12-4-2013

Usability and Security Support Offered Through ADSL Router User Manuals

Patryk Szewczyk
Edith Cowan University, p.szewczyk@ecu.edu.au

DOI: 10.4225/75/57b5691ecd8e8
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

USABILITY AND SECURITY SUPPORT OFFERED THROUGH ADSL ROUTER USER MANUALS

Patryk Szewczyk
School of Computer and Security Science and Security Research Institute,
Edith Cowan University, Perth, Australia
p.szewczyk@ecu.edu.au

Abstract
ADSL routers are often used as either the target or the means for cyber crime. Many ADSL router threats could be mitigated through the effective use of inbuilt security controls and firmware updates available from vendors. Unfortunately, end-users typically lack the technical expertise to correctly configure and secure the device. Subsequently, end-users are reliant on well documented procedures provided by vendors in their user manuals and quick start guides. This study investigates the usability and security recommendations and encouragements put forth by vendors in their user manuals. The study demonstrates that user manual usability does not conform to ideal technical publication practices. In addition, end-users are typically not encouraged to utilise the in-built security features and in a few instances are actually deterred from securing their ADSL router.

Keywords
User manuals, usability, ADSL routers, network security, end-users

INTRODUCTION

The Australian Bureau of Statistics has reported that broadband adoption has continued to increase with 98% of Australian internet connections based on a broadband technology (ABS, 2013). Consequently, a subset of Australian consumers are either unable to obtain broadband or are limited to relatively slow connection speeds. To counteract this issue, the Australian government is rolling out the National Broadband Network (NBN) which will provide widespread national network coverage coupled with increased network speeds, through fibre optic cable, fixed wireless or satellite technologies (DBCDE, 2013). The NBN is also open to existing broadband subscribers who may upgrade to experience a substantially faster internet connection.

The millennial generation are using broadband internet to access social communication, gaming, multimedia and educational resources, while baby boomers and baby busters may make use of live news, share trading, banking, online shopping, medical advice, and travel resources. Consumers have become accustomed in accessing the aforementioned services with ease. However, their technical expertise with managing and securing increasingly complicated home networks remains an ongoing issue (Xu, Wang, & Lee, 2012). McAfee reported in 2010 that Australian consumers were 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). Reports also suggest that home routers will be the next networking device of choice to compromise (Roberts, 2013).

Compromising ADSL routers is not a new occurrence. The first generation of Netcomm ADSL routers encompassed a web server vulnerability which permitted the device to be accessed, compromised and controlled remotely (Sajdak, 2009). The malware psyb0t hijacked consumer grade ADSL routers which were still utilising the default authentication credentials (Nusca, 2009). This threat was subsequently followed by the Chuck Norris botnet and ELF_TSUNAMI malware which both focused on devices which had not been configured and secured correctly (Čeleda, Krejčí, Vykopal, & Drašar, 2010; Mendoza, 2011). During 2011 nearly five million poorly configured DSL routers were compromised in Brazil which permitted the attackers to remotely view and control traffic propagating from the compromised devices (Cluley, 2012).

Many ADSL routers encompass fast, long range wireless capabilities, which increase the importance of correctly securing a wireless network. Watkins (2013) argues, that in some instances, lawyers are proclaiming that unsecured wireless networks encourage criminal activity. Watkins (2013) also discusses allegations of negligence to secure a wireless network are becoming increasingly prevalent. In one instance an individual decided to settle and pay $10,000 in a copyright infringement case and acknowledged that the failure to secure his wireless network presumably encouraged copyrighted material to be accessed and downloaded from his network (Masnick, 2011). End-users must be aware of the risk and encompass the technical expertise to correctly configure and secure their ADSL router. Anderson and Agarwal (2010) promote that need for end-users to be exposed to the threats surrounding computer and network security and then be actively encouraged to adopt and utilise security. Albrechtsen (2007) further validates this view by showing that encouragement and motivation can result in positive outcomes in end-users willingness to use security. In the context of ADSL router user manuals, it is important for vendors to demonstrate to end-users the issues associated with not applying and using a security feature and the subsequent steps required to use the security feature correctly. However, end-users associate ADSL routers as a physical means by which to access the Internet and do not associate the device as encompassing potential safeguards or as a threat to connected computers (Szewczyk, 2006).

The importance of a well written user manual is thus vital in not only allowing end-users to configure the device to access the Internet, but also to demonstrate that the device does encompass a layer of security which can be utilised at the end-users discretion. However, as identified by Johnson (1995) user manuals are often not written with the end-user in the mind. As a result, the end-user is faced with having to find technical and potentially unknown information which is scattered throughout a complex document. ADSL router user manuals should actively promote and encourage the use of good security practices. To date, three assessments have been undertaken between 2005 and 2011 which have investigated the usability and encouragement of security practices towards ADSL Routers (Andersson & Szewczyk, 2011; Szewczyk & Valli, 2009). This research paper builds on previous work focusing on newly released ADSL routers currently available through retail outlets.

METHOD

User manuals should be designed in a manner that allows end-users with varying technical competencies to locate desirable information with ease whilst being exposed to features not necessarily known previously by the end-user. Presumably many novice end-users would be unaware of the security intricacies of ADSL routers, so it the responsibility of the vendor to expose the end-user to the appropriate information in a context that the novice end-user would understand. Well designed manuals will encompass; well written procedures coupled with appropriate graphical images, information on the easiest and most effective method to complete a task, and be suitable for both skilled and novice end-users (Wieringa, Moore, & Barnes, 1993). Through research Perelman, Paradis and Barret (1998) identified that any manual designed with the end-user in mind will encompass:

1. Descriptive page headers and footers to enable end-users to understand the page structure.
2. A contents page and index to locate desirable information quickly and easily.
3. A detailed glossary to elaborate on technical or uncommon terminology.
4. Large, clear graphics with an associated description to allow the end-user to follow procedures.
5. Include statements detailing the intended audience, required level of expertise, and the overall structure of the manual.

The approaches used by vendors to design user manuals can significantly impact on its interpretation and the subsequent behaviour generated by the end-user. ADSL routers typically incorporate a varying assortment of security features dependant on the model and additional features of the product. However, there are ideal security practices which all ADSL routers

incorporate and thus can be evaluated. Subsequently, security practices which ADSL router vendors should be including within the user manual include;

1. Recommend changing the default authentication credentials.
2. Provide recommendations as to what constitutes a strong or ideal password.
3. Recommend updating the firmware on a regular basis.
4. Discuss the security benefits of updating the firmware on the device.
5. Outline the potential risks and threats with both enabling wireless networking and the potential issues if wireless security has not been implemented.
6. Discuss the benefits of positioning a wireless ADSL router in a central location to minimising wireless network access beyond the confines of the owner's property.
7. Recommend WiFi Protected Access (WPA) be used in place of Wired Equivalent Privacy (WEP).
8. Media Access Control (MAC) filter to filter which device may access the wireless network.
9. Providing a dedicated section within the user manual specifically for security.

Twenty-one user manuals were selected to evaluate the usability and security encouragement put forth by vendors. Each manual was scrutinised according to the five recommended publication practises, and the nine security recommendations depicted previously. Both large and small retail outlets from across Australia were selected to determine which devices were currently being sold. Subsequently, three devices were selected from each of the seven popular ADSL router manufacturers. All three devices had wireless as a feature and consisted of an entry level, middle, and high-end model. This approach was also utilised to identify if the user manual would be more or less usable based on different features offered in the product. The subsequent twenty-one devices chosen for this study are depicted in Table 1.

Asus DSL-N10 (Asus, 2013a)	Asus DSL-N12U (Asus, 2013b)	Asus DSL-N55U (Asus, 2013c)
Belkin F9J1001au (Belkin, 2013a)	Belkin F9J1002au (Belkin, 2013b)	Belkin F9J1102au (Belkin, 2013c)
Billion 7800DX (Billion, 2013a)	Billion 7800NX (Billion, 2013b)	Billion 7800NXL (Billion, 2013c)
D-Link 2740B (D-Link, 2013a)	D-Link 2770L (D-Link, 2013c)	D-Link 2870B (D-Link, 2013b)
NetComm NF3ADV (NetComm, 2013c)	NetComm NB604N (NetComm, 2013b)	NetComm NB16DG (NetComm, 2013a)
Netgear DGN1000 (Netgear, 2013a)	Netgear DGN2200 (Netgear, 2013b)	Netgear DGN3700 (Netgear, 2013c)
TP-Link W8951 (TP-Link, 2013b)	TP-Link W8968 (TP-Link, 2013a)	TP-Link W8980 (TP-Link, 2013c)

Table 1. ADSL Router User Manuals Assessed

USABILITY OF USER MANUALS

As demonstrated through Table 2 many characteristics considered essential in any good quality user manuals were omitted by vendors. In contrast to similar previous research (Andersson & Szewczyk, 2011) Netgear has continued to include at least some of the ideal features to make using and locating desirable information easy. In this instance, it appears that both Netcomm and TP-Link have begun introducing ideal characteristics into their user manual, which were not evident in previous research.

	Headers/ Footers	Contents Page	Index Page	Glossary	Large graphics	Image caption	Target audience	Contact support
Asus DSL-N10	✓	✓						✓
Asus DSL-N12U		✓						✓
Asus DSL-N55U		✓						✓
Belkin F9J1001au	✓	✓						
Belkin F9J1002au	✓	✓						
Belkin F9J1102au	✓	✓						
Billion 7800DX		✓						
Billion 7800NX		✓						
Billion 7800NXL		✓						
D-Link 2740B	✓	✓			✓			
D-Link 2770L	✓	✓						
D-Link 2870B	✓	✓						
NetComm NF3ADV	✓	✓				✓	✓	✓
NetComm NB604N	✓	✓					✓	✓
NetComm NB16DG	✓	✓					✓	✓
Netgear DGN1000	✓	✓	✓					
Netgear DGN2200	✓	✓	✓					
Netgear DGN3700	✓	✓	✓					
TP-Link W8951		✓			✓			✓
TP-Link W8968		✓			✓			✓
TP-Link W8980		✓			✓			✓

Table 2. Comparison of Usability Characteristics

Each manual encompassed a table of contents which represented the overall content of the user manual. However, the manner in which these were displayed varied considerably. The Billion, NetComm and TP-Link user manuals had numerous technical ambiguous acronyms throughout the table of contents yet no glossary was present. For a novice end-user this may make locating desirable information difficult especially in an era where there is a vast amount security terminology in reference Information Technology. Whilst all manuals made use of graphical images to represent procedural steps, only four user manuals as depicted by Table 2 encompassed large, clear images which would depict the entire user interface from the web browser's perspective. In the remainder of instances, the images would either be small (compared to the size of the page), cut out – thus representing only a particular element from the entire interface, or have steps missing – presuming that the end-user would be able to complete the in between procedures.

An index page was unfortunately only provided by Netgear despite it being an easy and time efficient method by which to locate information. This coupled with confusing and a poorly illustrated table of contents would make locating information difficult, resulting in the entire user manual needing to be read. Yet Schriver (1997) argues that reading a technical procedural manual from beginning to end contradicts natural human behaviour. Subsequently, end-users may genuinely overlook many critical aspects conforming to security located in the user manual.

SECURITY ENCOURAGEMENT OF USER MANUALS

Security recommendations and encouragement were overall quite disappointing amongst the twenty-one user manuals. Netgear as per previous research (Andersson & Szewczyk, 2011) continued to encourage using security from all perspectives. The simplest method by which to protect the ADSL router from many threats is to change the default username and password. Psyb0t and alternative malware forms specifically exploited devices which were still using the default

authentication credentials (Nusca, 2009). Yet less than twenty-five percent of the user manuals surveyed encompassed encouragement or advice pertaining to end-users needing or being required to change the default credentials.

	Changing password	Password choice	Recommend firmware update	Firmware update benefits?	Wireless risks?	Access point location	Recommend WPA	Use firewall?	MAC filtering	Security section
Asus DSL-N10										
Asus DSL-N12U										
Asus DSL-N55U										
Belkin F9J1001au										
Belkin F9J1002au										
Belkin F9J1102au										
Billion 7800DX										
Billion 7800NX				?						
Billion 7800NXL				?						
D-Link 2740B	?				?		?			
D-Link 2770L	?				?		?			
D-Link 2870B					?		?			
NetComm NF3ADV										
NetComm NB604N										
NetComm NB16DG										
Netgear DGN1000	?	?			?		?	?	?	?
Netgear DGN2200	?	?			?		?	?	?	?
Netgear DGN3700	?	?			?		?	?	?	?
TP-Link W8951										
TP-Link W8968										
TP-Link W8980										

Table 3. Comparison of Security Recommendations

Updating the firmware of an ADSL router can mitigate software related issues which may have been overlooked during the initial manufacturing of the device. However, many end-users may be use to the words "operating system" and thus could be unaware of the terminology associated with updating the firmware. Unfortunately, none of the vendors clearly outlined the benefits of updating or the benefits from a security perspective and in many instances may actually deter end-users by using points including;

> *"There is no need to upgrade the firmware unless the new firmware has a new feature you want to use..."*
> *"...your configuration setting may return to factory default settings, (when upgrading your firmware)...*
>
> *"The Router has the capability to automatically check for a newer version of firmware and alert you when it's available. You can choose to download the new version or ignore it."*

Only D-Link and Netgear user manuals outlined the potential risks of operating a wireless network. However, none of the vendors discussed ideal positioning of the wireless ADSL router to avoid neighbours being able to access the wireless network, and again only D-Link and Netgear emphasised the importance of using Wi-Fi Protect Access (WPA or WPA2) over the vulnerable Wired Equivalent Privacy (WEP). The remaining vendors showed clear instructions as to how to implement each of the wireless security protocols. However, from an end-users perspective it is almost confusing why so many security protocols exist and which one should be selected for optimal

wireless security. Similar information was available pertaining to MAC address filtering, with only Netgear providing a context as to why it is important and how it could benefit an end-user.

As evident through prior research (Andersson & Szewczyk, 2011) and this research, Netgear still continues to not only make their user manuals usable, but encourages the use of security with novice end-users in mind. For instance, many end-users could be aware of what constitutes a strong password, yet Netgear encourages changing the default authentication credentials and also recommends ideal password choices which meet industry best practices. Fortunately, many vendors have incorporated an automatic firmware checker for the ADSL router. This prompts the end-user of the availability of a firmware update should one become available. However, this requires that the end-user login to the device, which presumably few individuals would do on a regular basis.

End-users will often engage in poor security practices if they do not see the immediate consequence to themselves or their home network (Tama, Glassmana, & Vandenwauverb, 2010). Thus ADSL router user manuals should actively promote the need for using security by outlining the potential consequences if security is not utilised. Vendors can also encourage end-users to make suitable security choices by showing why a particular security setting is better over another. For instance, there are many wireless networking security protocols available yet vendors typically neglect to encourage that a particular setting is chosen. One could argue why an end-user would select a particular setting if there is no immediate explanation of its direct benefit.

CONCLUSION

The implementation of the NBN across Australia will see many end-users needing to upgrade their hardware should they wish to make use of the advanced technology. The newer hardware may encompass advanced functionality which may become a target of focused attacks. Thus there will be a greater requirement for end-users to apply security to the device to protect themselves, and their home network. However, as can be observed from this research, vendors are failing to encourage and motivate end-users to appropriately utilise security controls available on their ADSL router. There also appears to be little difference between the usability and security recommendations put forth in the entry level, middle and high-end range of ADSL routers as shown through this study. Future research will continue to focus on the usability and security recommendations used by vendors as they begin to release newer models for use directly with the NBN infrastructure.

End-users with prior advanced knowledge of the area in question would presumably have no reason to utilise the user manual. Thus vendors should assume no prior knowledge in the user manual and provide critical components such as an index, a glossary, and a simple table of contents to locate information efficiently. Vendors are also at the core of being able to educate end-users on simple computer and network security principles. Subsequently, by explaining security solutions in a simple manner, this may not only encourage end-users to utilise security properly, but may also reduce the impact and severity of ADSL router related cyber crime.

REFERENCES

ABS. (2013). Type of Access Connection. Retrieved September 5, 2013, from http://www.abs.gov.au/ausstats/abs@.nsf/Products/8153.0~December+2012~Chapter~Type+of+access+connection?OpenDocument

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly 34*(3), 613-643.

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.

Asus. (2013a). ASUS DSL-N10 B1. Retrieved August 28, 2013, from http://www.asus.com/Networking/DSLN10_B1/#support_Download_30

Asus. (2013b). ASUS DSL-N12U B1. Retrieved August 28, 2013, from http://dlcdnet.asus.com/pub/ASUS/wireless/DSL-N12U_B1/E7218_DSL_N12U_B1_Manual_English.pdf

Asus. (2013c). ASUS DSL-N55U. Retrieved August 28, 2013, from http://www.asus.com/au/Networking/DSLN55U_Annex_A#support_Download_30

Belkin. (2013a). Belkin F9J1001au. Retrieved August 28, 2013, from http://cache-www.belkin.com/support/dl/F9J1001_8820ed00838_N150_MR_uk.pdf

Belkin. (2013b). Belkin F9J1002au. eRetrieved August 28, 2013, from http://cache-www.belkin.com/support/dl/F9J1002_8820ed00839_man_uk.pdf

Belkin. (2013c). Belkin F9J1102au. Retrieved August 28, 2012, from http://cache-www.belkin.com/support/dl/F9J1102_8820ed00841_N600_uk.pdf

Billion. (2013a). Billion 7800DX. Retrieved August 28, 2013, from http://au.billion.com/downloads/usermanual/voip/BiPAC_7800VDP(O)X_FM2.31_UM_1-32.pdf

Billion. (2013b). Billion 7800NX. Retrieved August 28, 2013, from http://au.billion.com/downloads/usermanual/wireless/BiPAC_7800_N_X_L__FM_2.23_UM_1_02.pdf

Billion. (2013c). Billion 7800NXL. Retrieved August 28, 2013, from http://au.billion.com/downloads/usermanual/wireless/BiPAC_7800_N_X_L__FM_2.23_UM_1_02.pdf

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.

Cluley, G. (2012). How millions of DSL modems were hacked in Brazil, to pay for Rio prostitutes. Retrieved November 1, 2012, from http://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012/

D-Link. (2013a). D-Link 2740B. Retrieved August 28, 2013, from ftp://files.dlink.com.au/products/DSL-2740B/REV_F1/Manuals/DSL-2740B_F1_Manual_v2.01(AU).pdf

D-Link. (2013b). D-Link 2870B. Retrieved August 28, 2013, from ftp://files.dlink.com.au/products/DSL-2870B/REV_A/Manuals/DSL-2870B_A1_Manual_v3.00(AU).pdf

D-Link. (2013c). DLINK 2770L. Retrieved August 28, 2013, from ftp://files.dlink.com.au/products/DSL-2770L/REV_A/Manuals/DSL-2770L_A1_Manual_v1.00(AU).pdf

DBCDE. (2013). NBN technologies. Retrieved August 29, 2013, from http://www.nbn.gov.au/about-the-nbn/what-is-the-nbn/nbn-technologies/

Johnson, E. (1995). Computer Documentation: Writing about technology. *Computer and the Humanities, 29*, 409-411.

Masnick, M. (2011). No, Having Open WiFi Does Not Make You 'Negligent' And Liable For $10,000.

Retrieved August 12, 2012, from http://www.techdirt.com/blog/wireless/articles/20110801/04233815344/no-having-open-wifi-does-not-make-you-negligent-liable-10000.shtml

Mendoza, E. (2011). Router-Compromising Malware in Latin America. Retrieved 2011, August 11, from http://blog.trendmicro.com/trendlabs-security-intelligence/latin-america-router-compromising-malware-found/

NetComm. (2013a). NetComm NB16DG. Retrieved August 28, 2013, from http://media.netcomm.com.au/public/assets/pdf_file/0004/123997/NB16DG-User-Guide.pdf

NetComm. (2013b). NetComm NB604N. Retrieved August 28, 2013, from http://media.netcomm.com.au/public/assets/pdf_file/0013/100570/NB604N-User-Guide.pdf

NetComm. (2013c). NetComm NF3ADV. Retrieved August 28, 2013, from http://media.netcomm.com.au/public/assets/pdf_file/0014/104063/NF3ADV-User-Guide-v2.pdf

Netgear. (2013a). Netgear DGN1000. Retrieved August 28, 2013, from http://www.downloads.netgear.com/files/GDC/DGN1000/DGN1000_UM_29Feb12.pdf

Netgear. (2013b). Netgear DGN2200. Retrieved August 28, 2013, from http://www.downloads.netgear.com/files/GDC/DGN2200V3/DGN2200v3_UM_15May2013.pdf

Netgear. (2013c). Netgear DGN3700. Retrieved August 28, 2013, from http://www.downloads.netgear.com/files/GDC/DGND3700V2/DGND3700v2_UM_13MAR2013.pdf

Nusca, A. (2009). 'Psyb0t' worm infects Linksys, Netgear home routers, modems. Retrieved March 11, 2010, from http://www.zdnet.com/blog/btl/psyb0t-worm-infects-linksys-netgear-home-routers-modems/15197

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

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

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

Roberts, P. (2013). Home Invasion: Home Routers May Be The Next Big Hack. Retrieved May 20, 2013, from https://securityledger.com/2013/04/home-invasion-home-routers-may-be-the-next-big-hack/

Sajdak, M. (2009). *Remoterootshellon a SOHO classrouter.* Paper presented at the Confidence 2009, Krakow, Poland.

Schriver, A. K. (1997). *Dynamics in Document Design*. New York: USA: John Wiley & Sons.

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., & 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.

Tama, L., Glassmana, M., & Vandenwauverb, M. (2010). The psychology of password management: a

tradeoff between security and convenience. *Behaviour & Information Technology 29*(3), 233-244.

TP-Link. (2013a). TP-LINK TD-W8980. Retrieved August 28, 2013, from http://www.tp-link.com.au/Resources/document/TD-W8980_V1_User_Guide.pdf

TP-Link. (2013b). TP-Link W8951. Retrieved August 28, 2013, from http://www.tp-link.com.au/resources/document/TD-W8951ND_V5_User_Guide_1910010890.pdf

TP-Link. (2013c). TP-Link W8980. Retrieved August 28, 2013, from http://www.tp-link.com.au/Resources/document/TD-W8968_V1.0_User_Guide.pdf

Watkins, C. G. (2013). Wireless Liability: Liability Concerns for Operators of Unsecured Wireless Networks. *Rutgers Law Review, Forthcoming, 2013*.

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

Xu, K., Wang, F., & Lee, M. (2012). *HomeTPS: Uncovering What is Happening in Home Networks*. Paper presented at the 9th Annual IEEE Consumers Communications and Network Conference.