# Holistic Information Security Management for Home Environments

F. Alotaibi[1,4], N.L. Clarke[1,2] and S.M. Furnell[1,2,3]

[1]Centre for Security, Communications and Network Research, University of Plymouth, United Kingdom
[2]Security Research Institute, Edith Cowan University, Western Australia
[3] Center for Research in Information and Cyber Security,Nelson Mandela University, Port Elizabeth, South Africa
[4] Shaqra University, Saudi Arabia
e-mail: info@cscan.org

## Abstract

A wide and increasing range of different technologies, devices, platforms, applications and services are being used every day by home users. In parallel, home users are also experiencing a range of different online threats and attacks. Indeed, home users are increasingly being targeted as they lack the knowledge and awareness about the potential threats and how to protect themselves. The increase in technologies and platforms also increases the burden upon a user to understand how to apply security across the differing technologies, operating systems and applications. This results in managing the security across their technology portfolio increasingly more troublesome and time consuming. This paper presents a novel approach to managing security within the home, which focuses upon the dual need to educate but also provide usable and effective mechanisms for them to secure, configure and manage their computing-related technology in a holistic manner. The proposed approach is presented and evaluated in terms of several usability and functionality aspects by 434 participants. The result of the survey shows that participants are supportive of the approach, have responded positively regarding the usability designs and appreciate the reduced burden and increased usability of utilising policies as an approach to providing effective protection.

## Keywords

Security Management, Cyber Security awareness, Security Controls, Security Policy, Online Threats, Usability, Home Users

## 1 Introduction

With the rapid development of information technology including smart phones, computers, tablets, smart watches and Internet of Things, providing security for home digital devices and services become more essential and more challenging as many home users face online threats and attacks (Nthala *et al*, 2018). According to the Office for National Statistics (National Office of Statistics, 2018), 90% of households in Great Britain had internet access in 2018 including 81% of British adults using smartphones to go online, 63% use laptops and 57 % have tablets to browse the internet. Worldwide, there are around 27 billion Internet of Things (IoT) connected devices worldwide in 2019, an increase from 15 billion devices in 2014 and it is

expected to reach 75.44 billion devices by 2025 (Statista, 2019). Due to this increase in internet access and devices, more online threats and malicious attacks are experienced by home users.

NCSA and PayPal (2013) conducted a study to analyse the cyber security behaviors and perceptions of home users in the United of States. The result revealed that more than the half of the participants (55%) did not configure a PIN code to protect their smart phones, 14% used one password or PIN across all the online accounts and 20% never changed their passwords. In addition, less than one-quarter of the respondents (21.6%) installed security software such as antivirus. Another study was conducted by Watson and Zheng (2017) to assess the security awareness for the US mobile users. They found that around 20% of the participants did not configure any screen locking protection such as PIN or fingerprint. In addition, 20% used unofficial sources to download applications, 85% have had a virus and 80% have downloaded malicious applications.

The situation might get worse in the developing countries as evidenced by the study of Rao and Pati (2012) in India. The study shows that more than 80% downloaded software from untrusted websites such as torrent.com. None of the security controls such as password, internet and parental controls have been configured in their devices. In addition, around 80% did not have any knowledge about firewall, phishing, spyware and malware. 64% did not have Anti-virus software in their systems while only 10% had a licenced antivirus software.

The common attacks and threats targeting home users are: operating systems vulnerabilities, malware, viruses, phishing, identity theft and privacy violation (Rao and Pati, 2012). Nthala *et al*, (2018) state that all these threats usually are mitigated well in large organisations because they have security policies, segmented network architectures, firewall, Antivirus, IDS, IPS, patching management, backup solutions and IT support team. In contrast, very few security resources, ability, knowledge, skills and tools are available to protect home users from a wide range of threats and attacks. The lack of appropriate awareness, monitoring and management for the security configurations could make the digital devices at homes more vulnerable and easily compromised. Therefore, they might experience security breaches which could be used to attack critical infrastructures and services such as telecommunication and banking and other organisations (Ng and Rahim, 2005). For example, X-Box Live, the PlayStation Network, Dyn (DNS provider), UK's TalkTalk and Post Office online services have been affected by a DDoS attack which was a botnet coordinated through a large number of Internet of Things (IoT) devices in homes that had been hacked and infected with malware(Lunsford and Boahn, 2015; Reynolds, 2016).

Some researchers have claimed that most of the cyber security awareness and education courses and initiatives are designed and conducted for the organisations and the business environment (Kritzinger and Von Solms, 2010). Magaya and Clarke (2012) argued that online portals such as Get Safe Online (GetSafeOnline.org, 2016), Stay Safe Online (StaySafeOnline.org, 2016) are the available resources which are used by home users to enhance their cyber security awareness and get advice how to be secured while going online. However, these online programs and courses

sometimes are difficult to be used due to the poor structure especially for novice users. In addition, they are not up-to-date and not covering all the relevant security awareness and issues (Kritzinger and Von Solms, 2010).

The above studies and events show that the home users are vulnerable and targeted by many online threats due to applying weak security practice and controls, difficulty in monitoring and managing different digital devices, lack of appropriate security awareness. Many researchers argued that the security protection and practice can be improved by enhancing and promoting the security awareness for home users (Furnell *et al.*, 2007; Nouh *et al.*, 2014). Therefore, an alternative approach needs to be explored and proposed which has the ability to promote and increase security awareness amongst home users by providing a bespoke security awareness in a centralised and usable manner to meet the current needs of the users.

This paper presents the above evidence collected from different countries and different dates which indicate that there is a significant lack of knowledge and understanding of the security concepts and controls among home users. These gaps could make users more vulnerable and experience more attacks which could threaten their systems and networks. Section 2 presents an analysis of the current state of the art. Section 3 presents the details of the proposed information security management system. Section 4 provides the result of the evaluation for the proposed system. Section 5 provides the concluding remarks and future works.

## 2 Related Works

Table 1 shows a variety of studies which have tried to raise the security awareness of home users towards different online threats, including phishing attacks, social engineering attacks, security controls and configurations and general security. Some of these studies have tried to provide home users with cyber security awareness which are tailored to their needs in different aspects. A limited number of studies have tried to assess home users' security knowledge, restrict their online activity and force them to access awareness materials if they do not have sufficient knowledge (Kritzinger and Von Solms, 2010; Labuschagne and Eloff, 2012). Kritzinger and Von Solms (2010) have tried to provide an appropriate awareness content based on the level of security knowledge for the users. They proposed a theoretical E-Awareness Model (E-AM) which can provide awareness topics and materials based on the knowledge level of home users. The user must be tested in order to be assigned to the appropriate level of the three levels: novice, intermediate and advanced. However, they suggested that Internet Services Providers (ISPs) should host and handle the proposed tool in order to enforce home users to access awareness contents. This type of enforcement might interrupt home users and make them frustrated. In addition, some concerns might rise about financial, legal, technical and privacy issues.

However, Labuschagne and Eloff (2012) proposed a security awareness system by using a virtualized system on shared computers instead of being hosted by ISPs. The system assesses users' security knowledge and allows them accessing the internet if their level of security knowledge is satisfactory. Otherwise, they will be directed to awareness material to improve their knowledge. However, the tool might interrupt the

access of users and awareness contents are not provided based on their needs which might be generic and not useful for them.

Another tool was introduced by Magaya and Clarke (2012) to provide a bespoke recommendation and guideline by assessing the online behavior of home users and identifying and prioritizing the missing security controls from high to low. However, home users need to identify their security controls manually by which might be difficult for novice users. In addition, the same awareness content is provided for all home user regardless of their knowledge level in technical and security aspects.

Several studies were focused in enhancing the security awareness of phishing attacks (Jahankhani *et al.*, 2011; Maurer *et al.*, 2011; Sharifi *et al.*, 2011; Volkamer *et al.*, 2015). They proposed approaches and tools are intended to work as a browser extension and provide a bespoke awareness for users about phishing websites and the possible threats while surfing online. While other researchers proposed methods to raise security awareness about different online threats by developing awareness web portals (Tolnai and Von Solms, 2009; Smith *et al.*, 2013). However, these portals do not have the ability to provide a bespoke awareness content which can promote security awareness.

A review of these studies has revealed that most studies have made efforts in proposing "one-fits-all" solutions that do not have the ability to provide the users with a tailored awareness content based on some criteria such as the current needs, prior knowledge, and security priorities for each user. This review indicates that there is a need for an approach that can provide the users with bespoke awareness information which can enhance the security practice among home users as evidenced by some studies (LaRose, Rifon and Enbody, 2008; Davinson and Sillence, 2010). In addition, Ho*we et al* (2012) argued that there is current need to integrate all the security activities and configurations in a comprehensive tool which can improve the security and reduce the heavy load on home users in managing different security tools and settings for different threats. Another recent study was conducted by Nthala *et al.* (2018) revealed that there is a clear need to develop a usable convenient tool can be used by non-experts to manage the security configurations for different devices and services at home which could motivate home users for better security and simplify the task for them. In the same context, Rao and Pati (2012) identified in their study that there is a current need to develop a usable tool for awareness and security controls management based on users' knowledge and behavioural pattern which could improve home users' perception of information security.

Therefore, it is clear that there is a need for a bespoke individualized personalized approach that takes into account knowledge and awareness of the technologies, applications, and services that users use and provides bespoke information directly based upon the current security posture. In order to measure and understand how the home users are doing something (i.e. well or badly), it needs to be defined against something – in an organisation, this would be a security policy. Despite the fact that many approaches and tools have been proposed for the home users to promote cybersecurity, they are providing general, static and limited awareness content. Therefore, there is a need to propose an approach which has the ability to monitor and

manage the security practice for home users by applying some kinds of policies order to deliver customized awareness content and encourage the users to practice better security.

# 3 The Proposed Information Security Management System

Despite the fact that the above analysis of the literature review shows that many approaches and tools have been proposed for the home users to promote cybersecurity, they are providing general, static and limited awareness content. In addition, the above events and studies show that home users suffer from different issues such as lack of security knowledge, lack of understanding the security concepts, the lack of willingness to manage and monitor different security settings across different devices. In addition, there is a lack of providing a tailored security awareness beads on the users' needs. These leaves users open to a variety of attacks that would compromise their information, systems and networks.

Accordingly, it is clear that there is a need for a usable, educational bespoke individualized approach which can configure, manage and monitor information security across devices and technologies and services within the home. In the approach, it is suggested as part of the solution is to use and apply different security policies in order to measure and understand how home users are managing and controlling their security

It is envisaged that a novel architecture will have the core functionality which can allow the proposed system to identify, check and manage the security configuration and practice in devices connected to the home network. In addition, the proposed security management system can enhance security awareness amongst home users by providing them with bespoke awareness when it is needed. Several requirements need to be considered in order to offer an effective security management system:

- **Security policies:** different groups of security policies are required to be defined and assigned for devices and users. The policies should cover different operating systems and technologies including their security configuration, settings and controls which can enhance their protection and security once being configured and managed effectively.
- **Security levels**, the security policies can be configured and defined based on three levels: low, medium and high. This will provide good flexibility in the functionality of the system in order to meet the users' needs. For instance, the low level can contain the minimum requirements which need to be configured in the devices and it can be assigned for novice users who do not have good technology experience.
- **Usable interfaces:** the components of the system interfaces should be easy to access, use and understand in order to help the system to achieve its main objectives and goals. The interfaces need to be designed based on HCI and usability principles in order to meet the users' requirements and satisfaction.
- **Automatic recognition sensor:** the system should have automatic recognition feature which can allow it to scan, identify and recognise the new digital devices

which have not been enrolled in the system yet in order to be added. The system should have the ability to assign the appropriate security policy for the recognised device.

- **Automatic security check:** the proposed system should review continuously the configured security settings and controls on the managed devices in order to be compared with the assigned security policies in order to check the security compliance of the devices.
- **A tailored security awareness content:** the proposed system should be able to deliver a tailored awareness security message and content which is customised based on the users' knowledge and their current needs. This will help to deal effectively with different types of users who have different levels of knowledge and requirements.

### 3.1 Information Security Policy for Home Users

In the approach, it is suggested as part of the solution is to use and apply different security policies in order to measure and understand how home users are managing and controlling their security. Some of the processes and the controls in ISO 27002 which are mainly designed for organisations and they might be applicable to be implemented for the home users will be used to create and design information security policy for home users which will be utilised in the proposed tool. In addition, the official user guide documents for the devices with different operating systems have been reviewed in order to identify the most common security settings and configuration based on the best practice of security in each device or technology. For instance, Windows and Mac are selected for desktops and laptops, IOS, Android and Windows are reviewed for smartphones and tablets.

Different groups of security policies such as password policy, software policy, device security policy and internet browser policy are proposed to monitor and manage the security configurations across different technologies and devices at homes which could help to improve the security awareness and knowledge amongst home users. Each security policy is defined and proposed with three security levels in order to be configured and assigned based on the users' current needs. As an example, Table 1 presents the statements of the password policy with three security levels which can be applied in desktop and laptop devices.

| Category | Policy Statement | Indicative Parameter for The Security Level | | |
|---|---|---|---|---|
| | | **High** | **Medium** | **Low** |
| **Password Policy** | Password | Enabled | Enabled | Enabled |
| | Minimum Password Length | 12 characters | 10 characters | 8 characters |
| | Password Complexity | Enabled | Enabled | Disabled |
| | Maximum Password Age | 60 days | 90 days | 120 days |
| | Enforce Password History | 3 passwords | 2 passwords | 1 password |
| | Account lockout duration | 30 minutes | 15 minutes | Disabled |
| | Account lockout threshold for Invalid logins | 5 Invalid login attempts | 10 Invalid login attempts | Disabled |
| | Time before auto-lock | 3 minutes | 6 minutes | 10 minutes |

**Table 1: The proposed password policy for desktops and laptops**

### 3.2 The proposed design for the system

The proposed system consists of several components and elements such as the dashboard, the enrolment, the management and the policies. In addition, it includes messages, reports and support section in order to provide an efficient system. The HCI and usability principles are taken into consideration when designing the interfaces in order to make sure that they are designed to achieve the main goals for the system.

#### 3.2.1 The main dashboard interface

The aim of the dashboard is to organise data in a way which makes it easy to understand by the users. This helps to monitor all the home digital devices in a usable and cognitively effective manner. The dashboard is designed to provide information about the home devices such as settings alerts, the status of the enrolled users and their managed devices, statistical information about the status of the devices and their compliance with the assigned policies as shown in Figure 1. The non-compliant settings and devices are coloured in red and compliant settings are coloured in green in order to attract the administrator's attention in a usable method. In addition. The main interface and each section can be customised based upon the administrator's priority in order to select the appropriate layout.

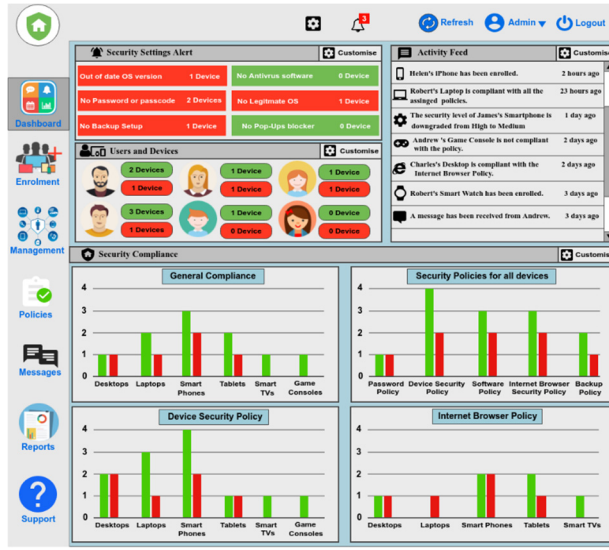


**Figure 1: The proposed design for the main dashboard interface**

### 3.2.2 The enrolment interface

The main aim of the enrolment interface is to add new users and new devices to the system by using a Point-and-Click approach in order to make the process easier as shown in Figure 2. First of all, the administrator needs to select a user. Next, the type of the digital device needs to be selected for the right user. Finally, the required security level, platform and security policies will be shown to be selected and assigned to the user profile.


**Figure 2: The proposed design for the enrolment interface**

### 3.2.3 The management interface

The management section is responsible for managing, monitoring and checking the compliance of the enrolled devices with their assigned policies. The interface is designed as a hierarchical style which can give a panoramic view for all the managed users and their enrolled devices or for a specific user as shown in Figure 3.


**Figure 3: The proposed design for the management interface**

Red and green colours are utilised to illustrate the non-complaint and complaint devices in order to facilitate the administrative tasks. In the interface, the administrator can do several tasks: viewing profiles, changing the assigned policies, changing the owner, sending messages to the users and removing the devices. The administrator can view a user's profile by clicking on the option of viewing profile in the previous interfaces, a comprehensive profile for the selected user is provided for the administrator which can show the device compliance in a usable way as shown in Figure 4. The policies are designed as a horizontal clickable menu with a green tick and a red cross icon to show the status of the compliance. In addition, the profile includes a recent activity section, a profile summary and the current alerts. Moreover, changing the current owner or the security level can be done via the interface. The whole layout of the profile or a specific section can be changed and customised based upon the administrator's priority in order to achieve the system's goals.

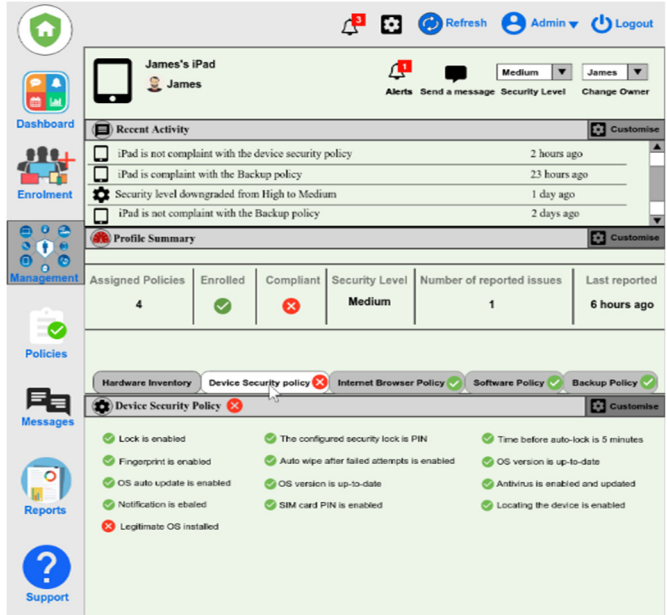


**Figure 4: The proposed design for the user's profile interface**

### 3.2.4 The agent interface

The main role of the agent is to provide a communication between the devices and the management security system scanning and checking the current status of the device and its compliance. In addition, the agent provides the users with sufficient information about their compliance with the assigned policies in collapsible sections which can make it easy for the users to navigate and move between the sections as shown in Figure 5.

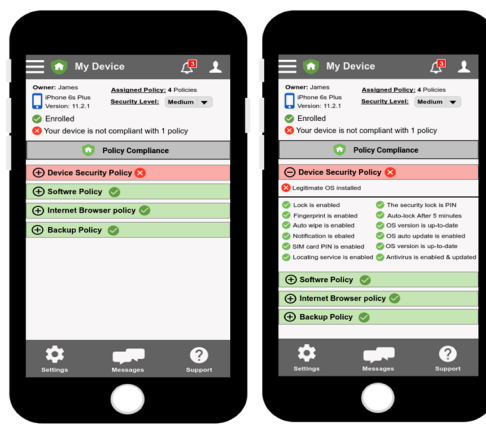


**Figure 5: The proposed design for the agent interface**

# 4 The Evaluation

The proposed interface designs were evaluated to its suitability for home users and to see whether there are current requirements for home users which might not be addressed by the tool. The survey contains several multiple choice questions where the participants can select the right option among the given options. The first section in the survey was to gather general demographic information about the respondents such as age, gender, education and IT experience level. The second section was to assess the different usability and the functionality aspects of each interface design.

All the interfaces were added to the online survey as Graphics Interchange Format (GIF image) in order to show the participants how the tool works in different scenarios. In each interface design, the participants were asked to evaluate the use of colours, icons and text in the interfaces. In addition, they were asked to assess the structure, coherence and the sequence of the sections in each interface. Next, the ease of use, the understanding of the interface purpose and the relevance of the information were evaluated for each design. A number of local researchers at the University of Plymouth were asked to participate in pilot questionnaires in order to get their feedback and comments which could help to enhance and improve the survey.

The survey was targeting public users who are 18 years or older. It was distributed via e-mail targeting students, staff and colleagues at the University of Plymouth. In addition, the social website and applications were used to reach more friends and relatives. A total sample of 434 participations was achieved for this study. It confirmed that their responses will remain anonymous and they have the right to withdraw at any stage upon until the completion of the survey. The survey has been approved by the Faculty Research Ethics Committee in order to comply with the ethical principles of the University of Plymouth.

## 4.1 Demographic information

The majority of the participants (72%) are males whilst the remaining respondents are females as illustrated in Table 1. Around 93 per cent of the participants are within the age range between 18 and 44. 27 participants are in the range between 45 and 54 and only two participants are 55 years old or older. With regards to the educational level, about 44% of the participants held a postgraduate degree (either a Master or a PhD degree). Whilst 42.17% of the participants held a bachelor's degree. In total, more than half of the participants had 5 members or more in their family.

## 4.2 The purposed interfaces

As shown in Figure 6, a high percentage with 95% of the respondents evaluated the structure of the interfaces with a good score and higher, the compound result gives an arithmetic mean of 4.20 which indicates that there is a very good acceptance for the interfaces' structure. The majority of the participants (76%) said that the use of colours, texts, and icons is excellent or very good in the proposed interfaces. This leads to an arithmetic mean of 4.07 for colours, 4.10 for text 4.10 for icons. The coherence

and the sequence of the interface were found excellent or very good by 76%, with an arithmetic mean of 4.09 and 4.12 respectively. 93% of the respondents had a good understanding or better of each interface's role, leading to an arithmetic mean of 4.09. Only 1% thought that the proposed interfaces might be difficult to use while 93% believed that the ease of use seems to be good or better with an arithmetic mean of 4.10. The relevance of the information was assessed with a good evaluation or higher by 94%, leading to an arithmetic mean of 4.11.

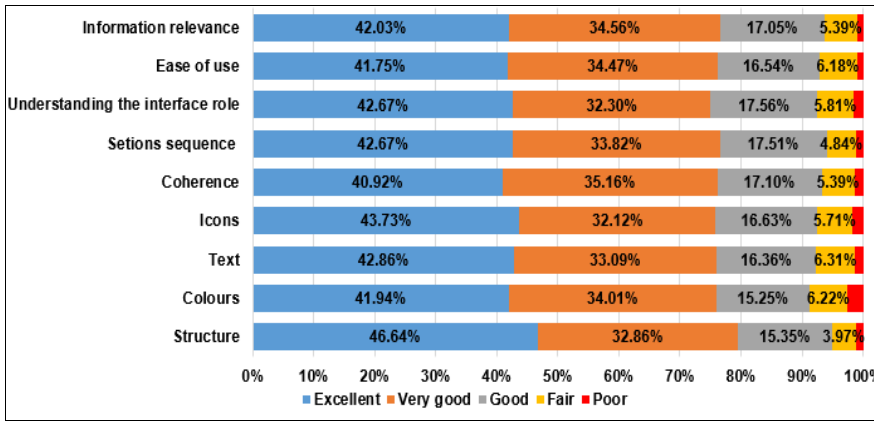


**Figure *6*: The participants' view on usability aspects of the proposed interfaces**

## 5 Conclusion and Future work

This paper focused on identifying the current gap in information security awareness and education for home users. The review indicates that there is a need for a usable, educational bespoke approach which has the ability to manage and monitor the security practice and postures across home devices and technologies. The paper suggests to use and apply different groups of security policies which could help to measure the security configurations in the devices. Several interfaces were designed for a holistic information security management tool for home users which could help users to manage their security better and make them aware of potential threats. The evaluation feedback received from the participants about different usability and functionality aspects was very satisfactory with high percentage. However, some suggestions have been made by the respondents which might help in improving the final solution. Future work will focus on developing the proposed tool in order to be examined for its suitability and functionality.

## 6 References

Furnell, S. M., Bryant, P. and Phippen, a. D. (2007) 'Assessing the security perceptions of personal Internet users', *Computers and Security*, 26(5), pp. 410–417.

GetSafeOnline.org (2018) *Get Safe Online | Free online security advice*. Available at: https://www.getsafeonline.org/ (Accessed: 22 December 2018).

Howe, A. E., Ray, I., Roberts, M., Urbanska, M. and Byrne, Z. (2012) 'The Psychology of Security for the Home Computer User', in *2012 IEEE Symposium on Security and Privacy*. San Francisco, pp. 209–223.

Jahankhani, H., Jayaraveendran, T. and Kapuku-Bwabw, W. (2011) 'Improved awareness on fake websites and detecting techniques', in *Global Security, Safety and Sustainability & e-Democracy*. Berlin, Heidelberg: Springer, pp. 271–279.

Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers and Security*. Elsevier Ltd, 29(8), pp. 840–847. Available at: http://dx.doi.org/10.1016/j.cose.2010.08.001.

Labuschagne, W. A. and Eloff, M. (2012) 'Towards an automated security awareness system in a virtualized environment', in *11th European Conference on Information Warfare and Security*. Laval: Academic Conferences International Limited., pp. 163–171.

LaRose, R., Rifon, N. J. N. and Enbody, R. (2008) 'Promoting personal responsibility for internet safety', *Communications of the ACM*, 51(3), pp. 71–76.

Lunsford, P. and Boahn, C. (2015) *How the Lizard Squad Took Down Two of the Biggest Networks in the World*. Available at: https://infosecwriters.com/Papers/JRollins_Lizard_Squad.pdf (Accessed: 1 March 2019).

Magaya, R. T. and Clarke, N. L. (2012) 'Web-based risk analysis for home users', in *10th Australian Information Security Management Conference, AISM 2012*, pp. 19–27.

Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017) 'A survey of distributed denial-of-service attack, prevention, and mitigation techniques', *International Journal of Distributed Sensor Networks*, 13(12).

Maurer, M., Luca, A. De and Kempe, S. (2011) 'Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness', in *the Seventh Symposium on Usable Privacy and Security*, p. 2.

National Office of Statisitcs (2018) *Internet access - households and individuals, Great Britain: 2018*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (Accessed: 2 March 2019).

NCSA and PayPal (2013) *2013 NATIONAL ONLINE SAFETY STUDY*. Available at: https://staysafeonline.org/download/datasets/7358/2013 NCSA Online Safety Study.pdf (Accessed: 22 June 2017).

Ng, B. B.-Y. and Rahim, M. A. (2005) 'A Socio-Behavioral Study of Home Computer Users ' Intention to Practice Security', *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 2003, pp. 234–247.

Nouh, M. *et al.* (2014) 'Social Information Leakage: Effects of Awareness and Peer Pressure on User Behavior', in Tryfonas, T. and Askoxylakis, I. (eds) *Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer International Publishing, pp. 352–360.

Nthala, N., Flechais, I., Nthala, N. and Flechais, I. (2018) 'Informal Support Networks : an investigation into Home Data Security Practices', *In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pp. 63–82.

Rao, U. H. and Pati, B. P. (2012) 'Study of internet security threats among home users', in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*. Sao Carlos, pp. 217–221. Available at:

Reynolds, M. (2016) *TalkTalk and Post Office customers hit by Mirai worm attack*. Available at: https://www.wired.co.uk/article/deutsche-telekom-cyber-attack-mirai (Accessed: 19 March 2019).

Sharifi, M., Fink, E. and Carbonell, J. G. (2011) 'SmartNotes: Application of crowdsourcing to the detection of web threats', *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, pp. 1346–1350.

Smith, A., Papadaki, M. and Furnell, S. M. (2013) 'Improving awareness of social engineering attacks', *IFIP Advances in Information and Communication Technology*, 406, pp. 249–256.

Statista (2019) *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. Available at: www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. (Accessed: 5 April 2019).

StaySafeOnline.org (2018) *National Cyber Security Alliance | StaySafeOnline.org*. Available at: https://staysafeonline.org/ (Accessed: 22 December 2018).

Tolnai, A. and Von Solms, S. (2009) 'Solving security issues using information security awareness portal', *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, pp. 1–5.

Volkamer, M., Renaud, K., Canova, G., Reinheimer, B. and Braun, K. (2015) 'Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness', in *International Conference on Trust and Trustworthy Computing, TRUST 2015,*. Cham: Springer, pp. 104–122.

Watson, B. and Zheng, J. (2017) 'On the User Awareness of Mobile Security Recommendations', *Proceedings of the SouthEast Conference*, (ACM), pp. 120–127.