Study among Rural area citizen regard to Cyber Security awareness & Factors relating to it

1Senthuran Nallainathan
1Software Engineer
1Self-Employed

Abstract - **Cyber Security is an emerging topic in today's world, but still the rural area security concerns are left behind. Cyber security awareness among rural area Vavuniya of Sri Lanka was studied in depth with yielded new findings and recommendations made to alleviate this issue. Rural area awareness was found to be high in a very general level, but application of such security prevention principles in their day-to-day life were extremely low. 2FA (Two Factor Authentication) awareness was only one-tenth of the population. There was significant positive co-relationship with Marital status (single) and Educational attainment, while negative co-relationship with age. Improving educational levels, organizing cyber security programs for professionals, housewives, retirees and pensioners were recommended to improve rural area cyber security awareness.**

keywords **- cyber security, rural area cyber security awareness, cyber security awareness, sri lanka cyber vulnerability, Vavuniya cyber vulnerability**

I. Introduction

Cyber Security is an emerging field in Computer Science. While many consider it in an industrial and urban context, Rural Areas Security issues and vulnerabilities are left behind. Cyber-attacks have seen rise during the past few years [1]. Cyber terrorism without physical invasion is the new trend with incidents increasing [2]. These show the importance of research in this sector. This research will assess the awareness level, availability of instructors, applicability and factors affecting their awareness and vulnerability found in and produce recommendations to address vulnerabilities found in rural areas. The factors which significantly co-relate to the awareness among rural area citizens are studied further. Rural areas are left behind who are expected to have reduced cyber security awareness and this will possibly adversely impact national security as a whole due to loopholes of rural areas. The objective is to understand the awareness levels and the understanding and knowledge of key cyber security principles including strong password usage, strong password characteristics and 2FA (2 Factor Authentication) implementation to any of their accounts. Cross-factorial analysis whether even if awareness is present, whether they are applied in their day-to-day practice (such as knowing 2FA, and using 2FA in any of their accounts).

II. Literature Review

In the recent past, there were very significant cyber security threats [1] which had gone far as taking lives in a hospital setup [3], which was solely due reliance of computer systems in healthcare [4] and the vulnerability of the existing systems. Critical aspects and importance on cyber security importance highly vulnerable rural areas are available [5]. In addition, the significant issues in Rural America were discussed by O Brien, and the impact of such cyber security threats which could cause something more than money, the people's lives [6].

Texas and Baltimore were affected due to cybersecurity threats which explains the fact that regardless of how large and developed the country is (i.e. United States) the periphery areas (i.e. rural areas) are prone and susceptible to cyber security threats [7]. The above literatures show the significance and importance of vulnerability awareness assessment especially among rural area residents.

Research onto overall citizens including rural areas of South Africa was performed while in-depth factorial analysis wasn't made [8]. The above discussion explains the knowledge gap in this field and the room for this research.

Internet natives [9] are more cyber security aware based on South African context [10] and awareness levels among countries and their co-relationships analyzed but Moti [11]. These lacks the study into Sri Lankan context and none of them considered Asian countries. [12]'s research in Sri Lanka during COVID-19 phase where online learning took prominence found out that forty-five percent of the university students lack awareness of the cyber security. This shows the significance of the issue while the research only emphasized university students and not rural areas.

III. Methodology

Due to rural area participants who are capable of using social media and other basic messaging applications (WhatsApp, Viber) but based on observation are still not tech savvy and aren't capable of filling out an online questionnaire, while finding and communicating with them through online medium has practical difficulties too, thus manually printed questionnaires issued and collected in their mother tongue (Tamil, English & Sinhala) for greater understanding and improved accuracy. Participation rate was lower in online mediums, due to personal communication and obligation not present in the participant's side, so printed questionnaires were handy.

Physically printed questionnaires were distributed and then collected and digitalized through data-entry, with re-checking to ensure reliability and accuracy of digital data. The data was then analyzed using advanced MS Excel functions and SPSS software.

Population size was 189,000 calculated based on average growth rate from last census year, while sample size stood at 320 and 450 questionnaires issued considering the rejection rate.

Age Group, Gender and Rural Area percentage were measurable external factors [13] while proportionate distribution was essential to understand the cyber security awareness and application among diverse range of rural population. Stratified sampling methodology used to cover all external factors such as Age Group and Gender proportionately. Equal distribution among population were effectively managed by issuing and calculating in 100 questionnaire group sets.

The research was performed in rural district Vavuniya, which is situated in the 30 year long civil war affected area of Sri Lanka, the northern province. Statistical significance and applicability of this results between rural areas within Sri Lanka were analyzed while applicability on similar areas in the World are possible with further applicability analysis.

Factor analysis including demographics and inter-variable analysis were performed through Digital softwares mentioned above to derive findings & come up with conclusions.

IV. Conceptual Framework

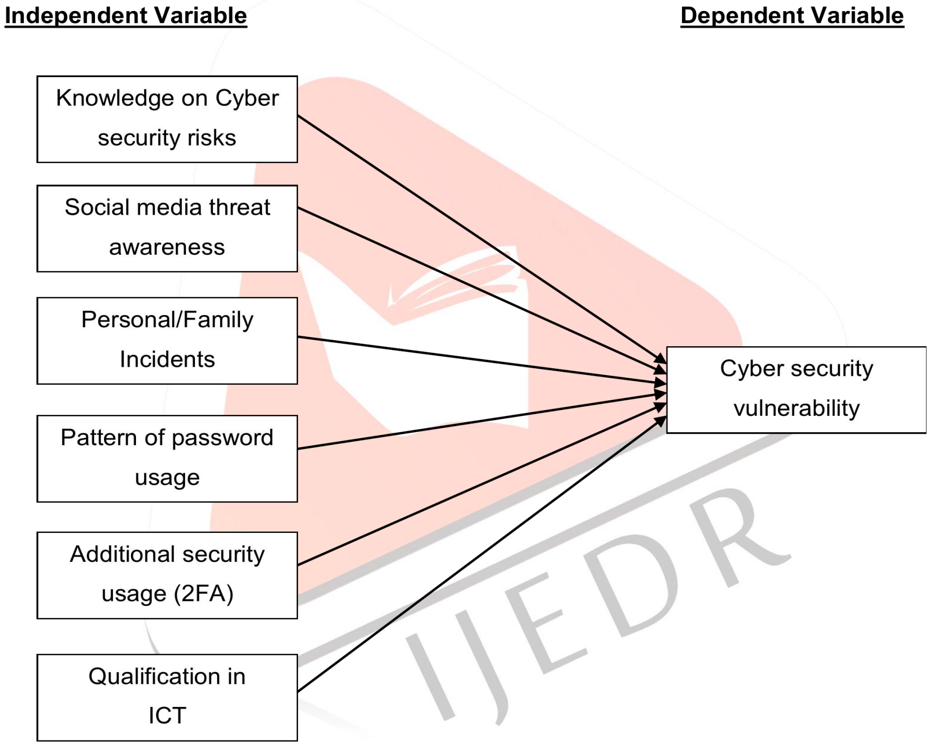

Independent Variable
Dependent Variable
Knowledge on Cyber security risks
Social media threat awareness
Personal/Family Incidents
Pattern of password usage
Additional security usage (2FA)
Qualification in ICT
Cyber security vulnerability

Figure 1 - Conceptual Framework

V. Distribution Plan

Gender Distribution Plan

Table 1 - Gender Distribution

Gender	Expected (should be)		Actual		Deviation
Male	200	49.20%	202	49.63%	+2 (+0.43%)
Female	207	50.80%	205	50.37%	-2 (-0.43%)

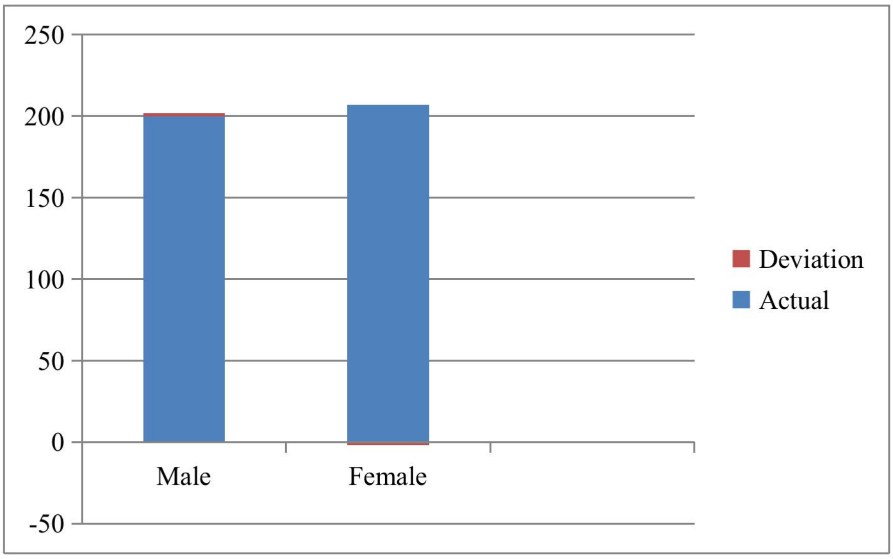


Figure 2 - Gender Distribution Graph

Age Distribution Plan

Table 2 - Age Distribution

Age Group	Percentage of Population	Expected to Collect	Actually Collected	Deviation
15-19	14.47%	59	59	0
20-29	23.39%	95	95	0
30-39	20.59%	84	84	0
40-49	16.42%	67	67	0
50-59	13.15%	54	54	0
60-69	7.88%	32	32	0
70-79	3.03%	12	12	0
80+	1.06%	4	4	0

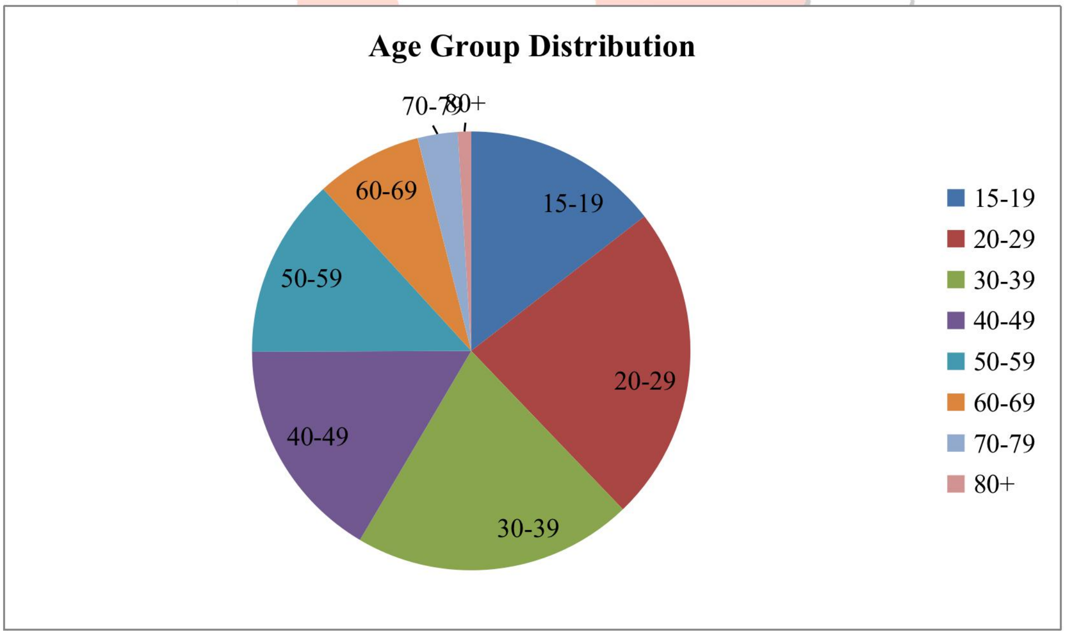
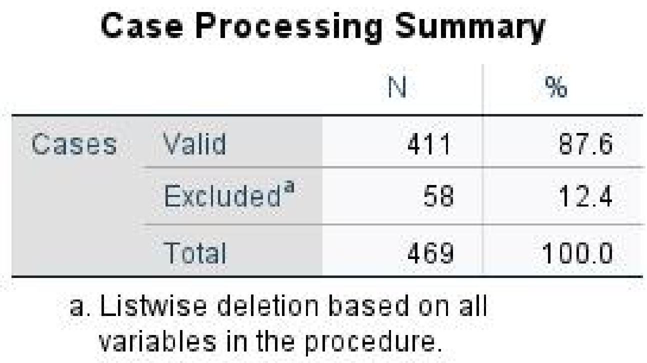


Figure 3 - Age Distribution Graph

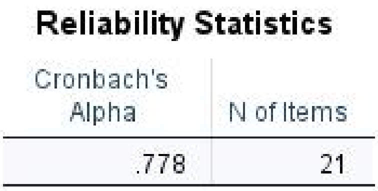
VI. Data Analysis & Findings



Case Processing Summary

		N	%
Cases	Valid	411	87.6
	Excluded[a]	58	12.4
	Total	469	100.0

a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	N of Items
.778	21

Above 0.7 Cronbach's Alpha value shows this study is reliable. 82.3% had cyber security and more than 50% of them perceived cyber threat as dangerous (4 or more, in a scale of 5). 25% were actually been victimized themselves and 20% had their friends or families accounts being hacked while 58% have discussed cybercrime & threats within their friends and family.

74% had read about serious cybercrimes through newspapers and shared messages (cybercrime news penetration to rural areas), almost half the population feels surveillance during usage of social media.

Applicability of cyber security safety principles to prevent vulnerability was assessed which shows almost half the population use the same password for more than one account, one-fifth use less than 8 characters as password which makes it more vulnerable to brute force attacks [14] [15].

Only alphabet or only number-based passwords are used by 72% of the population and almost half the population do not use capital letters in their passwords, four-fifth do not include special characters in their passwords.

This shows even high awareness (86%) is present, its only general in nature and there is no applicability of prevention mechanisms, even though they feel surveillance and rates cyber threat very dangerous. This could be lack of complete understanding, practical aspects of prevention aren't covered, reduced access to IT instructors and also could be due to ignorance and negligence of people. This also shows the lack of enforcement by social media and major internet service companies who do not enforce good password policy, which leads to people being able to create accounts with weak passwords.

New technologies such as 2 Factor Authentication (2FA) is only known to 10% of the population and those who knew it implemented it into at least one of their accounts. Three quarter of the 2FA known people use it in all of their accounts, while the rest found it inconvenient to use 2FA due to need of two devices. This shows penetration of 2FA and new cyber prevention technologies are very low (only 10%) and most of them are complying with such security measures if informed. This rule out ignorance and negligence of the population, and shows lack of awareness of new technologies has led to reduced cyber security prevention method application.

Eighty percent agrees to use a stronger password if they were instructed of such and the rest were found lazy of doing so due to the complexity of typing in longer, complex passwords during authentication.

57.5% had access to IT Instructors (when interpreting this data, this is actually affected by age group) and almost all of them agrees to abide by the instructions given by their IT Instructors. While 56.8% had learnt ICT at academic level of NVQ Level 3 (RQF Level 3 equivalent) or above. This shows almost all of the people who had access to IT Instructors was because they had studied at ICT at schools or thorough IT courses. So, the general public, and aged population (who completed schooling before IT was introduced in schools) lacks IT Instructors affecting their Cyber security skills and making them vulnerable.

Inter-variable analysis found that younger population has more awareness levels and have applied excellent cyber security prevention mechanisms in their day-to-day lives re-enforces the fact of learning IT at school, and more access to IT education gives them an edge in cyber security awareness and prevention over the older age people, especially this is applicable for population within 15-29 age group. Females had more general awareness on Cyber Security but practical application of it was significantly higher in their male counterparts.

Marital status plays a role in Cyber security awareness levels, where Singles were having higher Cyber security awareness and application of such principles, this analysis is distorted by the fact that Singles were usually younger.

One of the significant finding of this research was that with increasing overall educational achievement, the cyber security awareness and application of it increased significantly. It was found to be around 1.5 times higher of people who completed a Bachelor's degree or higher opposed to people who had only completed Olevel.

VII. CONCLUSION

In conclusion, general cyber security awareness was high where the concepts and significant recent news were understood by many and due to high penetration of such news into rural areas many had such knowledge. But still overall applicability of cyber security principles was extremely low such as knowing 2FA, this shows application of cyber security principles were lower (e.g. newspapers explain the news but don't explain how to prevent it).

Younger population had more application of prevention methodologies and general awareness while education attainment level shows positive and marital status (single) exhibit positive co-relationship.

Inconvenience factor due to 2FA and complex passwords were found to be of minimal impact during the decision-making process of security policy of people with regard to their own accounts.

Significant number of population (i.e. one quarter) are being victimized (i.e. hacked or blackmailed) among the rural area citizens, which shows the current issue prevalent in rural areas.

VIII. Recommendations

The lacking of cyber security awareness and prevention mechanism implementation is found to be severe in people over the age of 30. This current identified issue could be sorted by introducing general public programs to improve cyber security awareness levels through programs (such as including 2FA content, importance of strong passwords etc.) for professionals, housewives, retirees and pensioners. This could be funded by interested parties, well-wishers, NGOs and/or by the Government.

Even who had much knowledge and general awareness in cyber security through newspapers and other shared messages they didn't have the capability to use preventive mechanisms, so media can play a major role. If such medias are informed of such benefits to greater public, they could include preventive mechanisms and how to implement them in their articles with examples and consultation from cyber security experts.

As educational attainment has positive impact, it will be valid to consider improving the population's education levels and promoting them to study further which will likely improve cyber security awareness of them and also a greater good for themselves and society as a whole.

If the recommendations were applied effectively, it would be possible to alleviate the current cyber security threats present in rural area population.

References

[1] D. O. Thomas W.Edgar, "Chapter 3 - Starting Your Research," in *Research Methods for Cyber Security*, Burlington, Syngress, 2017, pp. 63-92.

[2] N. Myers, "Cyber Security: Cyber Crime, Attacks and Terrorism," *ODU UN Day 2020 Issue*, pp. 1-13, 2020.

[3] ALJAZEERA, "Ransomware cripples US emergency services, local governments," 21 10 2019. [Online]. Available: https://www.aljazeera.com/economy/2019/10/21/ransomware-cripples-us-emergency-services-local-governments/.

[4] K. Collier, "Cleveland-area hospital goes offline after apparent cyberattack," 30 09 2020. [Online]. Available: https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408.

[5] RHIhub, "Health Information Technology in Rural Healthcare," 09 11 2020. [Online]. Available: https://www.ruralhealthinfo.org/topics/health-information-technology.

[6] J. Wivoda, "Cybersecurity Threats in Rural America : How to Protect Your Critical Access Hospitals," 2016.

[7] L. O'BRIEN, "Cybersecurity for Rural Communities is Often Neglected," 20 12 2019. [Online]. Available: https://www.arcweb.com/blog/cybersecurity-rural-communities-often-neglected.

[8] M. &. D. Z. &. N. S. &. L. W. Grobler, "Towards a Cyber security aware rural community," 2011.

[9] e. Robert B Mellor with Gary Coulton, Entrepreneurship for Everyone: A Student Textbook, London: SAGE, 2009.

[10] P. E. Kritzinger, CYBER SECURITY AWARENESS AND EDUCATION RESEARCH, Gauteng: University of South Africa, 2020.

[11] G. K. D. L. Ł. W. F. C. a. H. N. B. Moti Zwillinga, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *JOURNAL OF COMPUTER INFORMATION SYSTEMS*, pp. 1-15, 2020.

[12] e. Ruwan Nagahawatta, "A Study of Cybersecurity Awareness in Sri Lanka," in *Australian Cyber Warfare*, Melbourne, 2020.

[13] CityPopulation.de, "VAVUNIYA," 25 02 2021. [Online]. Available: http://citypopulation.de/en/srilanka/prov/admin/northern/43__vavuniya/.

[14] J. S. B. B. L. Bošnjak, "Brute-force and dictionary attack on hashed real-world passwords," in *International Convention on Information and Communication Technology, Electronics and Microelectronics*, 2018.

[15] M. I. M. S. a. W. H. Mudassar Raza, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," *World Applied Sciences Journal* , pp. 439-444, 2012.