Understanding the Gap between Usability and Security

Mehul Raniga
Department of Computer Science
University of Auckland
mran073@aucklanduni.ac.nz

ABSTRACT

Users interact with computers primarily through the aid of an interface. HCI is the field which is concerned with the design of interfaces facilitating efficient comprehension of the functionality of interfaces. When using applications, users would have to deal with some level of security present within the interfaces. It is not the importance of the level of security offered by the applications; rather it is the matter of how well a user is able to understand the security feature within the interface and fully harness its capability. This paper mainly intends to explore the field of HCI-S and investigate the security usability criteria they present comparing it to the usability study conducted by Jackson et al. [1]. The evaluation would examine the criteria and analyze which ones were or were not well addressed in the usability study by Jackson et al. [1].

Keywords: HCI, human computer interaction; Information security; Usability; HCI-S

1. INTRODUCTION

The effectiveness of security features do not depend on the technical means alone but are also influenced considerably by the end-users [2]. An interface that is well designed could aid the user in successfully becoming accustomed to the interface and being able to efficiently accomplish tasks [3]. If users fail to understand and accurately utilize the security features within an interface, it forfeits its purpose. This hints at the design of interfaces which strikes an optimal balance between usability and security such that users can effectively utilize the security features. HCI-Security (Termed HCI-S) is the field which is concerned with establishing a "common ground" between users and security features present in interfaces therefore avoiding circumstances where users are reluctant to use or even bypass security features [3]. Badly designed security usability features can expose users to vulnerabilities which would result in systems being compromised [5]. This paper intends to explore the usability study conducted by Jackson et al. [1] and critique the design of the security features within the interfaces which users used while carrying out tasks to make security related decisions. This would be done by applying the HCI-S criteria and contrasting if the usability study had addressed those. The paper would firstly present the challenges of usable security faced by users followed by outlining the criteria of HCI-S in detail. Furthermore, the paper moves on to its crux contrasting which HCI-S criteria specified were addressed by the usability study and which ones were not and the implications of it on user's behavior. The paper would finally endeavor to make suggestions with respect to the HCI-S criteria as to what changes could be introduced in order to anticipate possible improvement in the way security features are presented in interfaces to users and aid them in creating reasonable choices to protect themselves.

2. THE CHALLENGES OF USABLE SECURITY

Security features within interfaces require certain characteristics that significantly impact the usability of the feature and consequently affects the level of protection that could be achieved. Furnell et al. [2] outlines some key principles that should be incorporated while designing security features to enhance usability. They are as follows:

a) **Understandable** – The presentation of options and descriptions should be afforded in a clear and uncomplicated manner where users are aware of the outcomes. The security domain in addition employs a substantial amount of technical jargon which not every user (especially novices) is knowledgeable of; thus, adequate help and support should be made available to the users to achieve understandability in order to gain the level of security required.

b) **Locatable** – The accessibility of security features is essential as users who spend an extensive period in search of security features would highly likely discontinue to do so and continue with their tasks despite being unprotected.

c) **Visible** – A fundamental feature any system ought to have is a status indicator through which a user is made known of a system's current status. An ideal system would issue warnings to the user via the system indicator which would then initiate the required action to be taken.

d) **Convenient** – Security features should not be presented in a manner that it would be considered invasive and interferes with the user's task. In such a scenario, users would most likely disable the feature in order to resume their task avoiding disturbance.

Analyzing some of the existing implementations of security according to the principles outlined above suggests that they may lack the usability characteristics. This issue was explored by the Computing Research Association (CRA) which recognized human error as the cause of configuration errors in one of their reports. This however, was attributable to the design of the system and its interface. The report also discovered a fact that is centered on the theme of this paper. It suggested that some security features aren't utilized extensively as users have difficulty using them. Reflecting this idea on a higher dimension; "There is a usability gap that translates directly into a usage gap" [2].

3. THE CRITERIA FOR HCI-S

The previous section outlined some general characteristics of a usable security feature in interfaces. Johnston et al. [3] discuss some criteria of HCI-S which could help improve the interface thereby improving security and making systems reliable, secure and robust. They are as follows:

a) **Aesthetic and minimalist design** – The main idea behind this notion is to display the precise amount of information as to not overwhelm the user with information and options that are irrelevant. Moreover, the usage of technical jargon should be kept at a bare minimum as to maintain simplicity and make the user more confident in using the interface. The minimalist design concept could be influential in improving the usability of security features. Figure 1 is such an example where information that might not be too relevant to the user or might increase the complexity is stored in a collapsed state (referring to the lock icon)

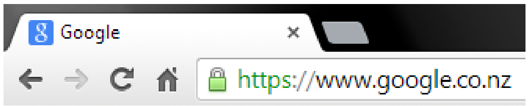


Figure 1

b) **Help users recognize, diagnose and recover from errors –**
Dealing with errors is one of the aspects in a security feature. Having said that, some errors tend to have a higher cognitive impact on users. For example, if a user is carrying out a banking transaction and is prompted with an error message, "Your interactive session is no longer active"; such messages displayed have the potential of placing the user in a dilemma. It is

therefore crucial that error messages are communicated in such a manner that they clearly indicate the purpose and action that should be taken. Additionally, the users should also be informed on how they could acquire support and help as required. Designers ought to focus their concentration on designing error messages that are user friendly as opposed to having a generic message for all errors.

c) **Convey features** – The criterion Visible, as discussed in the previous section places its focus on security features conveying to the users its status; the convey features criterion on the other hand indicates to the user of the availability of security features. This should be done in an apparent way through the interface that the user is made known of the existing capabilities. The security features of encryption are commonly found in web browsers. SSL is one of the well distinguished technologies used for encryption. When applied in browsers, it should be vividly display its functionality through the interface. Often novices may not be able to comprehend the functionality of such sophisticated security features; the use of graphics for example could be a clever way of conveying them.

d) **Satisfaction** – Designers of interfaces should realize that security is not the user's ultimate goal. According to this, a user's experience with security features should be made as satisfying as possible to avoid circumstances where a user who would undergo a lot of difficulty while using a security feature would most probably neglect it and continue to stay unprotected. Security might be considered intimidating to some users; in fact one should feel such a way considering the technicality of the field. Security features however should be presented in an approach such that users find it engaging.

e) **Learnability** – As mentioned by previous criteria, a user is likely to feel intimidated by security features, therefore these features ought to create a user friendly environment where features are very simple to learn. Imagine a scenario where a user revisits a particular software interface and would have to learn the functionality yet again; this would be highly undesirable. One of the ways to approach this problem is to associate the elements in the interface with the real world. Real world metaphors would be a perfect example. Keys and padlocks in interfaces for instance could put across the meaning of its functionality to the users (figure 2 portrays an example). One of the criteria in HCI dealing with standardization suggests not re-inventing the wheel but simply reusing the standard convention. Such consistency within interfaces is guaranteed to improve learnability. It is not only the visual cues but naming conventions that have to be standard across interfaces. A very general task users might encounter is logging in to a service. This involves entering a username and password into the text fields; however, if the text labels are not standard across different interfaces, it might cause the users to withdraw from entering their credentials.

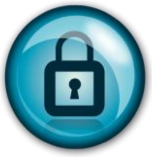


Figure 2

Johnston et al. [3] expressed their opinion on the HCIS-S criteria claiming that "the successful implementation of all the above criteria will lead to trust". When the interface of a system is able to foster trust, users would efficiently be able to utilize the security features to its maximum capability. This section and the section prior discussed the desired characteristics security features in interfaces ought to have. In the next section, the article by Jackson et al. [1] would be concentrated on primarily contrasting its security features with the usable security criteria and investigating if they are in accordance to it. Additionally possible recommendations would be made inorder to improve the security features.

4. STUDY DESIGN AND RESULTS

The usability study carried out by Jackson et al. [1] was designed as follows. The participants of the study were required to familiarize themselves with the two banking websites after which they were sorted into three groups and classified the websites as fraudulent or legitimate. The first group was the trained group where users had learnt about Extended Validation Certificates and other security features found in browsers such as the phishing filter. The second group was the untrained group where users were just shown the extended validation certificates but apparently did not receive any training on its meaning. The last group was the control group where users were neither shown the extended validation certificates nor received any training on its meaning.

The websites that the participants classified were divided into the following categories:

- **a)** The Real website.
- **b)** The Real website, but designed to induce confusion
- **c)** Site with Homograph attack.
- **d)** Homograph site that triggers a warning.
- **e)** Site with a Picture-in-picture attack.
- **f)** A Picture-in-picture attack with mismatched browser color scheme.
- **g)** A site with an IP address instead of domain name blocked by phishing filter

The results of the study are illustrated below

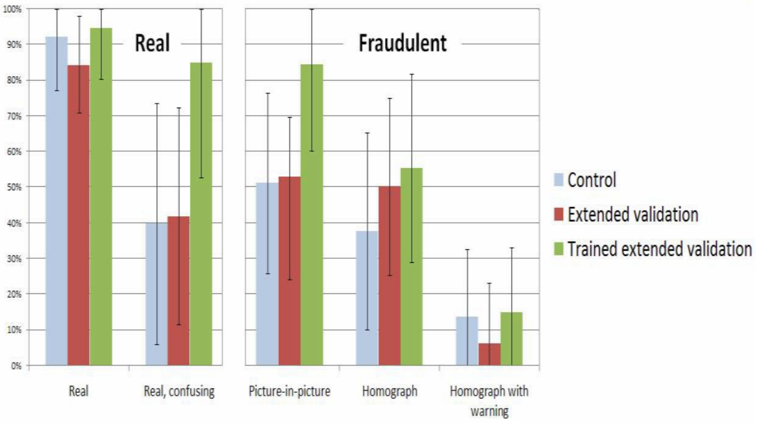


Figure 3: The frequencies of particular types of websites classified as legitimate.

4.1 THE USABILITY ANALYSIS

In the study carried out by Jackson et al. [1], users were exposed to a few security features which they utilized within the usability test; they are described in the paper as follows:

a) **Extended Validation** – Since phishing attacks have risen to a greater extent in the recent few years causing loss and damage to financial companies, certificate authorities have responded by introducing an innovative technology referred to as the extended validation certificates. These certificates not only indicate that a specific domain name is controlled by an owner, but it additionally confirms the identity of businesses that are legitimate. This feature is illustrated in different browsers in unique approaches. The browser designed by Microsoft, Internet Explorer (apparently the browser chosen for the usability study), demonstrates this feature through making the address bar green implying the presence of the certificate.

b) Phishing Warning System – A technique that could be applied to help protect users from phishing attacks would be simply to identify if the user has connected to a website that is marked as "untrustworthy" and issue a warning to the user. The success of this technique relies on the choice that users make; if they are able to comprehend the warning, they would withdraw from the page not providing any personal information to the phishing website. User's comprehension is therefore the key element. This security feature should meet the security usability criteria in order to ensure the feature is able to put across its intended message. Nevertheless, these systems are integrated in browsers today as security toolbars which depend on a blacklist to classify a website's authenticity. The data of the blacklist has an effect on the accuracy of the toolbar. Although the precision of these phishing filters might be questionable, they have become a standard tool available to users.

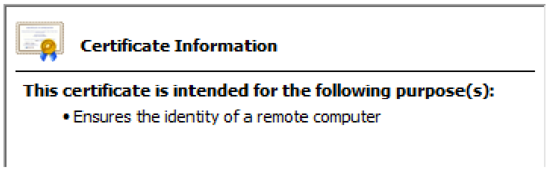
The paper now progresses onto its crux evaluating the security features with respect to the security usability criteria.

4.1.1 ANALYSIS OF EXTENDED VALIDATION

This section evaluates the security feature of extended validation. The discussion would focus more on the users from the untrained and control group due to the reason that the users from the trained group possessed an invalid assumption that the phishing filter would notify the users of an illegitimate website 100% of the time so it is difficult to determine whether the users gave heed to the security features and therefore does not place us in the position to be able to confidently argue of the feature's usability qualities. More importantly, the reason why the untrained and control group are highlighted is owing to the fact that they represent typical users who are not experts in the field of security but simply rely on the feature's usability qualities to be able to inform the user of the features functionality. The usability analysis is as follows.

a) **Understandable** – According to the results, the untrained group and the control group had performed quite similarly to each other across the various tasks; however in the post test results, none of the users acknowledged that they utilized the extended validation in the address bar to classify the websites. One of the postulations that could be made in this scenario is that users did not comprehend the purpose of the extended validation (essentially, they did not comprehend the meaning of a color running across the address bar). The browser does have provisions to clearly explain the meaning of extended validation which could be found in its menu which is two clicks away (as shown in figure 4).

Figure 4: The purpose of extended validation


Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

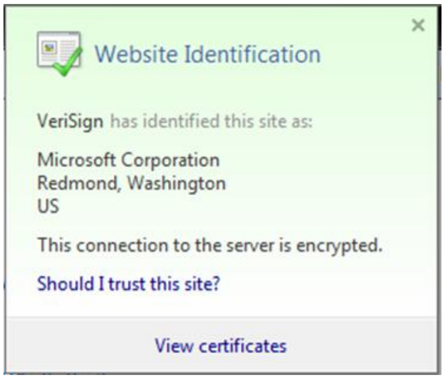
Since the presentation of the feature is not based on any real world metaphor and the users have to navigate a bit deeper in order to discover its actual purpose, users may not be capable of comprehending the functionality of the extended validation feature.

b) **Locatable** – The extended validation feature is neither stored in a collapsed state nor hidden deep within several layers of menu options; instead, it is presented clearly to the users as they access a web page that has a certificate available. It could have been displayed elsewhere; however, the designers of the feature smartly embedded it within the address bar for ease of access. Despite the fact that this feature is easily accessible, if users cannot pass the understandability phase, the feature forfeits it purpose.

c) **Visible** – The extended validation certificate vividly makes the user aware of the status through the simple gesture of a particular color running across the address bar indicating the legitimacy of a website. This is comparable to the usability study where the colors indicating a legitimate, illegitimate or suspicious website was previewed by the extended validation feature in the address bar. Although it could be assumed that this should be a very relevant source of indication, the rationale of why users did not give heed to this feature is completely absurd. In general, the extended validation feature is successful in indicating the current status of the system.

d) **Convenient** – The extended validation feature does not interfere with the user's tasks by presenting the user with numerous prompts while the user might be active in their respective tasks. This feature is not intrusive as far as it could be known. Even though in the usability study the participants did not pay too much attention to this feature, none of them reported the feature to be interrupting their tasks.

e) **Aesthetic and minimalist design** – The extended validation feature avoids displaying too much information overwhelming the user with information that might not be too relevant to them. The feature stores information regarding the feature in a collapsed state (as shown in figure 5); from that state the users could progress further through the links in order to acquire even more technical information. This is an ideal design of a feature where simple information is stored in close proximity whereas very technical information that might contain a lot of jargon is stored in a deeper state. Such design decisions could be influential in improving the usability of the security features. On the other hand, providing users with very minimal or even no information can be another concern. This issue can be related back to problems discussed in the understandable section. Fundamentally, a balance must be struck between providing an adequate amount of information and being able to get the meaning across to users.



Website Identification

VeriSign has identified this site as:

Microsoft Corporation
Redmond, Washington
US

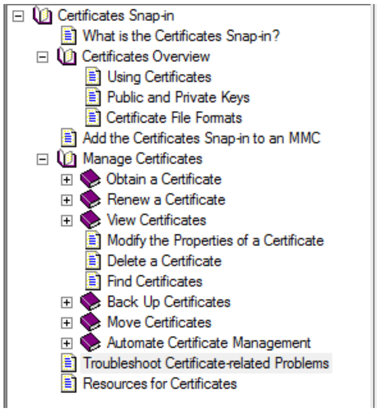
This connection to the server is encrypted.

Should I trust this site?

View certificates

Figure 5: Information stored in collapsed state

f) **Help users recognize, diagnose and recover from errors** – The extended validation feature is quite complicated than how it presents itself. It entails several technical aspects for instance keys and policies which could be inspected when need be. These however may not be relevant to novices and would only be employed by power users. Moreover if users do wish to learn about this security feature, a link to the help document is located in the options menu whereby clicking it leads the user to a library through which they could acquire the help and support as needed (as shown in figure 6)



- Certificates Snap-in
  - What is the Certificates Snap-in?
  - Certificates Overview
    - Using Certificates
    - Public and Private Keys
    - Certificate File Formats
  - Add the Certificates Snap-in to an MMC
  - Manage Certificates
    - Obtain a Certificate
    - Renew a Certificate
    - View Certificates
    - Modify the Properties of a Certificate
    - Delete a Certificate
    - Find Certificates
    - Back Up Certificates
    - Move Certificates
    - Automate Certificate Management
  - Troubleshoot Certificate-related Problems
  - Resources for Certificates

Figure 6: The help library

With the current implementation of the extended validation feature, it does diagnose the error; however, it does not significantly help users recognize (apart from the color indication) and recover from errors. In the usability test, the users were not able recognize the status of the extended validation certificate in which a solution could be developed where the users are prompted of the current status along with a list of options to recover from that particular situation.

g) **Convey features** – When connected to a page which has the security feature of extended validation, a particular status color runs across the address bar indicating the presence of that feature in contrast to just showing a stationary colored address bar. According to the design of this feature, it should be apparent to the users of the availability of the feature; in the usability study however, the users did not recognize this. Perhaps a different visual cue might help users recognize the availability of the security feature. A good example could be cited from the works of Shin et al. [6] who designed a visual cue in their usability study. The visual cue involved a blinking background indicating the status of a web page; this design was able to capture many users' attention according to results. What the extended validation and blinking background have in common is that they their visual cues are not stationary; the blinking background is a bit different though in the sense that it is persistent.

h) **Satisfaction –** The extended validation feature is designed in a way that may add to the user's experience considering that users do not have to go through such an extent of difficulty to utilize the feature, the feature is non-intrusive, it does not expose the user to irrelevant jargon and its design is uncomplicated. Through such characteristics, a user may feel more comfortable and confident in using the security features. Even though the feature is complicated it is afforded to the users in a simplistic manner whilst keeping the more technical information in a collapsed state.

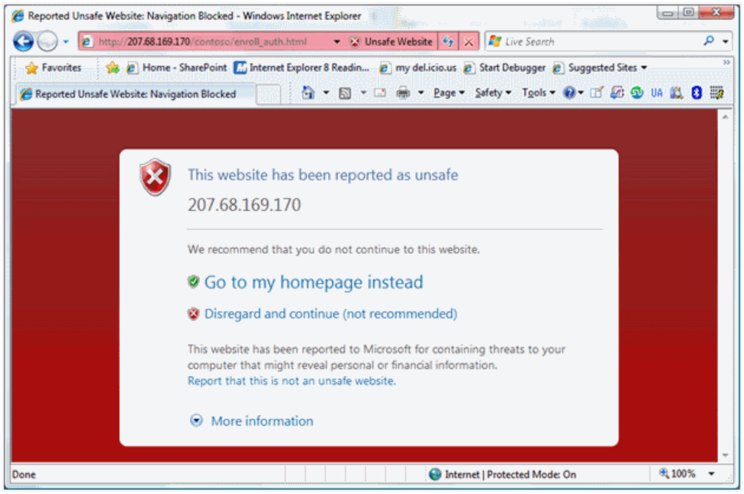
i) **Learnability –** Although the extended validation feature affords simplicity as discussed earlier, it might be difficult to foster learnability of the feature owing to the fact that it is not based on any real world metaphor for example keys or padlocks. Since it is not related to any real world elements, the users might find it difficult to learn its underlying functionality. Moreover it is not standard across various software applications therefore users may not be able to recognize the security feature. In the usability study, the users did not give heed to the extended validation security feature; had the feature been based on a real world metaphor, it could have captured the user's attention and easily elucidated the functionality that it entails. Nevertheless, it should be realized that not all features are capable of being transformed into a real life metaphor.

Evaluating the extended validation feature against the security usability criteria, it could be concluded that the feature satisfies most of the criteria but apparently no feature is flawless. The areas that have to be focused on for this feature are understandability and conveying of features. According to the usability study, the users may not have successfully understood the purpose of the feature; one of the suggestions to redesigning this feature would be to embed a real world metaphor such as a graphic that makes it obvious to the user that the extended validation certificate feature is available. The graphic should be persistent (as comparable to the blinking background feature designed by Shin et al. [6] which produced positive results), but it should not reduce the user experience at the same time. If all of these schemes still fail, the last resort could be to put an obvious indication in with the current implementation, a sign that says "Certificate Available".

4.1.2 ANALYSIS OF PHISHING FILTERS

This section evaluates the security feature of phishing filters. According to the results of the usability study, phishing filters have had a significant positive impact on users. In scenarios where upon users connected to a phishing website, the phishing filter warning system was able to convey information in a manner that users took heed of the warning and had withdrawn from the web page not disclosing any personal data. Through these findings we could postulate that the design of the phishing filter might be consistent with the principles of HCI-S. The analysis of the feature is as follows.

a) Understandable – As discussed previously of the positive results yielded by the phishing filter, it is most probable that users were successfully able to comprehend the information issued by the warning system and make an informed decision. The provision that this feature affords is through a warning. The design of the warning is such, that it conveys the message in a simplistic and efficient manner by means of various aspects. Figure 7 is an example of a phishing warning; focusing on each aspect, firstly the address bar turns red and explicitly states the status of the website, secondly it conveys further information of the event in the body of the browser using non-technical jargon. The usage of a particular color scheme to denote the circumstances also assist in understandability. Icons in addition complement the list (referring to the crosses and ticks). Due to the various number of elements presented in the browser, it is highly likely that a user would be capable of understanding the security feature.


Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/contoso/enroll_auth.html
Unsafe Website
Live Search
Favorites
Home - SharePoint
Internet Explorer 8 Readin...
my del.icio.us
Start Debugger
Suggested Sites
Reported Unsafe Website: Navigation Blocked
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

This website has been reported as unsafe

207.68.169.170

We recommend that you do not continue to this website.

Go to my homepage instead

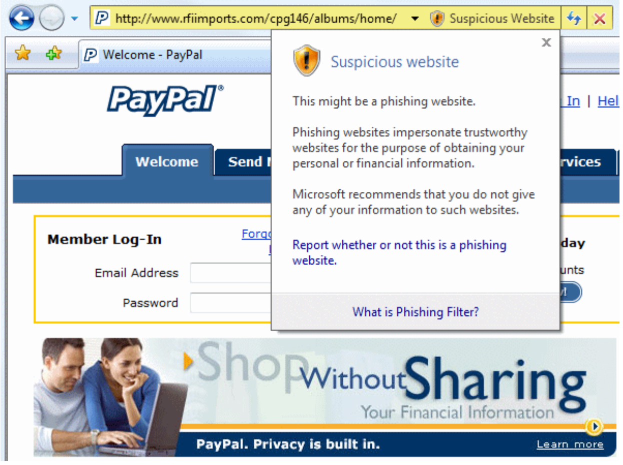
Disregard and continue (not recommended)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.

More information

Figure 7: A phishing warning

b) **Locatable** – The phishing system constantly analyzes the websites verifying if they happen to appear in the black list; the phishing warning system on the other hand is only activated upon encountering a website. When it does encounter a phishing website, it issues a warning in two ways, one warning covers the entire browser (as shown in figure 7) and the other is in the form of a popup (as shown in figure 8). Both techniques capture the user's attention as they are easily locatable.



Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

Figure 8: A phishing popup warning

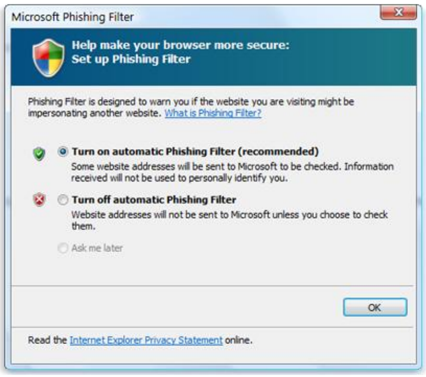
c) **Visible** – The phishing warning feature clearly indicates the current status of a page; this is achieved by changing the color scheme of the address bar, presenting an icon that represents the current state and explicitly indicating what the icon symbolizes. All of these are located within the address bar therefore a user is effectively made known of the current status.

d) **Convenient** – Even though the phishing warning system entails various elements, it is designed in a well structured manner to avoid cluttering the interface. The phishing filters may not be accurate in all cases, for instance if a legitimate website that a user frequently visits is now labeled as unsafe would disallow that user to progress to the site, this could be rather frustrating to the user. Nevertheless, due to the good user friendly design, the users have the rights to suggest whether or not a website is actually illegitimate (as seen in figures 7 and 8). The users in the usability study however did not report this feature as invasive or intrusive.

e) **Aesthetic and minimalist design** – The amount of information that is provided by the phishing warning system could be argued as to be overwhelming the users; however, the information is quite simplistic in nature and additionally it is sometimes a good idea to have redundant information in order to impart the underlying knowledge (this is what the extended validation feature might require). As discussed earlier, the use of technical jargon is kept at a minimum; if users are not able to grasp the warning then the feature would just forfeit its purpose. Moreover technical information that might not be too relevant to users is kept in collapsed state.

f) **Help users recognize, diagnose and recover from errors** – As discussed in previous criteria, the phishing warning system is efficient in helping users recognize the error. A point to note in the way the feature reports the error is that it seems less intimidating than messages for instance "this website will infect your computer". The main goal is to make the user confident of using the security feature. The feature in addition presents a few options to the user in order to recover from the error. If in a situation the user does not know which course of action to take, the feature has its own recommended suggestions for the user.

g) **Convey Features** – With the phishing warning system, a user cannot know whether the browser is equipped with one until they are issued with a warning or unless they navigate through the security options of the browser (as shown in figure 9). In general, there isn't any form of indication on the interface of the availability of the phishing warning system. Not all security features are exhibited to the users through the interface, some features quietly run in the background without the user's knowledge; however, would having an icon as a part of the interface increase the confidence of users to using the internet?, this could be a possible research question.



Microsoft Phishing Filter

Help make your browser more secure:
Set up Phishing Filter

Phishing Filter is designed to warn you if the website you are visiting might be impersonating another website. What is Phishing Filter?

● **Turn on automatic Phishing Filter (recommended)**
Some website addresses will be sent to Microsoft to be checked. Information received will not be used to personally identify you.

○ **Turn off automatic Phishing Filter**
Website addresses will not be sent to Microsoft unless you choose to check them.

○ Ask me later

Read the Internet Explorer Privacy Statement online.

Figure 9: Options for phishing filters

h) **Satisfaction** – The phishing warning feature is designed in a way that may add to the user's experience considering that users do not have to go through such an extent of difficulty to utilize the feature, the feature is non-intrusive, it does not expose the user to irrelevant jargon and its design is uncomplicated. Through such characteristics, a user may feel more comfortable and confident in using the security features. Even though the feature is complicated it is afforded to the users in a simplistic manner whilst keeping the more technical information in a collapsed state.

i) **Learnability** – The phishing warning system affords learnability as it employs elements which are associated with the real world metaphors such as a shield which signifies protection, a cross with a red color scheme which signifies danger and an exclamation mark which could signify a notice (as shown in figure 10). In the usability study, it could have been possible according to the results that when users encountered the phishing warning, without reading any content of the warning and merely looking at the icons, the users would have immediately reverted back.

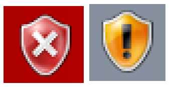


Figure 10: Icons of phishing warning system

Evaluating the phishing warning feature against the security usability criteria, it could be concluded that the feature satisfies nearly all the criteria defined; it is a well designed security feature that entails nearly all the aspects of HCI-S. It could also be deduced that in order to effectively warn users of the implications of security risks, adequate information must be provided (as the phishing warning feature did and what the extended validation feature might need). Now that the feature is reasonably able to demonstrate good usability qualities, security experts should work on expanding the blacklist to attain better precision and they should also endeavor to create higher levels of security around blacklists given that attackers may attempt to gain access to them and manipulate it to their advantage.

5. CONCLUSION

Comparing the security features against the HCI-S criteria gave a more detailed insight into the levels of usability a feature encompasses. It could now be understood how gaps in usability could convert directly into usage gaps, essentially meaning that if users are unable to comprehend the interface, they would be somewhat reluctant to use the features. According to the report of Jackson et al. [1], the results for the phishing warning system were statistically significant; however, its validity is arguable owing to the fact that participants were well aware that they were required to classify the websites. Perhaps for future work further tests ought to be carried out to re-confirm the validity of the results. As for the extended validation feature, tests need to be re-done with a well designed training session to analyze if training users could be a possible option to consider in resolving usability issues.

REFERENCES

[1] C. Jackson, D. Simon, D. Tan, and A. Barth, "An evaluation of extended validation and picture-in-picture phishing attacks," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin Heidelberg, 2007, vol. 4886, pp. 281-293. http://link.springer.com.ezproxy.auckland.ac.nz/chapter/10.1007%2F978-3-540-77366-5_27#

[2] S.M. Furnell, A. Jusoh, D. Katsabas, The challenges of understanding and using security: A survey of end-users, Computers & Security, Volume 25, Issue 1, February 2006, Pages 27-35, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2005.12.004.

[3] J. Johnston, J.H.P. Eloff, L. Labuschagne, Security and human computer interfaces, Computers & Security, Volume 22, Issue 8, December 2003, Pages 675-684, ISSN 0167-4048, http://dx.doi.org/10.1016/S0167-4048(03)00006-3.

[4] Kainda, R.; Flechais, I.; Roscoe, A. W., "Security and Usability: Analysis and Evaluation," *Availability, Reliability, and Security, 2010. ARES '10 International Conference on* , vol., no., pp.275,282, 15-18 Feb. 2010
doi: 10.1109/ARES.2010.77

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5438081&isnumber=5437988

[5] Alfayyadh, B.; Ponting, J.; Alzomai, M.; Jøsang, A., "Vulnerabilities in personal firewalls caused by poor security usability," *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on* , vol., no., pp.682,688, 17-19 Dec. 2010
doi: 10.1109/ICITIS.2010.5689490

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5689490&isnumber=5688739

[6] D. Shin and R. Lopes, \An empirical study of visual security cues to prevent the SSLstripping attack," in Proceedings of the 27th Annual Computer Security Applications Conference, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 287{296. [Online]. Available: http://doi.acm.org.ezproxy.auckland.ac.nz/10.1145/2076732.2076773