The Impact of Socioeconomic and Digital Inequalities in Cybersecurity in Higher Education

Jason W. McCarthy

Old Dominion University School of Cybersecurity

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

November 26, 2024

Table of Contents

The Impact of Socioeconomic and Digital Inequalities in Cybersecurity in Higher Education

Introduction

In developing countries, access is less than the expectation of well-developed countries like America. Healthcare is different, education is different, and job opportunities are different. When it comes to the digital landscape, often, few offerings are available. Wireless connectivity may not be widely available, and there will not be a wide variety of devices or manufacturers to choose from at first. As a nation develops, it takes time for everyone to be on the same page. This article review looks at differences in cybersecurity practices of students, their behavior, and the differences between genders in higher education in Pakistan, and their socioeconomic backgrounds. This study seeks to highlight the concerns of socioeconomic divides in relation to making use of good cyber hygiene in a developing country and to note the differences in cybersecurity practices between genders as an inequality.

Research methods

In previous studies, the researchers had difficulty in administering techniques like surveys due to the digital divide that exists in Pakistan. The study that was done works to address the digital divide and socioeconomic differences in its methodology. This study in particular makes use of a quantitative methodology. A question survey was administered using pencil and paper to measure computer and smartphone cybersecurity behaviors using existing scales (Khan et al., 2024).

For computer behavior, the Security Behavior Intention Scale was utilized. Smartphone security behavior was assessed by looking at three different behaviors. The first behavior is avoiding harmful smartphone behavior. The second behavior is that of using protection like add-

on utilities on smartphones. The last looks at actions taken for disaster recovery (Khan et al., 2024).

Several demographic variables were collected for this study. These variables include age, gender, department, and province. The number 1 represents ages 18 through 21, while 2 represents all ages above 21. No age below 18 was taken. The departments used a similar mechanism with It related fields getting a code of 1, medical or biological getting 2, 3 for business, and 4 for others. The study was conducted across 3 provinces. Other variables included and measured in the survey include digital divide, looking at frequency of internet access and internet access from different places, and socioeconomic differences looking at the status, residence, and poverty stratum of the respondents (Khan et al., 2024).

The sampling strategy used the Multidimensional Poverty Index. Districts that had a university were made note of, and then the universities were chosen at random to participate in a way that ensured that the results of the study were geographically distributed. Ethical concerns were address by the study assuring students that they would remain anonymous at the time of submitting their answers to the survey (Khan et al., 2024).

Research Questions Posed

Pakistan currently has 222 institutions of higher education with a total enrollment of 1.5 million coming from different backgrounds that experience disparity when it comes to what digital resources, they have access to. These students are typically victims of cybercrimes including harassment and blackmailing (Khan et al., 2024). This would not be such an issue if the institutions they attended took the initiative to raise awareness and educate their students on safe internet usage. The study asks several research questions revolving around students at these institutions. One of them asks what the computer security behavior of the students enrolled in

Pakistan is. The following asks what the smartphone security behavior of these students is. The third asks about the differences in cybersecurity behavior between the students coming from the different socioeconomic backgrounds and digital disparities. The last seeks to determine if there is a difference in smartphone security between these students coming from different upbringings (Khan et al., 2024).

Cybersecurity Practices alongside Gender and Socioeconomic Differences

The computer security efforts of female students were found to be lower than that of males. One such practice is caution in clicking on links from items like emails. Additionally, the study showed that students from the medical field showed lower usage of security habits. The medical field is a field that is largely dominated by women. Across all students, It was found that thirty-eight percent do not make use of the screen lock function and over sixteen percent do not lock their screen while away from the machine. Additionally, around forty percent do not look at the link of a website to see where they are going when using a web browser or when one is activated to make sure the link that they are going to is legitimate (Khan et al., 2024).

The smartphone security habits between men and women also vary. Women are not confident in their technical ability and women are less likely to grant third-party applications access to their personal information (Khan et al., 2024). Taking that stance is a good thing. Students in general who accessed the internet from different places using their smartphones exhibited better cybersecurity practices. Students who did not have great access to internet as opposed to those who are financially better off, exhibited better safety practices such as not handling financial information or transactions, not giving too much permission to sites or apps, being cautious downloading apps, and their practices when it came to connecting to insecure wireless internet. Across all students, it was discovered that forty-five percent don’t logout when

they are finished using their email or social media accounts. Forty percent of the students don't disable their GPS trackers or make use of anti-malware software. Lastly, when looking at Wi-Fi usage, it was discovered that over three quarters of the students make use of free to use networks. Most free networks are known to be unsecured and offer little to no security (Khan et al., 2024).

Based on a study that took place in the U.K., individuals from higher socioeconomic backgrounds tend to exhibit better cybersecurity practices than those from lower socioeconomic backgrounds (Khan et al., 2024). This socioeconomic factor plays a heavy role when determining access. Those of higher status or from wealthier families can afford better security software and training than those from not so well-off families or backgrounds. The question is how we make up for such a disparity in developing countries so that everyone can benefit from the same resources instead of being on an uneven playing field. There is the possibility that not everyone who is well off will want to do the right thing and may use this edge to take advantage of those who don't have the same tools.

Conclusion

Nations that are better off and not still developing will always have better access than countries that are still working towards the goal of better cybersecurity. While those nations can contribute resources to help countries like Pakistan and others that are still developing, it would be unethical for those countries to put their own people at any kind of disadvantage by doing so. As a global society, we should all be working to find solutions that tear down socioeconomic and gender-based divides so that we can come closer to achieving better access to and use of cybersecurity for all who make use of cyberspace and what it has to offer to the global community. By doing so, everyone can have some kind of protection against the cyber threats that face all of us.

References

Khan, N.F., Ikram, N. & Saleem, S. Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Secur J* **37**, 214–244 (2024). https://doi.org/10.1057/s41284-023-00375-4