3. A Review of Cyber Security Awareness Studies

With a view to examining the current state of the art, this section seeks to explore the academic literature within the information security awareness domain. A total of 20 papers have been identified and categorised into four domains:

- General security awareness: (4 papers)
- Security guidelines and controls (3 papers)
- Web threat awareness (6 papers)
- Gamification (7 papers)

The papers are analysed and summarised in Table 1 based on criteria such as awareness method, providing bespoke content, usability evaluation and the final result for each study.

Table 2. Studies Proposing Information Security Awareness Tools for Home Users

Authors	Method	Awareness Domain	Bespoke Awareness	Usability Evaluation	Result
Tolnai & Von Solms (2009) [7]	Portal	General Security	No	No	The proposed tool has been designed but not evaluated yet by the home users
Caceres & Teshigawara (2010) [9]	Security Tool	Security guideline & controls	No	No	A significant improvement in cyber awareness has been noticed among the home user after using the tool
Kritzinger and Von Solms (2010) [5]	Security Tool	General security	Yes	No	The model has been proposed only theoretically without designing any prototype
Sharifi et al. (2011) [11]	Browser Extension	Web threats	Yes	No	The functionality of tool has been tested successfully
Maurer et al. (2011) [12]	Browser Extension	Web threats	Yes	Yes	It improved the awareness of the home users
Arachchilage & Cole (2011) [13]	Game	Web threats	No	No	A prototype has been developed and tested successfully but no valuation by the home users
Labuschagne et al. (2011) [14]	Game	Security awareness	No	No	The functionally and the effectiveness of the game has not been evaluated yet.
Labuschagne & Eloff (2012) [6]	Security Tool	General Security	No	No	The functionally and the effectiveness of the tool has not been evaluated yet
Magaya & Clarke (2012) [15]	Security Tool	Security guideline & controls	Yes	Yes	It improved the security awareness among the home users
Jahankhani et al. (2012) [16]	Security Tool	Web threats	Yes	No	The model has been proposed only theoretically without designing any prototype
Fruth et al. (2013) [17]	Game	General Security	No	Yes	It improved learning about basic IT security threats among children
Juhari & Zin (2013) [18]	Game	General Security	No	Yes	A significant increase in the students' knowledge about Internet safety after using the game
Smith et al. (2013) [8]	Portal	General Security	No	No	It increased users' understanding of threat concepts
Potgieter et al. (2013) [19]	Browser Extension	Web threats	Yes	No	It is only a theoretical model without designing a prototype
Cetto et al.(2014) [20]	game	Web threats	No	No	It has been used effectively to understand privacy settings on Social Networks
Volkamer et al. (2015) [21]	Browser Extension	Web threats	Yes	Yes	It significantly reduced the number of entering password on the unsafe websites.
Rani & Goel (2015) [22]	Security Tool	Security guideline & controls	No	No	The system functionality has been tested successfully but not evaluated by the users
Hale et al. (2015) [23]	Game	Web threats	Yes	Yes	It improved the user the users awareness about different types of phishing attacks
Giannakas et al. (2015) [25]	Game	Web threats	No	Yes	It improved the children learning about cyber security
Karavaras et al. (2016) [26]	Security Tool	Web threats	Yes	No	It is only a theoretical model

3.1. General Security Awareness

A theoretical E-Awareness Model (E-AM) was suggested by Kritzinger and Von Solms [5] which contains an awareness and enforcement component. The awareness topics are classified based on the knowledge level of the home user which is divided into three levels: novice, intermediate and advanced and the users can be evaluated and tested at each level. However, it is suggested that the enforcement stage should be handled and hosted by Internet Services Providers (ISPs) to ensure that all the users cannot access the Internet without accessing E-Awareness portal. This type of restricted enforcement might annoy and disturb the users' activity which might lead them to try to bypass the portal. In addition, this suggestion which allows the ISPs to manage the security awareness could raise some concerns regarding some aspects such as additional financial cost, legal and privacy issue, technical issues and dealing with multiple devices connecting via different ISP.

Labuschagne & Eloff [6] proposed a security awareness system by using a virtualized system on shared computers The system tried to enforce the user to answer the security awareness questionnaire or to access the awareness content before using the Internet. The users will be prevented from accessing only the internet if their level of security knowledge is not satisfactory. In addition, the proposed awareness contents are not provided based on their needs which might be generic and not useful for them. In addition, this approach does not have a centralized management as it is proposed to work only with shared computers on virtual platforms.

Tolnai & Von Solms [7] proposed an Information Security Awareness Portal (ISAP) used as an educational source to learn about online threats. The proposed portal consists of several limited categories such as the internet, online transactions, and countermeasures. Another portal was designed by Smith et al. [8] which aims at providing awareness of social engineering threats and risk including materials and quizzes.

3.2. Security Guideline and Controls

Caceres & Teshigawara [9] proposed an approach to design a security guideline tool for home users based on international standards to help them to understand the online threats and allow them to stay protected. The tool succeeded in improving the cybersecurity knowledge of the users about some online threats. Nevertheless, the approach requires some information which needs to be provided by the users such as the symptoms of the threats or the current risk that they currently face. Therefore, it might not be useful if the user is not aware of the current threat. In addition, the tool is designed based on particular security standards which mean the threat which is not mentioned in the standards will not be included in the guideline.

A web-based risk analysis tool (WEBRA) was proposed for home users by Magaya & Clarke [15]. The tool utilised the ISO 27002 and NIST SP 800 – 30 standards in order to specify assets and the implemented controls. The user online behaviour will be evaluated in different topics such as passwords, backup, and encryption. In addition, the risk of the missing controls will be analysed and prioritized from high to low. As a final stage, the tool will provide the users with a recommendation page which contains recommendations and links to websites in order to help them to implement the missing security controls for each device. The tool is very easy to use and does not require any prior practical skills. However, the process of detecting the controls currently implemented is done in a manual way from the user side which could be difficult for some novice users. Moreover, the tool does not have the ability to check the effectiveness of each implemented control. For instance, if the user selects that the password is configured, the tool will exclude it from the missing control list without identifying the password strength which might be weak.

Rani & Goel [22] designed an Expert System for Cyber Security Attack Awareness (CSAAES) which assists the internet users to identify and solve the issues that their computers experience such as viruses, social engineering, SQL injection and data modification. The tool requires some symptoms which might be difficult for the home users to provide them due to their poor knowledge. In addition, the tool might not be accurate in identifying the threat because many threats have the same symptoms. Moreover, the suggested countermeasures are provided without a guideline how to implement each countermeasure.

3.3. Web threats Awareness

A number of studies have focused on mitigating the risk from browsing the Internet. Sharifi et al. [11] proposed a browser extension which can help to make users aware of the potential threats when they browse websites. The tool tries to make the user aware of the possible threats at the right time and this depends on the quality of the mutual cooperation between the users as it is a collaborative/ community-based approach. The tool does not try to provide the users with awareness topics or materials once the users are infected by online scams. Moreover, it has not been evaluated yet by the end users for assessing the functionality and the usability of the tool.

Another Firefox plugin was designed by Maurer et al. [12] to raise the cyber security awareness about phishing attacks, draw the users' attention and make them aware when they deal online with confidential data such as credit card numbers, passwords at the appropriate time. The tool has been evaluated in different case studies and the results showed the tool was acceptable by the participants and they were able to identify the phishing websites easily. A theoretical model was proposed by Potgieter et al. [19] which aims to promote information security awareness based on behavioral activities when a web browser is used. The model called Targeted Awareness Browser Extension plans to provide the users with particular awareness content when a possible threat might be experienced. For example, if a user is browsing a banking account, an awareness topic about phishing attacks will be shown to the user or awareness content about the risk of the malicious programs and attacks will be displayed if a user is browsing a website which has a malicious application or code. The main idea of the tool is generally good. However, the motivation option is not mentioned in the tool which could affect the functionality of the tool and might lead to uninstall the extension from the browser.

Volkamer et al. [21] developed a tool called *PassSec* which works as an add-on in Firefox browsers to provide security awareness about using passwords in unsafe websites. *PassSec* offers two main functions. The first task is to highlight all the password fields in different colors: green if the website is using HTTPS or red if it is using HTTP. The second task is to provide the users with an awareness dialogue when a password is typed in an unsafe website which is using HTTP. Moreover, *PassSec* can provide a secure mode which redirects the users to a secure connection (HTTPS) if it is available on the website, the tool was successful in providing the users with an awareness notification at the right time but it is very limited and only deals with password security in PCs and laptops.

Another theoretical framework, called Soc-Aware, was proposed by Karavaras et al. [26] which can provide awareness about the malicious links threats which might be experienced by Facebook users. Soc-Aware filters and checks URLs posted on the Facebook account and notify the users about how many times they experienced malicious actions supported with security awareness materials and guidelines in order to mitigate the threats experienced. The tool is only applicable for Facebook users and only covers one threat which is malicious URLs. In addition, the application requires an access permission in order to work which might be considered as a privacy threat.

3.4. Gamification

Cetto et al. [20] designed a game called Friend Inspector to enhance the privacy awareness among users of social network websites. At the end of the game, the user receives the overall score and recommendations to enhance their privacy settings. The game succeeded in making the user aware of the possible vulnerabilities which might be caused by the current implemented settings. However, the game requires access to a user's Facebook account which might be risky even though the authors claim that personal data is secured.

Arachchilage & Cole [13] designed a mobile game for home users to educate them how to avoid phishing attacks supported by a reference guide. Another educational mobile game called *CyberAware* was developed by Giannakas et al. [25] which aims to allow children to learn about cybersecurity principles and online issues such as malware and spam while they are playing the game. However, the game did not try to provide awareness materials based on the weaknesses of the users after completing all levels of the game.

Another game called CyberPhishing was proposed by Hale et al. [23] in order to provide online phishing awareness. The game simulates phishing attacks in three aspects: email, web browsing and social media. The users' behaviour and actions are analysed which can help to identify the user's weakness and the required training in order to mitigate the possible risk.

3.5. Discussion

A number of studies have tried to provide the home users with cybersecurity awareness which is tailored to their needs in different aspects. Providing an appropriate content based on the level of the cyber knowledge for the users was suggested by Kritzinger and Von Solms [5]. This approach might not be accurate due to the difference in the knowledge between the users. Another attempt was proposed by Magaya & Clarke [15] to provide a bespoke recommendation and guideline based on the result of the risk assessment for the home users but the security controls are identified manually by the users which might be difficult for the novice users. Therefore, it would be beneficial if the automation option was exploited in the tool.

Other attempts have been done by researchers to provide a particular awareness when the users are browsing the internet. Sharifi et al. [11], Maurer et al. [12] and Potgieter et al. [19] proposed a browser extension to make the user aware of the phishing websites and the possible threats while surfing online, whereas Volkamer et al. [21] designed a tool to show an awareness notification when the users are browsing insecure websites with password fields. While Karavaras et al. [26] and Cetto et al. [20] introduced approaches which can provide a tailored awareness for the Facebook users.

Some studies such as Kritzinger and Von Solms [5] Labuschagne & Eloff [6] have tried to restrict the home users' online activity and force them to read

awareness materials. This type of enforcement could create a level of undesirability which will result in the solution being switched off or uninstalled. In addition, it has been suggested in some studies that the cybersecurity awareness can be managed by the ISPs. However, this is not a workable solution because of many issues such technical, privacy, financial and legal issues. The functionality of this approach can become more complicated if there are multiple technologies which are working on multiple ISPs. The motivation for this suggestion is that the authors want to give this responsibility to someone who is better able to manage it. Therefore, it would be a good idea if an individual can take the lead. For example, a member of each family, who is interested in technology, can manage the home network and digital devices. In addition, the enforcement option might not be the best approach within the home environment due to the lack of auditing, policies, and penalties. In addition, the enforcement can cause a resistance from the family members which can lead to the system is not being used.

The vast majority of the educational games are dedicated in a single area, limited scope and they do not successfully adapt to the multi-threats, multi-technologies and services. They have not tried to provide tailor-made awareness content based on the present needs of the users. In addition, they are designed to offer cyber awareness for children without providing valuable awareness for the rest of the family members.

As most of the tools are optional to be used and their main stakeholder is the home users, it is important to encourage and motivate the users to get engaged with the tool in order to promote the cyber knowledge and awareness. The majority of the tools have not introduced any kind of motivations such as scores or digital certificates. For example, it can be easily introduced digital badges or a cyber-hero of the week in the family unit which could help to create a motivational environment between the family members.

In addition, the studies conducted by Rao & Pati [4] and Howe et al. [27] revealed that there is a clear need to design an friendly usable approach which can manage security controls, security configurations and installed software in a wide variety of platforms and devices in order to promote cybersecurity awareness and provide protection for internet users.

4. System Architecture

From the prior discussion, 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 provide the users with some kinds of policies which can be applied to monitor and manage the security practice for home users in order to deliver customized awareness content and encourage the users to practice better security. The security policies can be set and managed by a family member such as parent or a member who has good technical knowledge and skills.

It is envisaged that a novel architecture will have the core functionality which can allow the proposed system to check and manage the security configuration and practice in devices connected to the home network. The effective device management can enhance the awareness amongst home users by providing them with bespoke awareness when it is needed. Therefore, a group of different security policies needs to be defined, created and assigned to appropriate devices. Critically the system will have usable user interfaces which can help in managing the devices effectively, increasing the security awareness and reducing the potential threats. Figure 1 illustrates the proposed architecture. The architecture will begin by identifying the technologies used within the home network and create an appropriate policy for each digital device. Once the policy is assigned to the device, the agent will check the security settings and controls configured in the device in order to compare it with assigned policy. The policy manager will notify the users with appropriate awareness content if there is a vulnerability which could lead to a possible threat.

The proposed architecture will include a number of key components in order to enable the system to perform effectively:

A. The Agent: Due to the variety of technologies, two types of agents are introduced: individual and network-based agents. The main duty of the agent is to provide a communication between the devices and the policy manager, including scanning, checking, capturing and receiving information about the security controls and settings which are configured in the user's device. In addition, it will be responsible for providing the users with a notification and a summary of the status of the device and the device compliance with the assigned security policy

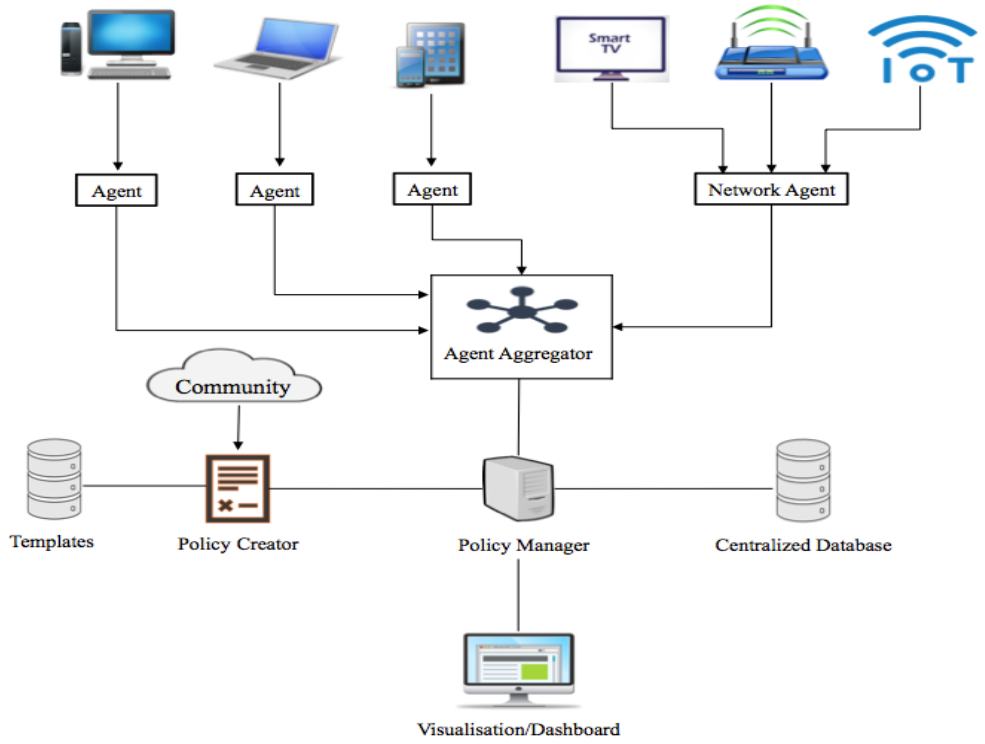

Figure 1. An architectural Overview of Information Security Management System for Home Users

B. The Agent: Due to the variety of technologies, two types of agents are introduced: individual and network-based agents. The main duty of the agent is to provide a communication between the devices and the policy manager, including scanning, checking, capturing and receiving information about the security controls and settings which are configured in the user's device. In addition, it will be responsible for providing the users with a notification and a summary of the status of the device and the device compliance with the assigned security policy.

C. The Agent Aggregator collects the required data from all the agents in one single location, and then sends it to the policy manager.

D. The Policy Manager is considered the backbone proposed system. The primary role of the policy manager is to check the information received from the agents and compare it with the assigned policy for each device or user in order to identify if there is a non-compliance with the assigned policy which might lead to a possible threat or risk. All of these details will be stored in a centralized database in order to retrieve them when they are required.

E. The Policy Creator is responsible for creating a policy for each user and each device. It will provide a wide range of policy templates which is compatible with different platforms. In addition, a community-based input will be utilized in the policy creator which can help to identify the popular policies and receive the users feedback about the policies.

F. The Dashboard is the core functionality to monitor all the home devices in a usable and cognitively effective manner. It will allow navigating and moving between the services available in the system. There are several tasks and sections can be reached from the main dashboard. Summary and statistical information about the current status of the devices can be provided. In addition, the management section can allow the administrator to manage the network and the connected devices by adding new devices, deleting devices, updating profiles and sending a notification to the non-compliant users in order to make them aware of the possible threats. Another task is to create, configure and manage all the policy configurations for the home devices.

5. Information security policy for home users

The main aim of the proposed framework is to provide users with bespoke awareness information directly based upon the current security posture. Therefore, a group of different security policies for

different technologies and devices should be utilised in order to measure the current security practice and settings implemented in the devices. A comprehensive review has been conducted in order to identify the most common security settings and configuration based on the best practice of security in each technology and service which can help to mitigate potential threats and vulnerabilities which might be experienced by the home users.

A number of policies will be proposed to manage and monitor the security configuration and practice in different technologies and digital devices such as:

- **Desktop PCs and Laptops policy.**
- **Smart Phones and Tablets Policy.**
- **Smart TVs and Game Consoles Policy.**
- **Wireless Broadband Devices Policy.**

In addition, each main policy contains some sub-polices which cover different security aspects of the digital devices:

- **Password policy:** it contains the most common password configurations which are applicable to be implemented in the devices such as password complexity and minimum password length.
- **Device Security policy:** it includes the most important features in the devices which need to be managed effectively in order to harden the security of the devices. For example, virus protection and up-to-date OS version.
- **Software security policy:** it is responsible for managing and controlling all the configuration and settings related to the installation of the applications and software such as applications auto update and installing apps from unknown sources.
- **Internet browser policy:** it has all the main security settings which need to be monitored and restricted in all the most popular internet browsers such as Pop-Ups blocker and saving login information.
- **Backup policy:** it covers all the configurations which can help the users to restore the original data after a data loss event such as backup schedule and setup.

6. Conclusion and future work

This paper proposed a novel architecture aimed at providing bespoke information security guidance in a usable, automated and visually engaging manner. In addition, a group of security policies are introduced which can be applied in a number of technologies in order to enhance the cyber security awareness.

In our future work, the development phase will be undertaken based upon the architecture proposed and it will explore how the security polices and management system can be developed in a usable and convenient manner to improve awareness effectively by providing tailored security awareness.

7. References

[1] Ofcom, "Adults' media use and attitudes," 2015. [Online].Available: ttp://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf. [Accessed: 25-Jun-2017].

[2] NCSA and McAfee, "2011 NCSA / McAfee Internet Home Users Survey," 2011. [Online]. Available:https://staysafeonline.org/download/datasets/2068/NCSA_McAfee_Online User Study_Final_11_15_11.pdf. [Accessed: 22-Jun-2017].

[3] NCSA and PayPal, "2013 NATIONAL ONLINE SAFETY STUDY," 2013. [Online]. Available: https://staysafeonline.org/download/datasets/7358/2013 NCSA Online Safety Study.pdf. [Accessed: 22-Jun-2017].

[4] U. H. Rao and B. P. Pati, "Study of internet security threats among home users," *2012 Fourth Int. Conf. Comput. Asp. Soc. Networks*, pp. 217–221, 2012.

[5] E. Kritzinger, S. Von Solms, and S. H. Von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Comput. Secur.*, vol. 29, pp. 840–847, 2010.

[6] W. A. Labuschagne and M. Eloff, "Towards an automated security awareness system in a virtualized environment," in *11th European Conference on Information Warfare and Security 2012, ECIW 2012*, 2012, pp. 163–171.

[7] A. Tolnai and S. Von Solms, "Solving security issues using information security awareness portal," *2009 Int. Conf. Internet Technol. Secur. Trans.*, pp. 1–5, 2009.

[8] A. Smith, M. Papadaki, and S. M. Furnell, "Improving awareness of social engineering attacks," *IFIP Adv. Inf. Commun. Technol.*, vol. 406, pp. 249–256, 2013.

[9] G. R. Caceres and Y. Teshigawara, "Security guideline tool for home users based on international standards," *Inf. Manag. Comput. Secur.*, vol. 18, no. 2, pp. 101–123, 2010.

[10] E. Kritzinger and S. H. Von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Comput. Secur.*, vol. 29, no. 8, pp. 840–847, 2010.

[11] M. Sharifi, E. Fink, and J. G. Carbonell, "SmartNotes: Application of crowdsourcing to the detection of web threats," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, pp. 1346–1350, 2011.

[12] M. Maurer, A. De Luca, and S. Kempe, "Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness," *SOUPS '11 Proc. Seventh Symp. Usable Priv. Secur.*, p. Paper 2, 2011.

[13] N. A. G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from phishing attacks," *Int. Conf. Inf. Soc. (i-Society 2011)*, pp. 485–489, 2011.

[14] W. A. Labuschagne, I. Burke, N. Veerasamy, and M. M. Eloff, "Design of cyber security awareness game utilizing a social media framework," *2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf.*, 2011.

[15] R. T. Magaya and N. L. Clarke, "Web-based risk analysis for home users," *Proc. 10th Aust. Inf. Secur. Manag. Conf. AISM 2012*, pp. 19–27, 2012.

[16] H. Jahankhani, T. Jayaraveendran, and W. Kapuku-Bwabw, "Improved awareness on fake websites and detecting techniques," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 99 LNICST, pp. 271–279, 2012.

[17] J. Fruth, C. Schulze, M. Rohde, and J. Dittmann, "E-learning of IT security threats: A game prototype for children," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8099 LNCS, pp. 162–172, 2013.

[18] S. F. Juhari and N. A. M. Zin, "No Educating Children about Internet Safety through Digital Game Based Learning," *Int. J. Interact. Digit. Media*, vol. 1, no. 1, pp. 65–70, 2013.

[19] M. Potgieter, C. Marais, and M. Gerber, "Fostering Content Relevant Information Security Awareness through Browser Extensions," *Inf. Assur. Secur. Educ. Train. 8th IFIP WG 11.8 World Conf. Inf. Secur. Educ.*, pp. 58–67, 2013.

[20] A. Cetto, M. Netter, and G. Pernul, "Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks," *arXiv Prepr. arXiv …*, 2014.

[21] M. Volkamer, K. Renaud, G. Canova, B. Reinheimer, and K. Braun, "Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness," in *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings*, M. Conti, M. Schunter, and I. Askoxylakis, Eds. Cham: Springer International Publishing, 2015, pp. 104–122.

[22] C. Rani and S. Goel, "CSAAES: An expert system for cyber security attack awareness," *Int. Conf. Comput. Commun. Autom. ICCCA 2015*, pp. 242–245, 2015.

[23] M. L. Hale, R. F. Gamble, and P. Gamble, "CyberPhishing: A game-based platform for phishing awareness testing," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2015–March, pp. 5260–5269, 2015.

[24] F. Giannakas, G. Kambourakis, and S. Gritzalis, "CyberAware: A mobile game-based app for cybersecurity education and awareness," *2015 Int. Conf. Interact. Mob. Commun. Technol. Learn.*, no. November, pp. 54–58, 2015.

[25] F. Giannakas, G. Kambourakis, and S. Gritzalis, "CyberAware: A mobile game-based app for cybersecurity education and awareness," *2015 Int. Conf. Interact. Mob. Commun. Technol. Learn.*, no. November, pp. 54–58, 2015.

[26] E. Karavaras, E. Magkos, and A. Tsohou, "Low User Awareness Against Social Malware: An Empirical Study and Design of a Security Awareness Application," *13th Eur. Mediterr. Middle East. Conf. Inf. Syst. (EMCIS 2016)*, pp. 1–10, 2016.

[27] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The Psychology of Security for the Home Computer User," *2012 IEEE Symp. Secur. Priv.*, pp. 209–223, 2012.

