Design Principles and Guidelines for Targeted Security Awareness

Najem Mahmoud[1, 2], Steven Furnell[1, 3] and Paul Haskell-Dowland[3]
[1]Centre for Security, Communications and Network Research, University of Plymouth, 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

Key aspects that weaken users' ability to use security are often related to the difficulty of comprehending the features/notifications within the interfaces of applications, inconsistency in the interfaces, and not receiving appropriate guidance or adequate security information. This often leads to confusion, limiting a users' ability to comprehend the risk, thus leaving them to make uninformed decisions that may lead to compromise of their IT system or abandoning attempts to address security altogether. This research has consequently focused upon supporting the user by ensuring that security guidance and feedback is available during the task in hand, providing effective information to help them make the right decision at the right time. This has led to introducing a targeted security awareness raising approach. A series of proposed design principles for security features are considered to enhance the users' experience and can be implemented to maximize the users' awareness of the security threats. In addition, they can be used to provide the necessary security information and security recommendations without directing the user to make a specific choice. To study the effectiveness of the proposed design principles and guidelines, existing applications have been examined in order to evaluate their consistency with these recommendations and have identified scope for improvement, which would in turn assist user awareness via a more targeted approach. This is illustrated through an example where the design principles and guidelines are applied to the appearance of email notifications that aim to assist users in spotting phishing threats. The results of the experimental work conducted during this research suggest that user 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. In addition, the findings demonstrate that the abstraction of design principles and guidelines allows the lessons to be transferred to other contexts. Furthermore, following and applying the guidelines enables subtle but relevant refinements to the user interface. Considering the application of this security lesson more broadly, guidance and feedback/nudges should be provided by default.

Keywords

Information Security Awareness, Targeted Security Awareness, Design Principles and Guidelines.

Introduction

The need for developing security features and tools available in computer systems and applications, which are used to make users aware of security risks while the task in hand, has increased significantly over the years to accompany the increased range of cyber security attacks.

While many computer systems and applications provide and use a wide range of security features that users can use or rely on to protect themselves against these security threats, the current design of some of these security features is often blamed for shortcomings in making users fully aware of the security risks that they may face. This reduces the level of protection that can be achieved by using the current design of the security features and tools particularly for novice and other non-technical computer users.

The findings of the prior experimental work conducted by Mahmoud et al. (2017), have revealed that user's security behaviours can be positively influenced through the provision of additional information, enabling them to make better-informed security choices even if the system does not provide any further means of enforcement. Furthermore, results suggests that users will appreciate if adequate security guidance is provided before making a security decision to help them to understand the security risks, so that they can make appropriate and informed security decisions that help to mitigate the security threats and protect their data and devices. Results also revealed that tools such as security level indicators (Security meters) with a combination of background colour codes, which demonstrate the security status and, supported by accompanying text to explain the security risks and proposed recommendations, have played a vital role by aiding users towards that end. Findings were used to identify design principles to assist targeted awareness raising. Seven valuable key security design principles were identified and proposed, each with underlying guidelines for system designers/developers to improve security features in their software to help to make users appropriately aware of the security threats they may encounter.

It can be argued that the existence of design principles and guidelines is imperative for the development of UI elements in a wide range of applications, for several reasons, including improving the usability of the IT systems, and user productivity through a user-friendly system. This should improve efficiency and reduce user errors. It can be achieved by producing consistent and less confusing UI elements of the applications. User confusion may occur because of the inconsistencies of UI elements of the same type of applications which will reduce the efficiency of these applications. Thus, the need to develop design principles and guidelines may continue as new issues arise, which need to be addressed by adhering to new design principles, to avoid confusion and provide applications of the same type in a consistent design.

The dominant objective of HCI is to facilitate the interaction between the user and the computer. Human-computer interaction field emerged as a part of intertwined roots in computer graphics, operating systems, human factors, ergonomics, industrial engineering, cognitive psychology, and the part of computer science systems. Human-computer interaction defined by Hewett et al., (1992) as "*a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them*".

The long-established HCI concepts can be used to design an interface or improve an existing one, taking into account aspects such as usability, which is used to determine the ease of use of a particular technology, the level of technology effectiveness according to the user's needs and user satisfaction with the results obtained using a particular technology to perform specific tasks (Muñoz-Arteaga et al., 2009).

With the development of computer software, the imperative need and the importance of creating design principles and guidelines for the development of applications have emerged. More specifically, for the development of UI elements for various types of applications so that they are easy to use, leading to reliability in these systems. It was noted that there should be specific design principles and guidelines that applications developers can rely on when developing their applications, which will reduce confusion for users, and ultimately increase their efficiency.

With the development of software applications and the emergence of new requirements aimed at increasing the security of information systems, there is a need for specific design principles that contribute to increasing the efficiency of these systems while providing protection to IT systems through adhering to new design principles and guidelines.

On the basis of the identified security design principles guidelines, one of the currently used applications have been evaluated in order to decide their consistency with these design principles, and have been identified to have important scope for improvements in order to improve user awareness by using the targeted security awareness-raising approach.

This paper provides an example of adhering to these principles with a view to improving the current design of this application. It also introduces the design principles and guidelines for targeted security awareness in order to make the users aware of the security threats in some scenarios and explore the opportunities in which there is some visibility in terms of the need to improve the currently used interfaces for some applications to help the users comprehend the security threats in a better way and a more effective manner.

The Need of Design Principles and Guidelines for Targeted Security Awareness

Usability is arguably one of the most important focusses in the field of cybersecurity, supported by the need for confidentiality, integrity, availability; these features have become common components of IT systems that require use by novices and experts alike. As security features are exposed to wider categories of the users, it is essential to ensure that these functions are highly usable. This is mainly because poor usability in this situation often translates into an inadequate application of cybersecurity tools and functionality and, as a result, ultimately limiting their effectiveness (Nurse et al., 2011).

In order to achieve this objective of highly usable security, there have been extensive studies in the cybersecurity literature focused on identifying security usability problems (Amran et al., 2017; Alsharnouby et al., 2015; Furnell, 2016; Furnell, 2007; Furnell et al., 2006). This has led to proposing guidelines and recommendations to address the usability issues (Chiasson et al., 2007; Jøsang et al., 2007).

Over time, requirements have changed, and new ones emerged with a more focused set of design principles and guidelines that have become necessary to address more specific issues and achieve specific objectives. For example, creating design principles and guidelines for designing UI elements which address issues related to the security of the IT systems.

Security HCI (HCI-S) was introduced to reflect the need to explicitly support security in the development of UI elements in the IT systems field. The HCI-S concept built mainly upon modifying and adapting traditional HCI concepts to focus on security aspects in order to improve the security of IT systems by improving the elements of their user interfaces (Muñoz-Arteaga et al., 2009). The term HCI-S was first introduced and defined by Johnston et al. (2003) as “The part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security” (Johnston et al., 2003).

Users interact with computers and technology through various user interfaces. These interfaces are designed to help users understand IT systems and increase productivity in using them. For example, a well-designed user interface assists the user to become skilled in operating the software in a short period of time. This helps to increase the user’s efficiency in completing a particular task, thus the user feels in control and satisfied with the technology. Conversely, if the interface is poorly designed, it can frustrate the user and hinder on completing the task successfully, which will result in decline and uncertainty about the use of specific technology in the future. The interface notifies the user of the available security functions and how to use them. A user may not be aware of the security feature or may be using it incorrectly. The interface should ensure that the user is appropriately guided in order to minimise the potential for the user to be the ‘weakest’ link (Johnston et al., 2003).

As such, Johnston et al. (2003) principles have come to balance the usability of systems while increasing their protection by adhering to new design principles to increase system protection without compromising usability at the same time. Although these principles exist for user interfaces are purposely oriented on the security environment, there is still a need to introduce new principles or develop existing ones to adapt to the new requirements such as increasing the users’ security awareness through the security features that are included in the user interfaces of the existing applications.

Although Johnston's security-related design principles have been widely cited in the literature, there is currently a need to introduce new principles to adapt to new requirements. For instance, in the case when users are exploring Wi-Fi networks and wanted to know the security concerns of the available Wi-Fi networks and what to use it for. In addition, in the case of spotting phishing emails using email applications. In these examples, there is a lack of design of the interfaces of these applications, which does not provide adequate security information to users about the type of security threat faced by the user during their daily use or interactions with these applications, as well as not providing recommendations to users to help them stay safe.

One example is connecting to insecure Wi-Fi networks. Kaspersky reported that 71% of the surveyed users use insecure public Wi-Fi (Kaspersky Lab, 2016). The interfaces currently used to select Wi-Fi networks do not provide sufficient security information to make users aware of the security risks associated with the use of unknown and potentially insecure Wi-Fi networks. As a result, it is not surprising the percentage of users who connect to insecure Wi-Fi networks is at these high levels.

Another example is the number of victims of phishing email attacks. 76% of the surveyed infosec professionals reported that their organisation experienced a steady or higher volume of phishing attacks in 2017 compared to 2016 statistics (Wombat Security Technologies, 2018), despite the availability of security awareness programs, which aim to increase the security awareness of users of this type of attacks and despite the availability of protection software. By examining the interfaces currently used in some email applications, it can be seen that these applications are inadequate to make the user aware of this type of security risks and there is a lack of information provided to increase security awareness of the users before taking any actions that may lead to compromise their systems.

In the two examples described above, there is a design flaw of the user interfaces of these applications in terms of properly making users aware of the potential risks, as with their current design, they do not provide adequate information or suitable recommendations to users to take appropriate actions or make proper and informed decisions. Ensuring that users are aware of the potential threats they may face, whether through phishing email or using an insecure Wi-Fi network, is the difference between the occurrence of a security breach and completely avoiding the risk. To mitigate these risks, there should an adoption of new methods to increase users' awareness of such risks.

Nonetheless, despite the existence of security awareness programs, many companies are unprepared to deal with cyber-attacks. 48% of the 9,500 executives in 122 countries surveyed by the 2018 Global State of Information Security Survey (GSISS) stated that they do not have an employee security awareness training program (PwC, 2018). Often, staff compromise security unintentionally. The Cyber security breaches survey 2017 reveals that 72% of reported security breaches occurred after they received a fraudulent email. Only 20% of the staff surveyed attended any form of cyber security training (IT Governance, 2018). Users are also prone to forgetfulness and therefore over time, users may forget their training. It is therefore imperative to ensure that user interfaces in applications provide the necessary security information to increase awareness of users.

Perhaps a part of the problem can also be blamed on the shortcomings of the current interface design of some applications. Whitten and Tygar (1999) stated that user errors contribute to most computer security failures, nonetheless user interfaces for security still tend to be inconvenient and confusing. They posed a question whether this is simply due to failure to apply some standard UI design techniques to security and whether the general user interface design principles are adequate for security. They argued that effective security requires, in contrast, a different usability standard and that the effective security will not be achieved through the user interface design techniques appropriate to other types of consumer software. Furthermore, they stated that user security interface designers should not assume that users will be motivated to read the manuals or to search for security controls that are designed to be not easily observed or noticed. Moreover, if security is very difficult, irritating or disturbing, users may completely abandon it. From the results obtained from their work, they conclude that the standard model of user interface design, particularly the once represented by PGP 5.0 (their area of study) is not sufficient to make computer security usable for people who are not already knowledgeable in that area.

From their work which was focused on evaluating PGP 5.0's usability, the standard principles of user interface design, is not sufficient to make computer security usable for users who have a lack of understanding and limited skills in that area. Their conclusion was precisely stating that user interface design for effective security remains a problem that needs to be further investigated, and argued that this problem remains open and unresolved (Whitten and Tygar, 1999).

It is clear that there is a need for specific design principles that aim to increase the security awareness of users in their daily usage of IT systems and ensure that sufficient information is available to users when needed and providing them with the necessary advice and recommendations.

Related Work

There is an absence of published research on the need for design principles that directly focus on the problem of the design of user interfaces that serve the objective of "making users aware" of the security threats through improving the user interfaces of the applications. Since users are primarily dealing with IT systems through user interfaces and the vast majority of the users of IT systems often find it difficult to deal with existing security risks because of having inadequate skills, it is imperative to investigate other existing design principles and compare them with the proposed design principles, to ensure that no essential design principles are ignored.

A General-purpose Usability Heuristics

Nielsen (1994) developed 10 Usability Heuristics for user interface design by comparing several published sets of usability heuristics with a database of existing usability problems derived from a variety of projects. Based on the analysis of the explanations, as well as the analysis of the heuristics providing a broader explanatory coverage of the problems, Nielsen introduced a new set of ten heuristics. This was to increase usability and address the problem of user interface inconsistencies. Nielsen (1994) also concluded that these heuristics seem to explain the usability problems previously found. This approach continues to be used for finding new problems, which is the main objective of heuristic evaluation (Nielsen, 1994). Nielsen's Usability Heuristics are presented Table 1 (Nielsen, 1995).

Table 1: Nielsen 10 Usability Heuristics

No	Criteria of HCI	Description
1	Visibility of system status	The system should always keep users informed about what is going on through appropriate feedback within reasonable time.
2	Match between system and the real world	The system should speak the users' language with words, phrases and concepts familiar to the user, rather than system-oriented terms. Moreover, it should follow real-world conventions, making information appear in a natural and logical order.
3	User control and freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo functions.
4	Consistency and standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. It should follow platform conventions.
5	Error prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. The system should either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
6	Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
7	Flexibility and efficiency of use	Accelerators — unseen by the novice user — may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. It allows users to tailor frequent actions.
8	Aesthetic and minimalist design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
9	Help users recognize, diagnose, and recover from errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
10	Help and documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, such as a list of concrete steps to be carried out, and not be too large.

A Security-specific User Interface Design Principles

The HCI-S design principles were introduced by Johnston et al. (2003) and are intended to address how the security features of the GUI can be made as user-friendly and easy to understand and operate as possible. This results in making the system easier to use, further improves the user experience, and makes less likely that the user will make mistakes or attempt to bypass the security feature, resulting in a more reliable system. The objective of HCI-S is to improve the interface in order to enhance the security. This makes the system more secure, robust and reliable. HCI is focused on making the IT system as easy to use as possible. However, security features are occasionally seen to make the system harder to use. HCI-S addresses the issue and balances between security and usability. However, the HCI-S concept introduced by Johnston et al. (2003) did not specifically state that it was intended to make users fully aware of the security threats nor particularly addressing the issue of the end users lack of security awareness. Table 2 presents the design principles of HCI-S introduced by Johnston et al. (2003).

Table 2: Johnston et al. (2003) HCI-S criteria

No	Criteria of HCI-S	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?

The Proposed Security Design Principles

Although the usability problem was a major design goal of the previously introduced design principles, these principles do not attempt to address the issue of making users aware of the security risks they may encounter.

In this paper, a series of related design principles and guidelines have been identified from prior work and utilized in the surveyed interface design to devise these security features by providing an adequate security information and recommended usage, to support users to recognise the security risk and understand the required actions that they need to take in order to avoid security risks. These key security design principles and guidelines could also be used to inform the design and implementation of security-related tools and interfaces to support and make users appropriately aware of the security risks they may encounter during their daily use of IT systems. The new proposed security design principles and guidelines are described in the following section.

Principle 1: Severity of the Security Risk

Aim: To signify the severity of the security risk, with the aid of tools and techniques used by software and operating systems, on a given scenario.

Guideline 1.1: Consider the use of a meter to highlight the severity and/or risk of the action they are about to undertake.

Guideline 1.2: The use of a status mechanism should aid in enhancing the users' selections/actions in a clear and easy way without interfering with the usage of the device.

Principle 2: Security Visuals

Aim: Users should receive a clear indication of the current security status, including specific notifications and warnings for events of interest or concern.

Guideline 2.1: Consider the use of background colour codes to attract attention and signify severity. The use of background colour codes is a key factor in demonstrating and clarifying the security status of any application that users are dealing with.

Guideline 2.2: Use visual indicators to convey information about the type of incident (pictorial representation, supplemented with brief words or hover-over text). These tools and techniques are also well-known to users and have been in use for a long time by software developers in a wide variety of applications to demonstrate the different status of IT systems.

Principle 3: Simplified Security Explanation

Aim: To transmit the message to the users in a manner that would be clear and simple to understand regardless of their vocational inclination.

Guideline 3.1: The language used should be suitable for first-time as well as advanced users. This will help users to comprehend and correlate the presented security visuals with the security explanation of the security threats they are facing.

Guideline 3.2: There should be a balance between providing enough information without overwhelming the user.

Principle 4: Proposed Recommendation

Aim: Users should have an action recommended in order to avoid/minimize a highlighted risk.

Guideline 4.1: There should be a supporting message with the appropriate recommendation for actions to be taken by the user to minimize/avoid the risk.

Guideline 4.2: The recommended actions should help to mitigate security implications and nudge users towards a better security behaviour and making better informed security decisions.

Guideline: 4.3: The proposed security recommendations should be intelligible and precise, without complexity, to allow users to take appropriate actions.

Principle 5: Minimal Intrusion

Aim: Interventions and/or alerts should not attempt to inhibit the user from completing their intended tasks.

Guideline 5.1: Users should not feel overwhelmed by the warning messages and their usage of a device should not be diminished due to the security measures implemented.

Guideline 5.2: The number of clicks should be as minimal as possible from the point when the security threat facing the user is presented (or identified) to the point where the user is provided with adequate security information and recommended usage about the security risk.

Guideline 5.3: The warning message should not interfere or affect the other components of the interface, i.e., it should not block, modify, overlap or make the interface harder to interact by the user.

Principle 6: Aiding the Decision Latency

Aim: To minimise the time the users spends assessing the information and making their decision without looking for further information.

Guideline 6.1: The process of making the user aware of the risk should be as simple and streamlined as possible. For example, the message should not contain more than 25 words length.

Guideline 6.2: The time required for users to spend assessing the information and making the decision, without the need to search for further information in order to understand the security risk encountered, should be as minimal as possible.

Principle 7: Level of Detail and Clarity

Aim: To provide a suitable level of detail and clarity to the user in order to ensure they are fully aware of the security issue encountered and able to make better-informed decisions.

Guideline 7.1: The user should be presented with enough information (ideally directly, but alternatively via a link) to know what is happening and (where appropriate) make an informed decision.

Guideline 7.2: The level of detail and clarity should assist the users without confounding them with unnecessary or superfluous details.

Comparison of the Principles to the Existing Usability Interface Design Principles

To discuss the design principles it is imperative to refer to the most important and well-established design principles in this field, namely Nielsen's usability heuristics (1994) and Johnston et al (2003). These two design principles are the fundamental principles proposed in the usability of IT systems literature to address both usability and consistency issues in the design of user interfaces in general, bearing in mind that the Johnston et al (2003) design principles are specifically for the security environment. Moreover, they are the essential design principles of the user interfaces referred to and appeared to be most commonly cited in the literature.

While the Nielsen's usability heuristics focus mainly on the usability problem, the identified principles and guidelines are to enable security awareness of end users and focusing on utilizing the existing tools and features to educate users, make them aware of the security threats they may face and subsequently help them in making informed decisions. Arguably, Nielsen's usability heuristics are reconciled to some degree with the identified principles in the way that both are focusing on the interface design or the UI elements but the ultimate objective for each one is different.

In comparison, while Johnston et al (2003) design principles address the design of UI elements to focus on the security environment in general as well, the identified principles address a specific issue which is to take into account the increased user security awareness and recommends specific principles that make the user aware of security threats through the development of user interfaces. This is to ensure that this should be taken into account by software developers during the development phase of user interfaces of the applications.

The identified principles also differ but some are intertwined to some degree when compared with those established by Johnston et al (2003). Although these are primarily established to assist in the development and design of interfaces used in a security environment, the identified principles are more security-focused. They also were established and derived from the prior experimental work for the security environment but more specifically are focused on making the users aware of the security threat they encounter. In addition, they have been broken down into guidelines to provide broader and more specific guidance on what and how to improve UI elements in order to increased users' security awareness.

Although both of the mentioned design principles address either the usability problem in general or the usability of the security systems, neither explicitly referred to the problem of security awareness of users. In contrast, the new principles provided broader details of how existing tools are invested and exploited so that they contribute effectively and increase security awareness of end users. Moreover, Johnston et al (2003) principles did not specifically address the lack of provision of adequate information about the security threats, nor the lack of providing recommendations that help users make better decisions which may lead to mitigating the security threats.

To avoid the reoccurrence of guidelines or mixing different concepts which may lead to confusion, it is useful to make a comparison between the mentioned principles. The comparison with the earlier principles and guidelines is requisite in order to inspect the identified principles and to ensure that no important aspect related to UI elements is ignored or neglected. Furthermore, it should be noted that only comparable and intertwined principles have been inspected bearing in mind that the ultimate motivation or objective may differ. Table 3 provides a comparison between the design principles identified from the previous experimental work, Nielsen's usability heuristics and Johnston et al (2003) principles.

Table 3: A comparison between the identified design principles, Nielsen's usability heuristics (1995) and Johnston et al (2003) principles

Source / Comparison criteria	The Identified principles	Johnston et al (2003) HCI-S principles	Nielsen's usability heuristics (1995)
Principle	**Security visuals**	**Visibility of system status**	**Visibility of system status**
Description	Aims to provide users with a clear indication of the current security status, including specific notifications and warnings for events of interest or concern.	It is important for the user to be able to observe the security status of the internal operations.	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Key differences	Although the descriptions are similar, the proposed identified principles are providing detailed description and mentioning to include specific notifications and warnings for event of either "interest" or "concern". They have also been broken down into guidelines for developers and focus more on how to best deliver products which raise the awareness of the user on a security perspective. For example, the colour coding to attract attention and alert the users of the extent of the risk they are facing.		
Principles	**Simplified security explanation**	**Aesthetic and minimalist design**	**Match between system and the real world**
Description	Aims to transmit the message to the users in a manner that would be clear and simple to understand regardless of their vocational inclination.	Only relevant security information should be displayed.	The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
Key differences	While the descriptions are also interrelated here, the proposed identified principle is explicitly stating the "target users" by focusing on all users' categories regardless of their skills or level of knowledge of the IT systems in terms of the language used. Moreover, it mentions to the "content" and states clearly that there should be a balance between providing enough information without overwhelming the user. They have also been broken down into two guidelines Guideline 3.1 and Guideline 3.2 to better deliver security features within their software products that help to raise the awareness of the user.		
Principles	**Level of detail and clarity & Proposed recommendation**	**Errors**	**Help users recognize, diagnose, and recover from errors**

Description	The first principle aims to provide a suitable level of detail and clarity to the user in order to ensure they are fully aware of the security issue encountered, and able to make better-informed decisions, while the second principle recommends an action in order to avoid/minimize the risk implicated to the security issue.	It is important for the error message to be detailed and to state, if necessary, where to obtain help.	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
Key differences	While the identified principles are clearly suggesting to provide a "suitable" level of detail and clarity to the user to make the users aware of the security issue encountered to make better-informed decisions, and the second principle suggesting to "recommends" an action in order to avoid/minimize the risk implicated to the security issue, Johnston et al (2003) is talking about error messages which is something different because error messages are not the same as the warning message and Johnston et al (2003) further suggested that the message to be "detailed" and did not state to which level of details it should be as providing too much details to the users may not be understandable by all users categories. Whereas Nielsen description is suggesting to provide a constructive solution and this different when compared to recommendations. Nielsen and Johnston et al (2003) principles are not explicitly intended to increase the users' security awareness.		
Principle	**Minimal intrusion**	**Learnability**	**Flexibility and efficiency of use**
Description	Intervention and/or alert should attempt not to inhibit the user from completing their everyday tasks.	The interface needs to be as non-threatening and easy to learn as possible.	Accelerators -- unseen by the novice user - may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
Key features and differences	While both Nielsen and Johnston et al (2003) description is stating that it needs to be as user-friendly, as easy-to-learn as possible and interactive, the identified principles are also suggesting this, plus the fact that it must not interfere with the completion of the user's tasks. They have also clearly state that the number of clicks should be as minimal as possible from the point when the security threat facing the user is presented or identified to the point where the user is provided with adequate security information and recommended usage about the security risk. Furthermore, they have also been suggesting that the warning message should not interfere or affect the other components of the interface, i.e., it should not block, modify, overlap or make the interface harder to interact by the user.		

Application of the Design Principles and Guidelines

On the basis of the security design principles discussed and recommended previously, one of the current scenarios has been evaluated in order to determine its consistency with these identified design principles and to have scope for improvement, by using the targeted security awareness-raising approach. In order to support this view, revised versions of the user interfaces are designed for this scenario, which exhibited the shortcomings in this regard and the room for improvement to make the users fully aware of the security risk that they are encountering. The next sections of the paper discuss the new security design adherence to these new principles and provides an example of adhering to these principles with a view to improving the current design of this application. Moreover, it will discuss in detail this scenario and suggest the potential solutions that may help mitigate the security risks by providing adequate security information and guidance.

The Need for Raised Awareness of Spotting Phishing Emails

There is no surprise that the main tools currently used as the first line of defence in combating phishing emails, are the filtering algorithms and tools that are used by email applications. However, there are some flaws that require improvement in this first line of defence. Some legitimate emails are often classified as spam or phishing emails and some spam or phishing emails may be classified as legitimate emails. It should be mentioned that it is out of the scope of this paper to examine the performance or the reliability of the algorithms used in the email filters, but rather it focuses on how to make users fully aware of the phishing email in the case that the email reaches the users' mailbox.

Users receive phishing emails almost every day. However, there is a lack of support to raise the security awareness for the users in the case that the phishing email has reached their mailbox. The current information provided to users regarding these phishing emails are often inadequate and sometimes misleading which makes it harder for users to be appropriately aware of the threats. This flaw and shortcomings are hindering the efforts to make users aware of the phishing emails threats and therefore users in such situations may not able to take the appropriate security precautions that help to protect them from the associated threats.

Users of the email application are provided with a means to block emails before reaching their mailbox or moving them to a junk email folder, however, they are not appropriately informed, warned and made aware of what the spam or phishing emails actually are.

Email services are among the preferred methods for cybercriminals to target users. To protect users, there are many tools and solutions that have been developed to keep users from being victims of cyber criminals. The majority of these tools and solutions are covering one side of the picture which is the technical side, and have not done enough in terms of increasing security awareness of users by informing them about potential risks associated with blocked phishing emails, and phishing links and attachments before they take actions that unblock the content. Increasing the awareness of users before unblocking any content is a key factor to avoid users becoming victims of this attack, and to avoid any possible security implications.

There is currently no adequate security guidance and feedback available within the email applications that provide support and help to users to make the appropriate security decision to protect themselves from the security risks associated with blocked email messages, which could potentially be scam or phishing emails. The currently available option is only alerting the user in an inadequate manner by informing the users that the email has been blocked. However, what is actually missing in this situation is to provide appropriate security guidance accompanying this risk. Furthermore, at this point, users need an appropriate security guidance to take the required security countermeasures that would mitigate the security risks which would help to protect them from the potential risks.

One of the candidate applications that have been evaluated and identified with flaws and shortcomings in making users appropriately aware when a phishing email reaches their mailbox is Microsoft Outlook.

The next section provides an example of the proposed solution and provides illustrative examples of how the current interface design of the Microsoft Outlook application can be improved by applying the identified design principles and guidelines.

Evaluation methods

The usability of the current Microsoft Outlook interface design was assessed using an informal cognitive walkthrough method. The current interface design has been inspected, and some aspects have been identified that could be improved based on the proposed design principles and guidelines.

As per Whitten and Tygar (1999), in order to conduct a cognitive walkthrough, the evaluators need to go step-by-step through the software as if they were novice users, trying to mentally simulate what the novices' understanding of the software would be at each point, and looking for potential errors and areas of confusion. As an assessment tool, cognitive walkthrough focuses primarily on the user's ability to learn, and as such, is an appropriate tool for assessing the usability of security.

While the provided analysis in this paper is primarily described as a cognitive walkthrough, it also combines aspects of another technique, primarily heuristic evaluation. In this technique, the user interface is assessed against a specific list of usability principles. The Heuristic assessment is ideally performed by people who are experts and are very familiar with both the application area and the techniques and requirements of use such as background of people expected to use the program (Whitten and Tygar, 1999).

Improved Interface Design of Spotting Phishing Emails Using the Identified Design Principles

The identified design principles and guidelines proposed for targeted security awareness have been introduced and discussed in detail in the previous sections. The reason for proposing these design principles and guidelines is to assist in the development and the design of interfaces that are associated with the security environment, and particularly treating and overcoming the flaws of the user interface design, by ensuring that the users are provided with the necessary information that makes them aware of the risks they may encounter. These design principles are identified from the prior experimental work. They have been established and introduced to address the essentials in a security environment and in particular to serve the objective of increasing users' security awareness through improving the security features that are included in some applications that users deal with on a daily basis. These principles are perceived as a security domain-specific user interface design that focused on specific design issue in the security environment which should make them easier to comply with and be implemented.

In the next section, some of the design principles are discussed in more detail by illustrating the current interface design of the surveyed application and the improved interface design of Microsoft Outlook using the identified design principles, which should assist the user on how to spot phishing emails and provide a clear indications and enhanced security visuals of the security risks associated the suspected blocked email.

An example of Applying Principles 1 and 2: Severity of the Security Risk and the Security Visuals

The interface should always keep users informed about the current state of the security risk through the use of appropriate visual indications before taking any actions. Currently, in order to identify and inspect the sender's email, users need to click on the email and determine whether the email is from a legitimate address. Figure 1 shows the only way that users can inspect and identify the sender's email using the current version of Outlook. Although it has been detected as a phishing email, it does not provide any security information or guidance for the user before or while making a decision to unblock the email content.

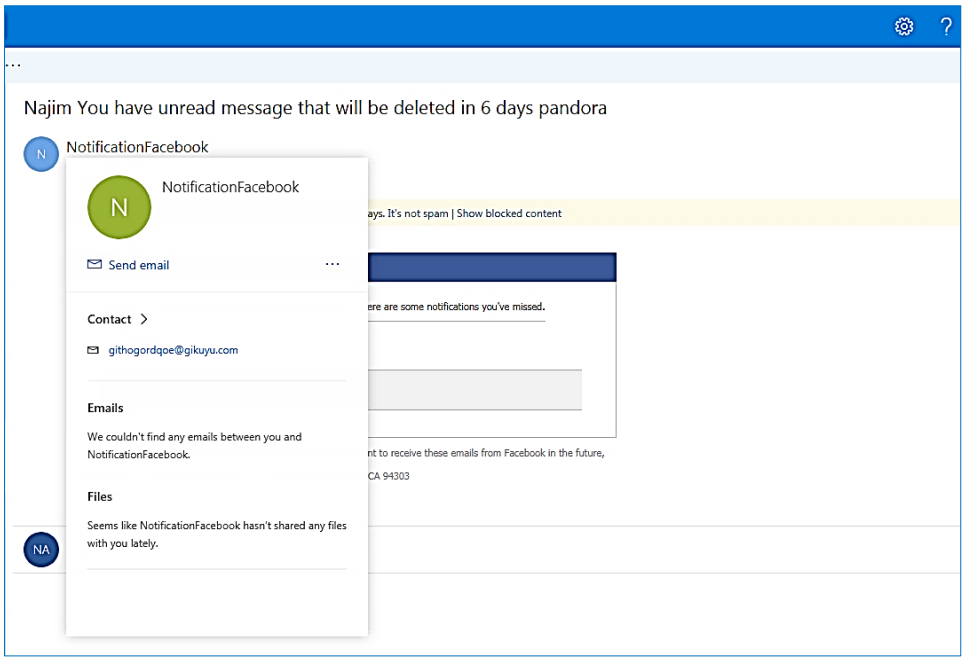

Figure 1: Inspecting the sender's email using Microsoft Outlook taken in 2017

In such situation, it is unlikely that novice users or users with average computer skills would have the experience to take these security precautions. It would be challenging for them to identify and inspect the sender's email, given the lack of awareness.

The screenshots presented in Figures 2 and 3 are illustrating some examples of the current notifications used by Microsoft Outlook to inform the user about the blocked emails.

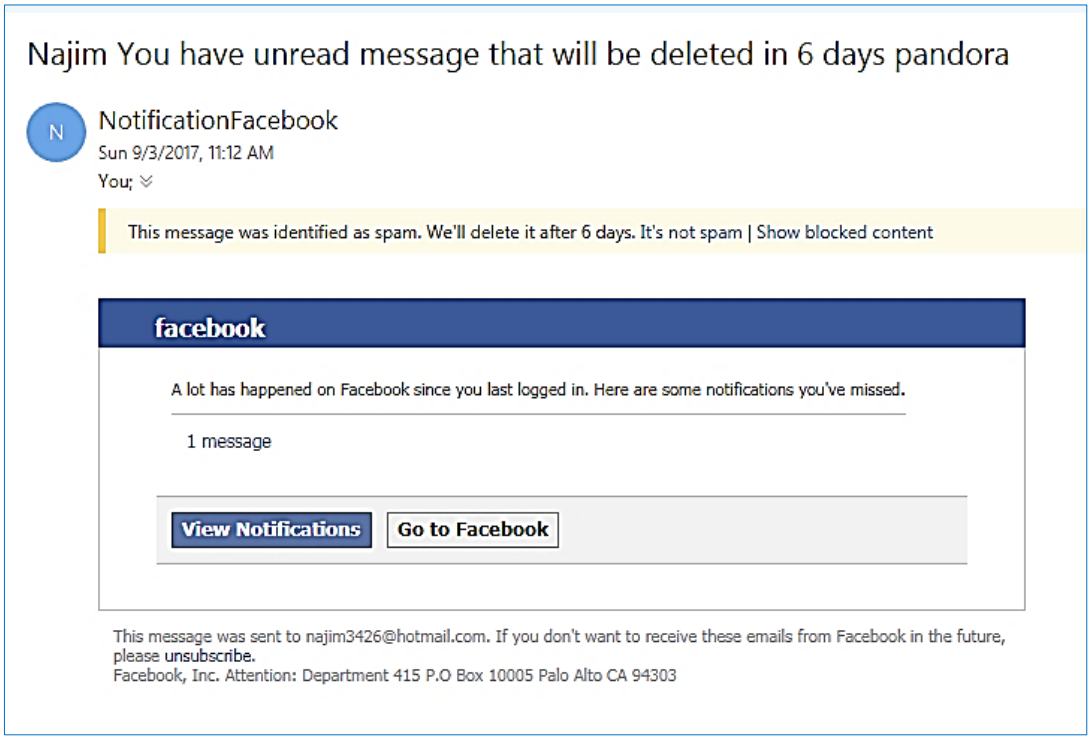

Figure 2: The current Microsoft Outlook warning message for blocked email

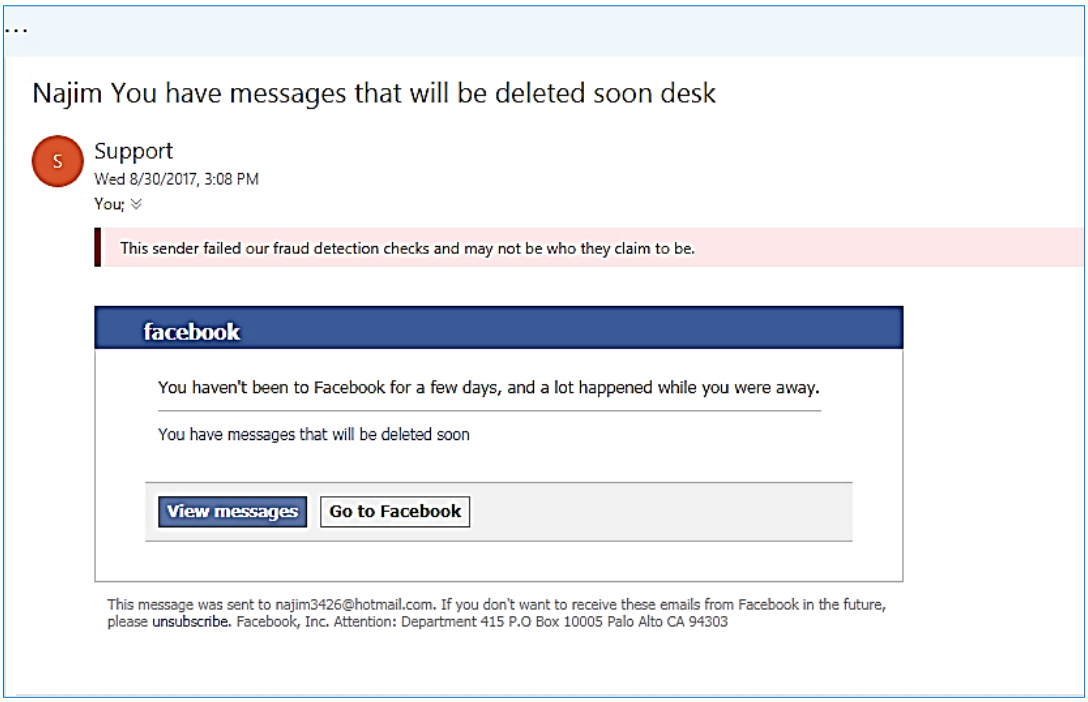

Figure 3: Different warning message for blocked email by Microsoft Outlook

Clearly users should be alerted to the severity of the security risk of the blocked email, to avoid confusion to the user. Users should also receive a clear indication of the current security status, including notifications and warnings. This will allow the user to easily observe the security risk of the blocked email. An example of this is the use of varied banners with background colour codes to attract attention and signify the severity of the security risk and/or inform the user whether the email is from a trusted sender. This should be accompanied with suitable warning signs, for example by using coloured warning triangles which all users are familiar with, which is displayed in the left corner of the banners as shown in Figures 4 and 5, to attract attention and signify severity. This should persuade the user to take the required precautions and appropriate actions. This proposed clear visible security warning message should help users to comprehend the security risk quickly and make them aware of the risks in a consistent manner.

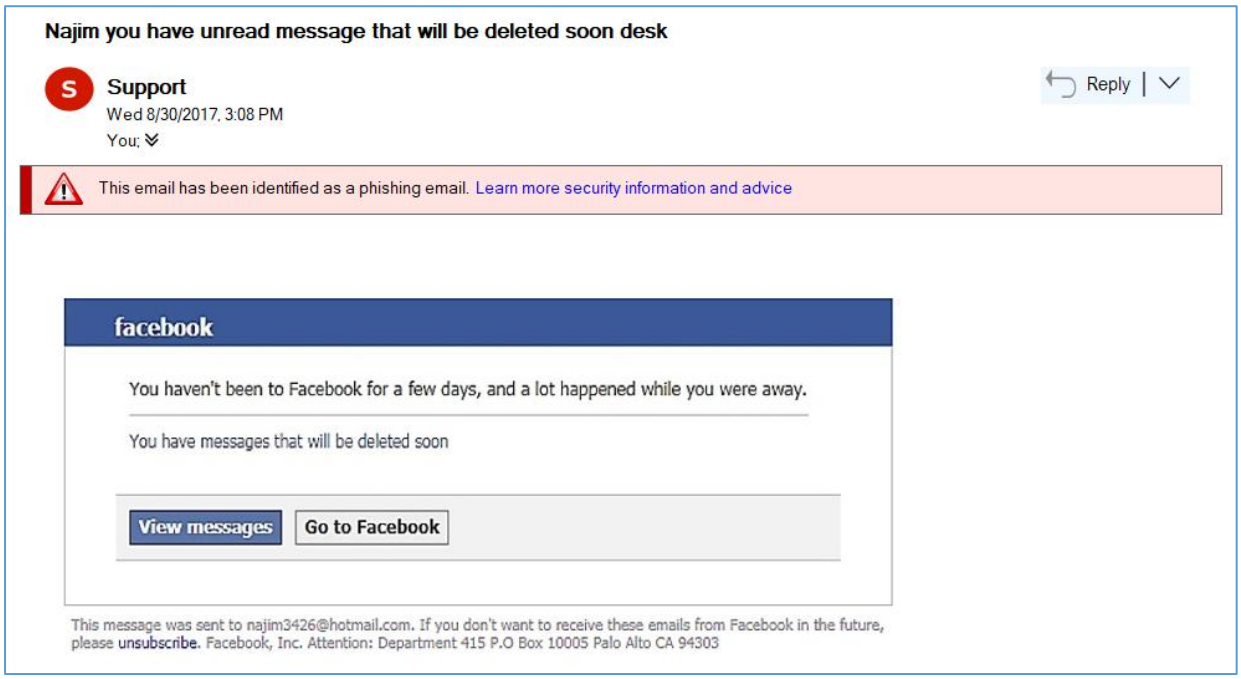

Figure 4: Proposed warning message when a phishing email is identified

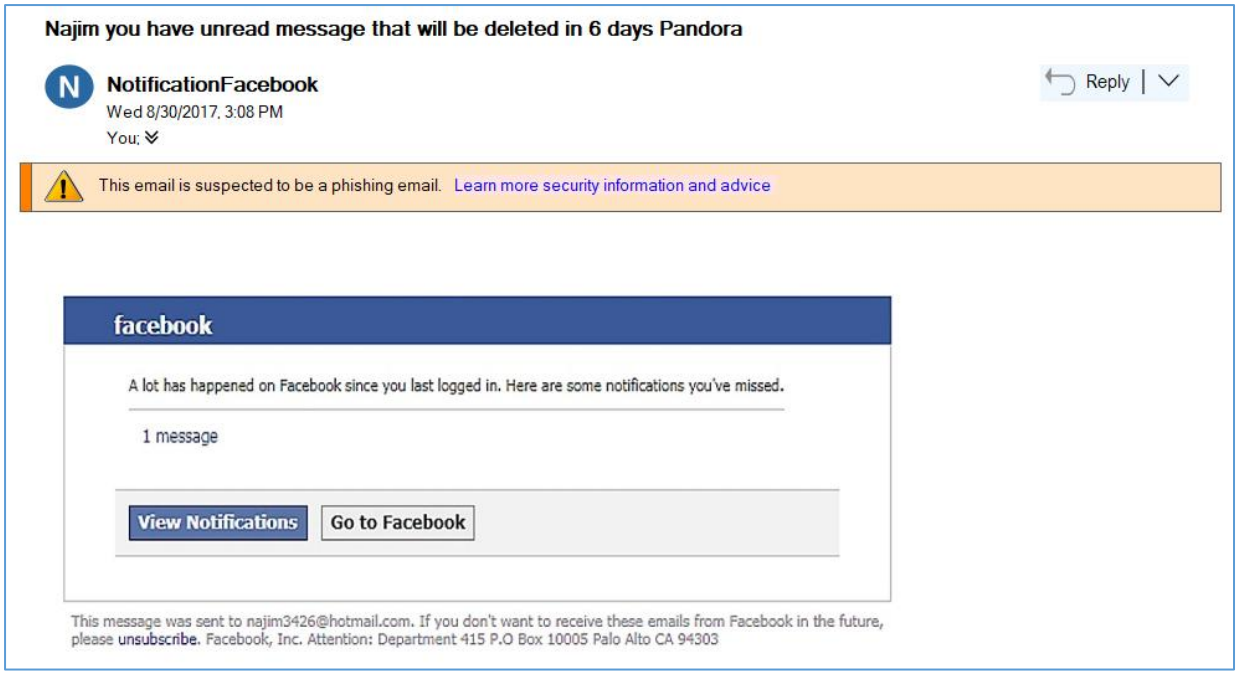

Figure 5: Proposed warning message when a suspected phishing email is detected

Applying Principle 4: Proposed Recommendation

It has been noticed from prior experimental work that there is significant advantage of providing adequate security information and advice to the users to deal with the security risks. This is required to enable the users to take the necessary actions that safeguard their crucial IT systems and data. For example, providing a *Learn more security information and advice* link could be offered to the users in this situation to provide preliminary security guidance and feedback when necessary that can help the user make informed decisions at the right time and when it needed. The security guidance should be brief, specific about the risk and with the necessary information that has the least possible use of technical terminology.

An example of what an adequate security information and security advice in this situation might include when the users click for learn more security information and advice:

Security information:

- *This email has been blocked because our email filters were unable to verify the sender's integrity.*
- *There is a potential that this email might be sent to you by a hacker or scammer to trick you into disclosing personal information and passwords that will result in stealing your sensitive and valuable information.*
- *There is a potential risk that your computer gets malware if you unblock the content of this email.*

Security advice:

- *You are advised to check the sender's or the company's email by checking the sender's address to verify the integrity of the sender by clicking or hovering over the email address of the senders.*
- *Do not block the content if you are unsure about the content or the sender and delete this email immediately.*
- *Never follow links or open attachments in suspicious or unsolicited emails. If in doubt, or if you need further assistance, contact directly the company that claims to have sent it.*
- *Please check that your anti-virus is up to date to avoid acquiring malware as a result of unblocking the content of this email.*

This security information and advice has the potential to help and support users by making them aware of the threat, thus contributing to mitigate the security risks that the users may encounter if a suspicious email has reached their mailbox. However, as with the current settings of the notification

message used in Microsoft Outlook, offering a link to the user to unblock the content without providing adequate security guidance and adequate information, may result in the user becoming a victim of a scam. In the case that users are still in doubt, a wider information could be offered to them to learn more about the blocked email for example by offering a webpage that provides further security information and details associated with the encountered threat.

In the proposed security message that contains the security information and advice, users are also offered a link to (*Learn more information about how to recognize phishing email messages*) at the bottom of the security message, to acquire more information if they are still not appropriately aware of what is the risk to learn more security information and advice about phishing emails, as shown in Figures 6 and 7. This will be critical if the users are uncertain about the blocked email. Providing this additional feature will give the users the opportunity to learn more information about how to recognize phishing emails. Microsoft has provided a webpage to educate users on how to protect themselves from phishing. However, at present, Microsoft has not provided this opportunity when the task in hand within Outlook when a suspicious phishing email is identified or blocked. The webpage is provided here: https://support.microsoft.com/en-ph/help/4033787/windows-protect-yourself-from-phishing.

The security information and the recommended advice provided in the new proposed design, should help to raise the security awareness for the users before taking actions to unblock suspected phishing emails. This proposed design approach has the potential to provide support to users at the point of need, in order to take the necessary security precautions and make informed decisions.

Figure 6: Proposed appearance of security message for detected phishing emails

Figure 7: Proposed appearance of security message for suspected phishing emails

The above design of the warning pop-windows could be criticised as not an ideal friendly user interface with a high volume of text on the information, and recommendations provided. However, this could be revised and improved by reducing the amount of information and making it as focused and concise as possible.

Conclusions

This paper proposed and discussed new design principles for security features that can be used to improve the security of IT systems by modifying application interfaces to increase the security awareness of users. This objective can be accomplished by educating users about the security threats they are facing and assisting them by providing security recommendations so they can make informed decisions.

Security issues are being increasingly recognised by IT users, as more security-related features are being introduced in a range of applications. However, based on the examples discussed in this paper, it is clear that the current efforts to highlight security issues are still inadequate in terms of raising awareness among users about the security risks they encounter in their daily use of IT systems.

The interface design of a system is crucial, especially when it relates to making security decisions in standard IT applications. The new proposed design principles for security features are considered to enhance the users' experience with the security issue and can be implemented to maximize the users' awareness of the security threats. Furthermore, they can be used to provide the necessary security information and security recommendations without directing the user to make a specific choice. This will result in a system that is fundamentally reliant on making the user aware of the threat which should assist the user to make informed security decisions without any form of enforcement. Additionally, it can also be used by software developers to ensure that the objective of making "users aware" is developed into the security interface or within the security features of the IT system. The new proposed design principles and guidelines can also be used to evaluate the interfaces of new security products. They can also provide direction, from a security point of view, on how an interface can be improved in the way that helps to make users appropriately aware of the security threat encountered.

Furthermore, the proposed design principles are considered to be achievable. To demonstrate this, improvements were made to the warning messages and notifications that are currently used in the interface of the Microsoft Outlook email application, which either do not exist in the current version, or that requires improvement. These improvements are intended to redesign the graphical user interface in a manner that will help make the users aware of the security threat encountered and simultaneously be easier to use. Additional attention was paid in the newly proposed interfaces so that the use of security features would be improved.

Although this research has conveyed an interesting result in terms of opportunities for improvement, it has only achieved an assessment of the appearance level of the surveyed application and how the proposed design principles and guidelines would help to make users aware of the encountered security threat in a more apparent manner.

The new proposed design principles and guidelines have been applied to the interface of the application and compared with the current interface design of the application. The results reflect the need for improvement of the current design, which will raise the awareness of the user to aid them in spotting phishing threats.

References

Amran, A., Zaaba, Z. F., Singh, M. M., & Marashdih, A. W., 2017. Usable security: Revealing end-users comprehensions on security warnings. Procedia Computer Science, 124, 624-631.

Alsharnouby, M., Alaca, F., & Chiasson, S., 2015. Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.

Furnell, S., 2016. The usability of security–revisited. Computer Fraud & Security, (9), 5-11.

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

Furnell, S. M., Jusoh, A., & Katsabas, D., 2006. The challenges of understanding and using security: A survey of end-users. Computers & Security, 25 (1), 27-35.

Chiasson, S., van Oorschot, P. C., & Biddle, R., 2007. Even experts deserve usable security: Design guidelines for security management systems. In SOUPS Workshop on Usable IT Security Management (USM) (pp. 1-4).

Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. & Verplank, W., 1992. ACM SIGCHI curricula for human-computer interaction, (pp.5). ACM.

Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M., & McNamara, J., 2007. Security usability principles for vulnerability analysis and risk assessment. In Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007) (pp. 269-278). IEEE.

IT Governance. 2018. The biggest cyber security threat is inside your organisation. Retrieved from: https://www.itgovernance.co.uk/blog/the-biggest-cyber-security-threat-is-inside-your-organisation/ (Accessed 5 March 2018).

Johnston, J., Eloff, J.H. and Labuschagne, L., 2003. Security and human computer interfaces. Computers & Security, 22(8), pp.675-684.

Kaspersky Lab. 2016. Consumer Security Risks Survey, Connected But Not Protected. Kaspersky Lab. Retrieved from: https://dl.acronis.com/u/pdf/Kaspersky_B2C_survey_2016_report.pdf (Accessed 30 March 2017).

Mahmoud N, Furnell SM, & Haskell-Dowland PS, 2017. Towards Targeted Security Awareness Raising. In Proceedings of the Annual Information Institute Conference, Las Vegas, USA, ISBN: 978-1-935160-18-2.

Muñoz-Arteaga, J., González, R.M., Martin, M.V., Vanderdonckt, J. & Álvarez-Rodríguez, F., 2009. A methodology for designing information security feedback based on User Interface Patterns. Advances in Engineering Software, 40 (12), pp.1231-1241.

Nielsen, J., 1994, April. Enhancing the explanatory power of usability heuristics. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 152-158). ACM.

Nielsen, J., 1995. Ten Usability heuristics. Retrieved from: https://www.nngroup.com/articles/ten-usability-heuristics/ (Accessed 10 December 2017).

Nurse, J.R., Creese, S., Goldsmith, M. & Lamberts, K., 2011. Guidelines for usable cybersecurity: Past and present. In Cyberspace Safety and Security, 2011. Third International Workshop on Cyberspace Safety and Security (CSS), (pp. 21-26). IEEE.

PricewaterhouseCoopers LLP. PwC. 2018. Strengthening digital society against cyber shocks. Key findings from The Global State of Information Security Survey. Retrieved from: https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf (Accessed 5 March 2018).

Whitten, A. & Tygar, J.D., 1999, August. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In USENIX Security Symposium (Vol. 348).

Wombat Security Technologies. 2018. State of the Phish. Retrieved from: https://www.wombatsecurity.com/hubfs/2018%20State%20of%20the%20Phish/Wombat-StateofPhish2018.pdf?submissionGuid=1bfe9271-60af-4391-a854-98a7e47f5bf6. (Accessed 30 January 2018).