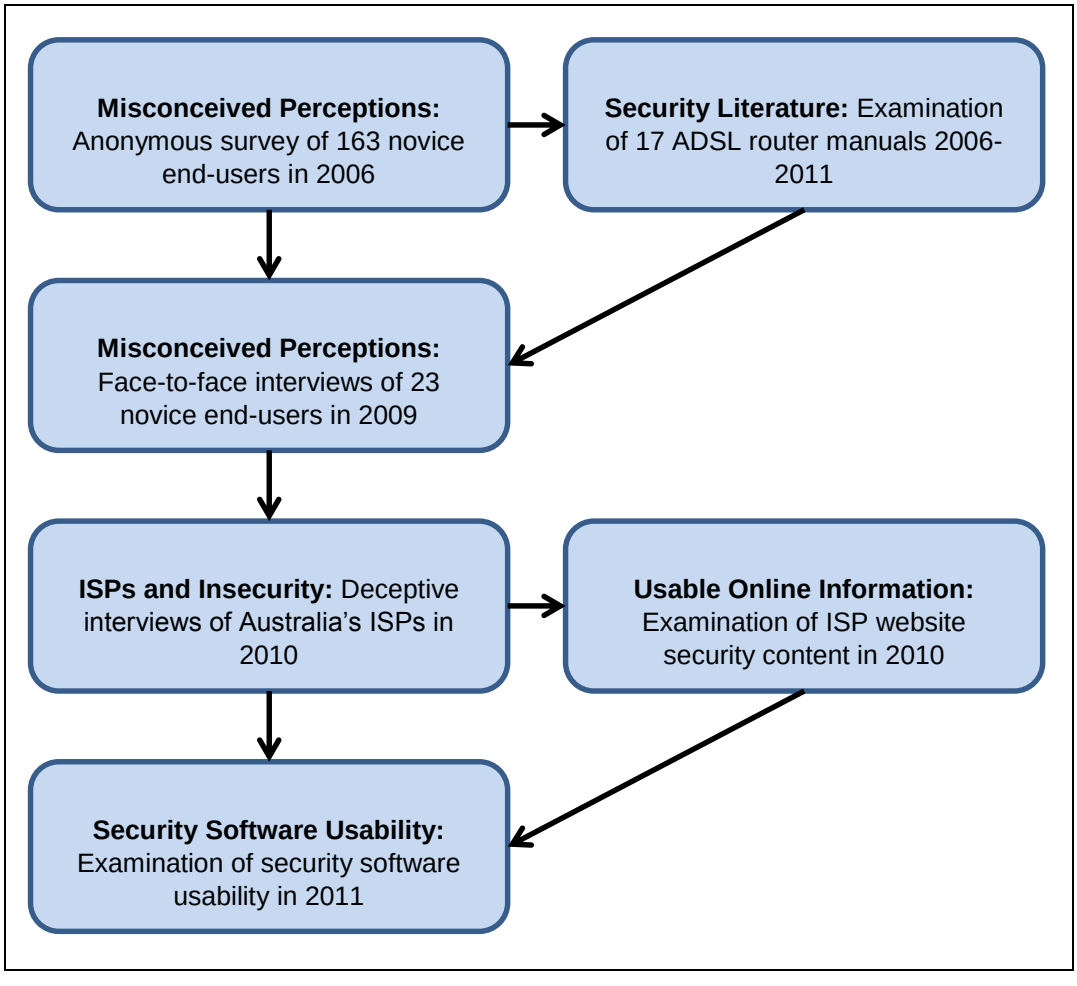

Figure 1 Timeline of Research Events

2. SECURITY CHALLENGES

In 2010, a two week study of 13 anti-virus vendors identified that on average each vendor was able to detect and provide a solution, for only 90% of newly released malware (Cyveillance, 2010). Vendors may often struggle to detect malware and release signature updates, due to malware developers using anti-forensics and anti-avoidance techniques (Brand, Valli & Woodward, 2010). Vendors were also challenged by the 300% surge in newly released malware specimens throughout 2009 (ScanSafe, 2009). The statistics indicate the safety limitations to end-users who purchase such software particularly as malware takes on new forms. Modern

malware is targeting devices other than the traditional PC paradigm including; Asymmetric Digital Subscriber Line (ADSL) routers, smart phones and gaming consoles (Čeleda, Krejčí, Vykopal, & Drašar, 2010; Symantec, 2009). The malware specimen known as 'psyb0t' alone had the capability of infecting 55 types and models of ADSL routers, and had been pre-populated with 6000 usernames and 13000 passwords (Paul, 2009), yet consumers were generally unaware of such threats with the worm's attributes generally reserved for industry professionals and academics.

Most current ADSL routers incorporate an 802.11 wireless access point; however many are sold with the wireless access point pre-enabled. If the end-user has no need for a wireless network, and does not manually switch off the feature, they are providing access to their wireless signal in the immediate neighbourhood. An open wireless network, coupled with Wi-Fi pineapples (Simpsons, 2012), can be used by cyber criminals to intercept and capture private data. When an end-user attempts to connect to their open wireless network, they would connect unknowingly, through the Wi-Fi pineapple of a cyber criminal, who can capture and misuse private data (Purvis, 2012). This is further problematic with local governments and retailers in large cities providing free wireless internet access (Hutchinson, 2012). Vendors typically promote the benefits of using a wireless network, yet fail to highlight the dangers. Accordingly, an ill-informed end-user could leave a wireless network unsecured.

3. MISCONCEIVED PERCEPTIONS

The millennial generation are encouraged to utilise the Internet to access a range of services, with many retailers for instance offering incentives or discounts if consumers purchase items or services online. Senior citizens or those who have retired from work cannot easily escape the realm of online services. Traditionally, they used a passbook to access their savings account but are now encouraged to use the Internet for personal monetary transactions, unaware of the associated risks (Cook, Szewczyk, & Sansurooah, 2011). Senior citizens who have created a portfolio of savings may need to access or manage it through online systems. Unfortunately, regardless of the age, qualifications and occupation, many end-users are unfamiliar with the associated security risks of using the Internet for such day-to-day tasks (Szewczyk & Furnell, 2009).

Since the 1960's psychological research has explored the link between an individual's attitude and their subsequent behaviour (Ajzen, 1980; Eagly & Chaiken, 1993). A positive attitude towards a given subject has been shown to result in a positive, proactive behaviour towards that same subject matter. Therefore, should an end-user have a positive experience and attitude in

configuring an ADSL router, or security software, this should result in a positive, and ongoing interest in ensuring the product operates correctly. However, end-users who attempt to configure and secure their home networking products themselves perceive it as an unpleasant, difficult and a time consuming experience generally blaming product manuals, quick start guides, and after sales support (Szewczyk, 2006).

To initiate the security research into end-user attitudes and perceptions, an online survey was created and deployed targeting novice end-users (Szewczyk, 2006). Respondents were encouraged to only attempt the survey if they felt they were inexperienced in computing. The anonymous survey was completed by 163 respondents and showed that over 75% felt unsafe when using the Internet. Many knew that online dangers existed, but could not specifically name or identify any potential threats moreover, thirty percent of respondents claimed that they applied appropriate safeguards to their ADSL router. Factors such as access point placement, and adjusting signal strength were beyond the comprehension of many respondents, with most end-users utilising trial-and-error approaches to successfully configure their ADSL router.

The survey allowed a large sample of responses and was complemented by face-to-face interviews with 23 novice end-users during 2009. The 23 individuals were selected based on their self-confessed skill level in security and computing. The aim was to better understand end-users perceptions and attitudes towards their security and privacy when using the Internet (Szewczyk & Furnell, 2009). Most respondents generally felt unsafe when conducting financial transactions online, but felt that they had no other choice. Some felt that large corporations were deciding how and where money could be accessed. Many banks for instance will offer a small additional interest rate on a savings account which can only be accessed via that bank's website. Interviewees often felt alone when requiring help with such security. Respondents were questioned on where they would acquire support from when needing assistance in relation to security. Most respondents (20) stated that they would seek support from ISP employees. The prominent reason for this was that the respondents felt that ISP employees were actually trained, and had the expertise to provide reliable and trustworthy advice and guidance on computer and network security.

Individual perceptions as to whether users would ever be targeted online by criminals varied considerably, with many perceiving that their financial status will be influential. This in-turn influenced how much security will be applied to their computer system. Many respondents believed that a criminal would purposefully avoid attacking the computer of an individual with a lower financial income (Szewczyk & Furnell, 2009).

Naive individuals may not only be targeted online by criminals, but by staff who opportunistically seek sales. One interviewee claimed that they took their wireless ADSL router to a computer store and were sold another device, with no wireless antenna, yet the wireless functionality can be disabled effortlessly on all ADSL devices. A lack of awareness and miscommunication between a novice user and a salesperson could frequently result in poor outcomes. For instance, many interviewees saw anti-virus software as a preventative solution. However, many respondents believe that the only viable solution to a computer that is infected with malware was to replace the hard drive with a new one. This misconception is not surprising, in that many retail outlets, who remove malware from a computer, use terminology suggesting that a new hard drive and software are being installed.

The current attitudes and perceptions of many end-users towards security are flawed from a security perspective. End-users must understand that they can be a target regardless of their financial income or sensitivity of information on their computer. For those in the workforce, some individuals may be provided with Security Education, Training and Awareness (SETA) courses at their place of employment, which then can be passed on and applied in their home environment. Current research has shown that senior citizens are enthusiastic in attending training and education seminars (Cook, Szewczyk, & Sansurooah, 2011). Initial surveys showed that many senior citizens increased their understanding of security risks considerably following simple dissemination of online threats and solutions. The key to increasing awareness is making the content enjoyable, appropriate for the given audience, and most importantly, simple to comprehend. Television media does discuss wireless threats (Seymour, 2010), but generally does so in a complicated manner. For instance television media showing criminals using the BackTrack Linux Distributions (BackTrack, 2012) may not only further confuse the audience, but may also leave them thinking that such an attack may never target them, only occurring in science fiction movies.

4. SECURITY LITERATURE

End-users' perceptions of computer and network security and the associated threats were shown to be inaccurate and their understanding of how to secure an ADSL router and wireless network more questionable. Each ADSL router is operational out of the box. At most, the end-user will need to run a software wizard, or utilise the provided CD to appropriately configure the device. The research indicated that many users struggled to apply the appropriate safeguards, and often blamed the product literature. In the online survey of 163 individuals, 87% stated that they had difficulty interpreting and applying the installation procedures.

Information technology manuals should theoretically present end-users, who have varying technical competencies, with simple and effective instructions on how to install and secure the given device. Wieringa, Moore and Barnes (1993) suggest that a well-designed and usable manual will include; a well written set of procedures, information on the most effective way of completing a task, and be suitable for both a skilled and novice user. Perelman, Paradis and Barret (1998) assert that five criteria should be embedded in all high quality procedural literature. A technical manual should have or use:

1. A well designed index page for quickly locating desirable information quickly;
2. Descriptive page headers and a table of contents;
3. An outline of the reasons for its creation, the intended audience, and required level of expertise;
4. A detailed glossary to elaborate on uncommon terminology; and
5. Numerous, large, labelled graphics, clearly depicting each step in the procedure.

The way in which procedures are written and presented by vendors may significantly impact their interpretation. End-users placing the blame on poorly written manuals could be correct or they were not willing to follow the instructions. From 2005 through to 2011, 17 manuals were examined from the leading manufacturers of ADSL routers in Australia (Andersson & Szewczyk, 2011; Szewczyk & Valli, 2009). Informative content to setup and secure the device was undeniably present within the manuals; however, the manner in which it was presented was questionable, which could leave an end-users confused.

Since the initial examination of ADSL router manuals in 2005, little has improved through to 2011 (Szewczyk & Valli, 2009). As portrayed through Table 1, many manuals do not encompass many of the essential elements to ensure that the product manual is usable. The most important element being the index page has been omitted from the majority of manuals. The computing industry uses a copious amount of technical language thus a glossary could easily be used to explain complicated terminology. Unfortunately less than fifty percent of the manuals examined incorporated this feature. Many computing words have become mainstream, but for those with little understanding, the terms Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) may have little meaning in the context of novice end-user security.

The procedures and graphics are a separate and complicated issue. In many instances the graphics are on a small scale and difficult to interpret. Coupled with the issue of manuals referring to firmware version 1.x, yet the device encompassing firmware version 2.x creates another dilemma in that the interface and functions are usually entirely different. Not only does this leave the end-user

stranded, but any future updates to the firmware and its associated interface will only further make the manual entirely redundant for a novice end-user. Aside from a security perspective, vendors do not adequately encourage the use of security. For advanced end-users who know which security features should be used, the process of following the procedures may seem simple. However, for the novice end-user who bases their judgements on the recommendations provided by the vendors, this creates an entirely new issue. As shown through Table 1 only Netgear continued to encourage and recommend that specific security features be implemented. Many vendors would unfortunately stipulate what security features are available without justifying their use or benefits. This is problematic in that an end-user has little motivation to update the firmware if for instance they are unaware of the protection it may provide from embedded malware.

Table 1 Comparison and Contrast of Product Literature Design

ADSL Routers / **Criteria**	Page Headers	Contents Page	Index Page	Glossary	Clear Graphics	Graphic Captions	Intended Audience	
Billion 7202		□						2005
D-Link G604T Gen 1		□			□			
Motorola SBG900		□		□				
NetComm NB5PlusW		□		□	□			
Netgear DG834G	□	□		□		□	□	
Siemens 6520		□						
Belkin F5D7633au4A		□		□				2009
D-Link G604T Gen II		□			□		□	
NetComm NB5PlusW		□		□	□			
Netgear DG834g V5	□	□			□	□	□	
TP-Link TD-W8901G		□			□	□		
Billion 7800N		□			□			2011
Netgear DGN 1000	□	□	□			□		
D-Link DSL-2740B	□	□			□			
Netcomm NB6		□	□	□			□	
TP-Link TD-W8151N		□			□			
Belkin F7D1401	□	□			□			

The adoption of a broadband internet connection will presumably continue to

increase. The ADSL router provides a simple yet effective security solution at the entry point to a home or commercial network. For instance, the manufacturer Quality Network Appliance Provider (QNAP) incorporates a feature within its devices which notifies the end-user when a firmware update is available. This is achieved via a notification window when the end-user logs in to configure the device. End-users may unfortunately follow a "setup-and-forget" approach meaning there is no reason to access the configuration options on a regular basis. Subsequently, manufacturers should incorporate simple software on the already included configuration media which checks and downloads any appropriate updates to the ADSL router should it become available – similar to anti-virus software. There is enough deterrence with updating firmware as it is, with many manufacturers including numerous warnings regarding how the device may become damaged with an inappropriate firmware upgrade. A streamline approach may not only ensure an end-users safety online, but also remove any unnecessary confusion presented to the end-user.

5. INTERNET SERVICE PROVIDERS AND INSECURITY

The research interviews and surveys described above identified that many respondents re-iterated their perception of employees, working within Internet Service Internet Providers (ISPs), as being experts in computer and network security (Szewczyk, 2006; Szewczyk & Furnell, 2009) yet such employees are not necessarily employed to provide guidance or advice on security. Furthermore, the role of an employee working on a help desk may attract an inexperienced individual, who may rely on opinion on computing and security. However, ISP employees are perceived as a convenient, 24 hour, 7 days a week source of advice. To evaluate the quality of advice provided by ISP staff, the research utilised a deceptive interview approach, whereby the researcher mimicked a novice end-user over the telephone (Szewczyk, 2010). Seven of the largest ISPs in Australia were contacted over a three month period and questioned over methods for both securing an ADSL router, and a computer.

Unsurprisingly, whilst novice end-users may perceive ISP employees as experts, their guidance and recommendations were far from ideal from a security viewpoint when compared to current industry recommendations and best practices (Goodrich & Tamassia, 2011; Nahorney, 2009). When the issue of securing an ADSL router were raised, ISP staff would either direct the researcher towards the product manual, the ISP's website, or in one instance provide a very invalid response by stating that "ADSL routers do not have security settings" (Szewczyk, 2010). Clearly, the manual itself lacks readability and encouragement for the end-user. However, to claim that the device has no security functionality may clearly endanger an end-user.

The employees at times did provide realistic and ideal responses, yet many continued to provide erroneous responses. When questioned over recommended wireless or computer security options, opinion, rather than fact began to emerge. Many ISP employees continued to re-iterate that WEP was the ideal wireless security setting, whilst others would direct the researcher to utilising information found on the ISP website, or towards Google – with no clear indication as to what terms should be searched for. In terms of computer security advice, the employees were more skilled when recommending that a personal firewall and anti-virus software be installed. Two employees, from two ISP were unhelpful and unaware, stating that Windows 7 is secure out-of-the-box and does not need any additional modification. In one instance, the employee stated that the local computer store should be approached for advice and recommendations on which software would be more suitable.

The results of the survey indicate that the employees within ISPs, whilst being somewhat helpful, did not possess the knowledge or skill set required to suitably advise customers seeking help when compared industry best practices for safeguarding a computer or ADSL router. Whilst there is not just one solution to a particular security issue, there are at least ideal answers which could have been provided. An additional outcome amongst the feedback provided by employees was that of the content located on their website. Many employees re-iterated that there was an abundance of information on the ISP website which detailed best practices for ensuring that a computer, network and ADSL router are secured appropriately.

From the information reviewed, no-where amongst help pages or contact information provided by Australian ISPs does it state that it is the job of the help desk employees to provide security advice. This could be a positive characteristic because it reduces the amount of training that employees needed to function in their role. Being an entry level position in the IT industry, many help desk employees would be beginning their career at such a premise. So why then, do the employees take it upon themselves to not only provide advice on security related matters, but more seriously provide incorrect recommendations? Whilst these employees may feel the need to help those seeking guidance, in many instances they have been identified as providing inappropriate advice. In the majority of instances, the end-user seeking guidance would have been additionally vulnerable to internet based attacks. An ISP needs to train staff appropriately to handle such incidents where a customer seeks guidance. Alternatively, employees within an ISP need to be directed that they do not provide any security related guidance.

6. UNUSABLE ONLINE INFORMATION

ISP employees encouraged customers to utilise the security information on their website. In most occurrences the employees were unable to direct the customer to the exact location of the information. Empirical investigations conducted by Tan and Wei (2006) demonstrated that a well-structured website will facilitate end-users in locating desirable information and accomplishing their goals. Hence, security information on each ISP website should be easily located and designed in a manner which will permit the end-user to navigate to the required sections. More importantly, the website should attract an end-user into the security section so that security can be applied or reviewed if it hasn't already been done so. Eleven websites of ISPs in Australia were examined for their accessibility, currency, and accuracy of security related content (Szewczyk, 2010). Unfortunately, only two ISPs had content which was easily accessible, simple to locate, and relevant for the time period, equipment and operating systems currently utilised.

There are numerous issues which emerged from the examination of ISP based online security information. In some instances, even though Windows 7 has been available for a considerable period of time, many were still referring to, and showing step-by-step instructions for Windows 98 or Windows XP. Subsequently, in some instances an ISP would demonstrate how to install a specific piece of software (personal firewall, or anti-virus software), although would be showing a product which is outdated by three to five years. Locating security related information on many of the ISP websites was almost impossible. As demonstrated in Figure 2 and 3, a search for "wireless security" can yield entirely diverse results. One ISP has results which related to the purchase of wireless based products from within their online shopping portal, whilst the second ISP did actually yield correct and appropriate results.

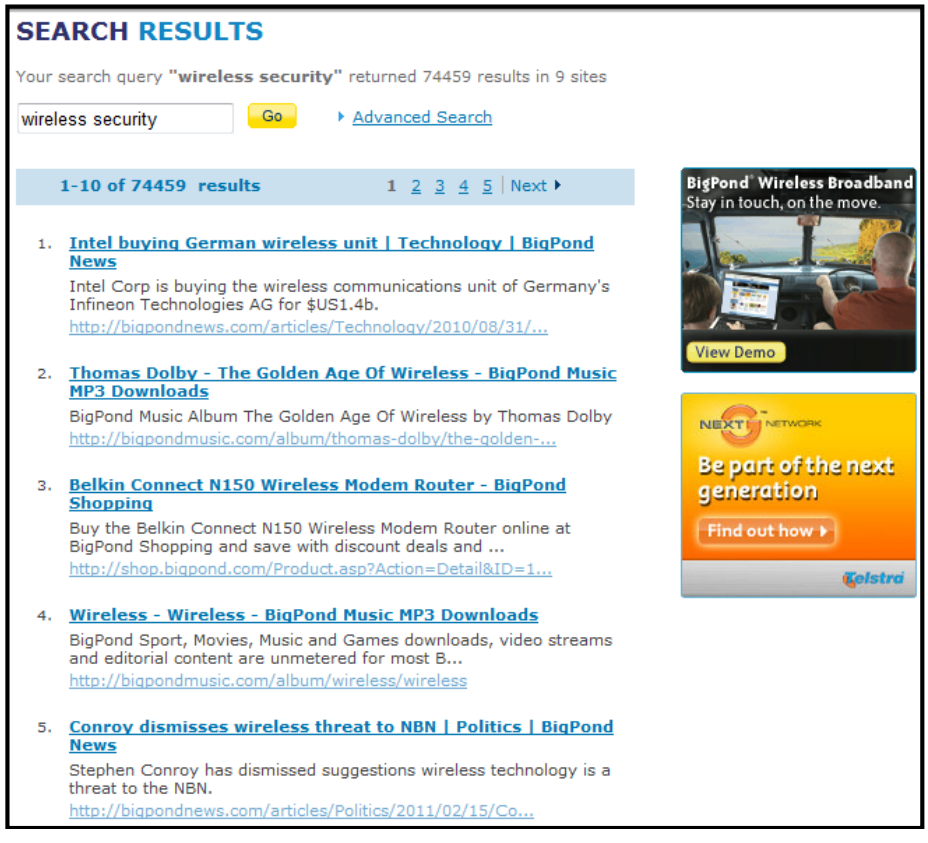

Figure 2 Bigpond Search Results for Wireless Security

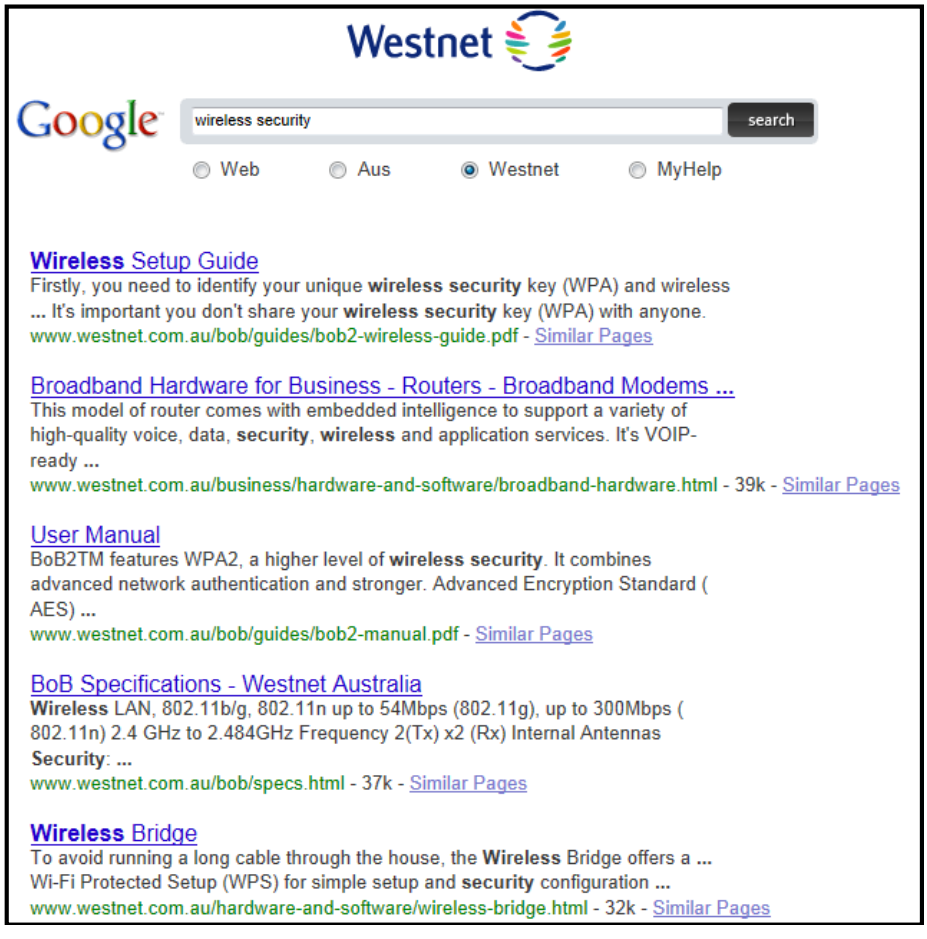

Figure 3 Westnet Search Results for Wireless Security

Two of the eleven ISPs examined encompassed security information which was easily accessible, current and accurate. These two ISPs – iinet and Westnet are generally targeted towards heavy internet users or those individuals who could be perceived as IT professionals and enthusiasts. However, large Australian ISPs such as Bigpond or Optus who are generally utilised by novice and leisurely end-users did not encompass any usable security information. This is ironic in that it is these novice end-users who would usually require the most support and guidance when utilising the Internet, rather than being sold products that they have no real use for.

A significant issue amongst the security related information of the remaining seven ISPs was that of how the information is actually presented. It is of no benefit to an end-user to state that an ADSL router password should be changed –

if there is no recommendation on good password practices, or details as to how the password should actually be changed. Many ISPs also shifted the security on Internet Security Suites, as an all in one solution for mitigating any internet related threats. On the other hand, Bigpond and Optus, were not only using scare tactics but also marketing their own proprietary security software as a world market leader according to their own independent studies. These products were relatively expensive, claimed to be top of the range, and discouraged the use of freely available security software. There are many freely available software packages available which provide reasonable online protection, yet many ISPs would negate the quality of the freely available software.

It is not surprising that many ISP employees were unable to direct the research towards the security information on the ISP website, seeing that in most instances, the information did not actually exist. There are eleven prominent ISPs in Australia, yet only two of these emphasise security and privacy to its customers. The information on many of these websites needs to be regularly updated and easily accessible. In addition ISPs need to focus on showing freely available products to their customers as a means of securing their computer as this may not only protect the end-user, but may also prevent potential attack on the ISP or its other customers.

7. SECURITY SOFTWARE USABILITY

The security information supplied by ISPs on their website was generally outdated and difficult to locate, and in most instances did not adhere to good website design practices (Tan & Wei, 2006). However, many of the statements did encourage the use of security software. Whilst traditional security software made use of a personal firewall and a separate anti-virus program, many vendors today are integrating each of these elements into an Internet Security Suite. There is also a trend with vendors marketing their products as usable, easy-to-use, and simple. ZoneAlarm's Product Manager Jordy Berson (2005) claims – even his parents could utilise his product. The usability of security software has been a long standing issue. In 1975 it was identified that end-users would fail to adopt security systems unless they were easy to use (Saltzer & Schroeder, 1975). In the paper "Why Johnny Can't Encrypt" (Whitten & Tygar, 1999) the researchers identified that with a well-designed interface, participants in their study were still unable to use the software effectively. Retail outlets and ISPs are encouraging end-users to utilise Internet Security Software. This initiated the question of how usable are the available Internet Security Suites.

The top ten Internet Security Suites were acquired and evaluated for their responses and subsequent usability – when presented with current malware, recent

phishing sites, and penetration testing network scans (Szewczyk, 2011). Well-designed Internet Security Suites can play an important role in both protecting and educating end-users. Should an end-user visit a malicious website, the software may either block the website, or block and educate the end-user as to why the website could be malicious. Many personal firewalls will react and notify the end-user if a service is attempting to access the Internet. An unrecognisable service name has little merit in helping the end-user decide if they should allow or deny the service, or internet access. Meaningful explanations coupled with the potential risks of permitting the service to access the Internet have significant advantages in allowing the end-user to make the correct decision.

Many of the Internet Security Suites incorporated elements which would deter or prevent a novice end-user from protecting themselves effectively. Kaspersky raised a notification on the bottom of the browser stating "dangerous URL". It did not provide any further information, or explain what a URL is, potentially leaving an end-user confused with how to proceed. Alternatively eScan would block a phishing website with text stating "Access Denied" followed by "Suspected Phishing Site", without a definition or possible consequences should an end-user proceed. In a similar manner Bit Defender presented the user with "The webpage has been blocked" because it "included objects that were infected", providing little information as to what an object is, or where it originated. There is little merit from the end-users perspective, for security software to block access to a website, without any justification. If a potential threat is detected, it would be appropriate for the security product to provide a brief outline of why the website has been blocked, dangers associated with the website, and a recommendation on how to proceed.

The guidance provided with relation to dealing with malware appears to be an overlooked task by vendors. Mimicking the process of an end-user downloading a malicious file - a malware specimen was placed on the desktop of the test workstation. Bit Defender, Eset, and Norton, immediately block access to the binary. No explanation was provided as to why the file was inaccessible; instead an alert was raised informing the end-user of a virus. Norton in particular would not permit the file to be deleted. In every instance that an attempt was made to delete the file, Norton would alert that a threat was present, and that file was inaccessible. However, once a system virus scan was initiated, the file was removed. Such a process is not only confusing and complicated for a novice end-user, but also does not clearly provide step-by-step instruction as to what needs to be undertaken to remove the threat.

One of the prevalent outcomes of the experiment was how little control an end-user has once a workstation is infected with malware. Software alerts are generated notifying of the threat. However, the end-user is predominantly

instructed to click through a series of acceptances to initiate a scan or to agree in removing the malware specimen, in technical uninformative instructions. Trend Micro, and ZoneAlarm did raise an alert of a potential virus when accessing the website containing the malware specimen. This fortunately did permit the user to agree or disagree in downloading the potential threat to their system. Whilst an explanation of the threat was raised, no recommendations were generated as to whether or not the user should continue with the download or omit it entirely.

Security software usability will always be an ongoing issue. However, vendors do have the options to simplify the decision making process and even educate the end-user as to what could happen if a certain option is chosen. The term virus has become mainstream throughout the years, so anytime the word virus appears; this should come across as dangerous to the end user. However, other controls are more technical and require advance knowledge, or further education before any decision can be made. When a Windows service requires access to the Internet, the firewall will stipulate the process name that requires access. These process names can be quite meaningless. However, the process could be an anti-virus software requiring access to update its signatures, or a malicious host attempting to access the workstation.

8. EDUCATION AS A SOLUTION

The fundamental criteria for helping end-users use security effectively is education. Senior citizens are perhaps most impacted by having to undertake in many online activities, yet a simple education program designed to explain security concepts has shown success in early trials (Cook, Szewczyk, & Sansurooah, 2011). In a similar manner that a child learns mathematics and languages in primary school, end-users must learn security techniques and best practices from the ground up. A group of senior citizens were told how and why a criminal may want to send phishing scams via email. A collection of legitimate and phishing emails were then shown to the group with a greater emphasis placed on the emails that were misleading. The group was shown step-by-step how to identify phishing emails, and within a short space of time were able to confidently identify fraudulent emails themselves.

Applying this method to online, security information portals; product manuals; and security software may successfully improve end-users' awareness and understanding of online threats. The predominant flaw amongst all information sources was assumed prior knowledge, which end-users usually do not have. For instance, if security software has an option to enable phishing detection, an end-user may disregard this if they are unfamiliar with its purpose. In the context of wireless network, vendors could outline the potential consequences of using a

wireless network and complement these with step-by-step solutions to mitigate each of the risks. Internet Security Suites are flawed in a similar manner, in that end-users may not necessarily know which feature should be enabled on a personal firewall or anti-virus software. However, providing a "ground-up" tutorial on common threats, and how the software can mitigate these, may educate the end-user, and act as a selling point for the software provider.

9. CONCLUSION

There is no doubt that end-users must protect themselves online, but the question remains who should be initiate this task. End-users are constantly presented with new challenges in the online world. The media has raised concerns over the Facebook timeline feature, showing end-users how to implement privacy settings on their account (Jacobsson, 2012). However, no where does it actually stipulate specific dangers if this is not adequately secured. Subsequently, end-users must be made more aware of the risks if proper action is not taken, but it must be explained using a jargon free, non-technical language.

This research has been undertaken over a six year timeframe to determine if using security is in fact a difficult task or if end-users are at fault when becoming a victim to an Internet based attack. Each research project emerged from a prevalent outcome from the previous research project. The research suggests that there are in fact many factors which could potentially deter or prevent an end-user from being secured. Security will never be adopted and usable by end-users if vendors continue to develop products without novice end-users as a part of the design process. ISPs are currently perceived by novice end-users as a reliable source of information, yet the deceptive study showed that the advice could have been improved upon significantly. In Australia, there is no call centre for end-users to communicate with an expert in cyber security. As a result, ISPs could take it upon themselves in providing security support to its customers.

Academics, commercial organisations, and governments have all attempted to help end-users use security effectively. Future research will focus on formulating and testing methods to educate novice end-users on the ways to implement, use and understand cyber security. This is vitally important in that technology is evolving at a rapid pace and is in-turn allowing criminals to exploit and develop threats for devices beyond the traditional PC. Subsequently end-users must have the appropriate educational material to protect themselves from future online dangers.

REFERENCES

ABS. (2012). Type of Access Connection. Retrieved January 12, 2012, from http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter3Dec%202011

Ajzen, M. F. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, N.J: Prentice-Hall.

Andersson, K., & Szewczyk, P. (2011). Insecurity by Obscrutiy Continues: Are ADSL router manuals putting end-users at risk. Paper presented at the 9th Australian Information Security Management Conference.

BackTrack. (2012). BackTrack Linux - Penetration Testing Distribution. Retrieved March 5, 2012, from http://www.backtrack-linux.org/

Berson, J. (2005). ZoneAlarm: Creating Usable Security Products for Consumers. In L. F. Cranor & S. Garfinkel (Eds.), Security and Usability: Designing Security Systems That People Can Use. North Sebastopol, CA: O'Reilly Media.

Brand, M., Valli, C., & Woodward, A. (2010). Malware Forensics: Discovery of the Intent of Deception. Journal of Digital Forensics, Security and Law, 5(4), 31-42.

Čeleda, P., Krejčí, R., Vykopal, J., & Drašar, M. (2010). Embedded Malware - An Analysis of the Chuck Norris Botnet Paper presented at the 2010 European Conference on Computer Network Defense (EC2ND), Technische Universität Berlin, Germany.

Cook, D., Szewczyk, P., & Sansurooah, K. (2011). Seniors Language Paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. Paper presented at the 9th Australian Information Security and Management Conference, Citigate Hotel, Perth, Western Australia.

Cyveillance. (2010). Malware Detection Rates for Leading Malware Solutions. Retrieved April 5, 2011, from http://www.cyveillance.com/web/docs/WP_MalwareDetectionRates.pdf

DBCDE. (2011). What is the NBN? Retrieved October 20, 2011, from http://www.nbn.gov.au/about-the-nbn/what-is-the-nbn/

Eagly, A. H., & Chaiken, S. (1993). The Psychology of Attitudes. Orlando, FL: Harcourt Brace Jovanovich.

Get Safe Online. (2012). Get Safe Online. Retrieved January 14, 2012, from http://www.getsafeonline.org/

Goodrich, M. T., & Tamassia, R. (2011). Introduction to Computer Security. Boston, MA: Pearson Education.

Hutchinson, N. (2012, February 14). Free WiFi on horizon. Guardian Express, p. 1.

Jacobsson, S. (2012). Facebook Timeline Privacy Tips: Locak Down Your Profile. Retrieved January 21, 2012, from http://www.pcworld.com/article/249019 /facebook_timeline_privacy_tips_lock_down_your_profile.html

Nahorney, B. (2009). Linux.Psybot—Is Your Router Secure? Retrieved November 21, 2011, from http://www.symantec.com/connect/blogs/linuxpsybot-your-router-secure

Paul, I. (2009). Nasty New Worm Targets Home Routers, Cable Modems. Retrieved April 20, 2010, from http://www.pcworld.com/article/161941 /nasty_new_worm_targets_home_routers_cable_modems.html?tk=rss_main

Perelman, L. C., Paradis, J., & Barret, E. (1998). The Mayfield Handbook of Technical & Scientific Writing. Mountain View, CA: Mayfield Publishing Company.

Phippen, A., & Furnell, S. (2007). Taking responsibility for online protection - why citizens have their part to play. Computer Fraud & Security, 2007(11), 8-13.

Purvis, C. (2012). The Pineapple Express: Hak5 Builds A Bigger, Better WiFi Honey Pot. Retrieved January 28, 2012, from http://securitymanagement.com/news/pineapple-express-hak5-builds-a-bigger-better-wifi-honey-pot-009470

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 1278-1308.

ScanSafe. (2009). ScanSafe Annual Global Threat Report 2008. Retrieved December 11, 2010, from http://www.scansafe.com/downloads/gtr/2008_AGTR.pdf

Seymour, B. (2010). Drive-by-hackers. Retrieved May 10, 2011, from http://au.todaytonight.yahoo.com/article/7907101/consumer/drive-hackers

Simpsons, D. (2012). WiFi Pineapple. Retrieved January 27, 2012, from

http://hakshop.myshopify.com/collections/frontpage/products/wifi-pineapple

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

Symantec. (2009). Linux.Psybot—Is Your Router Secure? Retrieved March 2, 2010, from http://www.symantec.com/connect/blogs/linuxpsybot-your-router-secure

Szewczyk, P. (2006). Individuals Perceptions of Wireless Security in the Home Environment. Paper presented at the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Szewczyk, P. (2010). Security Information Supplied by Australian Internet Service Providers. Paper presented at the 8th Australian Information Security Management Conference, Duxton Hotel, Perth, Western Australia.

Szewczyk, P. (2011). Usability of Internet Security Software: Have They Got it Right? Paper presented at the 5th International Conference on Network and System Secirty, Milan, Italy.

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.

Tan, G. W., & Wei, K. K. (2006). An empirical study of Web browsing behavior: Towards an effective Website design. Electronic Commerce Research and Applications, 5(4), 261-271.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Paper presented at the 8th USENIX Security Symposium, Washington, D.C.

Wieringa, D., Moore, C., & Barnes, V. (1993). Procedure Writing. Piscataway, NJ: IEEE Press.