2012

A survey of computer and network security support from computer retailers to consumers in Australia

Patryk Szewczyk
Edith Cowan University

DOI: 10.4225/75/57b55f01cd8de
10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

A SURVEY OF COMPUTER AND NETWORK SECURITY SUPPORT FROM COMPUTER RETAILERS TO CONSUMERS IN AUSTRALIA

Patryk Szewczyk
SRI - Security Research Institute, Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au

Abstract

Previously undertaken research suggests that novice end-users rely on computer retailers for security advice and support during and after a sale has occurred. This paper documents the survey results of computer and network security support provided to consumers by retailers in Perth, Western Australia between 2011 and 2012. The conducted survey shows that in the majority of cases, computers retailers were favourable in providing support and recommendations. However, these views were found to be flawed, confusing and do little to ensure that end-users are not victimized by cyber crime.

Keywords
Computer security, network security, ADSL router security, end-users, cyber crime

INTRODUCTION

There is no doubt that global cybercrime has become a significant issue. Anti-virus vendors are struggling to keep up with the constant evolution of new threats such as financially driven malware (Cyveillance, 2010). Criminals are harvesting and monetizing non-financial data including utility statements, medical records, user accounts, and access to vulnerable computers. These are then auctioned off to the highest bidder through underground channels (RSA, 2012). With such a large influx of cyber threats, one could question how home users or those with little to zero understanding of computer or network security are managing this issue.

Consumers may repeatedly fall victim to cyber crime as a result of being unable to securely configure their home computer and network (Szewczyk, 2006). The networking devices utilized to access the Internet can often provide a significant layer of defense if configured appropriately. There is also a plethora of commercial and free security software on the market, yet Australian consumers are continually falling victim to Internet crime. In 2008, AVG reported that Australia had the highest level of cyber crime in the world (Rust, 2008). McAfee reported in 2010 that Australian consumers were still one of the top targets for cyber crime in the world (Roberts, 2010). Private Investigator Ken Gamble from the Internet Fraud Watchdog stated that in 2012 cyber crime in Australia had reached “epidemic proportions” compared to the rest of the world (Offner, 2012). Subsequently, Australian’s susceptibility to cyber crime presents an ongoing concern and challenge.

Numerous studies have investigated the usability of security software (Furnell, 2007; Shang, Broderick, Koranda, & Hyland, 2006; Whitten & Tygar, 1999). These studies suggest that security software is complicated, misleading, and not intended to be used by novice end-users. ZoneAlarm has identified that novice end-users are unable to use security software (Berson, 2005). As a result, ZoneAlarm has been developing software with design principles including;

- Knowing and thinking like the target audience.
- Eliminating product clutter and complexity.
- Minimizing ineffective feedback to the end-user.

Subsequently, security software usability experiments show that ZoneAlarm Internet Security does in fact make using security easy for novice end-users (Szewczyk, 2011). Unfortunately, an end-user must be made aware of the free or commercial versions of the ZoneAlarm program, shown how to obtain it and lastly trained to use it effectively on their computer system.

Online information sources do exist in Australia and around the world, with the intention of providing simplified and accurate security information and instructions to end-users (CyberSmart, 2012; StaySmartOnline, 2012). Many of the websites containing security information do make reference to the requirement of security software as a first line of defense. However, consumers have stated that they are often unaware of many online security information portals, and those who have come across these websites, often find them unusable, confusing and

give up quickly (Furnell, Bryant, & Phippen, 2007; Szewczyk & Furnell, 2009). Whilst end-users generally do believe they are responsible for their own computer and network security, factors such as awareness of threats, and availability of usable resources tend to prevent the adoption and implementation of safeguards (Aytes & Connolly, 2004).

Television, print and online media continually promote the vulnerabilities by which home computers can be accessed through the Internet and subsequently have their data stolen (Seymour, 2012). However, simply highlighting the online risks, without providing solutions, may not result in effective actions by the end-user. Whilst a broad spectrum of solutions do exist, it is important for the end-user to understand when and why a particular safeguard should be utilized. Fortunately, computer retail outlets sell a broad array of both hardware and software security solutions which consumers may utilize to safeguard their computer and network. Even though many consumers are changing their shopping behaviors and purchasing goods online, there is still a significant number of individuals who utilize physical retail outlets as they prefer to obtain advice and recommendations from a sales person (Irvine, Richardson, Fear, & Denniss, 2011). As a result computer retail outlet sales people are at the forefront of not only encouraging end-users to adopt safe computer and internet practices, but to also make viable recommendations at the time of a sale.

DECEPTIVELY INTERVIEWING COMPUTER RETAILERS

Previous research suggests that end-users feel comfortable communicating directly with another individual, especially when they perceive that individual to be an expert in the field of security (Furnell, et al., 2007). A retailer, who attempts to sell a consumer a specialized product, will presumably know and understand the intricacies of the product being sold. Subsequently, one would hope that a retailer who sells specialized computer equipment, security hardware and software, could offer competent support, recommendations and advice to the consumer. Respondents in previous research felt they were offered accurate advice, but later discovered that they were often mislead or deceived into purchasing goods they did not require, to secure their computer or network (Szewczyk & Furnell, 2009).

To date, there is no evidence of research which has deceptively interviewed retailers who sell computer and network security products. There is an abundant array of freely available security products and recommendations on the Internet, which do provide a sound level of protection. Hence the type of person who physically visits a store to purchase security products would presumably be ill-informed of what is available. That same person may require additional support in choosing the correct product. By physically visiting a store, an end-user may also be provided with tutorials or demonstrations regarding the product being purchased.

This paper investigates the security knowledge, advice and guidance provided by computer retail outlets throughout Perth, Western Australia. Subsequently, this paper attempts to address the question of, do sales people offer accurate and unbiased security advice to novice end-users? The chosen retail outlets include four large franchises found nationally, and three small independent stores. The researcher attempted to visit all the franchises during the ethics approved time period, however this was not possible. Subsequently 19 stores were approached and included in the survey. Each store was visited at least four times resulting in 82 ethically approved informal interviews. During each of the visits, the researcher attempted to communicate with a different individual.

The researcher approached each of the retail outlets seeking advice in the area of computer and network security. The researcher is knowledgeable in the area of computer and network security but deceived the sales person into thinking they were a naive and ill-skilled end-user. Intentional errors were made to demonstrate to the sales person the researchers' lack of skills in computer and network security. The sales person was unaware as to whom they were communicating with or the specific skill set of the researcher. Upon entering each of the stores the researcher clearly stated that they would like to speak to someone who had significant knowledge of computer and network security. In the majority of cases this would result in the same sales person.

The researcher informed the sales person that they were a returning customer and had previously purchased equipment at that store thus establishing a degree of customer loyalty. Prior to each interview, the researcher would establish with the sales person that they were very confused and unsure about the area of computing. To further help the sales person, the researcher stated that they purchased a D-Link ADSL router (i.e. D-Link G604t), but could not remember the product version or what it exactly looked like. Whilst each interview was informal and open-ended, there were four main survey questions and areas predominantly focused on including;

- I would like to secure my ADSL router. What security measures or advice can you recommend?
- I use wireless on my ADSL router. Do I need to do anything to protect it?

- On television I heard the reporter use the terms malware, phishing and broadband theft. What is it, and what do I need to protect myself from these?
- What do I need to do to secure my computer?

The survey questions were selected as they encompass the security topics that consumers have previously stated that they struggle with (Szewczyk & Furnell, 2009), areas deemed important by third party security information portals (CyberSmart, 2012; StaySmartOnline, 2012), and often receive significant attention from television media (Seymour, 2012). A recording device was not utilized during the interview process. The researcher attempted to extract sufficient information from the sales person to be able to appropriately secure their computer and network. Furthermore, the researcher focused on the sales persons' willingness to be supportive, accuracy of information given, knowledge of online threats and alternative safeguards, and the ability to customize a security solution based on the researchers' needs and requirements.

SURVEY OUTCOMES

Overall the study was completed successfully with interesting research outcomes. The results indicate that many of the sales people are very willing to not only offer support, but sell additional products not required. The security skill set possessed by many of the sales people was at a novice level. Furthermore, none of the sales people appeared to have appropriate training or expertise in security, and subsequently voiced their personal experiences and opinions.

Securing ADSL routers

Whilst there are no explicit rules for securing an ADSL router, there are least ideal practices which could be followed. These may include; updating the default firmware, changing the default username and password, choosing a strong password, enabling the firewall, utilizing network address translation, disabling domain host control protocol, and using an access control lists. A total of five individuals (from 82) were able to offer appropriate and accurate guidance on some aspects of ADSL router security. A large group of 71 sales people attempted to convince the researcher that the device was a finite product which did not have mechanisms to protect itself or the computers connected to it. Alternatively, six sales people openly admitted that they were unsure if security was available on the aforementioned D-Link device.

The five individuals, who were able to offer advice to secure an ADSL router, were not aware or able to discuss all available ADSL router security practices. Recommendations were made to change the default password. This was coupled with an explanation detailing that if the default password were to be used then an intruder could access the network. Three of the five individuals briefly touched on the topic of restricting access to the Internet, to only specific computers (presumably access control). However, they did state that the process is complicated, and that step-by-step instructions would be provided in the instruction manual accompanying the device. None of the other security practices were mentioned, even after the researcher re-prompted the same question.

Wireless Security

The area of wireless security was an area that each sales person had a significant view or opinion to express. From the 82 individuals interviewed, 79 had comments to make regarding wireless security. It is widely accepted that a vulnerable wireless network is one that would encompass no security. Whilst Wired Equivalent Privacy (WEP), does provide a basic level of protection, only WiFi Protected Access (WPA) provides an appropriate level of security. Placement of the wireless access point, and adjusting signal strength are additional features that could be used to protect a wireless network.

From the 79 individuals who did express a view on wireless security, 21 attempted to sell a wireless product which supposedly encompassed a significantly greater level of security than the D-Link device used by the researcher. Interestingly, the sales person was not yet made aware of the model the researcher had. These 21 individuals would promote the security jargon present on the box of wireless ADSL router to enforce and demonstrate that the researchers' current device would be either inadequate or missing many of these security features. A Netgear DG834g wireless ADSL router for instance advertises on the box that "Double firewall and wireless encryption protect your network and data" in-conjunction with "Secure access to your office or corporate network using VPN pass-through". Whilst these features may be present, it does not necessarily mean that the device will be secure out-of-the-box. The VPN feature for instance would require another VPN device for the end-to-end communication which may not always be feasible for a novice end-user.. In all 21 instances, the sales people would iterate in some manner that a device with such features would guarantee a secure wireless

network. When the researcher questioned if the existing D-Link device which is no more than a year old, could provide the same level of protection, they were immediately told that only the products sold in the store would ensure protection of the network and private information.

A total of 34 (of the 79) sales people mentioned the requirement for WEP and WPA in a wireless network. Fifteen sales people had conflicting interpretations of what WEP and WPA meant with personal interpretations including; Wireless Encryption Protocol, Wireless Encryption Protection, Wireless Extreme Protection, and Wireless Protected Account. These same 15 individuals had difficulty distinguishing between the benefits and issues associated with WEP or WPA, but concluded with saying that one of these is significantly safer than not having any security on the wireless network. The remaining 19 (from 34) individuals did have knowledge in the area of wireless security and made recommendations on which type to use. Specifically, each of the 19 were able to articulate through their own personal explanation that WEP was previously an adequate wireless security standard, but that in time it has become obsolete and that now WPA is the newer and ideal security approach if supported by the wireless devices utilized.

A total of 20 sales people (of the 79) offered not only little guidance in the area of wireless security, but also discussed the drawbacks of implementing and utilizing a secure wireless network. Some of these drawbacks included having to remember and retype a lengthy password every time the computer is connected to a wireless network. In addition, the speed at which the wireless network operates would substantially reduce as a result of processing the encrypted data. Three of the 20 sales people discouraged using any means of security as the threat of someone accessing the private wireless network was extremely small, and also illegal.

Fortunately, four sales people were more than happy to provide beneficial advice, and suggested using WPA2, access control lists, and even recommended specific strong pre-shared keys – with accurate explanations as to why the keys are needed and how they function. In each of these cases the sales person was willing to setup and configure the wireless ADSL router, had the researcher brought it in to the store. As portrayed through Fig. 1 the 82 responses by sales people shows that the predominant recommendation to ensure wireless security was to purchase an alternative product. The second highest response was unfortunately to not use security.

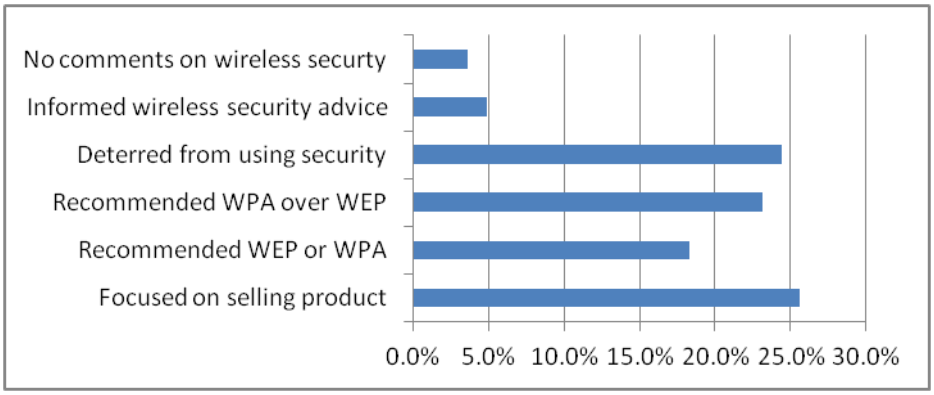

Figure 2 Breakdown of wireless security recommendations

Security Jargon

Television, print, and online media have traditionally used the term virus to describe all software based threats, but fortunately have begun using correct terms to describe the specific threats. However, for those who have not been exposed to computers for a significant portion of their life, may be unaware of common security terms including malware, phishing and broadband theft. The sales person was asked if they could not only explain the terms briefly but also provide solutions to these threats. Malware can be controlled through the use of anti-virus software. Phishing attacks are often counteracted through Internet Security Suites which offer spam and phishing detection and prevention. Broadband theft on the other hand is managed by controlling access to an Internet connection by protecting the wireless network or physical Ethernet access ports.

As portrayed through Figure 2, the sales people were generally aware of what a phishing scam was (49/82 respondents) validated through an accurate explanation. Surprisingly, malware was a term that many sales people were not aware of. Only 22 respondents provided an accurate response, stating that it was to do with viruses and other programs which have negative consequences. Broadband theft was known by only 14 individuals. Many of the sales people (19) thought that broadband theft was a fictitious term and stated that it

was not a true threat. Alternatively, a large portion (49) believed that broadband theft related to an individual obtaining broadband account credentials and using the account as their own.

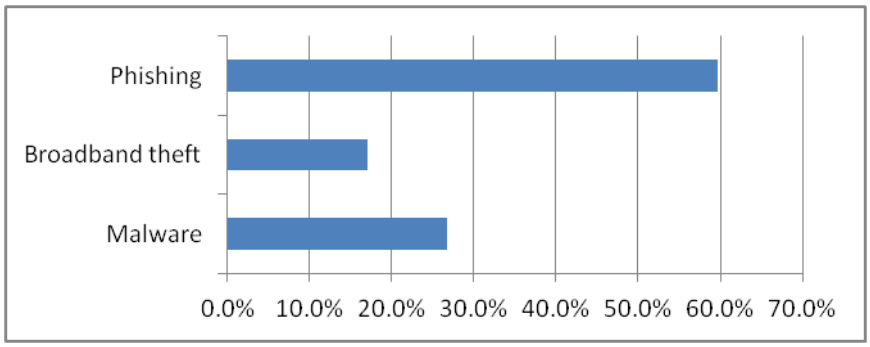

Figure 3 Percentage of retailers who had accurate knowledge of specific threats

Whilst many sales people didn't explicitly understand the threat of phishing, malware and broadband theft they did continually promote the use of Internet Security Software. 76 sales people stated that security software mitigated all known internet threats, and that reliable software would effectively protect the researcher from many threats. This is false in that many anti-virus products are struggling to detect and remove new malware (Brand, Valli, & Woodward, 2010). Many of the retail outlets would stock and sell security software from numerous vendors. Consistency appeared to be an issue in that when the same retail outlet was visited numerous times, the recommended or 'best' software continually changed from sales person to sales person. Each sales person outlined the benefits of the software they were trying to sell and would use benefits including; being a market leader, most trusted, highly used around the world, or the most prominent benefit being – the sales person only uses that particular product at home. Unfortunately, whilst the Internet contains plenty of free personal firewalls and anti-virus products, none of these were recommended or mentioned – which at the same time is not surprising from a retail financial perspective. In one instance the sales person attempted to sell multiple security software packages, advising that two products would substantially increase the level of protection.

Computer Security

The final question which was asked of the sales people was what security hardware or software should be used to protect the recently purchased computer. 63 sales people used this opportunity to find out more about the type of computer and usage habits. Even though each sales person was informed that the laptop contained sensitive work related documents, and was carried between home and work, only one recommendation was made to purchase and use drive encryption software. All sales people encouraged the researcher to purchase at least one additional external hard disk to backup data. Aside from the security software as discussed by sales people previously, 13 people mentioned the importance of running Microsoft Windows update to make sure the actual operating system is protected.

Final comments made by 49 sales people mentioned that availability of security information portals located online, that were operated by the Australian Government. Whilst none of the 49 sales people had ever used the online portals, they did have positive comments to make on their behalf. When prompted if they could write down the web address of the portals, only 17 individuals were able to specify the correct address. The remainder stated that a search online would locate the websites with ease.

CONCLUSION

This paper investigated the security advice and recommendation provided to consumers by sales people working within computer retail outlets. The deceptive informal interview approach has proven highly effective in evaluating how consumers are supported and guided when it comes to computer and network security support. Whilst there isn't one answer to address all the possible security threats there are at least ideal solutions which could be issued. Whilst many of the sales people happily sold computing or network equipment, it was evident that very few understood the security intricacies. There was also very little difference in the accuracy of information and support provided by the large franchises versus the small independent retailers.

Most computer retail outlets sell many ADSL routers with and without wireless capability from numerous manufacturers. Yet few sales people could offer any after sales support or service for these devices. Without knowing the capabilities of the researchers' equipment, many sales people immediately dismissed the security abilities of the device. In the same manner that a car sales person should be knowledgeable in relation to the car they are selling, a computer sales person should be knowledgeable in relation to the features and security aspects of the devices sold. Many sales people could not offer the most desirable answer to securing a wireless network. In some instance the advice would make the home network more vulnerable. In terms of security software, very few sales people could provide accurate information beyond what was stipulated on the product box.

This research shows that sales people from computer retail outlets are a source of misinformation that could lead to a false sense of security and potentially lead to an introduction of vulnerabilities. Very few sales people admitted not knowing an answer to one of the questions, instead falsifying information on the spot in an attempt to sell a product. It is evident through this research that sales people should be trained specifically in the area of computer and network security. Many of the recommendations were overall inaccurate and could further harm or expose the end-users to cyber crime. One could then question whether or not retailers could be held responsible for not only offering inaccurate advice, but recommending that a particular security setting be employed even though it is significantly inferior when compared to others.

REFERENCES

Aytes, K., & Connolly, T. (2004). Computer Security and Risk Computing PRactices: A Rational Choice Perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

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.

CyberSmart. (2012). CyberSmart - Internet and mobile safety advice and activities. Retrieved September 13, 2010, from http://www.cybersmart.gov.au/

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

Furnell, S. (2007). Making security usable: Are things improving? *Computers & Security, 26*(6), 434-443.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410-417.

Irvine, B., Richardson, D., Fear, J., & Denniss, R. (2011). The rise and rise of online retail. Retrieved June 12, 2012, from http://www.sciencemedia.com.au/downloads/2011-5-24-3.pdf

Offner, S. (2012). Could you be Australia's next cyber crime victim? Retrieved June 15, 2012, from http://newsroom.unsw.edu.au/news/law/could-you-be-australia%E2%80%99s-next-cyber-crime-victim

Roberts, G. (2010). Australia a top 10 target for cyber crime. Retrieved April 14, 2012, from http://www.abc.net.au/worldtoday/content/2010/s2800551.htm

RSA. (2012). RSA 2012 Cybercrime Trends Repot. Retrieved July 29, 2012, from http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf

Rust, L. (2008). Australia tops cyber crime list Retrieved April 11, 2012, from http://www.crime-research.org/news/20.06.2008/3422/

Seymour, B. (2012). Drive-by-hackers. Retrieved 2011, May 10, from http://au.news.yahoo.com/today-tonight/lifestyle/safety/article/-/7907101/drive-by-hackers/

Shang, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006). *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software.* Paper presented at the Symposium on Usable Privacy and Security, Carnegie Mellon University, Pittsburgh, PA.

StaySmartOnline. (2012). Stay Smart Online - About. Retrieved October 12, 2010, from http://www.staysmartonline.gov.au/about

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. (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.

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.