TOWARDS TARGETED SECURITY AWARENESS RAISING

Najem Mahmoud[1, 2], Steven Furnell[1, 3] and Paul Haskell-Dowland[3]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]Computer Department, Faculty of Science, Sebha University, Sebha, Libya
[3]Security Research Institute, Edith Cowan University, Perth, Australia
info@cscan.org

Abstract

Users are frequently cited as being the weakest link in the information security chain. However, in many cases they are ill-positioned to follow good practice and make the necessary decisions. Part of the reason here is that, even if security awareness, training and/or education have been provided, some of the key points may have been forgotten by the time that users find themselves facing security-related decisions. A potential solution in this context is to ensure that security guidance and feedback is available at the point of need, providing effective information to help users to make the right decision at the right time to avoid security risks. This paper examines the issue of targeted security awareness raising, and presents the results of an experimental study conducted to test the effectiveness of the approach. This experiment was based around the scenario of connecting to Wi-Fi networks, and determining whether participants could make informed and correct decisions about which networks were safe to connect to. Four alternative interfaces were tested (ranging from a version that mimicked the standard Windows Wi-Fi network selection interface, through to versions with security ratings and additional guidance). The aim of the experiment was to determine the extent to which providing such information could affect user decisions when presented with a range of networks to connect to, and help to move them more effectively in the direction of security. The findings revealed that, while they still exhibited far from perfect behaviour in terms of selecting more secure networks in preference to less protected ones, there was a tangible improvement amongst the users that had been exposed to the selection interfaces offering and promoting more security-related information. In common with findings from other security contexts, these results suggest that users' security behaviours can be positively influenced purely through the provision of additional information, enabling them to make better choices even if the system does not provide any further means of enforcement.

Keywords

Information Security awareness, Security warnings, Context sensitive awareness, Targeted security awareness.

Introduction

The wide and increased use of information technology systems for storing, exchanging, and processing information has made the security and safety of these systems more important and more challenging than ever before. One of the key undertakings for any organisation is to ensure that its staff acts in an appropriate manner by increasing their IT security awareness to avoid security breaches (Kessel, 2012). The staff of the organisations in general can be considered as the weakest link in ensuring information due to the lack of awareness and experience. They can also pose a threat to their organisations from inside, and this is in addition to the vulnerabilities of people that can be exploited by the considerable outside threats (Bulgurcu et al., 2010; Shaw et al., 2009). For example, a study conducted to evaluate the trade-offs between computer security protection and accessibility concluded that employees are more likely to bypass security measures in order to complete a task (Ifinedo, 2012).

Indeed, users are frequently cited as being the weakest link in the information security chain (Sasse et al., 2001; Patrick et al., 2003). However, in many cases, they are ill-positioned to follow good practice and make the necessary decisions. Part of the reason here is that, even if security awareness, training and/or education have been provided, some of the key points may have been forgotten by the time that users find themselves facing security-related decisions.

One of the emerging and promising ways to increase user security awareness that can be relied on is to use the targeted awareness raising approach that provides guidance and nudges during the task in hand. The use of the targeted security awareness raising approach to increase the security awareness of users has become more imperative than ever before. It is an emerging area that has the potential to be considered as a valuable method for raising the security awareness of end-users by ensuring that security guidance and feedback is available at the point of need, providing effective information to help the users to make the right decision at the right time to avoid security risks.

In response to these challenges, this paper presents in detail an experimental work that examines the issue of targeted security awareness raising approach and discusses the results of testing the effectiveness of such approach on real users. The next section discusses the importance of introducing new security user awareness approaches and why the targeted security awareness raising approaches can be the most suitable candidate. The discussion then considerers the drivers for selecting wireless networking as an area of focus within the experiments. The main objectives of the developed experiment, and the methodology of how this work has been conducted are then presented, along with an overview of four different users' interfaces are used for the trials. The results and findings of the experiments are then discussed, leading to conclusions arising from this work in the final section.

Requirement for Updated User Security Awareness Approach

As technology advances, there has been a significant and continuing shift in terms of responsibility and duty. Users must have some level of security awareness and ability to protect themselves as there is a large number of threats making it harder for technology to give a complete answer. Moreover, recently many users find themselves ill-equipped to operate. There are still many users who have a lack of understanding about the technology and therefore find it harder to ascertain the associated threats (Furnell and Clarke, 2012).

In order to raise IT security awareness for staff, many organisations employ IT security awareness programmes to raise the security awareness of their staff and to reduce end-users' errors. Providing IT security awareness programmes to increase IT awareness of security risks that emerge every day is one of the challenges facing many organisations for several reasons. These include: the emergence of fast-evolving threats, the lack of resources and skills; resource constraints; and the limited security awareness training (Kessel, 2012).

There is no doubt that there is a real need to increase the security awareness for the users; however, passive promotion, such as using posters up around the office or PowerPoint slides, do little to capture the interest of the users (Randell, 2013). The biggest threats to information security in any organisation is often not related to the presence of weakness in the technology control environment, and it is more related to the action or inaction by employees which can often lead to security incidents (PCI, 2014).

One of the recognisable means to make the users aware of any security risks in their daily activities when dealing with IT systems is the use of security warnings. The security warning is used to warn the user about the potential security risks. However, the current security warnings do not seem to be effective and have flaws. Zaaba et al. (2014) identified six common problems related to security warnings including attention towards warnings, understanding of warnings, the use of technical wordings, evaluation of risk from warnings, user's motivation towards heeding warnings, and user's assessment of implication of warnings. Moreover, regardless of the fact that there are a wide variety of technical countermeasures to mitigate security risks such as malware-related risks, users are in fact the last line of defence against security incidents and indeed users represent the last gate in the decision-making process (Silic and Back, 2017).

Targeted security awareness raising is an emerging and promising approach that has the potential to be effective in raising the security awareness of the users by providing guidance and nudges during the task in hand. An apparent example of the targeted security awareness raising approach is the use of password meters. These are used to encourage and help users to choose an acceptable password in terms of its strength. An investigative study conducted by Ur et al. (2012) on the use of passwords-strength meters found that the password-strength meter influences the user in terms of changing behaviour and security. Password strength meters guide the user to make longer passwords. However, this study found that unless the meters scored passwords stringently, the chosen passwords were only slightly more resistant to password cracking attacks. Despite the extra strength that these more stringent meters convey, it has been observed that there are many more lenient meters deployed in practice. The study findings suggest that as long as these password meters are not overly onerous, employing more rigorous meters would increase security. The principles embodied by password meters

could also be applied to other user-facing aspects of security in which risky security decisions are often made and a relevant example in this context is connecting to insecure Wi-Fi networks.

Security Threats Inherent in Insecure Wi-Fi Networks

Wi-Fi is known for being fast, convenient and reliable; on the other hand, free Wi-Fi hotspots are increasingly seen as an IT security risk. In an era where data breaches make the main news almost daily, it would be justified for businesses to place a firm restriction to access their systems from the outside world. However, it is also apparent that modern businesses demands are sometimes prioritized over security. For such businesses, the benefit of having their employees able to access email and corporate data on the move far outweighs possible IT security risks. As a result, just over half (51%) of mobile users stated that their companies allow them to use personal devices to access corporate data via public Wi-Fi hotspots (iPass, 2016a).

For the most part, people make security decisions and choices on a daily basis without fully considering the security implications of those decisions and choices. Organisations depend on their staff to frequently make security decisions when carrying out different tasks both whilst in the workplace and on the move. Indeed, choosing a secure and trustworthy Wi-Fi connection is one of the top 10 security behaviours that are encouraged on sites like www.staysafeonline.org (Turland et al, 2015). Nonetheless, many studies have found in general that users are impetuous about security risks related to the use of Wi-Fi hotspots (F-Secure, 2014). This has increased the need for further investigation of the attitudes of Wi-Fi users towards security risks related to the use of unknown Wi-Fi networks (in particular, the use of unknown Wi-Fi networks within public areas). To further evidence the problems, Table 1 gathers findings from various sources to demonstrate the tendencies of users on connecting to insecure Wi-Fi and accessing sensitive information.

Table 1: Summary of evidence of users' trends towards using insecure Wi-Fi networks

Source	Key findings
(Kaspersky Lab, 2016).	• 71% of the surveyed users use insecure public Wi-Fi. • 15% of questioned consumers stated that they use public Wi-Fi to shop, bank, or make payments online without additional precautions. • People are still using their devices without equipping their devices with security solution and acting negligently. • As a result, 29% have been affected by online threats. • Consumers continue engaging with the online world at every opportunity, with 42% using free but potentially insecure public Wi–Fi, and only 13% using a secure VPN connection. • Kaspersky Lab concluded that the figures indicated a lack of security awareness among consumers in this regard. This places their valuable data at risk. Consumers share data insecurely, conduct important transactions on public Wi-Fi and treat their passwords without additional precautions. In addition, while these habits continue, only 60% of consumers protect themselves with a security solution on every device they own.
(iPass, 2016a).	• The report highlights that although mobile data services are available to users on the move, these services still cannot surpass the quality that the Wi-Fi hotspots provide in terms of speed, cost, convenience and performance. • 63% of respondents will choose a Wi-Fi hotspot over mobile data services. • Worryingly, employees know the security risks of public Wi-Fi; nevertheless, many are still used it anyway. • 66% of respondents stated they were concerned about the security of Wi-Fi hotspots. However, only 28% of respondents said they use a VPN all the time, and more than a third 38% never do. • The iPass report concluded that mobile users expect to remain connected and productive at all times working as they see fit, not based on the type of the communication method used to connect to the Internet. • Mobile users do not want to waste their mobile data on draining business/personal applications or use slower connectivity options which may not provide the reliability and performance they require. They want to go Wi-Fi first.

(iPass, 2016b).	• 94% of organisations see public Wi-Fi as a threat. In the meantime, 88% of organisations admitted that they find it difficult to consistently implement a safe mobile usage policy. • Businesses are struggling to create security policies that provide mobile users with the flexibility they demand. • The report also highlights that many employees still choose high-risk connectivity options despite knowing the potential security risks. • 66% of mobile users said they were worried about data security when using free public Wi-Fi hotspots, yet 42% still access company data using public Wi-Fi hotspots.
(F-Secure, 2014).	An independent investigation was conducted by the Cyber Security Research Institute and the German penetration testing company SySS on behalf of F-Secure company. • It found hundreds of people are regularly logging onto "trojanized ' free Wi-Fi hotspot service that was created to carry out their experiment. • The research also revealed the presence of significant weakness in the Wi-Fi system which allows the usernames and passwords for users who use email accounts on the POP3 protocol which is widely used to be easily discovered when users send emails through Wi-Fi hotspots. This vulnerability can be exploited by any criminal offering and controlling a Wi-Fi hotspot to gather account information that would allow them to impersonate the user through their email account. • The experiment highlighted that people pay no attention to computer security when they are on the move.

While using unknown Wi-Fi networks, users should be made aware of the security risks that are associated with the use of such networks and its security policies. Users awareness should be raised before they get access to these networks. This ought to be done at the operating system level or the operator of the network should offer this opportunity before the users proceed to join the network. This perhaps will help users to know the security risks and hence have their chance to better decide whether to use or abstain from the offered Wi-Fi connection.

In response to these issues and in order to achieve a comprehensive study, an experiment has been conducted to assess users' attitudes towards the use of unknown Wi-Fi networks in a public environment using four different user interfaces.

The findings of the research will enable the identification of the level of guidance that is required to help Wi-Fi users when performing routine online tasks without unduly interrupting or overloading them with vast amounts of information.

There is a lack of investigation into the existing systems in terms of whether the users are getting best support and advice before they get connected to unknown Wi-Fi hotspots.

Most existing platforms seem to not provide adequate security recommendations and security guidelines that nudge users towards selecting appropriate Wi-Fi hotspots based on their need and to mitigate user's security risks of connecting to insecure networks. The only available option that the existing platforms provide to users is the padlocks, for indicating that the wireless network (Wi-Fi hotspot) is protected with a password. This is mainly for the Apple iOS and Android platforms on mobile phones. For the Microsoft Windows OS, a message is provided to alert that the information flowing through the network can be seen by third parties.

An apparent example is that when a user is trying to look up for available wireless networks within the Microsoft Windows 7 platform a Wi-Fi dialog window will appear as per the screenshot shown in Figure 1. Although this window is to inform the users about the available Wi-Fi networks within their area alongside with their signal strength and the name of these Wi-Fi networks, and users also can get additional information about these available wireless networks by pointing the pointer at the name of any of these networks. However, this information may not sufficient in terms of providing sufficient security guidance to users to whether these networks trustworthy or to give them the chance to better decide or abstain from these Wi-Fi hotspots. Users perhaps would not understand abbreviations and technical terms such as "Security Type: WPA2/ WPA2-PSK", what actually users need at this point is

some advice like whether these networks are trustworthy or not, whether to use any of these networks or not and perhaps what can be used for. Additional useful information that have the potential to support the users decision may include some characteristics of these networks such as informing the user whether the network is using or providing an encryption protocols or if it is not using an encryption protocols at all, also giving users more advice and security guidance of the sort of activities that they can carry out or the sort of activities they should not carry out based on the characteristics of these networks and the security considerations if the user connect to it. This type of security advice may have the potential to be very useful in supporting the user's decisions at the point when needed (i.e. in making a decision whether to use the Wi-Fi or not).

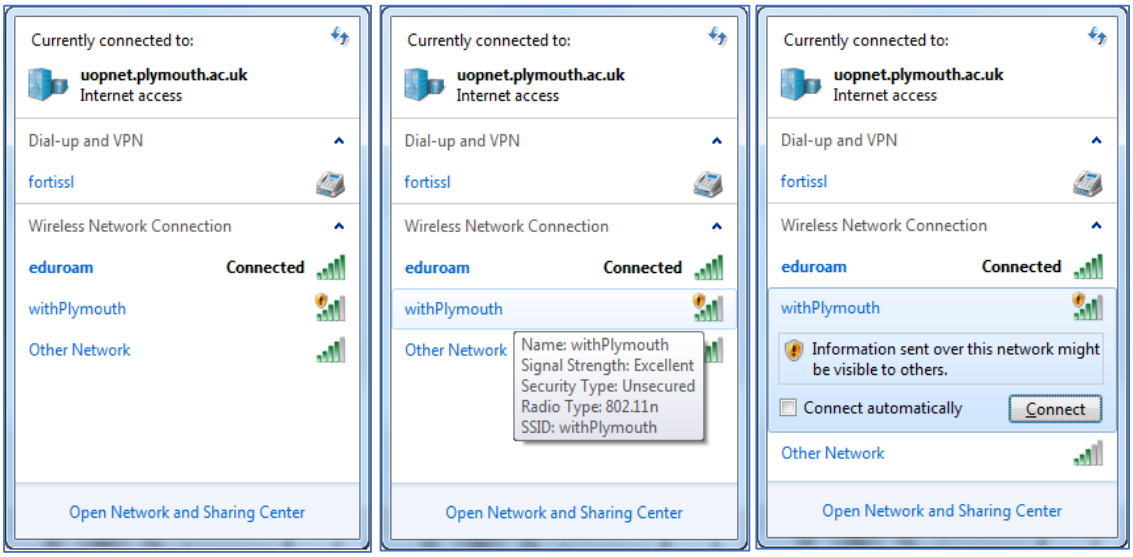

Figure 1: Selecting Wi-Fi network using Microsoft Windows 7

An Experimental Trial of Alternative Wi-Fi Selection Interfaces

The main aim of this research work is to utilise different user interfaces of Wi-Fi networks in order to evaluate the usability and the security of the developed interfaces to overcome some of the information limitations presented by existing user interfaces. The purpose of the user trials is to investigate the usability, security and clarity of different user interfaces and to determine whether they have an effect upon user decisions.

Experimental Methodology

Four prototypes were developed, existing interface used in MS Windows platforms; improved user interface with warning message; and an advanced interface with a security meter (Design 1) and (Design 2), these were developed to simulate the user interface of Wi-Fi networks in order to address the main objectives of the proposed experiment.

The aim of this research experiment was to identify whether users will connect or will continue to connect to unknown Wi-Fi networks in public areas if they have been provided with adequate security information about the available networks.

All interfaces contained two known Wi-Fi networks to participants namely the eduroam and withPlymouth, which users normally expect to see during their Wi-Fi interactions on the university campus, and two unknown Wi-Fi networks namely BellaCostaCafe and eduroamhighspeed. Eduroamhighspeed was named purposely to test if this name will affect participants' selection as to whether they will be attracted to the name as it implies a high speed network and includes wording of a high-speed with the existence of the known and trustworthy network eduroam. BellaCostaCafe was named to test if users will recognise that this name is not known to them within the university campus environment and hence they would abstain from connecting to it.

The design of the experiment was to examine whether users would connect or continue to connect to unknown Wi-Fi networks if they have been provided adequate security information about the presented Wi-Fi networks. To achieve this, the first and second interfaces were designed to analyse whether the user is tempted to connect to unknown Wi-Fi network in case a trustworthy network would be inaccessible. In contrast, the third and fourth interfaces present a padlock, on the trustworthy network,

to indicate that an authentication is required. However, when clicked it connects the user without requiring authentication. This was to investigate whether users would recognise this flaw on the network and its potential threat.

The participants for this work were divided randomly into four groups, and were asked to try one of the four interfaces to choose an appropriate Wi-Fi network and to perform the task that was stated in the following given scenario:

> *"Experiment Scenario*
>
> *Consider yourself at the university campus, and you are connecting to a Wi-Fi hotspot to browse the Internet in order to use applications such as emails, online banking, and social networking services.*
>
> *You are requested to use the wireless network selection interface to choose an appropriate network from which to conduct these activities.*
>
> *Please note that you only need to select and connect to an appropriate network; you will not actually be required to send emails, or perform any of the other tasks mentioned above.*
>
> *You will then be asked to comment upon the usefulness or suitability of the interface that was used."*

The study involved 100 participants who were 18 years of age and older, divided randomly into four groups (25 participants for each interface), with all data and responses treated anonymously. The users were involved in only one session of the study. This means trying only one of the proposed four interfaces for approximately 15 minutes.

The experiment procedure required participants to use the prototype software that simulated the process of viewing available Wi-Fi networks and asked them to connect to the most appropriate network in a given scenario as mentioned earlier.

After completing the session, users were also asked to fill out an online survey that took approximately 15 minutes. The survey was used to investigate users' acceptance of the developed interfaces from both the aspect of security and usability.

All users' interactions in the four groups with the four interfaces were captured and stored on the computer that was used for the experiment to collect the results for later analysis and to examine if the improvements of the interface were helpful in making users change their behaviour of connecting to unknown Wi-Fi networks in a public environment. In addition, there was a screen recording for the user interaction with the interfaces to assist in analysis and for reviewing later.

Experimental Prototypes

The prototypes were implemented as an application to run on the Microsoft Windows platform, and the trial design considered four different user interfaces for selecting Wi-Fi networks. The first interface was designed to simulate the Wi-Fi dialog window that is used in the Microsoft Windows platforms when a user is searching for Wi-Fi networks. We chose the Windows 7 over the later versions of the OS because participants were most likely to be familiar with this version on the basis that (a) it was the version of the OS used on campus at the time of the study and (b) it was the most prevalent version of Windows in general use at the time of the study and remains so at the time of writing (Netmarketshare, 2017).

The screenshots presented in Figure 2 illustrating the designed first interface that was used in the experiment. This interface is defined as "*Existing interface used in MS Windows platforms*".

The second interface was also designed to simulate to the Wi-Fi dialog window that is used in the Microsoft Windows platforms. However, it also has some improvements and changes. These improvements and changes include a dialog window that appears when the users click the connect button as shown in the screenshots below to alert the users and allow them to choose either to "*Accept*" or "*Reject*" the connection. It also has the padlocks which are no longer used in recent Microsoft Windows platforms to indicate to the user whether the network requires a password to access it or not. See the screenshots in Figure 3. This interface is defined as "*Improved user interface with warning message*".

The third interface was designed differently when compared to the Wi-Fi dialog used in the Windows platforms, with improved information security panels that have security information about the explored Wi-Fi network and recommended usage. This interface also had security meter indicators for each available Wi-Fi network that presents the extent of the security level that the Wi-Fi network had as illustrated in Figure 4. This interface also had the advantage of having a "*Click for more information*" link opposite each security meter. When a participant clicked, a dialog window was presented (Figure 5) to alert participants and give them more security information about the Wi-Fi network that they are exploring and allow them to make their decision based on the security information and recommended usage. This interface is defined as "*Advanced interface with security meter (Design 1)*".

In order to influence the security behaviour of users in terms of making more security-oriented decisions, four security meter settings were used. The first security level (Excellent) was specified with the colour code green, the second (Good) with yellow, the third (Fair) with amber and the fourth (Poor) with red. The security panels were also designed to have a traffic light design where green was used to indicate that the setting(s) are (Enabled) for the security protocols or for the encryption protocols for the presented Wi-Fi networks in the interface and red to indicate that the setting(s) are (Disabled). The green colour was also used in the start-up time setting to indicate that the Wi-Fi network was in operation for a long time and red was used to indicate that the Wi-Fi start-up time is very recent. Moreover, green was also used in the settings of previously connected to indicate that the Wi-Fi network has been used previously and red to indicate that it has not been used before. Finally, yellow was also used to indicate that there was a change in the setting(s) of the presented Wi-Fi network and green to indicate that there were no changes. Users also have the feature to hover the pointer over the traffic lights to gain more information about the traffic lights by providing a brief explanation of why the traffic light is yellow, amber or red.

The fourth interface (illustrated in Figure 6) was designed to be similar to the third interface with the only difference being that users will see the security panels that have security information about the explored Wi-Fi network and recommended usage if they either clicked on the link "*Click for more information*" or if they clicked on the button "*Connect*" and in the latter case users would have the choice to either "*Accept*" or "*Reject*" connecting to the selected network. This will ensure that users have the chance to know about the security information and the recommended usage for any network they select before they make their decision to gain access. Figure 7 illustrates the improved information security panels with two buttons to allow the user to either "*Accept*" or "*Reject*" connecting to the selected network. This interface is defined as *"Advanced interface with security meter (Design 2)*".

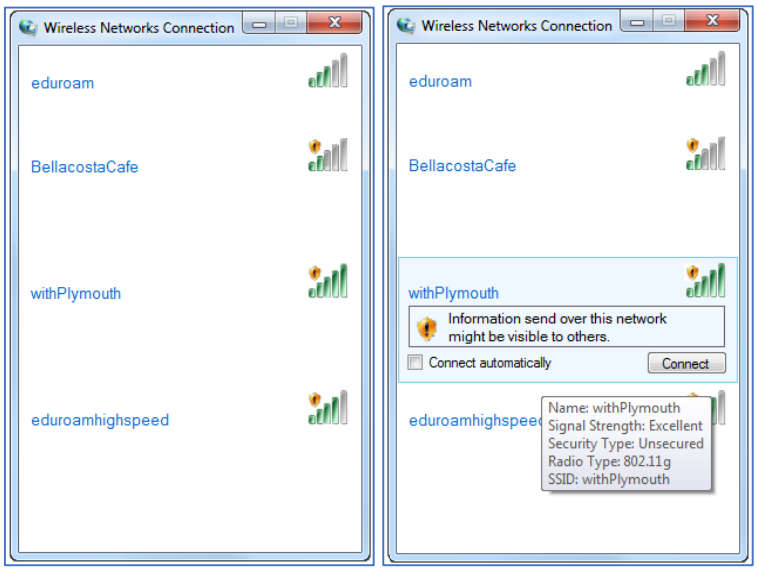

Figure 2: Screenshots of the first interface

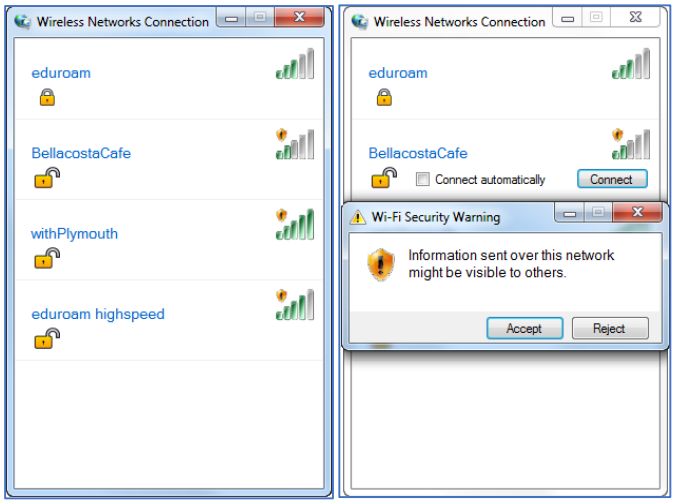

Figure 3: Screenshots for the second interface

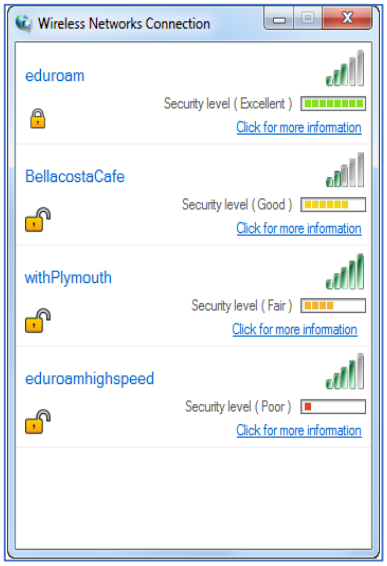

Figure 4: Screenshot of the third interface

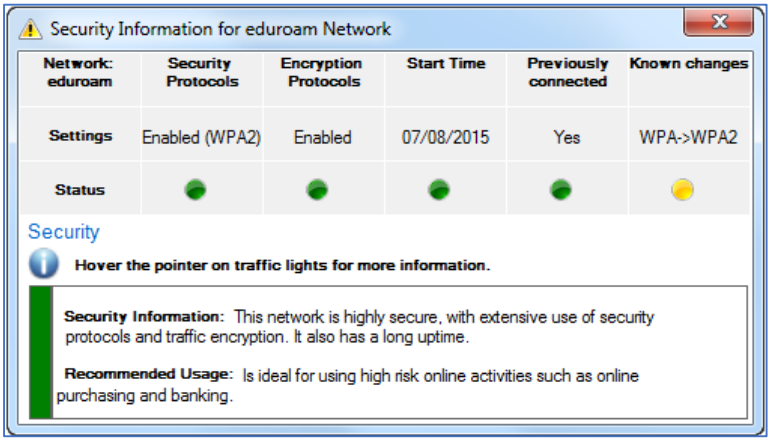

Figure 5: Screenshot of the security panel for the first Wi-Fi network within the third interface

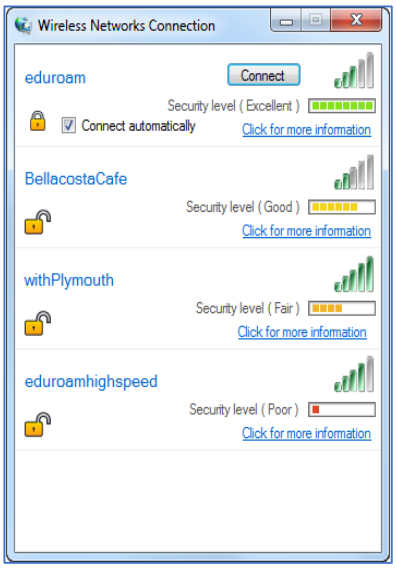

Figure 6: Screenshot of the fourth interface

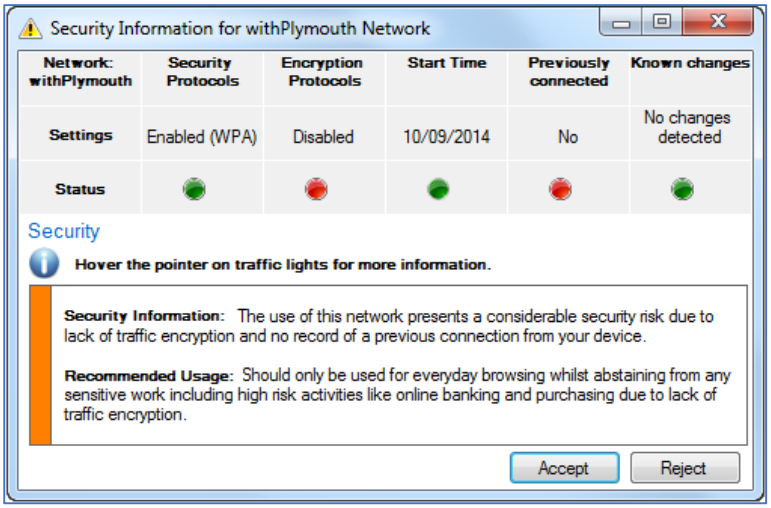

Figure 7: Screenshot of the security panel for the third Wi-Fi network within the fourth interface

Results

The participants' selection choices of the Wi-Fi networks of the four interfaces are presented in Figure 8. For the first interface, given that most participants are students and that the experiment was carried out within the university campus, it is not surprising that 60% of them selected the eduroam Wi-Fi as their first choice, as this is the network managed by the university.

Despite being unknown, 8% of the participants chose BellaCostaCafe after being unable to connect to eduroam with their credentials.

Because of its name (or due to its nomenclature), it was expected that the withPlymouth network would be within the main selection of the participants. The network is also managed by the university, however, it is intended for guests and therefore it only provides four hours of connection each day at no cost or authentication. It must also be noted that this connection does not use any encryption protocols, making it less secure than eduroam. Nevertheless, 20% of the participants chose this network as their first choice, whereas 24% of them selected this network after not being able to connect to eduroam.

Despite being unknown to participants and not within the networks managed by the university, the eduroamhighspeed network attracted 16% of the participants as their first choice and 28% of the participants as their second choice. The implied speed of the network clearly measured as a great factor on the influence of the selection, as participants chose this network on the basis that it is a high-speed connection, as the name implies.

On the second interface, 76% of the participants selected the eduroam network as their first choicefor the same reasons described previously. In contrast to the first interface, the warning message seems to make participants hesitant on connecting, as only 4% of them chose the BellaCostaCafe as their second choice, compared to the 8% on the previous interface. From these results, the impact of the design on the decision of the users can be recognised, as the warning message made the participants think more before selecting the network. Nevertheless, 4% of the participants chose this network as their third and fourth choice, raising some concerns on a small portion of the participants not paying enough attention to the warning message.

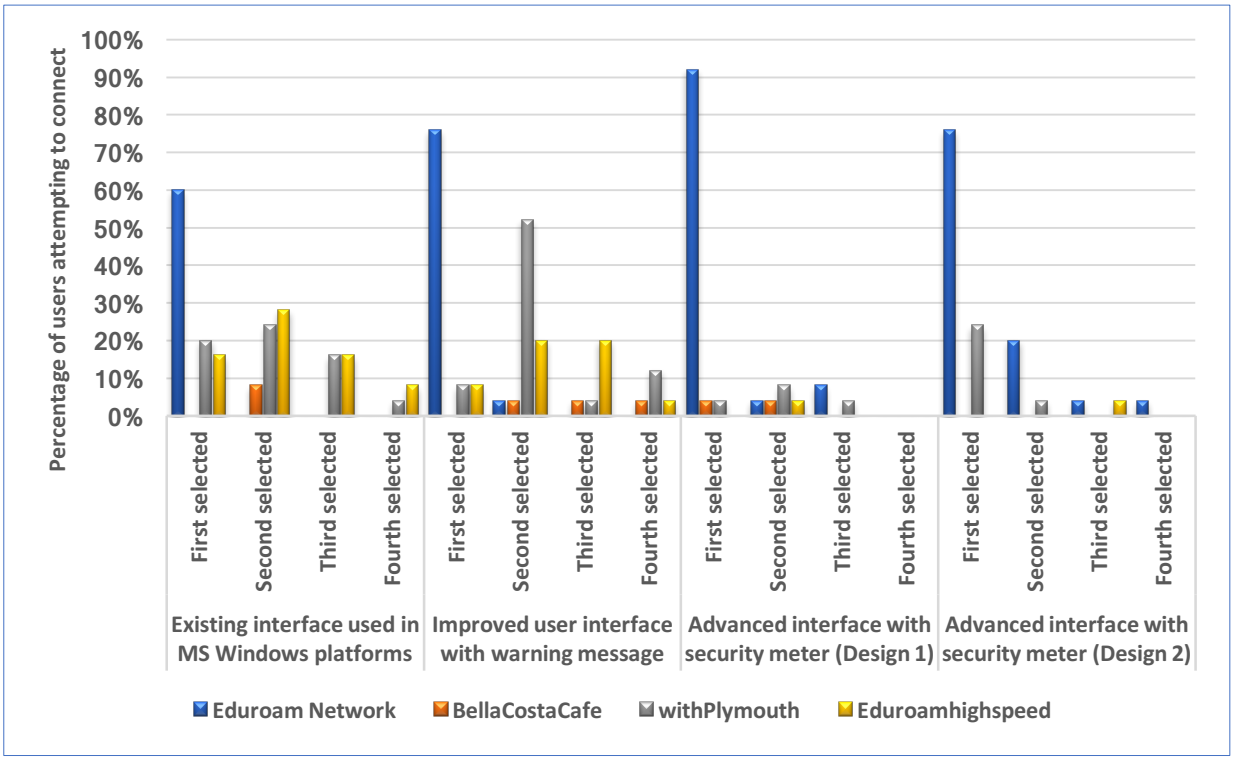

Figure 8: User's Wi-Fi network selections for the four interface

8% of the participants chose the withPlymouth network as their first choice and 52% selected as their second choice after being unable to connect to eduroam. As mentioned earlier, this network is within the main selections, as it is known to most of the participants.

Similar to the BellaCostaCaffe network, the eduroamhighspeed selection also showed signs of improvement, as only 8% of participants chose it as their first choice, as opposed to 16% on the first interface. Despite this, 20% chose it as their second choice and third choice, compared to 28% and 16% on the first interface respectively, raising concerns over the name high speed influencing the choice of the user.

With regards to the third interface, 92% of the participants chose eduroam as their main choice. This is not surprising, as the full green security meter and the encouraging security information motivated participants to choose this network. On the other hand, this raises some concerns as the interface was designed to allow access without any authentication. The padlock was only to demonstrate that the network is secured, and to test whether users would recognize this flaw and the abnormal behaviour. Surprisingly, only one user detected this, whereas others did not recognize the flaw and continued to connect without any perception.

Regarding the BellaCostaCafe, the security meter and the advice message influenced the users on deciding to connect to the network and, as a result, only 4% made it their first and second choice equally. The impact of the security meter along with the security advice proves to be a better approach, as participants hesitate more to connect to unknown networks although the security meter shows that this network is the second best network in terms of its security compared to the other presented networks, as opposed to the previous interfaces.

The withPlymouth network attracted 4% of the users to choose it as their first choice, 8% as their second choice and 4% as the third choice. Alarmingly, this demonstrates that a small portion of participants trust the network by the name and therefore ignore the security warnings, despite being told that the connection is insecure. Looking at the results of eduroamhighspeed, none of the participants chose it as their first, third or fourth selection, and only 4% selected it as their second choice. Although it highlights a big improvement compared to the previous interfaces, there are still reasons for concern, as some users still selected it as one of their choices, despite being an unknown network and alarms being raised regarding its poor security

For the fourth interface, 76% of the participants chose eduroam as their main choice compared to 92% in the third interface. Although the design of the fourth interface is quite similar to third interface, there were some users who selected withPlymouth over eduroam because it has a better signal taken into account that they are both trustworthy because participants are familiar with both networks.

With regard to the BellaCostaCafe Wi-Fi network, none of the participants selected this network although the security meter shows that this network is the second best network in terms of its security features based on the security information provided in the security information panel. This demonstrates that some participants are tends to make their choices based on the familiarity of the network name but not of the security features the network.

24% of the users made the withPlymouth network their first choice, whereas 4% made it their second. None chose it as their third or fourth selections. This shows a significant improvement over the previous interfaces, nevertheless, there is still some reason for concern, as many users still chose this network despite the security warnings, due to the fact that they are familiar with the network name.

Regarding the eduroamhighspeed Wi-Fi network, there were a few participants who selected this network as their third choice and none of the participants chose this network as their first, second or fourth choice. Although this is a great improvement compared to what has been seen in the first and the second interfaces, it arguably shows that some people will ignore whatever advice is given.

Discussion and Findings

From the results described above, it was perceived that the name of the network has a significant impact on the participants when choosing an appropriate network to access the Internet within a known environment like the university campus. Results obtained from the experiment revealed that in the absence of security information, users are very prone to connecting to names that look like a known name.

As presented in Figure 8, a considerable number of the participants in the first, second, third and fourth interfaces have chosen to connect to the eduroam Wi-Fi network as their first choice. This was driven by the recognition of the Wi-Fi network as the main used Wi-Fi network in the university campus. When participants were asked what their reasons were for choosing the eduroam network as their first choice, their answers were because they are familiar with the name of this Wi-Fi network and recognise it within the university campus and considering that the network name indicates that it is run and managed by the university and therefore it is trustworthy. It seems that the users greatly trust the location as an assumption that there is a correlation between the network name and location. For example, students and staff within an academic environment have become accustomed to the fact that the eduroam Wi-Fi network is run and managed by the university and hence it is a trustworthy network. However, it is well known that the network name can be modified to any name or spoofed which indicates the confidence of the users in the network name could be interpreted as a lack of knowledge of this security issue.

This reflects the lack of security awareness for the participants regarding the possibility of falling victim of a spoofed network. In a wider setting, in places such as shops and shopping malls, restaurants and cafes, where the user will focus only to get access to a free Wi-Fi network and will be looking to any Wi-Fi network that has partly or totally the name of the place within the users range like a name of a shop, restaurant or cafe, this increases the possibility of the users falling victim to deception and getting access to spoofed Wi-Fi networks.

In addition, it appears that claimed signal strength is also a persuading factor, especially if the Wi-Fi network name includes an indication that it is a high-speed Wi-Fi network. This explains the selection of 16%, 28% and 16% of the participants to eduroamhighspeed network who tried the first interface as their first, second and third choice respectively. Similarly, with the second interface 8%, 20% and 20% of the participants who tried the second interface choose this Wi-Fi network as their first, second and third choice respectively. The large proportion of the participants who have selected the eduroamhighspeed network as seen in the first and second interfaces reflects the extent of the danger which could be exposed to these participants because of their lack of knowledge of the associated risks of unknown Wi-Fi networks, and the extent of the damage that they may be subjected to when connecting to fraudulent Wi-Fi networks and more importantly this proves that the first and the second interfaces have limited capabilities in providing the required security guidance and feedback to participants to allow them to choose the most appropriate Wi-Fi network.

However, as few as 4% participants chose the eduroamhighspeed Wi-Fi network as their second choice with the third interface and same chose this Wi-Fi network as their third choice with the fourth interface which proves that the advanced interfaces with security meter (Design 1 and 2) have educated users and made them aware of the security risks associated with use of this unknown Wi-Fi network. This proves that users are influenced if suitable security guidance and visible feedback is provided at the point of need to help the users to make the right decision at the right time to avoid security risks associated with risks of using unknown Wi-Fi networks.

This has also highlighted the fact that some participants access Wi-Fi networks which provide greater speed rather than focusing on the security aspects of the Wi-Fi networks. This demonstrates that the need for speed in the eyes of a few participants sometimes outweighs the security concerns.

Moreover, it was also observed during the experiment that the participants interacted with the second interface with disinterest when the warning message pop up as some of them read the warning message without giving it enough consideration and then clicked either the "*Accept*" or the "*Reject*" button, while others dealt with it quickly without reading its content and without paying any attention to the message. This perhaps can be explained because of the fact that this is the first time participants perceived such a warning message when they tried to connect to Wi-Fi network using the MS Windows platform.

It was also perceived during the experiment that since it is often difficult for users who have a limited knowledge of computer systems to understand the security issues and concerns of Wi-Fi networks, most users will simply connect to the network with the greatest signal or the greatest speed and will not look into the security details. Additionally, participants' interactions with the four interfaces showed that they intend to connect to the next best network in terms of speed or best signal if they could not access the more secure one. For example, one of the participants commented: "*I wasn't able to connect to the preferred secure network, so I connected to the network with the best signal that was unsecured*".

The new design of the interfaces with the security meter and the information security panels that provides the security information and the recommended usage for the users about the Wi-Fi networks has proven that the new design is a promising approach in providing adequate information for the users before they make their decision, educate and make them aware of the security implications before

connecting to insecure Wi-Fi hotspots in public areas. Only 4% of the participants who tried the third interface selected the network that has poor security "eduroamhighspeed" as their second choice and only 4% of the participants who tried the fourth interface selected this network as their third choice. Participants made their decision on the basis that it is a high-speed Wi-Fi network as its name implies.

Moreover, it should also be mentioned that the name of the network is still a vital fact that keeps influencing the participants when selecting the network especially if the name of the network is known to the users and is seen in the environment they are familiar with. This is obtained from the results of the third and the fourth interfaces. For example, the network named "withPlymouth" is well-known to the participants within the university campus and it has been designed in the experiment to have a fair level of security in the third and fourth interfaces, however, 8%, 52%, 4%, 12% of the participants who tried the third interface selected this network as their first, second, third and fourth choice respectively. Similarly, with the fourth interface, 24%, 4% of the participants who tried the fourth interface selected this network as their first and second choice respectively.

Conclusions

This paper has presented the results of an experimental study that examined the effectiveness of using targeted security awareness-raising approach. The study has shown that while users did not exhibit perfect behaviour, there was a tangible improvement with interfaces offering more security-related information. In common with other security contexts, results suggest that users' behaviour can be positively influenced purely through the provision of additional information and better choices can be made even if the system does not provide any further enforcement.

The results have also proven that the new design of the Wi-Fi interfaces has made an important improvement in terms of the security behaviours of the participants before connecting to insecure Wi-Fi hotspots in public areas.

Moreover, the results revealed that known Wi-Fi networks for participants are mostly treated as trustworthy networks, although the network name has the potential to be spoofed. This conceivably highlights the lack of knowledge of the participants regarding this security issue.

From the obtained results, it was also perceived that the network name has greatly affected some of the participants' decisions especially if its name implies that it has a high speed without paying any attention to security issues. This demonstrates that the speed in some cases outweighs the security concerns in the eyes of the participants.

The results have also demonstrated that the existing user interface of the Wi-Fi dialog window used in Microsoft Windows platforms is inadequate for providing security guidelines and security information to users when selecting Wi-Fi hotspots that were considered insecure. This has proved the urgent need for the provision of a new way to increase the security awareness of users about the security risks associated with the use of Wi-Fi networks, especially if it is unknown and insecure (i.e. in public areas).

References

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34(3), 523-548*.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31(8), 983-988*.

F-SECURE. (*2014*). TAINTED LOVE: HOW WI-FI BETRAYS US. F-Secure Corporation. Retrieved from: https://fsecureconsumer.files.wordpress.com/2014/09/wi-fi-experiment_uk_2014.pdf. (Accessed 28 November 2014).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31(1), 83-95*.

iPass. (2016a). iPass Mobile Professional Report 2016. Retrieved from: https://www.ipass.com/wp-content/uploads/2016/11/iPass-Mobile-Professional-Report-2016.pdf. (Accessed 24 March 2017).

iPass. (2016b). 2016 Mobile Security Report. Retrieved from: https://www.ipass.com/wp-content/uploads/2016/05/iPass-2016-Mobile-Security-Report.pdf. (Accessed 24 March 2017).

Kaspersky Lab. (2016). Consumer Security Risks Survey, CONNECTED BUT NOT PROTECTED Kaspersky Lab. Retrieved from: https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf. (Accessed 30 March 2017).

Kessel, P. V. (2012). Fighting to Close the Gap: Ernst & Young's 2012 Global Information Security Survey. *Ernst & Young's, 5, 23-31.*

NETMARKETSHARE. (2017). Desktop Operating System Market Share. April 2017. Retrieved from: http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0)&qpsp=2016&qpnp=1&qptimeframe=Y. (Accessed 30 March 2017).

Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems (pp. 1056-1057)*. ACM.

PCI. Security Standards Council. Security Awareness Program Special Interest Group. (2014). *Best Practices for Implementing a Security Awareness Program*. October 2014. Version: 1.0. September 25 2015. Retrieved from: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf. (Accessed 10 December 2014).

Randell, C. (2013). Why security awareness campaigns fail. MWR InfoSecurity. Retrieved from: https://www.mwrinfosecurity.com/our-thinking/why-security-awareness-campaigns-fail/. (Accessed 20 November 2014).

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal, 19(3), 122-131.*

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52(1), 92-100.*

Silic, M. and Back, A. (2017). Deterrent Effects of Warnings on User's Behavior in Preventing Malicious Software Use. *In Proceedings of the 50th Hawaii International Conference on System Sciences.*

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging towards security: Developing an application for wireless network selection for android phones. *In Proceedings of the 2015 British HCI conference (pp. 193-201). ACM.*

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., ... & Christin, N. (2012). How does your password measure up? The effect of strength meters on password creation. *In USENIX Security Symposium (pp. 65-80).*

Volkamer, M., Bartsch, S., & Kauer, M. (2013). Contextualized Security Interventions in Password Transmission Scenarios. *In EISMC (pp. 12-22).*

Zaaba, Z. F., Furnell, S. M., & Dowland, P. S. (2014). A study on improving security warnings. In *Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on (pp. 1-5).* IEEE.