A Review of Using Gaming Technology for Cyber-Security Awareness

Faisal Alotaibi[1], Steven Furnell[1, 2, 3], Ingo Stengel[1, 4], Maria Papadaki[1]
[1] *Plymouth University, Plymouth, UK*
[2] *Edith Cowan University, Perth, Western Australia*
[3] *Mandela Metropolitan University, Port Elizabeth, South Africa*
[4] *University of Applied Sciences Karlsruhe, Germany*

Abstract

Rapid development has been observed in the deployment of communication technologies and the use of the Internet across the globe. Information exchange is the main aspect of use of such technologies in everyday life. Crimes associated with the misuse of information on the Internet are on the increase and are resulting in various losses. Saudi Arabia is one of the fastest developing countries in the Middle East, where the uptake of communication technologies such as the Internet and mobile technologies has risen sharply in recent years. These technologies are relatively new to the region when compared to developed countries. Therefore, the crimes associated with these technologies may be new to the people in the region. Our previous study has found that there is an immediate need for launching awareness programs about cyber security and cyber-attacks, keeping in view of the rising Internet and mobile usage in the country. A mobile gaming application was preferred by the participants in the previous study to address the issue of creating awareness.

Considering the results from the previous study, this paper reviews various studies focusing on gaming applications and the effectiveness of their usage in creating cyber security awareness. Different gaming applications are studied and compared, and majority of the studies proved to be effective in creating awareness among the users. However, there are few aspects which need to be considered such as suitability or tailoring the applications/games according to the user needs and requirements, issue specific games etc. The review of the previous studies and gaming applications in this paper has found that mobile gaming applications are effective in creating cyber security awareness.

1. Introduction

The scale of the rise in cybercrimes is alarming. The cost of cyber breaches in the UK alone is estimated to be £3.14 million [1]. The Business Email Compromise (BEC) scams worldwide were estimated to be more than $ 3 billion [2]. The impact of cybercrime is not just assessed solely in terms of costs incurred but also in terms of breach of data privacy which can affect many consumers. The projected losses for the businesses by the year 2019 due to cybercrime are estimated to be in the region of $2 trillion [3]. While the number of cyber security attacks in large companies has been decreasing, in medium and small sized companies it is increasing significantly, which could be a major concern for developing countries [4].

Saudi Arabia, which is one of the fastest developing countries in the Middle East, has seen enormous growth in the use of communication technologies, the Internet and mobile technologies in recent years. It is estimated that approximately 66% of the population, which equals more than 18 million users, have access to the Internet. Facebook and Twitter are used by the majority of these users [5]. About 39% of the population that uses the Internet buys products online, and the country's E-commerce business is about $520 million [6].

The penetration of the Internet and the boom in smartphone usage in KSA is relatively new.

Therefore, it can be assumed that understanding of the importance of cyber security and information on security measures which can be taken is limited.

Focusing on these aspects, a previous study investigated the cyber security awareness of the people in Saudi Arabia in different contexts. A quantitative online based survey was conducted using a survey questionnaire for gathering the information related to cyber security awareness in Saudi Arabia. The study found that though the participants have good knowledge of IT, their awareness regarding the threats associated with cybercrime, cyber security practices, and the role of government and organizations in ensuring the information safety across the Internet is very limited. The results indicated that the levels of cybercrime experiences are on the rise in recent years, and there is no specific approach being followed in the region for increasing cyber security awareness except CERT regulations, and online information on government websites. Additionally, Chi-Square test results (t(627)=3.85, p=0.013) indicated that the Internet skills have an effect on the cyber security practices from the users end, and association of the level of skills of the people with the available security measures being implemented by the responsible organizations in the region. The study has found that there is an immediate need for developing an application for creating cyber security awareness in the region in order to combat cybercrime.

The key findings of the previous study (survey) are that there is a high usage of Internet mostly on daily basis amongst participants. Another important observation was that over 90% participants use smartphones primarily for Internet access for various activities including banking, shopping activities. The general observation was that even though the survey shows good IT knowledge amongst users, the cyber security awareness was weak amongst them. It was observed that apart from anti-virus and firewall as relatively common cyber security practices, the participants' responses showed that they have relatively less cyber security awareness and have weaker practices such as creating easy passwords.

Though Saudi Arabia has experienced a significant growth in the use of technologies, but use of security technologies (and the extent of related awareness) has not kept pace, and citizens are experiencing problems and prefer an effective role of responsible organizations in improving cyber security awareness; and support the concept of using mobile applications for increasing security awareness among them. It is clearly evident from the survey results as majority of the participants has experienced cyber-attacks

One of the best ways of combating cybercrime is by creating awareness and adopting better cyber security practices among the people. The survey responses in the previous study has indicated that the users are insecure about their data security and are willing to adopt better practices to secure their devices and data. The survey responses also indicated that a cyber-security awareness application would enable the users to improve their cyber security practices. Therefore, it is important that different approaches for creating cyber security awareness in Saudi Arabia must be developed and deployed to combat cybercrime. As preferred by the participants a mobile application for this purpose can be an effective approach in combating cybercrime and raising awareness. However, the application needs to be engaging users and effective in educating and training the users.

Therefore, the awareness programs must be developed in such a way that it perfectly meets the changing needs of the people, and considers the lifestyles and cultural practices in the country, and must be engaging. Considering these factors, this study has reviewed various studies and mobile applications coupled with gaming technology for generating security awareness.

2. Background Study

To increase awareness about cyber security, it is essential that the users are provided with training. There are various modes of creating cyber security awareness like education, promotion etc. However, it is essential that these modes have to be effective in creating an impact on the users. Serious games can be an effective method to provide training to the users. Serious games are games that are designed with a purpose rather than just intended for pure entertainment. They are proved to be effective tools for training and achieving a behavioral change. Such methods of using games for training is also referred as games based learning approaches. Though games based learning methods are mainly utilized in school education, increasingly, these methods are also adopted in healthcare, advertising, behavioral change, and recently in cyber security training [7].

Learning through mobile games is an educational process where the users are required to perform learning activities by using a game or a series of games designed for specific learning activity [11, 12, 13]. The digital games on mobiles can be effective in providing fidelity of simulations and problem solving tasks, which could enhance the learning activity and motivate the users. Understanding its scope, researchers have suggested that gamification can be a key concept for learning security awareness concepts in future [13]. While few studies have identified the potential of gaming in learning, other studies have already identified the change in the implementation [14]. Different studies have found the huge potential of implementing gaming technology in different areas. In a study [15] focused on gaming for learning, it was identified that learning process can be significantly improved by mobile gaming education. Another study [16] has found that gaming process can improve literacy levels among children.

Research studies have found that games are an effective education tool widely popular and effective in teaching, especially puzzle games. A study conducted by Costabile, et al. [17] has explored how a mobile phone can be used to teach archaeology through game based learning. Another study has identified and explored the importance of mobile learning integrated with technology in education. The games based learning method has several advantages. The obvious advantage is that games based learning method provides an interactive approach to train or educate the users about a specific program. It enables the players to acquire skills and to enable thought processes in a fun and interactive way. The adaptability and flexibility of games approaches enables to design the game to suit almost every training subject possible [8].

A well designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world. The games based approach would motivate the player to move towards the goal with required actions and also see the consequences without facing penalties in the real life. Further, when compared to the traditional method of training, games based methods are more engaging, relatively cost effective, easily transferrable to a large number of trainees, customized to each player, etc. [9]. Moreover, there are limited studies that have explored games based learning approaches for cyber security awareness in Saudi Arabia context. Therefore, this paper explores the potential of the gaming technology to support several key areas of security awareness/learning.

3. Methodology

The number of mobile and computer games has been on the rise in the past few years. With a rapid increase in the smartphone usage across the world, there has been a rise in the number of various mobile gaming applications. As the games are effectively engaging the users, the possibility of using them for cyber security awareness is being considered as one of the major areas of research. As the growth of these applications is observed to be at a rapid pace, the design and developments are going on in both academic and commercial settings. Therefore, it is necessary to consider both existing applications used for cyber security awareness and also the studies associated with them. Thus, this paper is divided in to two parts. The first part focuses on a structured review of research literature and the second focusing on the applications/product search. The structured review was carried out in November and December 2016, which includes studies and papers published in various journals and conferences. The literature search was conducted using Google Scholar, which is one of the popular search engines for academic releases and has various options for filtering the results. The following keywords and their combinations are used for literature search.

- Game based learning
- Computer game
- Serious Games
- Mobile learning
- Security education
- Safety Gamification
- Cyber Security Awareness

The search was initially focused on considering the studies with an outcome using some measurement techniques. However, as there were only few studies found that were focusing on cyber security awareness and training using gaming applications, the search was expanded to include any academic paper describing a cyber-security game. The literature search yielded 68 results, which were inspected by the authors, and a final selection of 12 papers was made considering the purpose (cyber security awareness) of the gaming applications. These studies were grouped by the games they describe, type, methods used, and the results (whether significant or not?). As the Google search shows large number of results only the first 15 results for each keyword or their combination are considered for inspection.

The application/ Product search was carried out in November and December 2016, and updated in January 2017. The search was conducted using Google Play store, Google Search (UK), Bing, Apple App Store, and other popular gaming websites (www.gamespot.com; http://serious.gameclassification.com/). Only those gaming application focusing on cyber security were considered, and included for inspection if the information was freely available to assess their relevance (awareness; education) to the study. The search yielded 19 games, out of which 10 games were considered for review according to their relevance.

4. Review of Game based cyber-security studies

12 papers have been identified, which were focusing on cyber security awareness and training through games. These papers are presented in table 1. Out of these only 6 studies were conducted in 2010 or before, and remaining 6 papers post 2010, which reflects the area of study as relatively new. These studies focus on analyzing different games for creating cyber security awareness and training using technologies that include 3D virtual world or simulation, 2D framework, mobile applications and web based application technologies. Most of the games focused on general cyber security awareness, network security, and phishing and end-user PC protection.

As the number of studies in the area of cyber security training has been increasing, most of these studies were focusing on the general public. Very few studies are found to be focusing on training professionals in the aspects of internal threats. Any study has to evaluate the application to identify the suitability and the usability of such applications. Out of the reviewed papers only few studies have evaluated the applications which include Anti Phishing Phil, NGSEC, and Control-Alt-Hack. All these studies have indicated positive feedback on utilizing games for creating cyber security awareness. However few studies including [22], [24], [26], and [27] have suggested some improvements and recommendations, while all other studies have stated positive results.

Studies including Anti Phishing Phil and Security games by Next Generation Security (NGSEC) have shown significant improvements in using games for learning purpose, but the sample sizes used in these studies were quite small. Other games have resulted in positive feedback from users but did not evaluate the impact and effects on learning outcomes; while

Table 1. Major studies focusing on gamification for cyber security awareness

Authors	**Game**	**Type**	**Methods**	**Results**
Arachchilage N. A. G. and Love S., 2013[18]	Anti-Phishing Phil	Mobile gaming application: Training for links (URL) safety	Usability questionnaire	Improved learning and susceptibility of phishing
Arachchilage N. A. G. and Love S. 2014 [19]	Anti-Phishing	Mobile gaming application: Training for links (URL) safety	Review	Improved learning
Nyeste P. G. and Mayhorn C. B., 2010 [20]	Anti-Phishing	Mobile gaming application: Training for links (URL) safety	RCT, pre & post experimental study	Improved learning and susceptibility of phishing
Ariyapperuma S. and Minhas A., 2005 [21]	Next generation security - NGSEC	Web based gaming application	Review of tasks and performance	Significant improvements identified among users in performing security tasks
Gondree et al., 2013 [22]	-	Mobile Board game	Multi-player assessment (group study)	Positive feedback, need for more evaluation
Dasgupta et al., 2013 [29]	Control Alt Hack	Mobile Puzzle game	Assessment based on Puzzles	Effective in creating awareness
Denning et al, 2013 [23]	-	Review	Survey of teachers	Effective game for model dissemination
Geers K., 2010 [24]	Baltic Cyber Shield-BCS	Training exercise with virtual attackers and defenders	Review	Recommendations for improving IT infrastructure
Kayali et al., 2014 [25]	Internet Hero	Puzzle game	Experiment study	Improved awareness
Irvine C. E. and Thompson M, 2003 [26]	The Internet	-	Review	Positive impacts of games with recommendations
Pastor et al., 2010 [27]	-	Multiple games	review	Recommended developing and using more tools in games
Schweitzer D. and Brown W., 2009 [28]	-	Visual presentation	Presentation (Education) case study	Positive experience of users in using interactive visualization

other studies did either not study effects on learning outcomes, or the results were not quite conclusive, but the authors were convinced they gave a positive "early indication".

A review of these studies has indicated that the cyber security awareness approach through gaming is relatively quite new and needs extensive research studies and evaluation approaches for analyzing various security issues and the related gaming techniques. As the cyber security is a large area were the threats may appear in various forms, a streamlined gaming techniques are necessary for generating awareness according to the types of threats.

5. Review of Cyber-security Games

Various games have been identified which are related to specific aspect of cyber security or threat. Out of these 10 popular games are listed in table 2, along with type, intended learning, and target audience. Majority of the games are available for free and are mainly focused on teenagers, students and children. Corporate training games designed for professionals with more detailed threats awareness programs were found in [30] and [36] where awareness regarding data loss prevention, information management etc. was provided. However, no information was found regarding the effectiveness of any of these games in creating cyber security awareness. The review has found that there are various games developed for specific issues

Table 2. Popular Cyber-Security Games

Authors	**Game**	**Type**	**Audience**	**Intended Learning**
Health-IT [30]	Cyber security contingency planning	2D –Click & turn based	Health Decision Makers	Data loss prevention
Onguardonline [31]	OnGuard	2D –Click & turn based	Teenagers	Online Security. Protection from viruses and malware
Australian Department of Broadband Communications and the Digital Economy [32]	Buddie	2D –Click & turn based	Children	Online Security while browsing and social networking. Protection from viruses and malware.
NSteens [33]	NSteens	Mini 2 D games – Click & turn based	Teenagers	Online Security while browsing and social networking. Protection from viruses and malware.
cybersecurity challenge UK [34]	The Cybersecurity Challenge	National Competition (Physical role)	Students	Various topics including Online Security, prevention techniques, threats etc. Protection from viruses and malware
Global CyberLympics. [35]	High School Cyber Security Game - global cyberlympics	Global Competition	Students	Forensics, network security, threats prevention
IASE [36]	CyberProtect	2D graphic game	Students & Professionals	Cyber security and information management
McGoogan C [37]	Cyphinx	Puzzles in virtual environment	Students & Adults	Forensics, network security, threats prevention, Cyber security and information management
FBI [38]	FBI Cyber Game	Puzzle	Children	Online safety management
NOVA Labs [39]	PBS Cybersecurity Lab	2 D puzzle games with narrative scenes	Children	Scams identification and defending against various cyber attacks

relating to cyber security which are intended for children, teenagers and professionals.

6. Discussion and Future Work

Cybersecurity is a wide area involving various aspects from software, hardware, human resources, operational processes, and psychology. Similar is the scope of security threats, which can be in various forms causing damages at different levels. Therefore awareness and training is an effective approach in dealing with the threats of cyber security. Games, as discussed in the previous sections can be an effective tool in achieving this target. However, the concept of gamification for cyber security is relatively new and developing field. Threats can take various forms, however, the user need to be alert and aware of various precautions necessary in order to prevent any event of security attack. Usually the user side awareness includes recognizing web-based attacks, phishing and spam emails etc. As the previous study has found that there is an immediate need for developing applications for creating cyber security awareness in Saudi Arabia, this paper reviews the gaming as a tool for this purpose, and the related aspects necessary for developing an effective gaming technology addressing the specific security issue completely.

Various studies have been reviewed, out of which most of the studies have indicated positive results in using gaming technologies as a tool for creating awareness and training. However few studies are not evaluated and few of them used small sample population in the studies. From the review it is evident that there is a need for in-depth and robust evaluations to conclude the effectiveness of serious games for cyber security, and also the need for using large sample population in these studies.

This paper also reviewed few popular games available for raising cyber security awareness. Most of these games are developed by governmental organisations or charitable intuitions. Most of these games were targeted at children or teenagers, and two of them for professionals. It was found that there are relatively few games focused particularly among the adult population in general. In addition most of the games were focusing on general cyber security aspects, and issue specific games were not found. Therefore there is a need for streamlining the game development according to the requirements and the types of security threats that are occurring frequently. In addition there is a need for continuous monitoring and games updating necessary as there are new threats emerging every day.

From these reviews it was identified that though there are various studies supporting the positive impact of gaming in creating cyber security awareness, there is a need for regress study involving large sample populations to evaluate the impact; and there is also a need for considering issue specific gaming applications to evaluate effectively which can help in concluding the impact of gaming technologies in cyber security awareness and training, as most of the studies reviewed focused mainly on general cyber security issues. Therefore it can be concluded that Gamification offers a potential option in this respect, and the future research would therefore explore how it can be applied to support several key areas of security awareness/learning, and also the suitability of such applications in the country like Saudi Arabia.

7. References

[1] Ashford, W. "Top 10 cyber crime stories of 2015", Computer Weekly, 2015.

[2] "Internet Crime Complaint Center (IC3) | Business E-mail Compromise: The 3.1 Billion Dollar Scam", Ic3.gov, 2016. [Online]. Available:https://www.ic3.gov/media/2016/160614.aspx. [Accessed: 16- Sep- 2016].

[3] Juniper Research, "Cybercrime will Cost Businesses Over $2 Trillion by 2019 - Juniper Research", Juniperresearch.com, 2016. [Online].http://www.juniperresearch.com/press/pressreleases/cybercrime-cost-business-over-2trillion. [Accessed: 16- Sep- 2016].

[4] Symantec, "Attackers Target Both Large and Small Businesses", 2016. [Online]. https://www.symantec.com.content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf. [Accessed: 16- Sep- 2016].

[5] Miniwatts Marketing Group, "Middle East Internet Statistics, Population,Facebook and Telecommunications Reports", Internetworldstats.com, 2016.[Online]. Available: http://www.internetworldstats.com/stats5.htm. [Accessed: 16- Sep- 2016].

[6] CMO Council Middle East, ‘Facts & Figures’, 2015. [online]. Accessed: http://www.cmocouncil.org/mena/facts_stats.php [Accessed: 28- Nov- 2015]

[7] Hendrix, M., Al-Sherbaz, A. & Victoria, B., 2016. Game based cyber security training: are serious games suitable for cyber security training?. International Journal of Serious Games, 3(1), pp. 53-61.

[8] Boyle, S., 2011. An Introduction to Games based learning, s.l.: UCD Dublin.

[9] Trybus, J., 2014. Game-Based Learning: What it is, Why it Works, and Where it's Going, s.l.: New Media Institute.

[10] Denk, M., Weber, M. and Belfin, R., 2007. Mobile learning challenges and potentials, Int. J. Mob. Learn. Organ., 1, pp.122-139.

[11] Ghazvini, F., Earnshaw, R.A., Robison, D. and Excell, P.S., 2009a. Designing Augmented Reality Games for Mobile Learning Using an Instructional-Motivational Paradigm, International Conference on CyberWorlds, CW '09, pp.312-319, 7-11 September 2009,

[12] Kurkovsky, S., 2009. Engaging students through mobile game development. ACM SIGCSE Bull, 41, pp.44-48.

[13] Shih, Y. H., Hou, H. T. and Wu, Y. T. T., 2011. A Review on the Concepts and Instructional Methods of Mini Digital Physics Games of PHYSICSGAMES.NET, Edutainment'11, Proceedings of the 6th international conference on E-learning and games, edutainment technologies, LNCS, 6872,pp.517–521.

[14] Molnar, A. and Frias-Martinez, M., 2011. Educamovil: Mobile educational games made easy, In Proceedings of the World Conference on Educational Multimedia, Hypermedia and Telecommunications,pp. pp.3684–3689, Chesapeake, VA: AACE.

[15] Banerjee, A., Cole, S., Duflo, E. and Linden, L., 2007. Remedying education: Evidence from two randomized experiments in India, Quarterly Journal of Economics, 122 (3), 1235-1264.

[16] Tian, F., Lv, F., Wang, J., Wang, H., Luo, W., Kam, M., Setlur, V., Dai, G., and Canny, J. 2010. Let's Play Chinese Characters: Mobile Learning Approaches via Culturally Inspired Group Games, Proceedings of 28th International Conference on Human Factors in Computing Systems, Atlanta, 1 (4), 1603-1612.

[17] Costabile, M. F., Angeli, A. C. D., Lanzilotti, R., Ardito, C., Buono, P. and Pederson, T., Explore! possibilities and challenges of mobile learning, Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, 05-10 April 2008, Florence, Italy.

[18] Arachchilage N. A. G. and Love S., “A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013.

[19] Arachchilage N. A. G. and Love S., “Security awareness of computer users: A phishing threat avoidance perspective,” Comput. Hum. Behav., vol. 38, pp. 304–312, 2014.

[20] Nyeste P. G. and Mayhorn C. B., “Training Users to Counteract Phishing,” in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960, 2010.

[21] Ariyapperuma S. and Minhas A., “Internet security games as a pedagogic tool for teaching network security,” in Frontiers in Education, 2005. FIE’05. Proceedings 35th Annual Conference.

[22] Gondree M., Peterson Z. N., and Denning T., “Security through play,” Secur. Priv. IEEE, vol. 11, no. 3, pp. 64–67, 2013.

[23] Denning T., Lerner A., Shostack A., and Kohno T., “Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 915–928, 2013.

[24] Geers K., “Live fire exercise: preparing for cyber war,” J. Homel. Secur. Emerg. Manag., vol. 7, no. 1, 2010.

[25] Kayali F., Wallner G., Kriglstein S., Bauer G., Martinek D., Hlavacs H., Purgathofer P., and Wölfle R., “A Case Study of a Learning Game about the Internet,” in Games for Training, Education, Health and Sports, Springer, pp. 47–58, 2014.

[26] Irvine C. E. and Thompson M., “Teaching objectives of a simulation game for computer security,” DTIC Document, 2003.

[27] Pastor V., Díaz G., and Castro M., “State-of-the-art simulation systems for information security education, training and awareness,” in Education Engineering (EDUCON), 2010 IEEE, pp. 1907–1916, 2010.

[28] Schweitzer D. and Brown W., “Using visualization to teach security,” J. Comput. Sci. Coll., vol. 24, no. 5, pp. 143–150, 2009.

[29] Dasgupta D., Ferebee D. M., and Michalewicz Z., “Applying puzzle-based learning to cybersecurity education,” in Proceedings of the 2013 on InfoSecCD’13: Information Security Curriculum Development Conference, p. 20, 2013.

[30] “Cybersecure Contingency Planning.” [Online]. http://www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html. [Accessed: 02-Jan-2017].

[31] “OnGuardOnline.” [Online]. http://www.onguard online.gov/media. [Accessed: 02-Jan-2017].

[32] Australian Department of Broadband Communications and the Digital Economy, “Stay Smart Online Cybersecurity Education Modules - Primary.” [Online]. Available: https://budde. staysmartonline.gov.au/ primary/main.php#. [Accessed: 03-Jan-2017].

[33]“NSteens.” [Online]. http://www.nsteens.org/ [Accessed: 03-Jan-2017].

[34] “cybersecurity challenge uk.” [Online]. Available: http://cybersecuritychallenge.org.uk/. [Accessed: 03-Jan-2017]

[35] “High School Cyber Security Game,” Global CyberLympics. .

[36] Information Assurane Support Environment, “CyberProtect.” [Online].http://iase.disa.mil/eta/Lists/ IA%20Simulations/AllItems.aspx. [Accessed: 03-Jan-2017]

[37] McGoogan C., “Cyphinx could recruit the cybersecurity experts of the future (Wired UK),” Wired UK. [Online]. http://www.wired.co.uk/news/archive/2015-10/01/cyphinxcybersecurity-game. [Accessed: 03-Jan-2017].

[38] “Kids Games,” FBI. [Online]. Available: https://www.fbi.gov/fun-games/kids/kids-games. [Accessed: 03-Jan-2017].

[39] “Cybersecurity Lab | NOVA Labs | PBS.” [Online]. Available: http://www.pbs.org/wgbh/nova/labs/lab/cyber/. [Accessed: 03-Jan-2017]