Synthesizing Cybersecurity Issues And Challenges For The Elderly

Nurul Huda Nik Zulkipli[1], Nor Aimuni Md Rashid[2], Anwar Farhan Zolkeplay[3], Alya Geogiana Buja[4]

[1,2,3,4]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Melaka, Kampus Jasin 77300 Merlimau., Melaka, Malaysia
[1]nurulhuda8450@uitm.edu.my, [2]aimuni5294@uitm.edu.my, [3]anwarfarhan@uitm.edu.my, [4]geogiana@uitm.edu.my

Abstract: There are millions of users using the Internet daily including senior citizens or the elderly. This group is defined for users who are in the age range of 50-60 years old. In cybersecurity, the elderly is one of the most vulnerable groups of Internet users that is prone to cyberattacks. They are always the target and victimized by attackers, especially in cybercrime cases. However, not many pieces of research have been done on this specific group of users. Therefore, this paper will review and discuss cybersecurity issues and challenges involving the elderly. The main objective of this paper is to investigate the critical factors that contribute to the involvement of the elderly in cybercrime. It also includes the patterns of Internet usage, level of IT knowledge, and their awareness of the danger in the digital world. One of the reasons for the surge of the cyberattack vectors is due to lack of awareness on cybersecurity defence among Internet users. From the literature synthesized, the outcome of this paper proposes a framework of cybersecurity awareness for the elderly which can be used as a guide to educate and prevent them from being exploited in cybercrime.

Keywords: Cybersecurity, Elderly, Cybercrime, Awareness.

1. INTRODUCTION

Cybersecurity concerns involving the elderly are seldom discussed and most of the time, this matter has been neglected. Most of the research usually focus on issues related to general groups of users like the youngsters and adults. In fact, there are only several pieces of literature that emphasize issues related to the elderly, especially in cybersecurity.

Firstly, the term "cybersecurity" needs to be clearly understood. Tons of previous research tried to indicate the firm definition of cybersecurity. In addition, this term has been largely viewed academically and it varies in dimensions from a particular perspective and has been discussed in the literature. For instance, in [1], the researchers synthesized that this term is utilized broadly, and its definitions are significant factors, context-bound, regularly subjective, and uninformative. According to [1], the researchers proposed the definition of cybersecurity in their research work as

" the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."

Other than that, a former Director of Research at the National Security Agency in the United States also addressed the multiple knowledge domains cybersecurity as stated in [2],
"A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed.".

In this paper, the word "cybersecurity" refers to a set of security processes, resources, and parameters that can be used to defend cyberspace from any kind of incidence and misuse. Next, one of the perspectives that needs to be highlighted in the cybersecurity points of view is the types of users. Previous research did focus on studying the behaviours, educating the awareness among certain users of groups like youngsters, adults, and children to prevent them from being abused and targeted by the attackers [3]. Literature shows that there is lack of research that covers the more mature adults, who are also known as the elderly (age range of 50-60 years old). Just like the younger generation, the elderly is becoming a part of the main users of Internet, especially in banking, health care, e-commerce, and emerging smart systems. However, these systems are commonly not intended to cater the needs of the elderly who might require a certain kind of features due to their conditions, and because of their

novelty, complexity, and propensity to collect and communicate large quantities of sensitive information, can raise significant privacy and security concerns [4].

Efforts to address these concerns should be focused on an in-depth understanding of the behaviours and preferences of older adults about data privacy and security of these technologies and it should represent variations in physical and cognitive abilities. Hence, this group of users is vulnerable and prone to be involved in cybercrime cases. In [5] and [6], the researchers reported that cybercriminals had stolen almost $40 billion from vulnerable elderly. In fact, elder abuse and neglect cases are increasing in the United States [7], [8].

Therefore, the aim of this paper is to review related literature on cybersecurity issues and challenges related to the elderly. To achieve this, the current study investigates the critical factors that contribute to the involvement of the elderly in cybercrime cases. From the findings, this paper proposes a framework for the elderly which can be used as a guide to develop cybersecurity awareness with the aim to educate the elderly to be more alert to the varied cyber threats and the vulnerability of devices and data to these cyber threats [9]. Besides educating users, cybersecurity awareness also intends to help alerting Internet users on current situations of cybersecurity issues including cyberattacks and cyber threats [10]. This paper is outlined as the following; (i) Cybersecurity Issues and Challenges Among the Elderly, (ii) Reviews on Case Study On Cyber-Attacks On Elderly,(iii) Reviews on Cybersecurity Awareness Among Elderly, (iv) Proposed Framework, and finally the Conclusion.

2. CYBERSECURITY ISSUES AND CHALLENGES AMONG THE ELDERLY

The elderly makes up one of the fastest-growing groups of Internet users [11]. Research done by [12] showed that over 50% of senior citizens use the internet and the number is gradually increasing. The number has triggered, and further investigation is required to understand cybersecurity issues and challenges that affect the elderly. Apart from that, it is also important to investigate the factors from the literature on why these types of users are susceptible to be exploited and compromised in cybercrime. There are a few factors from literature involving the elderly in cybercrime cases which are further described under several headings as the followings:

2.1 Technology versus Age

Many pieces of literature as stated in [12], [13], [14] and [15] have agreed that the elderly are generally not technology savvy and the technology gap makes them not interested to learn about new security hacks. This is because a majority of the elderly have physical conditions or health issues that make it difficult for them to use new technologies as they need assistance to use a new device [16]. Their devices are often not properly secured. For instance, they do not know the importance of installing and using security software such as anti-virus software and anti-spam software on their devices. In addition, some of them do not let their devices be updated. Consequently, this makes the devices become more vulnerable and easily targeted by cyber criminals [12]. Besides, some of them are very sceptical about the benefits of technology. [16].

2.2 Behaviour Factors

According to [17], the elderly is a group of users that are less likely to report the crime to authorities if they get involved in a cybercrime case. This is due to a combination of two main factors. Firstly, most of them do not know where to report fraud cases and later, they do not know how to handle these situations. Moreover, they may also feel embarrassed about what had happened to them for instance, for those who involved in love scams. Furthermore, the elderly are politer to strangers which makes them easily disclose their confidential details through social engineering to cyber criminals like fraudsters.

2.3 Cybersecurity Skills Among the Elderly

Most of the applications need the user to login before they can continue browsing. Hence, password management among the elderly also needs attention. The age factor also contributes to this matter. For example, in this age, they tend to use simple passwords rather than the complex ones. The complex combination of passwords makes it hard for them to memorize especially if they have health problems like dementia [17],[18] Consequently, they prefer to use easy 'remember' or common words as their passwords. Plus, they tend to use the same password for each application they have.

2.4 Internet Skills Among the Elderly

The "skills gap" problem of the older people and the problem of social exception from the information society has been reduced at the workplace. Working with the elderly "promotes social change, problem-solving in human relationships, and the empowerment and liberation of people to enhance well-being" [19]. The evolution of hardware and software also contributes to the gaps. Some of the elderly do not know how to use their browsers

properly. In addition, they do not know how to adjust security settings on their device, managing browsing history, clearing cache, and Internet cookies [20].

2.5 Cybersecurity Awareness Among the Elderly

Cybersecurity awareness is significant for the elderly as a preventive step to fight cyberattacks [4], [18]. Without knowing the right ethics online and awareness on cybersecurity among them, they are easily exploited by attackers. Many cases have been reported on the impacts of being compromised. For example, [21] explained that the identity theft victims among senior citizens suffer shocking effects [21] including the

- Loss of all their life savings
- Disgrace for being victims
- Diminished self-confidence
- Exacerbated illnesses to include premature death

Having said this, it is very important to educate them about the awareness which can avoid the elderly from being targeted to the most common forms of cyberattacks; besides, it can be used as a guide while surfing on the Internet.

3. REVIEWS ON CASE STUDIES ON CYBER-ATTACKS ON THE ELDERLY

Cybercriminals preying on the elderly has become a serious problem nowadays. This is due to a lack of cyber awareness among the elderly and proneness to possible cyber threats. According to [16], there are four common types of cyber-attack used on the elderly in 2020. The cyber-attacks include phishing, behavioural attack, consumer attack, and identity theft. The elderly are the most targeted internet users by the fraudsters and cybercriminals. The elderly can be categorized as the most vulnerable targets among the online scammers.

A. Phishing Scams

Phishing is the spoofing of Internet websites or emails intended to trick users in providing sensitive information [22]. A study by [23] was conducted to determine whether elderly people are more prone to computer-based phishing attacks.
It was reported that 53.47% of the older adults were possible in becoming the phishing attacks' victims, twice the younger adults which was 26.37%. Meanwhile, 47.47% of the older adults were prone to phishing attacks and more likely to let their guard down often while at home. The research shows that the elderly was at high risk of phishing attacks.

Most phishing techniques take in the use of social engineering and language manipulate the emotional reactions such as fear and curiosity. Phishing may use a medium such as voice call, sending an SMS, and through emails. According to the FBI's IC3 2018 Internet Crime Report, the most growing fraud crime is the tech support fraud which had caused the public to lose about $39 million total in 2018. The most reported victims were people over age 60 [24].

B. Romance Fraud

According to CyberSecurity Malaysia, the existence of many online dating applications has increased the number of scamming incidents due to thousands of users' data are being at the scammer's fingertips. Usually, the scammers initiate the relationship with the victim online and start to build trust among them. Senior citizens become the target because they may be less knowledgeable and lonely.

One of the scamming techniques is by luring the victims with expensive parcel deliveries and persuading the victims to transfer an amount of money [16]. CyberSecurity Malaysia released a statistic on Spam in between January to March 2020 indicating that there is a 93% increase in reported cases compared to 2019. Furthermore, a statistic shows that there is an increasing number of reported cybercrime incidents for January to March 2020 (34%) compared to the same period in 2019. Based on the increasing trend, it can be concluded that cyber incidents are one of the biggest issues in Malaysia and the elderly can be categorized as a vulnerable group of users that needs attention and education on cyber awareness in order to prevent them from falling as cyber-attack victims.

Based on the FBI's IC3 report, in 2018, romance fraud was the seventh most reported fraud and became the

second most costly scam in terms of victim loss and complaint received. The actor uses a trust-based relationship with the elderly victim as one of the deceiving techniques. The criminals claim themselves to be either one of the victim's family members or love interest. The criminals build the relationship to convince the victim in providing personal and financial information, to launder money unknowingly and to give money or buy expensive gifts. This monstrous cybercrime most commonly targets lonely elderly women, including recently widowed.

C. Identity theft

According to [19], identity theft may occur in many forms including medical identity theft, identity tax refund theft, and Social Security theft. It may occur without engaging a victim, through an online platform or even over the phone. The fraudster will use any possible methods to steal the victim's information as per examples:

1. Medical identity theft:

A criminal uses the victim's insurance or medical card information to pay services, make fraudulent payments or even make a fake service charge and pocket the money. This causes the victims potentially to be in a high debt risk and in charge of thousands of dollars. Therefore, qualifying for insurance will be difficult in the future, due to the link of the victim's information and the imposter's health record.

2. Identity theft tax refund fraud:

This type of identity theft involves fraudulent tax returns caused by the criminal. The imposter either steals the victim's personal and financial information or forces the victim to provide the information. The imposter makes a claim on the tax refunds by submitting the fraudulent tax returns on behalf of the victim. According to the U.S Senate Special Committee on Aging, in 2016, this type of identity theft and fraud cost $1.7 billion losses.

3. Social Security theft:

Social Security theft is the most common type of administration phone scams in the U.S. Nowadays, it has started to become dangerous and aggressively scamming the elderly. Through this technique, the criminals convince the victim about fraudulent activity that involves the victim's Social Security number. The criminals would claim that they are from the authority and threaten the victim with false law charges if they do not follow certain demands. Other consequences in getting the victim's personal information is, the imposter may steal the victim's income payment.

These case studies showed various examples of cyberattacks that targeted the elderly. The next section will review the cybersecurity awareness among the elderly which may help prevent the elderly from being exploited and compromised.

4. REVIEWS ON CYBERSECURITY AWARENESS AMONG THE ELDERLY

Cybersecurity is a process of protecting and recovering the computer systems, networks, devices, and programs from any type of cyberattack while cybersecurity mindfulness includes informing the Internet clients of online protection issues and dangers, just as improving their comprehension of digital dangers so they can be completely dedicated to grasping security when they utilized the web. Cybersecurity is important as it will ensure that sensitive data and personal information from the misuse of cybercriminals. Usually, the cybercriminals target the elderly because they lack knowledge and awareness about cyber risks. Therefore, the elderly need to be more alert and aware of the dangers and risks of involvement in the cyber world in their daily life [26].

4.1 The Importance of Awareness for the Elderly

Due to age-related problems, the elderly might be easier to be compromised by attackers by sending them a 'trust' message that looks legitimate to the elderly. Without delay, the elderly will send the attacker their personal data including financial and medical information. Therefore, cyber security awareness is important for the elderly. The awareness can be delivered in terms of campaigns using videos or activities. Through this, the elderly can have better understanding and embrace the security of the Internet user, especially the threats of using the Internet. Hence, the governments and the communities should work together in ensuring that the elderly are fully aware of the potential dangers such as phishing attacks and using unsecured Wi-Fi networks, as well as how to lessen the impacts of cyberattacks.

Without any prevention strategy, the elderly might become compromised, their identity gets stolen, and they will suffer a few consequences as mentioned in Section 2. Therefore, an effective approach will give a huge impact on the elderly's lives, especially during the COVID-19 pandemic whereas the cybercrimes are escalating rampantly and causing utter chaos to the cyber world [27].

Up to this knowledge, there is no specific awareness created for the elderly and most of the literature did list out the do's and don'ts for this group of users. Determination on the types of cyber privacy and security awareness that could be important for the elderly. There are six factors that could persuade the information security behaviour which are i) knowledge, ii) impact, iii) severity, iv) controllability, v) awareness, and vi) possibility. To cope with this issue, awareness regarding this issue should be gained [21].

4.2 Recommendations for the Elderly

One of the preventive strategies is through education. Educating through the internet is one of the effective initiatives especially for the everyday internet users. Even though most of the survey participants have a very least amount of knowledge in cyber threats, some of them still being a victim of cybercrime. Cyberthreats are quite concerning since it could affect professional life and personal life. Many participants were interested to learn further regarding cybersecurity and some also demanded more advanced seminars and suggested that each employee should at least have some knowledge about cybersecurity [30].

Thus, a follow-up survey was conducted to know more about the idea of cybersecurity among the elderly whether it is interesting or just trivial for them [28]. To reduce the risk among the elderly, there are seven recommendations that might help the elderly to stay safe online:

Keep updating software – Installing and using anti-virus and anti-spyware software is an essential top to protect the elderly online. The program that is installed properly is critical and running updates on a regular basis. It is important to ensure the new threats are mitigated. Besides, keeping computers, tablets, and mobile devices updated from time to time is vital as it protects users from bugs and provides software patches to protect from hackers.

Secure access to accounts – To avoid attackers stealing personal information, the elderly must enable two-factor authentication where it is offered and avoid sending or sharing personal information to strangers. It is also important to use a strong password and avoid common words, date of birth, ID number, or any guessable word. Strong passwords are a combination of a mix of upper/ lower case, numbers, and symbols.

Think twice – Email is one of the methods that attackers commonly use to steal information from the elderly. Users should avoid responding to emails asking for personal information. Besides, they should also ignore any suspicious link in the email even if it claims that it is sent by financial institutions as legit financial institutions never request customers to reply or send any information through emails. Always call and discuss any issues with the bank if there is any arising problem.

Online shopping activities and accessing social media safely – Do online shopping activities on trust. Often read other reviewers' comments and rating before proceeding to checkout. In addition, the elderly that use credit cards should never share their card details and CVV number with anybody. The same goes for social media accounts where cybercriminals can easily pose as a 'friend' on social media websites, like Facebook. Users should avoid sharing any confidential information as the fraudsters can steal and gain access to users' social media accounts by posing as another person to create a fake account and become an impostor.

Support System – If they need help, they should refer a trusted institution, for example, by phone calling bank's customer service upon any confusion if an email, communication, or transaction looks wrong. They should also keep updating themselves with cybersecurity awareness as it can help to educate the elderly about known scams and tactics for staying cautious and gain more confidence using the technology.

Adjust browser safety settings – Adjusting the browser settings and set for maximum security level are also vital. Elderly users should consider clearing browsing history after every time they use a browser.

Signing out – The elderly users should also be reminded to log out of apps and websites after they are done using it as leaving the apps and websites open on the computer screen may expose the user to vulnerable security and privacy risks.

5. THE PROPOSED FRAMEWORK

After the synthesizing process, the findings were gathered using the triangulation method and the awareness framework for elderly is proposed as depicted in Fig.1. These factors are significantly important to ensure the awareness level among elderly at the optimal level. Hence, it will help minimize cybercrime cases among the elderly.
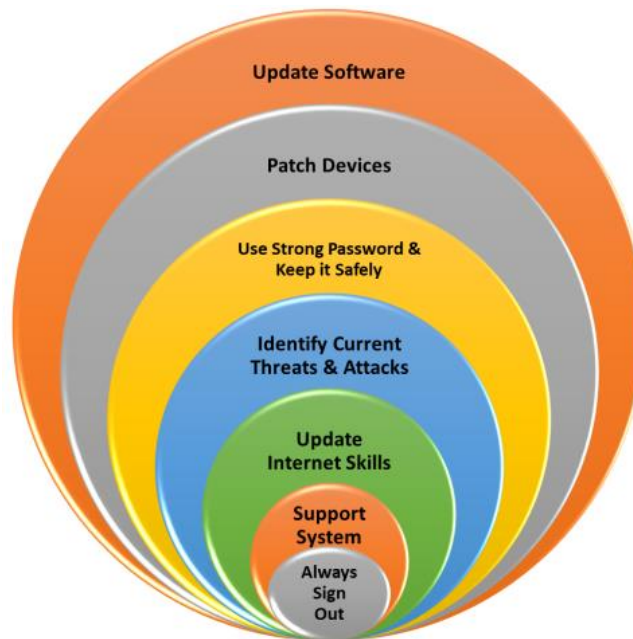

Fig.1 Cybersecurity Awareness Framework for the Elderly

The framework was further validated by digital experts and practitioners. Questions were asked to what extent they agree/familiar/aware with the statements/ questions associated with factors. After completed the designing of the questionnaire, the validity and reliability tests were considered to ensure the statements measure the factor accurately [29].

6. CONCLUSION

This paper presents a review on cybersecurity issues and challenges for the elderly. After synthesizing the literature, seven awareness factors were identified. By using a triangulation methodology, it combines several techniques to study the same research area. It is useful in exploring and discovering the overlaps and differences in an area subject. Further investigations need to be carried out in the future to test the effectiveness of the framework in a large-scale environment.

ACKNOWLEDGEMENT

REFERENCES

1. Craigen D, Diakun-Thibault N, Purse R. Defining cybersecurity. Technology Innovation Management Review. 2014;4(10).
2. Chang FR. Written Testimony of Dr. Frederick R. Chang Bobby B. Lyle Centennial Distinguished Chair in Cyber Security Southern Methodist University

Nurul Huda Nik Zulkipli[1], Nor Aimuni Md Rashid[2], Anwar Farhan Zolkeplay[3], Alya Geogiana Buja[4]

3. Nocentini A, Calmaestra J, Schultze-Krumbholz A, Scheithauer H, Ortega R, Menesini E. Cyberbullying: Labels, behaviours, and definition in three European countries. Australian Journal of Guidance and Counselling. 2010;20(2):129.

4. Blackwood-Brown, C., Levy, Y., Terrell, S. (2016). Senior Citizens and Cybersecurity Awareness.

5. Munanga A. Cybercrime: A new and growing problem for older adults. Journal of Gerontological Nursing. 2019 Jan 29;45(2):3-5

6. Leiber, N. (2018, May 3). How criminals steal $37 billion a year from America's elderly. Retrieved from https://www.bloomberg. com/news/features/2018-05-03/america-selderly-are-losing-37-billion-a-year-to-fraud.

7. Hardin, E., and Alia Khan-Hudson. "Elder abuse--"society's dilemma"." *Journal of the National Medical Association* 97 1 (2005): 91-4.

8. Kratcoski PC, Edelbacher M. Trends in the criminality and victimization of the elderly. Fed. Probation. 2016; 80:58.

9. Siponen MT. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Management & Computer Security. 2000 Dec 1.

10. Abd Rahim NH, Hamid S, Kiah ML, Shamshirband S, Furnell S. A systematic review of approaches to assessing cybersecurity awareness. Kybernetes. 2015 Apr 7.

11. Iyer R, Eastman JK. The elderly and their attitudes toward the internet: the impact on internet use, purchase, and comparison shopping. Journal of Marketing Theory and Practice. 2006 Jan 1;14(1):57-67.

12. Claar CL, Johnson J. Analyzing home PC security adoption behavior. Journal of Computer Information Systems. 2012 Jun 1;52(4):20-9.

13. Joel Holmberg (2019, January 23). Real Facts about the Elderly and the World Wide Web. Retrieved from https://axesslab.com/real-facts-about-the-elderly-and-the-world-wide-web/.

14. Carlton M, Levy Y. Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In Southeast Con (2015) 2015 Apr 9 (pp. 1-6). IEEE.

15. König, R., Seifert, A. & Doh, M. Internet use among older Europeans: an analysis based on SHARE data. Univ Access Inf Soc 17, 621–633 (2018). https://doi.org/10.1007/s10209-018-0609-5

16. S. Boral, 4 Most Common Cyber Attacks Used Against Older People in 2020, 2020. Accessed on:09.29,2020[Online]. Available: https://www.maketecheasier.com/common-cyber-attacks-used-against-senior-citizens/

17. Nurse, Jason. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. 10.1093/oxfordhb/9780198812746.013.35.

18. Blackwood-Brown CG. An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills.

19. Carlson EL. Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow. Elder LJ. 2006; 14:423.

20. Grimes GA, Hough MG, Mazur E, Signorella ML. Older adults' knowledge of internet hazards. Educational Gerontology. 2010 Feb 11;36(3):173-92.

21. Jones, T. L. (2001). Protecting the elderly. Law & Order, 49(4), 102-106.

22. N.Z. Othman, (2020, February 14). #TECH: Many lonely hearts are still falling for online fake lovers. New Straits Times. Retrieved from http://myjms.moe.gov.my/index.php/ajress https://www.nst.com.my/lifestyle/bots/2020/02/565459/tech-many-lonely-hearts-arestill-falling-online-fake-lovers

23. Zhao R, John SE, Karas S, Bussell CA, Roberts J, Six D, et al. The highly insidious extreme phishing attacks. Proc IEEE Int Conf Comput Commun Networks (ICCCN); 2016.

24. Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of

25. executive functioning. PloS one, 12(2), e0171620. https://doi.org/10.1371/journal.pone.0171620

26. C. Crane, 3 Cyber Fraud Tactics Targeting Seniors and Why They are So Effective. CyberCrime Magazine,2019. Accessed on:09.29,2020[Online]. Available: https://cybersecurityventures.com/3-cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/

27. Swee-Leng, O.T., Vergara, R.G., Khan, N., Khan, S. (2020). Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia, Asian Journal of Research in Education and Social Sciences, Vol. 2, No. 2, 72-76.

28. Morgan, J. A. (2015). Exploring Senior Citizen Perceptions of Their Cyber Data Privacy and Security (Doctoral dissertation, Capella University.

29. Breitinger, F., Ricci, J., Baggili, I. (2018). Survey Results on Adults and Cybersecurity Education. Education and Information Technologies, 24(1), 231-249.

30. Field A. Discovering statistics using spss. Vol. 1, Sage Publications. 2009. 1689–1699 p.

31. Choo KK. The cyber threat landscape: Challenges and future research directions. Computers & security. 2011 Nov 1;30(8):719-31.