Security Journal
https://doi.org/10.1057/s41284-023-00375-4

ORIGINAL ARTICLE

Effects of socioeconomic and digital inequalities on cybersecurity in a developing country

Naurin Farooq Khan[1] · **Naveed Ikram**[1] · **Sumera Saleem**[1]

Accepted: 7 April 2023

Abstract

In developing countries, increased reliance on cyberspace for carrying out educational activities has implications for cybersecurity threats. In the light of stratification model of diffusion of technologies, socioeconomic and digital disparities are reproduced in the use of digital knowledge and skills. Cybersecurity is a digital skill that is affected by socioeconomic and digital inequalities; specifically in the developing nations. With lack of digital divide's empirical evidence in terms of cybersecurity, this study employs a face-to-face survey to understand the computer and smartphone security practices of students enrolled in higher education institutes (HEIs) across Pakistan. A multi-stage stratified sampling technique was used to recruit a sample of 758 participants located in socioeconomically and geographically diverse cities in the country. Analysis was carried out using descriptive and Pearson's Chi-square statistics. The results show lax cybersecurity behavior of students both on computer and smartphone devices. Significant differences were found in the cybersecurity practices of students in terms of socioeconomic and digital divide variables. This highlights that the individuals with lower socioeconomic status and who are digitally less connected are at a greater risk of falling victims to cyber-threats. The implications of the study state to impart tailored cybersecurity trainings with respect to digital divide and socioeconomic status of the students.

Keywords Cybersecurity awareness and behavior · Computer security · Smartphone security · Higher education institutes · Digital and socioeconomic disparities

✉ Naurin Farooq Khan
naurin.zamir@riphah.edu.pk

Naveed Ikram
naveed.ikram@riphah.edu.pk

Sumera Saleem
sumera.saleem@riphah.edu.pk

[1] Faculty of Computing, Riphah International University, Islamabad, Pakistan

Published online: 22 April 2023

Introduction

The advancement of ICTs has brought with it the new opportunities; however, it has also increased cyber-threats. With digital transformation, nations are facing cyber-threats on a global scale that are attributed towards disruption of economic development (Świątkowska 2020) costing trillions of US dollars (Lallie et al. 2021). One of the factors attributed towards the increase in cybercrimes is low knowledge and awareness of the individuals regarding cyber-threats. Cybersecurity awareness is defined as "the knowledge and overall understanding of information-security-related problems and their repercussions as well as what needs to be done to handle them" (Kim et al. 2019; Bulgurcu et al. 2009). One of the most affected organizations from cybercrimes are higher education institutes (HEIs), which are known to be one of the least secure environments since early 2000 (Chapman 2019; Luker and Petersen 2003). University-going students are vulnerable due to their increased amount of time spent online, reckless use of technology (Aliyu et al. 2010), and low cybersecurity knowledge to evade such risks (Sarathchandra et al. 2016).

The enactment of actions to avert cybersecurity risks is influenced by an individual's placement in the social stratification system (Dodel and Mesch 2018). The social inequalities seep into digital realm and hinder uptake of ICTs creating digital divide (Van Dijk 2005). Social and digital disparities negatively affect the development of knowledge and skills to enact cybersecurity practices (Dodel and Mesch 2018). Although the research on cybersecurity awareness has recently gained ground (Parsons et al. 2017), there is a lack of research that considers the influence of social and digital disparities (Robinson et al. 2015) on cybersecurity—specially in developing countries where such disparities are rife. The topic of cybersecurity awareness is of particular pertinence for Pakistan—a developing country where individuals hail from different socioeconomic backgrounds and digital divide is acute in urban and rural areas (Jamil 2020). Cybercrime is rife due to geopolitics and numerous military conflicts of the region (Shad 2019) and cybercriminals exploit low cybersecurity knowledge of the individuals to launch cyberattacks at individual, organizational, and national level. Studying cybersecurity in Pakistani HEIs is of particular concern as the youngsters are the main driving force behind Pakistan's freelance economy—the fourth largest in the world (Pofeldt 2019; TechABU 2022). The safety of these individuals is important for continuation of the upward freelance trend and entails practicing cybersecurity behavior. Moreover, there are multiple systematic literature reviews that have made research calls to study cybersecurity behavior in HEIs in developing nations (Bongiovanni 2019) specifically in Pakistan (Khan et al. 2022a). Therefore, this study focuses on cybersecurity behavior of university-going students in Pakistan who hail from different socioeconomic backgrounds and experience digital divide.

Higher education institutes and cybersecurity

The cybersecurity dynamics in HEIs are different from traditional organizations (Hina et al. 2019). Universities are open-by-design (Borgman 2018), decentralized

and transient platforms. Multiple stakeholders interact with the universities' platforms for teaching, research, and innovation purposes (Bongiovanni 2019). For attackers, universities are considered a treasure trove because of huge amount of data that can be exploited (Zhang and Li 2015). Hackers can use the computational power of the universities' IT infrastructure (Katz 2005; Rezgui and Marks 2008) to launch denial of service (DOS) attacks and can even mine cryptocurrency. The Bring Your Own Device (BYOD) policies and the usage of universities' IT infrastructure have further opened doors for criminals to exploit not only the mobile devices of an individual but also the HEI's sensitive data by compromising universities' networks (Parker et al. 2015). The intensity of these attacks has increased in the wake of the COVID-19 pandemic (Lallie et al. 2021). With the increased reliance of universities on learning management systems and dependence on digital education post COVID-19 pandemic, HEIs need to be vigilant of cybersecurity breaches (Taha and Dahabiyeh 2021).

Cybersecurity and socioeconomic and digital disparities

The cybersecurity awareness is affected by disparities that are rooted in socioeconomic status and access to digital technologies. The socioeconomic status of the individual affects the cybersecurity awareness and behavior (Redmiles et al. 2015). The individuals belonging to lower socioeconomic backgrounds have dismissive attitude towards security (Mohammad et al. 2022). A number of studies have been conducted to show the direct role of socioeconomic status on cybersecurity behavior of individuals (Reyns et al. 2016; Büchi et al. 2017). A study conducted in UK reports that individuals from lower socioeconomic groups lagged behind in use of security software. Similarly, Dodel and Mesch (2017) report consistent results on association between higher socioeconomic status and higher safety digital skills. Socioeconomic status have been reported to be the main source of differences in digital skills (Van Deursen et al. 2017; Helsper and Eynon 2013; Witte and Mannon 2010) along with demographics and education. One of the reasons is that the impact of pre-existing social inequalities and their interaction with technology is not redistributive (Van Dijk 2005). Despite ICTs growth, these technologies are disseminated in the society in an imbalanced way (Lal 2017). This leads to the digital divide where access to ICTs is stratified among the population as per the socioeconomic status (Cik et al. 2018).

Digital disparity is one of the most prominent forms of inequalities and has surfaced with the dawn of the digital age (Robinson et al. 2015). It is present among individuals as well as among nations and Khan et al. (2022b) has the potential to influence life chances in a variety of ways—one being acquisition of digital skills. The core of the digital divide concept states that better digital uptake of ICTs in terms of usage and participation leads to digital advantages culminating in positive outcomes for an individual as well as the society (Livingstone and Helsper 2013). Digital engagement of the individuals leads to different positive outcomes such as academic performance and entrepreneurship (Robinson et al. 2015). The young adults who grew up with less digital opportunities find barriers in entering

workforce due to organizations' preferences for tech-savvy workforce (Chesley 2014). This inequality in access to digital technologies also has implications for cybersecurity. Few studies have been conducted that use digital divide variables to study cybersecurity behaviors (Dodel and Mesch 2017, 2018, 2019). The study by Dodel and Mesch (2019) has shown that digital skills are the antecedents of online safety behaviors. Moreover, the study reported that individuals with earlier Internet experience and more frequent usage of the Internet demonstrated greater level of safety skills and engagement in cybersecurity behavior. Similarly, digital disparities reproduced themselves in the enactment of cyber preventive behaviors (Dodel and Mesch 2018) with individuals experiencing greater digital divide showing low cybersecurity practices. It was also reported that digital divide affects the acquisition of cybersecurity knowledge and skills (Dodel and Mesch 2018). As argued by Van Deursen et al. (2017) interaction with the Internet garners benefits since some activities provide opportunities and increase resources for individuals. Cybersecurity is one such activity since enactment of cybersecurity behavior allows individuals to mitigate their chances of being victims of cybercrimes (Dodel and Mesch 2018), hence affecting their cybersecurity posture. Studies have shown that digital divide affects the developing countries comparatively more than the developed countries because of financial constraints (Abascal et al. 2016). As a result of which they experience impediments in the deriving benefit from capital-enhancing activities such as cybersecurity on the Internet.

Pakistan: digital divide, socioeconomic disparities, and cybersecurity

The developing countries experience digital divide (Robinson et al. 2020) despite crossing the access divide threshold. This is specifically true for Pakistan where the use of ICTs has increased during the past decade. The digital divide in Pakistan is reported to be acute (Jamil 2020) with only 14% of household having access to computer/laptop and the Internet (Shair et al. 2022) and is emerging in urban–rural areas of Pakistan (Jamil 2021). Of different ICTs, the access and use of the Internet among Pakistani population has the most disparity (Siegmann 2009), which hampers the capital-enhancing activities of the Internet. With increased digital reliance, the cybersecurity posture of Pakistan is weak as is the case with most of the developing nations. Globally, the nation is far behind in cybersecurity preparedness with its global cybersecurity index (GCI) to be at 79th position ("Global Cybersecurity Index" 2021). Cybercrimes are increasing in the country (Shad 2019). Majority of the victims are students enrolled in HEIs. There are a total of 222 universities in Pakistan as recognized by the higher education commission (HEC). Post COVID-19 majority of the universities are using learning management systems (Tabassum et al. 2022) to impart education (Guoyan et al. 2021). A total of 1.5 million students are enrolled in HEIs who hail from different socioeconomic backgrounds and experience disparities in access to digital resources. Evidence suggest the students are victims of cybercrimes such as cyber (Khan et al. 2023a, b) harassment (Saleem et al. 2021) black mailing (Khan 2017a) and recruitments by banned outfits (Khan 2017b). However, the awareness of safe and secure usage of the Internet is missing

and is neglected in Pakistani HEIs (Khan et al. 2021). With limited empirical evidence, there is a need to understand the cybersecurity behavior of students considering digital disparities along with socioeconomic status in Pakistan. To the best of our knowledge, this is the first study that assesses the cybersecurity practices of students—both computer as well as smartphone security—at a national scale taking into consideration social and digital disparities.

The following research questions are posed:

RQ1 What is the computer security behavior of the students enrolled in the universities of Pakistan?

RQ2 What is the smartphone security behavior of the students enrolled in the universities of Pakistan?

RQ3 Is there a difference in computer cybersecurity behavior of the students with respect to digital disparities and socioeconomic differences?

RQ4 Is there a difference in smartphone security behavior of the students with respect to digital disparities and socioeconomic differences?

The paper structure is as follows: "Theoretical background" section presents the theoretical background followed by related literature. "Methodology" section details the research methodology employed in this research. The results are described in "Results" section, whereas discussion and practical implications are presented in "Discussion" section. "Conclusion" section concludes the study.

Theoretical background

From a theoretical perspective, the stratification model of diffusion of technologies states that pre-existing advantages will replicate itself in the online world (Robinson et al. 2020; Van Dijk 2005). This means that the countries and social groups that already have Internet advantage will maintain their edge in the digital realm even when the disadvantaged groups and countries increase their digital uptake (Van Dijk 2005; Dodel and Mesch 2018). As a result social inequalities in offline world will be magnified online. At the same time, the individuals' Internet capacities will not be distributed evenly (Helsper 2012). Invariably, the digitally disadvantaged individuals will not only have barriers in further access to resources but will also lag behind in deriving benefits from capital-enhancing activities of the Internet (Van Ingen and Matzat 2018). Capital-enhancing activities on the Internet are considered more beneficial relatively to others since they help increase opportunities and resources (Van Deursen et al. 2017). One capital-enhancing activity is the cybersecurity awareness and behavior of the individuals (Dodel and Mesch 2018). Studies have shown that cybersecurity behavior requires digital knowledge that translates into skills

by repeated practices and knowledge accumulated through the use of the Internet (Dodel and Mesch 2018). Moreover, there is compelling evidence that socioeconomic status and other structural inequalities feed the digital disparities. Research has found that socioeconomic disparities not only directly play part in differences in Internet skills and access (Van Dijk 2005) but also affect cybersecurity behavior (Dodel and Mesch 2017, 2018).

This study takes into consideration the digital inequalities in which access to the Internet more frequently and from various places affects the cybersecurity practices along with the socioeconomic status of the university-going students. These variables have not been taken into consideration in the light of the stratification model as presented in the related literature on cybersecurity discussed in the next "Computer security and university students" and "Smartphone security and university students" sections.

Computer security and university students

In literature, there are a number of studies that have been carried out to gauge computer security of individuals. These studies involved individuals employed in various organizations (Cain et al. 2018) from different countries (Pattinson et al. 2015; McCormac et al. 2017; Sawaya et al. 2017).

There are few studies that take into consideration the computer security awareness and behavior of students from tertiary institutes. One of the earliest studies conducted to measure the computer security of students was carried out by Slusky and Partow-Navid (2012). The study showed that students were lacking computer skills along with knowledge and associated practices related to data encryption and data loss. Another study was conducted by Kim (2013) in the USA. The findings showed low computer security of the students in the use of encryption and anti-virus software, files backup, and changing passwords. The students from Turkey were less aware and practiced low computer security when compared with the university's staff and faculty members as identified by Öğütçü et al. (2016). Another study reported poor cybersecurity practices of the students pertaining to passwords and showed that they lacked appropriate cybersecurity knowledge (Moallem 2018). The students from Nigerian universities possessed rudimentary knowledge of the cybersecurity but failed to protect their digital information online (Garba et al. 2020). A recent study by Alharbi and Tassaddiq (2021) carried out an online survey of 576 university students in Saudi Arabia. It was found that students were lacking in passwords, web security, and security countermeasure knowledge mirroring the findings from an earlier study (Alotaibi et al. 2016).

Smartphone security and university students

In smartphone security, there are studies (Das and Khan 2016; Zhang et al. 2017; Shah and Agarwal 2020) that have been carried out in organizational settings. Few other studies on smartphone security awareness and behavior have been carried out on the students' population from HEIs. A survey conducted on students belonging to

one of the universities in Bangladesh showed that almost half of them lacked proper smartphone security practices (Nowrin and Bawden 2018). The students lagged behind in the adoption of smartphone settings and add-on utilities and failed to adequately remove data from their devices before disposal. Another study carried out at a university in Greece (Stylios et al. 2016) reported even more insecure behavior by the students. It was found that they stored sensitive data such as bank account details and other PINs in their smartphones and did not give consideration to change passwords. A number of studies have been conducted in the USA to understand the smartphone security awareness and behavior of the students. One of the earliest studies in USA was conducted by Harris et al. (2014) to ascertain the smartphone security preparedness of the university's students as well as that of the staff members. The results showed the inadequacy of practicing smartphone security by the staff members as well as students. There has been a continuous measurement of smartphone security behavior of the students belonging to a large regional university in the USA. The first study was carried out in 2012 (Jones and Heinrichs 2012) that showed lax smartphone security measures of the students in terms of use of antivirus software, encryption, backing up of data, and data clean before disposal. The second study was conducted in 2015 by the same authors (Jones and Chin 2015). The results suggested even less secure behavior of the students who were opening multimedia attachments received from unknown sources and downloading apps that accessed their personal information. The same authors carried out another evaluation of the smartphone security of the students in 2020 (Chin et al. 2020) which highlighted better practices in some areas while worse in others.

Limitations in the previous studies

There are a number of limitations that should be noted in the previously presented literature in HEIs. First and foremost is the limited research that incorporates digital divide and socioeconomic variables in understanding the cybersecurity phenomenon (Dodel and Mesch 2017, 2018, 2019; McGuire and Dowling 2013). These studies incorporate one or more cybersecurity practices and fail to study cybersecurity in terms of computer and/or smartphone devices collectively. The second reason is the lack of empirical evidence in understanding both computer as well as smartphone security practices of the students in a single study except (Taha and Dahabiyeh 2021; Breitinger et al. 2020). The study (Breitinger et al. 2020) carried out cybersecurity evaluations of individuals on the general population and not university students via an online survey, while Taha and Dahabiyeh (2021) compared eight security practices which are common in computer and smartphone devices. The security behavior pertaining to mobile devices are different from those of computers, therefore the study (Taha and Dahabiyeh 2021) does not cater for smartphone security behavior fully.

Thirdly, there is a lack of a national representative sample in Pakistan (Khan et al. 2021) to study the cybersecurity phenomenon which hinders the generalizability of results. Fourthly, the online surveys are problematic considering digital divide variables as they miss out on the representativeness of digitally less connected and

lack correlative coverage (Robinson et al. 2015). The data collected via online surveys lead to inaccurate results due to failure to understand Internet penetration and proficiency (Robinson et al. 2015). The urban population with access to broadband connections is more likely to respond, skewing the results (Robinson et al. 2015). Therefore, studies employing online surveys miss out on the representation of digitally less connected individuals.

Present study

This study overcomes the limitations of the previous work by incorporating digital divide and socioeconomic variables, and carries out a national survey in Pakistani HEIs. In contrast to Khan et al. (2021), the population of this work comprises university-going students and the sample has been drawn from geographically distributed cities across three provinces in Pakistan. To mitigate the non-representativeness of the digitally less connected participants, the survey is carried out face-to-face by traveling to different cities of the country. The sampling strategy is designed in a way that captures the socioeconomic status of the participants based on the multidimensional poverty index (MPI) of Pakistan ("Multidimensional Poverty in Pakistan" 2018) and urban/rural areas of living. Doing this allows capturing different socioeconomic classes in the country. This study gauges the cybersecurity behavior of the students in a broader context of computer and smartphone security as a whole hence extending the work of Khan et al. (2021) in which only computer security was measured.

Methodology

The methodology adopted for this research is quantitative. A questionnaire-based survey is conducted to measure computer and smartphone cybersecurity behaviors using existing scales. In the next subsection, the details of the scales, the variables used, sampling strategy followed, and the procedure to perform the research are discussed in detail.

Measures

Computer security

To measure the computer security behavior of the students, Security Behavior Intention Scale (SeBIS) was used (Egelman and Peer 2015). It is a validated instrument consisting of 16 Likert scale items. SeBIS consists of four underlying constructs namely (1) *Device Securement (DS)*, (2) *Password Protection (PS)*, (3) *Proactive Awareness (PA),* and (4) *Updating Behavior (UP)*. SeBIS scale's internal consistency and criterion validity has been established previously in the literature therefore, the self-report measures are valid (Egelman et al. 2016).

Smartphone security

Smartphone security behavior was measured by adopting an instrument from the literature. The questionnaire was taken from Chin et al. (2020) and Jones and Chin (2015) and consists of three main constructs. The first construct measures the *avoidance of harmful smartphone behavior & attitude* and consists of 17 Likert scale-like items. The second construct measures the *protection behavior using add-on utilities and settings* having 2 dichotomous and 3 Likert scale-like items. The third construct measures the smartphone behavior taken to recover from disastrous events (*disaster recovery*) such as phone loss. It contains 7 dichotomous items.

Demographic variables

The demographic variables taken for this study are gender, age, department, and province. Gender is a dummy variable with 1 representing males and 0 representing females. Age is coded as 1 representing age group 18–21 and 2 representing age group above 21. The department variable is categorical with 1 representing IT-related departments (Computer Science, Software Engineering, and Information Technology), 2 representing medical and biological sciences departments (zoology, botany, pharmacy), whereas 3 represented business-related departments (business and financial studies) and 4 represented other departments such as English and Education. The province variable was coded as categorical. Province of Punjab was coded as 1, Sindh was coded as 2, and Khyber-Pakhtun-Khawa was coded as 3.

Digital divide variables

The digital divide was measured using two variables: frequency of Internet access and Internet access from different places. It should be noted that the operationalization of digital divide in terms of Internet access and usage (level 1&2 digital divide) (Anrijs et al. 2022)—the ICT which has the highest disparity in Pakistan (Shair et al. 2022). The frequency of Internet access is coded as 1 to represent access multiple times a day and 2 to represent access once a day or once a week. The Internet access from different places is coded as 1 to represent access from home, 2 to present access from university, 3 to represent access from work/friends/family, and 6 to represent access from multiple places.

Socioeconomic variables

Two variables were used to measure the socioeconomic status of the participants, urban/rural residence and poverty stratum the participants belonged to. The participants who were living in rural areas of the country were coded as 0, whereas those living in the urban areas were coded as 1. The poverty stratum was measured by taking the (multidimensional poverty index) MPI of Pakistan ("Multidimensional Poverty in Pakistan" 2018). The country's districts/cities are divided

into 8 poverty strata as per the MPI. The cities having a poverty level of 70% and above were coded as 8, while the cities having a poverty level of less than 10% were coded as 1. The other six poverty strata are given in Table 1.

Table 1 Frequencies and percentages

Variables		Frequency	Percentage
Demographics	*Gender*		
	Male	353	46.60
	Female	405	53.40
	Age		
	18–20	448	59
	21 and above	310	41
	Department		
	IT-related	366	48.30
	Medical-related	117	15.40
	Business-related	189	24.90
	Others	86	11.30
	Province		
	Punjab	244	32
	Sindh	301	40
	Khyber-Pakhtun-Khawa	213	28
Digital Divide	*Frequency of Internet Access*		
	Once a Day	649	85.60
	Multiple Times a Day	109	14.40
	Access of Internet from Different Places		
	Access from Home		
	Access from University	425	56.10
	Access from Work/family/friends	115	15.20
	Access from Multiple Places	98	12.90
		120	15.80
Socioeconomic Status	*Living area*		
	Urban	465	61
	Rural	292	38
	Poverty stata		
	< 10% poverty	132	17.40
	10 to 19.9% poverty	65	8.60
	20 to 29.9% poverty	110	14.50
	30 to 39.9% poverty	65	8.60
	40 to 49.9% poverty	73	9.60
	50 to 59.9% poverty	283	37.30
	60 to 69.9% poverty	30	4.00

Sampling strategy

Stratified multi-stage sampling was employed for measuring the university students' cybersecurity behavior. The MPI was used to identify the poverty strata of the districts in the country. Those districts which had a HEC recognized university were listed down. Universities were randomly selected from the MPI-based strata in the country. To ensure the diversity of the sample, the selection of universities was made in such a way that they were geographically dispersed and belonged to different provinces of Pakistan. This resulted in a total of twelve universities in the three provinces of Pakistan—Punjab, Sindh, and Khyber-Pakhtun-Khawa. From each university, students from bachelor programs were randomly selected.

Procedure

The paper and pencil approach was used to carry out the execution of the questionnaire-based survey. The authors of the study physically visited twelve universities to collect the data. The universities were contacted through Office of Research Innovation and Commercialization (ORIC) offices. After getting the permission, a detailed visit schedule was made and execution of the research was carried out in three phases. In the first phase, Khyber-Pakhtun-Khawa province was chosen and data were collected from the three cities in three separate road trips. In the second phase, Northern Punjab was chosen and data were collected in the fourth road trip. In the third phase, Southern Punjab and the province of Sindh were targeted in the fifth road trip which lasted 15 days. A total of 817 participants filled in the questionnaire and 758 responses were used for analysis. The percentage of female students (53.4%) was a little higher than that of males (46.6%) as shown in Table 1. Almost 60% were in the age group of 18–20 and a majority of them were pursuing IT-related degrees (48.3%). The digital disparities existed in the sample with a very less percentage (15%) having to access the Internet multiple times a day and from multiple places. From a socioeconomic perspective, the majority of students (66%) lived in the urban areas but belonged to poor districts in terms of MPI-based poverty strata (Table 1).

Ethical approach

The university students were assured of their anonymity by the authors who were physically present at the time of the filling of questionnaires. The participants were given a consent form to sign before filling the questionnaire to show their voluntary participation and were free to withdraw.

Results

The analysis was carried out using frequencies to present descriptive statistics. Statistical software IBM SPSS V.21 was used for analysis. Research questions 1 and 2 (RQ1 and RQ2) are answered in "Descriptive statistics" section. The categorical

analysis was carried out using Pearson's Chi-square statistics ("Categorical analysis computer security" and "Categorical analysis smartphone security" sections). Significant results underwent Bonferroni correction to carry out post hoc analysis when the categorical analysis involved more than 2X2 matrix. Where the assumptions of the Chi-square statistics were violated, categories of the independent variables were combined. Research questions RQ3 and RQ4 are answered in "Categorical analysis computer security" and "Categorical analysis smartphone security" sections, respectively.

Descriptive statistics

Computer security

The descriptive statistics of computer security behavior are shown in Table 2. A total of 38% of the students did not use the computer screen lock function, whereas 16.8% did not lock their screen while being away from their devices in *device securement (DS).* In *password protection (PS)*, almost 70% of the students did not change their passwords and about half of the participants kept simple passwords. Passwords are the most common form of authentication and are used as the first line of defense; therefore, this passwords-related security behavior is alarming. In *proactive awareness (PA)*, almost 30–40% of the students did not look at URL bar and opened links without verification (Table 2). Such insecure behavior can lead to the susceptibility of the students to phishing attacks. The *updating behavior (UP)* was comparatively better than the others with only 25% of the students 'never' used an anti-virus program and updated their software.

Smartphone security

In smartphone security, the descriptive statistics are present in Table 3. In the *avoiding harmful behavior & attitude (AHBA),* a total of 45% of students 'never' logged off from emails or social networks after using them. Since it is convenient to access email with a touch of a finger, students kept logged-on in their accounts preferring convenience over security. Similarly, a vast majority of the students downloaded applications from sources that were not trustworthy; and even gave permissions. Trust in these apps and the hosting platforms seem to play a significant role in such insecure behavior. The users trust that these platforms have already carried out security scans and are safe to download (Alsaleh et al. 2017). This is specifically alarming when a significant number (62%) of these students used smartphones for financial purposes. Students showed low smartphone security behavior by neglecting *protection through add-on utilities & settings (PAUS).* Approximately, a total of 40% of students 'never' disabled their global positioning system (GPS) or used anti-virus software. Since most of the users perceive security settings to be a one-time effort (Bonné et al. 2017), therefore they fail to disable their GPS. On the other hand, a total of 75% made use of free Wi-Fi networks. The *disaster recovery (DR)* practices of the students were comparatively better than the previous two. Although a number

Table 2 Descriptive statistics of computer security awareness and behavior

SeBIS	Always/often	Sometimes/seldom	Never
Device securement			
DS1: I set my computer screen to automatically lock if I don't use it for a prolonged period of time	342 (45.1%)	128 (16.9%)	288 (38%)
DS2: I use a password/passcode to unlock my laptop or computer	615 (81.1%)	51 (6.7%)	92 (12.1%)
DS3: I manually lock my computer screen when I step away from it	466 (61.5%)	165 (21.8%)	127 (16.8%)
DS4: I use a PIN or passcode to unlock my mobile phone	658 (86.8%)	52 (6.9%)	48 (6.3%)
Password protection			
PS1: I do not change my passwords, unless I have to	508 (67.0%)	165 (21.8%)	85 (11.2%)
PS2**:** I use different passwords for different accounts that I have	344 (45.4%)	199 (26.3%)	215 (28.44%)
PS3: When I create a new online account, I try to use a password that goes beyond the site's minimum requirements	333 (43.9%)	196 (25.9%)	229 (30.2%)
PS4: I do not include special characters in my password if it's not required	379 (50.0%)	177 (23.4%)	202 (26.6%)
Proactive awareness			
PA1: When someone sends me a link, I open it without first verifying where it goes	227 (29.9%)	236 (31.1%)	295 (38.9%)
PA2: I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar	331 (43.7%)	214 (28.2%)	213 (28.1%)
PA3: I submit information to websites without first verifying that it will be sent securely (such as ssl, https, lock icon)	243 (32.1%)	167 (22.0%)	348 (45.9%)
PA4: When browsing websites, I mouse over links to see where they go, before clicking them	277 (36.5%)	219 (28.9%)	262 (34.6%)
PA5: If I discover a security problem, I continue what I was doing because I assume someone else will fix it	252 (33.2%)	199 (26.3%)	307 (40.5%)
Updating behavior			
UP1**:** When I'm prompted about a software update, I install it right	315 (41.6%)	242 (31.9%)	201 (26.5%)
UP2: I try to make sure that the programs I use are up-to-date	408 (53.8%)	229 (30.2%)	121 (16.0%)
UP3: I verify that my anti-virus software has been regularly updating itself	327 (43.1%)	214 (28.2%)	217 (28.6%)

Table 3 Descriptive statistics of smartphone security

Smartphone security	Always/often	Sometimes/seldom	Never
Avoiding harmful behavior & attitude			
AHBA1: Log off from emails/social networks when done using them	226 (29.8%)	191 (25.2%)	341 (45.0%)
AHBA2: Opening attachments from unknown source	138 (18.2%)	283 (37.3%)	337 (44.5%)
AHBA3: Click links from unknown source	102 (13.5%)	234 (30.9%)	422 (55.7%)
AHBA4: Use smartphone for Financial Purposes	224 (29.6%)	246 (32.5%)	288 (38.0%)
AHBA5: Download apps from untrusted source	146 (19.3%)	271 (35.8%)	341 (45.0%)
AHBA6: Permission to personal information when downloading apps	204 (26.9%)	250 (33.0%)	304 (40.1%)
AHBA7: Check smartphone updates	365 (48.2%)	237 (31.3%)	156 (20.6%)
Protection through add-on utilities & settings			
PAUS1: Disable GPS	319 (42.1%)	148 (19.5%)	291 (38.4%)
PAUS2: Connect to unsecure Wi-Fi	396 (52.2%)	167 (22.0%)	195 (25.7%)
PAUS3: Use anti-virus software	261 (34.4%)	157 (20.7%)	340 (44.9%)
	YES		NO
PAUS4: Set idle time out to shorter than factory default	440 (58.0%)		318 (42.0%)
PAUS5: Wakeup Idle password	540 (71.2%)		218 (28.8%)
Disaster recovery			
DR1: Use of remote-wipe	183 (24.1%)		575 (75.9%)
DR2: Use of remote-lock	189 (24.9%)		569 (75.1%)
DR3: Use of phone location services	466 (61.5%)		292 (38.5%)
DR4: Store PINs/password in smartphone	433 (57.1%)		325 (42.9%)
DR5: Make back up of data	492 (64.9%)		266 (35.1%)
DR6: Wipe data from smartphone before disposal	575 (75.9%)		183 (24.1)
DR7: Noting IMEI number	493 (65.0%)		265 (35.0%)

of students did not employ remote wipe/remote lock features for their phones, they did use phone location services to keep track of their devices. A greater percentage of students (57%) stored PINs/passwords of their bank accounts.

Categorical analysis computer security

Demographic

The results of the Pearson's Chi-square statistics found seven differences between gender and computer security (Table 4). A Bonferroni correction suggested that female students fell short in the use of complex passwords and the use of different passwords for different accounts. In *PA*, females were more apt in scrutinizing the links; however, they were poor in the verification of sent data. Females also showed poor *UP* by failing to install software updates and anti-virus programs. A total of five significant differences were found between age and computer security

behavior. A post hoc Bonferroni adjustment revealed that students who were younger (18–20 years) exhibited low computer security in the three categories (Table 4). In the department variable, four significant differences were found. Students pursuing medical-related degrees showed low-security behavior by failing to use various passwords, updating software, and other programs. It should be noted that students belonging to other departments were vigilant in discovering security problems and not ignoring them. A total of four significant differences were found between the variables province and computer security (Table 4). A post hoc Bonferroni correction showed the students belonging to the province of KPK had lax attitude towards updating software and anti-virus program, whereas those belonging to the province of Punjab kept their program updated. The students belonging to Sindh province used different passwords for their different accounts, therefore, exhibited good *PS*.

Table 4 Pearson's Chi-square results of computer security and demographic variables

SeBIS	Demographic			
	Gender	Age	Dept	Province
Device securement				
DS1	–	$\chi^2(2) = 14.01$, $p = 0.001$	–	–
DS2	–	–	–	–
DS3	–	–	–	–
DS4	–	–	–	–
Password protection				
PS1	–	–	–	–
PS2	$\chi^2(2) = 8.92$, $p = 0.01$	$\chi^2(2) = 7.06$, $p = 0.02$	$\chi^2(6) = 14.09$, $p = 0.02$	$\chi^2(4) = 12.33$, $p < 0.01$
PS3	$\chi^2(2) = 8.89$, $p = 0.01$	$\chi^2(2) = 9.008$, $p = 0.01$	–	–
PS4	$\chi^2(2) = 8.35$, $p = 0.01$	–	–	–
Proactive awareness				
PA1	–	–	–	–
PA2	–	–	–	–
PA3	$\chi^2(2) = 13.57$, $p = 0.001$	–	–	–
PA4	$\chi^2(2) = 19.95$, $p < 0.001$	–	–	–
PA5	–	–	$\chi^2(6) = 18.61$, $p = 0.005$	–
Updating behavior				
UP1	$\chi^2(2) = 28.12$, $p < 0.001$	–	$\chi^2(6) = 54.78$, $p < 0.001$	$\chi^2(4) = 27.48$, $p < 0.001$
UP2	–	$\chi^2(2) = 10.74$, $p = 0.005$	$\chi^2(6) = 22.02$, $p = 0.001$	$\chi^2(4) = 26.21$, $p < 0.001$
UP3	$\chi^2(2) = 15.27$, $p < 0.001$	$\chi^2(2) = 7.63$, $p = 0.02$	–	$\chi^2(4) = 16.06$, $p = 0.003$

Digital divide

A total of ten significant differences were found in the frequency of Internet access and computer security (Table 5). A post hoc Bonferroni correction was applied. The results showed that students who accessed the Internet multiple times a day were proficient in all the four elements of *DS* of automatic lock, password protection, manual lock, and use of PIN for devices. On the other hand, students who accessed the Internet less frequently showed low security in all the elements of *UP*, having various passwords and quality of passwords (minimum requirement) and in *PA* of mouse over links for confirmation before clicking. A total of six significant differences were found between the variables access of the Internet from various places and computer security. A post hoc Bonferroni correction showed that students who accessed the Internet from multiple places had good *UP* and used different passwords for different accounts. On the other hand, those who accessed the Internet from university had low password/PIN protection, while those who accessed from work/friends/family submitted their information without confirming SSL or HTTPS links. Therefore, these students who had limited access to the Internet exhibited low security.

Socioeconomic status

One significant difference was found for urban/rural living with students belonging to rural areas not updating their programs thereby showing low-security *UP* (Table 5). Three significant differences were found between poverty strata and computer security. Students who belonged to rich areas showed better *UP* of programs, while students who belonged to medium poverty also showed better software *UP*. On the other hand, students who were poor showed better security behavior of discovering a computer problem and not continuing their work thinking someone else will fix it for them, which was in complete contrast to those students who belonged to rich socioeconomic classes.

Categorical analysis smartphone security

Demographics

In demographics, significant differences were found between gender, age, department and province variables; and smartphone security (Table 6). For gender, two differences were from *PAUS*, whereas four differences were in *AHBA* and *DR* each. A post hoc Bonferroni correction revealed that females exhibited better smartphone security in *AHBA*. The percentages of females who 'never' opened attachments and downloaded applications from untrusted sources were greater. Moreover, females were better at not giving excessive permission to the downloaded apps. On the other hand, males showed better smartphone security in disabling GPS and use of wakeup after password thereby making them better in the utilization of *add-on utilities* for

Table 5 Pearson's Chi-square results of computer security and socioeconomic & digital divide variables

SeBIS	Socioeconomic level		Digital divide	
	Urban/rural	Poverty strata	Internet access from various places	Frequency of internet access
Device securement				
DS1	–	–	–	$\chi^2(2)=32.25, p<0.001$
DS2	–	–	$\chi^2(6)=17.81, p=0.007$	$\chi^2(2)=37.99, p<0.001$
DS3	–	–	–	$\chi^2(2)=24.90, p<0.001$
DS4	–	–	$\chi^2(6)=15.32, p=0.01$	$\chi^2(2)=23.08, p<0.001$
Password protection				
PS1	–	–	–	–
PS2	–	–	$\chi^2(6)=17.86, p=0.007$	$\chi^2(2)=21.30, p<0.001$
PS3	–	–	–	$\chi^2(2)=16.54, p<0.001$
PS4	–	–	–	–
Proactive awareness				
PA1	–	–	–	–
PA2	–	–	–	–
PA3	–	–	$\chi^2(6)=22.29, p=0.001$	–
PA4	–	–	–	$\chi^2(2)=13.79, p=0.001$
PA5	–	$\chi^2(4)=16.55, p=0.002$	–	–
Updating behavior				
UP1	–	$\chi^2(4)=16.818, p=0.002$	–	$\chi^2(2)=28.21, p<0.001$
UP2	$\chi^2(2)=13.41, p=0.001$	$\chi^2(4)=15.07, p=0.005$	$\chi^2(6)=30.19, p<0.001$	$\chi^2(2)=36.21, p<0.001$
UP3	–	–	$\chi^2(6)=16.83, p=0.01$	$\chi^2(2)=13.80, p=0.001$

smartphone security. A similar pattern was found in *DR* in which they made use of the remote lock, remote wipe, and phone location services and made back up of phone data along with noting the IMEI number of their smartphones. Five significant differences were between age and smartphone security. Students belonging to the age group 18–20 years showed better smartphone security practices in *AHBA* by never downloading apps from sources that could not be trusted or giving excessive permissions to their personal information. On the other hand, the younger student (18–20 years) exhibited low *DR* by not backing up their smartphone data and wiping their phones clean before disposal. Moreover, these students also failed to set the idle time out to short when compared with their older counterparts.

Department-wise categorical analysis revealed seven differences as shown in Table 6. Students who were pursuing medical-related professions showed better smartphone security behavior in avoiding giving application permission to personal information, whereas business students used their phones for financial purposes thereby making them vulnerable to smartphone security breaches. An Alternative pattern was observed in *PAUS* with business students showing good security by changing shorter Idle time out than the default, whereas medical students exhibiting poor smartphone security in disabling GPS when not in use. In *DR*, medical students did not back up their data and did not use phone location services hence were less equipped to handle recovery from incidents such as phone loss or theft. On the other hand, business students were better at backup and use of phone location services but failed to use remote lock features. Therefore, both medical and business students showed inability to recover from disaster.

A total of nine differences were for the province variable (Table 6). Post hoc Bonferroni correction analysis of *AHBA* category showed that the students who belonged to the province of Sindh downloaded apps as well as opened attachment from untrusted sources and also used their smartphones for financial purposes therefore showed low security. The significant results in *PAUS* and *DR* showed mixed results for individuals belonging to KPK and Punjab.

Digital divide

There were ten significant differences between the variables Internet access from different places and smartphone security behavior (Table 7). The students who accessed the Internet from multiple places showed better security behaviors in all three smartphone security categories. A Bonferroni correction showed that the students who had Internet access from different places exhibited better security by not downloading apps from untrusted sources or giving them excessive access. However, these students did use the smartphone for financial purposes. Similarly, in *PAUS*, students accessing the Internet from various places disabled GPS when not in use, used passwords, and set the idle time out to short. In the same vein, these students backed up and erased data from the smartphone upon its disposal and made use of phone location services thereby were better prepared for *DR*. There were eleven significant differences between the frequency of Internet access and smartphone security behavior. Four significant differences were found in *AHBA* and *PAUS* each. In the former category, students who accessed the Internet less frequently were

Table 6 Pearson's Chi-square results of smartphone security and demographic variables

Smartphone security	Gender	Age	Dept	Province
Avoiding harmful behavior and attitude				
AHBA1	–	–	–	–
AHBA2	$\chi^2(2)=12.143, p=0.002$	–	–	$\chi^2(4)=15.54, p=0.004$
AHBA3	–	–	–	–
AHBA4	$\chi^2(2)=7.53, p=0.023$	–	$\chi^2(6)=15.24, p=0.01$	$\chi^2(4)=24.63, p<0.001$
AHBA5	$\chi^2(2)=24.50, p<0.001$	$\chi^2(2)=11.61, p=0.003$	–	$\chi^2(4)=10.71, p=0.03$
AHBA6	$\chi^2(2)=11.41, p=0.003$	$\chi^2(2)=9.39, p=0.009$	$\chi^2(6)=13.44, p=0.03$	–
AHBA7	–	–	–	–
Protection through add-on utilities & settings				
PAUS1	$\chi^2(2)=24.60, p<0.001$	–	$\chi^2(6)=29.61, p=<0.001$	$\chi^2(4)=11.93, p=0.01$
PAUS2	–	–	–	–
PAUS3	–	–	–	–
PAUS4	–	$\chi^2(1)=8.13, p=0.004$	$\chi^2(3)=9.04, p=0.02$	–
PAUS5	$\chi^2(1)=8.87, p=0.003$	–	–	$\chi^2(2)=9.25, p=0.01$
Disaster recovery				
DR1	$\chi^2(1)=5.49, p=0.019$	–	–	–
DR2	$\chi^2(1)\,\chi^2(1)=12.47, p<0.001$	–	$\chi^2(3)=10.461, p=0.01$	$\chi^2(2)=21.88, p<0.001$
DR3	$\chi^2(1)=17.53, p<0.001$	–	$\chi^2(3)=23.63, p<0.001$	$\chi^2(2)=29.97, p<0.001$
DR4	–	–	–	–
DR5	$\chi^2(1)=23.65, p<0.001$	$\chi^2(1)=5.23, p=0.02$	$\chi^2(3)=29.86, p<0.001$	$\chi^2(2)=25.20, p<0.001$
DR6	–	$\chi^2(1)=4.17, p=0.04$	–	$\chi^2(2)=14.00, p=0.001$
DR7	$\chi^2(1)=12.97, p<0.001$	–	–	–

better at not downloading apps from untrusted sources, giving them excessive permissions and not using the smartphone for financial purposes. However, these students did not check their updates regularly when compared to those with a lesser digital divide. Students who accessed the Internet multiple times a day disabled GPS when not in use, used anti-virus software, and used password to wake up after Idle; therefore, were better equipped with practices to protect through add-on utilities. However, these students connected to insecure Wi-Fi networks. On the other hand, the students who had less frequent Internet access were more vigilant in the use of Wi-Fi networks. There were three significant differences in *DR* with students accessing the Internet more frequently exhibiting more secure smartphone security practices in the use of phone location services, making back up of data and its erasure before phone disposal (Table 7). Therefore, students who were from a lesser digital divide were better in the majority of the smartphone security practices hence showing good security habits.

Socioeconomic status

There were two significant differences found between urban/rural areas of living and smartphone security behavior and one difference between poverty status and smartphone security (Table 7). The students belonging to urban areas showed better practices in *AHBA* (Idle time out) and in recovering from disaster (phone location services). Only one significant difference was found for the poverty status in *DR*. Students belonging to rich backgrounds were better at disposing off the phone while making sure to erase data.

Discussion

This study enhanced the literature on cybersecurity by examining socioeconomic and digital disparities and their effects on computer and smartphone security practices. By taking the lens of stratification of diffusion of technology, we investigate the current state of cybersecurity posture of university-going students. The findings point towards the unequal distribution of computer and smartphone security practices and hence solidifies evidence that pre-existing inequalities due to digital divide and socioeconomic status prevail in the online settings.

In computer security, a vast majority of the students have weak practices regarding passwords. This shows that the state of password protection is still an area where users are ignoring safe security practices despite more than four decades of research (Taneski et al. 2014). Password-related insecure behavior is still present despite its recognition in 1970. Factors such as difficulty to memorize complex passwords and multiple passwords are responsible for low password security (Taneski et al. 2014). Another area where students exhibit comparatively weaker practices in computer security is their ability to proactively browse the Internet. Students are lax in confirming the links they get in their emails, visit websites without looking at the URL bar, and do not verify a secure connection. These findings are in line with a meta-analysis of phishing susceptibility rates where individuals' propensity to be

Table 7 Pearson's Chi-square results of smartphone security and socioeconomic & digital divide variables

Smartphone security	Socioeconomic level		Digital divide	
	Urban/rural	Poverty strata	Internet Access from various places	Frequency of internet access
Avoiding harmful behavior and attitude				
AHBA1	–	–	–	–
AHBA2	–	–	$\chi^2(6)=17.05, p=0.009$	–
AHBA3	–	–	–	–
AHBA4	–	–	$\chi^2(6)=22.07, p=0.001$	$\chi^2(2)=19.87, p<0.001$
AHBA5	–	–	$\chi^2(6)=12.76, p=0.047$	$\chi^2(2)=10.67, p<0.005$
AHBA6	–	–	$\chi^2(6)=21.17, p=0.002$	$\chi^2(2)=18.16, p<0.001$
AHBA7	–	–	–	$\chi^2(2)=17.56, p<0.001$
Protection through add-on utilities & settings				
PAUS1	–	–	$\chi^2(6)=24.46, p<0.001$	$\chi^2(1)=14.56, p=0.001$
PAUS2	–	–	–	$\chi^2(1)=29.12, p<0.001$
PAUS3	–	–	–	$\chi^2(1)=8.79, p=0.01$
PAUS4	$\chi^2(1)=8.02, p=0.005$	–	$\chi^2(3)=26.43, p<0.001$	–
PAUS5	–	–	$\chi^2(3)=17.35, p=0.001$	$\chi^2(1)=26.83, p<0.001$
Disaster recovery				
DR1	–		–	–
DR2	–	–	–	–
DR3	$\chi^2(1)=7.93, p=0.005$	–	$\chi^2(3)=30.62, p<0.001$	$\chi^2(1)=35.49, p<0.001$
DR4	–		–	–
DR5	–	–	$\chi^2(3)=16.82, p=0.001$	$\chi^2(1)=7.64, p=0.006$
DR6	–	$\chi^2(2)=10.04, p=0.007$	$\chi^2(3)=13.82, p=0.003$	$\chi^2(1)=4.413, p=0.03$
DR7	–	–	–	–

susceptible to attacks is as large as 68% (Sommestad and Karlzén 2019). Attackers can easily carry out phishing attacks as approximately 35% of the security breaches are attributed to low proactive awareness of the users (Sommestad and Karlzén 2019). Similar patterns are found in the smartphone security practices of the students for their device, i.e., in updating smartphones, use of a password in wakeup after idle, disposing of smartphones after cleaning and deleting the personal data. However, university students stored their PINs/passwords in their smartphones thereby making them vulnerable to financial crimes. The misconception of security associated with the physical ability to control smartphones (Serrano-Tellería 2018) partly explains the storage of sensitive information in these devices. Similar to computer security, students have low-security practices of opening attachments, clicking links, and connecting to insecure Wi-Fi from their smartphone devices. As pointed out (Sombatruang et al. 2019), low mobile data are responsible for insecure Wi-Fi usage due to the zero cost. In contrast to computer security, a majority of the students do not use anti-virus software on their smartphones. Since smartphones' anti-virus is expensive compared to computer anti-virus programs, therefore students do not install them on smartphones. For security practices that are exclusive to smartphones, students show lax behavior. Overall, students have a low computer as well as smartphone security practices which are in line with the results from Filippidis et al. (2018).

Computer security posture of university students

Gender-wise results of our study are in line with those of Farooq et al. (2015a, b), Gratian et al. (2018), Solic et al. (2019) where females are reported to show lower practices in computer security. Other studies have also shown that gender has a significant relationship with some of the security practices such as being careful in clicking links (Alzubaidi 2021). The results are in contrast to McCormac et al. (2017) in which females exhibited better computer security practices and Cain et al. (2018) with no significant difference between males and females. Age-wise differences of our study show younger students to have lax computer security practices similar to the study (Farooq et al. 2015a; Gratian et al. 2018). The results are not in line with Cain et al. (2018) where no significant difference was found with respect to age. In contrast to the study (Farooq et al. 2015a), where students from IT backgrounds showed the highest computer security, our findings were insignificant. However, students belonging to non-IT degree programs such as medicine-related professions showed low computer security in our study.

The computer security results pertaining to digital divide variables show students experiencing greater digital divide exhibit low-security practices. Similar to the studies (Dodel and Mesch 2019; Öğütçü et al. 2016), access to the Internet from multiple places and more frequent access tends to heighten the security practices and vice-versa. The highest number of differences was found in digital divide variables with results echoing the stratification model of diffusion of technologies in which digital disparities have an amplification effect. Socioeconomic background differences in terms of the rural and urban area of living in this study

are similar to Farooq et al. (2015a) where students hailing from metropolitan areas have better computer security practices. Our results related to poverty level are also in line with those of Dodel and Mesch (2019) where the socioeconomic status is taken with respect to the educational background. Therefore, it is found that socioeconomic status has a significant effect on the computer security of the students, regardless of their educational level.

Smartphone security posture of university students

Gender-wise differences of this study pertaining to *AHBA* are similar to those of (Zhang et al. 2017) with females not granting downloaded apps access to personal information. The results are similar to Nowrin and Bawden (2018), where males have better *DR* management and *PAUS*. As evidenced in Jones and Chin (2015) and Jones and Heinrichs (2012), females are not very confident in their technical abilities that surface in their cybersecurity behavior which involve technical knowledge. Age-wise differences of our study are in contrast to Das and Khan (2016), Stylios et al. (2016), Shah and Agarwal (2020) where younger students show lower security practices in downloading apps from untrusted sources and give access to their personal information. Similarly, our findings are also not in line with those of Jones and Chin (2015), where age did not have any influence on smartphone security awareness and behavior. Department-wise differences revealed non-IT students specifically of medical and business backgrounds to have overall poor smartphone security practices. The department-wise smartphone security are also found to be low in those students who pursued IT-related degrees (Nowrin and Bawden 2018).

Students who accessed the Internet more frequently and from multiple places exhibited better smartphone security in all three categories. The findings are in line with Dodel and Mesch (2018, 2019) in which having Internet access for a longer period of time as well as having more frequent access to the Internet directly influenced the computer security awareness and behavior. The only exceptions where students suffering from a larger digital divide performed better than those who had better Internet access were the smartphone security practices of downloading apps, giving excessive permission, using smartphones for financial purposes, and connecting to insecure Wi-Fi. A plausible explanation is that students who possess lesser Internet access get lower opportunities to free Wi-Fi and thereby lesser opportunities to download apps and giving them excessive permissions. The low Internet access also dictates the lesser usage of the phone for carrying out financial transactions. The low security in terms of checking updates regularly was also observed in students who accessed the Internet less frequently, attributed to their limited access to the Internet. The socioeconomic status of the students was significant for both urban/rural and poverty status variables with students from urban areas and rich socioeconomic status showing better smartphone security. These findings mirror those of Dodel and Mesch (2017), where participants from lower socioeconomic backgrounds were not well versed in security practices such as the use of anti-virus.

Theoretical and practical implications

The results of this study have many theoretical and practical implications. From a theoretical point of view, this study has examined the way in which digital and socioeconomic disparities generate digital disadvantages such as computer and smartphone cybersecurity skills. As per the diffusion of technologies theory, the digital inequalities reinforce already existing social disparities and carry them into the online settings (DiMaggio and Garip 2012). Our results reinforce this theory since the digital disparities in terms of frequency of Internet access and from various places are carried out in the online behaviors of computer and smartphone security. The face-to-face survey method employed in this study allows us to capture those participants who have a little digital footprint, thereby making our results generalizable to large aggregates of university-going students. Therefore, the results can be extrapolated and serve as groundwork for further digital inequality mitigation strategies.

Our study has focused on the exploration of HEIs in terms of cybersecurity in the light of digital disparities, which can help form a framework that can reduce cyber risks. Recommended security practices are to be inculcated in university students as per demographics, socioeconomic and especially digital disparities. By identifying digitally less connected students, tailored cybersecurity and digital skills development programs can be delivered to allow these students to mitigate cyber risks, while at the same time taking advantage of other online opportunities. Considering Pakistan as a developing nation—which is constantly at cyber risk due to political and hostile regional conflicts (Shad 2019) and at the same time coexisting with 'startups' being the fourth largest digital economy ("Payoneer | The Global Gig-Economy Index: Q2 2019" 2020)—the findings of our study have far-reaching practical applications. The global security index of Pakistan has decreased from 66th position to the current 79th position, with a serious lack of intervention planning in cybersecurity capacity building ("Global Cybersecurity Index" 2021). Measuring the computer cybersecurity of the students is the first step towards that intervention planning that is necessary for the smooth surfing in the cyberspace. The digital economic growth of the country is fueled mainly by the younger population (Malik et al. 2020) that entails accumulation of substantial knowledge and behavior in terms of cybersecurity. The low cybersecurity practices hinder the beneficial economic activities on the Internet; therefore the education of these individuals in university settings is mandatory to ensure the continuity as well as the growth of the freelance economy.

Limitations

There are a few limitations in this study. First of all, the results are the product of self-report data and may suffer from measurement errors (Spector 1992). Cybersecurity behavior is hard to measure objectively as the actual incidents may or may not occur (Parsons et al. 2014). This is due to the low probability and high consequence

of cybersecurity threats. When such incidents do happen the consequences associated with them are dire. Then, there are ethical issues associated with the actual measure of cybersecurity behavior. Therefore, relying on self-reported behavior is a valid alternative to measuring actual incidents. Another limitation is the operationalization of digital divide variables which captures the frequency and accessibility of the Internet (without considering other ICT devices) (Vehovar et al. 2006). Although this operationalization is a simple one, it takes into consideration the context of Pakistan where the penetration of the Internet is one of the lowest compared to other ICTs (Shair et al. 2022; Siegmann 2009). Furthermore, it does not consider other aspects of this multidimensional concept such as affordability, quality of Internet, and degree of preparedness of the nation to participate in and benefits from development of ICTs. With digital divide being a complex construct, the internal dynamics of different factors as suggested by Barzilai-Nahon (2006) are also missing in this operationalization. Moreover, the level of observation is at an individual level and does not take into account community, national or international level.

There is also the propensity of dispositional and situational characteristics due to self-report biases (Donaldson and Grant-Vallone 2002). In order to reduce dispositional characteristics, before carrying out the survey, we explained to the students that their input in answering correctly will be beneficial for them as well as for the research. We also ensured students about anonymity and confidentiality of their data and catered for any situational characteristics that may result in students giving socially desirable answers. Another limitation to note is the sample derived from a population of undergraduate students which may not generalize well for the students at the graduate and postgraduate level as well as for the student population outside Pakistan.

Conclusion

This study has contributed towards the interrelations of digital and socioeconomic disparities with higher education institutes as a result of research call by Robinson et al. (2015). Although the research on digital inequality is still evolving, this study never-the-less contributes towards the stratification model of diffusion of technologies by understanding the computer and smartphone security awareness and behaviors of students enrolled in the tertiary institutes of Pakistan. The results from our study show substantial cybersecurity differences in terms of the digital divide as well as socioeconomic status and demographics. The hindrance to digital technologies does influence digital skills in terms of computer and smartphone security and consequent capital-enhancing activities on the Internet. The research findings call for educational interventions by including governments, tertiary institutes' management along with cybersecurity researchers. Moreover, continual training efforts are recommended to better the cybersecurity posture at a national scale that aid in the enhancement of GCI. Future studies should be carried out to longitudinally measure the smartphone and computer security awareness and behaviors of the students with respect to digital and socioeconomic disparities. Another direction is to see the association of cybersecurity behaviors and cybercrimes prominent in universities such as

cyberbullying (Saleem et al. 2022). With the availability of national data on cyberbullying (Saleem et al. 2021), the authors plan to carry out cross analysis of security practices and that of cyberbullying victimization among students. Moreover, the cultural perspective should be taken into account in future endeavors by adopting celebrated cultural frameworks such as Hofstede (2011).

Author contributions All the authors contributed equally in the research.

Funding This research was funded by Riphah International University.

Data availability The data are subject to intellectual property rights and will not be shared.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Ethical approval The research was carried out by getting permissions from the different universities through ORIC offices. The students signed consent form to participate in the research.

Consent for publication The participants voluntarily and anonymously filled in the questionnaire and were told about the research and its publication.

References

Abascal, Julio, Simone D. J. Barbosa, Colette Nicolle, and Panayiotis Zaphiris. 2016. Rethinking Universal Accessibility: A Broader Approach Considering the Digital Gap. *Universal Access in the Information Society*. https://doi.org/10.1007/s10209-015-0416-1.

Alharbi, Talal, and Asifa Tassaddiq. 2021. Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing* 5 (2): 23.

Aliyu, Mansur, Nahel A. O. Abdallah, Nojeem A. Lasisi, Dahir Diyar, and Ahmed M. Zeki. 2010. Computer Security and Ethics Awareness among IIUM Students: An Empirical Study. In *Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference On*, A52–A56. IEEE.

Alotaibi, Faisal, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. A Survey of Cyber-Security Awareness in Saudi Arabia. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 154–158. IEEE.

Alsaleh, Mansour, Noura Alomar, and Abdulrahman Alarifi. 2017. Smartphone Users: Understanding How Security Mechanisms Are Perceived and New Persuasive Methods. *PLoS ONE* 12 (3): e0173284.

Alzubaidi, Abdulaziz. 2021. Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia. *Heliyon* 7 (1): e06016.

Anrijs, Sarah, Ilse Mariën, Lieven De Marez, and Koen Ponnet. 2022. Extending the Third Level of Digital Divide by Applying a Capability Approach: Who Is Unable to Reach Basic Needs through the Internet? In *72nd Annual ICA Conference*.

Barzilai-Nahon, Karine. 2006. Gaps and Bits: Conceptualizing Measurements for Digital Divide/s. *The Information Society* 22 (5): 269–278.

Bongiovanni, Ivano. 2019. The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education. *Computers & Security* 86 (September): 350–357. https://doi.org/10.1016/j.cose.2019.07.003.

Bonné, Bram, Gustavo Rovelo, Peter Quax, and Wim Lamotte. 2017. Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumptions of Mobile Device Users. *Information* 8 (3): 76.

Borgman, Christine L. 2018. Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier. *Berkeley Tech. LJ* 33: 365.

Breitinger, Frank, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2020. A Survey on Smartphone User's Security Choices, Awareness and Education. *Computers & Security* 88: 101647.

Büchi, Moritz, Natascha Just, and Michael Latzer. 2017. Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection. *Information, Communication & Society* 20 (8): 1261–1278.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2009. Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. *AMCIS 2009 Proceedings*, 419.

Cain, Ashley A., Morgan E. Edwards, and Jeremiah D. Still. 2018. An Exploratory Study of Cyber Hygiene Behaviors and Knowledge. *Journal of Information Security and Applications* 42: 36–45.

Chapman, John. 2019. *How Safe Is Your Data?: Cyber-Security in Higher Education*. Higher Education Policy Institute.

Chesley, Noelle. 2014. Information and Communication Technology Use, Work Intensification and Employee Strain and Distress. *Work, Employment and Society* 28 (4): 589–610.

Chin, Amita G., Philip Little, and Beth H. Jones. 2020. An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University. *International Journal of Education and Development Using Information and Communication Technology* 16 (1): 44–61.

Cik, Visnja Krizanovic, Drago Zagar, and Kresimir Grgic. 2018. A Framework for Optimal Techno-Economic Assessment of Broadband Access Solutions and Digital Inclusion of Rural Population in Global Information Society. *Universal Access in the Information Society* 17 (3): 517–540.

Das, Amit, and Habib Ullah Khan. 2016. Security Behaviors of Smartphone Users. *Information & Computer Security*. Emerald Group Publishing Limited.

DiMaggio, Paul, and Filiz Garip. 2012. Network Effects and Social Inequality. *Annual Review of Sociology* 38: 93–118.

Dodel, Matias, and Gustavo Mesch. 2017. Cyber-Victimization Preventive Behavior: A Health Belief Model Approach. *Computers in Human Behavior* 68: 359–367.

Dodel, Matias, and Gustavo Mesch. 2018. Inequality in Digital Skills and the Adoption of Online Safety Behaviors. *Information, Communication & Society* 21 (5): 712–728.

Dodel, Matias, and Gustavo Mesch. 2019. An Integrated Model for Assessing Cyber-Safety Behaviors: How Cognitive, Socioeconomic and Digital Determinants Affect Diverse Safety Practices. *Computers & Security* 86: 75–91.

Donaldson, Stewart I., and Elisa J. Grant-Vallone. 2002. Understanding Self-Report Bias in Organizational Behavior Research. *Journal of Business and Psychology* 17 (2): 245–260.

Egelman, Serge, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5257–5261.

Egelman, Serge, and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (Sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882. ACM.

Farooq, Ali, Johanna Isoaho, Seppo Virtanen, and Jouni Isoaho. 2015a. Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *2015a IEEE Trustcom/BigDataSE/ISPA*, 1:352–59. IEEE.

Farooq, Ali, Johanna Isoaho, Seppo Virtanen, and Jouni Isoaho. 2015b. Observations on Genderwise Differences among University Students in Information Security Awareness. *International Journal of Information Security and Privacy (IJISP)* 9 (2): 60–74.

Filippidis, Adam P., Constantinos S. Hilas, Georgios Filippidis, and Anastasios Politis. 2018. Information Security Awareness of Greek Higher Education Students—Preliminary Findings. In *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, 1–4. IEEE.

Garba, Adamu, Maheyzah Binti Sirat, Siti Hajar, and Ibrahim Bukar Dauda. 2020. Cyber Security Awareness among University Students: A Case Study. *Science Proceedings Series* 2 (1): 82–86.

Global Cybersecurity Index. 2021. *ITU*. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. 2018. Correlating Human Traits and Cyber Security Behavior Intentions. *Computers & Security* 73: 345–358.

Guoyan, Sun, Asadullah Khaskheli, Syed Ali Raza, Komal Akram Khan, and Faiza Hakim. 2021. Teachers' Self-Efficacy, Mental Well-Being and Continuance Commitment of Using Learning Management System during COVID-19 Pandemic: A Comparative Study of Pakistan and Malaysia. *Interactive Learning Environments*, 1–23.

Harris, Mark A., Steven Furnell, and Karen Patten. 2014. Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals. *Journal of Information Privacy and Security* 10 (4): 186–202.

Helsper, Ellen Johanna. 2012. A Corresponding Fields Model for the Links between Social and Digital Exclusion. *Communication Theory* 22 (4): 403–426.

Helsper, Ellen Johanna, and Rebecca Eynon. 2013. Distinct Skill Pathways to Digital Engagement. *European Journal of Communication* 28 (6): 696–713.

Hina, Sadaf, Dhanapal Durai Dominic Panneer. Selvam, and Paul Benjamin Lowry. 2019. Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing World. *Computers & Security* 87: 101594.

Hofstede, Geert. 2011. Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture* 2 (1): 8.

Jamil, S. 2020. *A Widening Digital Divide and Its Implications for Democracy and Social Inequalities in Pakistan*. London: Palgrave Macmillan.

Jamil, Sadia. 2021. From Digital Divide to Digital Inclusion: Challenges for Wide-Ranging Digitalization in Pakistan. *Telecommunications Policy* 45 (8): 102206.

Jones, Beth H., and Amita Goyal Chin. 2015. On the Efficacy of Smartphone Security: A Critical Analysis of Modifications in Business Students' Practices over Time. *International Journal of Information Management* 35 (5): 561–571.

Jones, Beth H., and Lynn R. Heinrichs. 2012. Do Business Students Practice Smartphone Security? *Journal of Computer Information Systems* 53 (2): 22–30.

Katz, Frank H. 2005. The Effect of a University Information Security Survey on Instruction Methods in Information Security. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, 43–48.

Khan, Arif, Muhammad Ibrahim, and Abid Hussain. 2021. An Exploratory Prioritization of Factors Affecting Current State of Information Security in Pakistani University Libraries. *International Journal of Information Management Data Insights* 1 (2): 100015.

Khan, Mohammad Hussain. 2017a. Sindh University Student Naila Rind 'Committed Suicide after Exploitation, Blackmail': Police. *DAWN.COM*. December 4. https://www.dawn.com/news/1374502.

Khan, Naurin Farooq, Amber Yaqoob, Muhammad Saud Khan, and Naveed Ikram. 2022a. The Cybersecurity Behavioral Research: A Tertiary Study. *Computers & Security* 120: 102826.

Khan, Naurin Farooq, et al. 2022b. Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. *Security Journal* (2022): 1–33.

Khan, Naurin Farooq, et al. 2023a. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security* 125 (2023a): 103049

Khan, Naurin Farooq, et al. Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes 52.1* (2023b): 401–421

Khan, Nighat Dad | Shmyla. 2017b. Naila Rind Killed Herself Because Pakistan's Cybercrime Laws Failed Her. *DAWN.COM*. January 7. http://www.dawn.com/news/1306976.

Kim, Eyong B. 2013. Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective* 22 (4): 171–179.

Kim, Hyungjin Lukas, HanByeol Stella. Choi, and Jinyoung Han. 2019. Leader Power and Employees' Information Security Policy Compliance. *Security Journal* 32 (4): 391–409.

Lal, Kashmiri. 2017. Investigating ICT Infrastructure to Develop an Information Society in India. *Universal Access in the Information Society* 16 (2): 517–528.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers & Security* 105: 102248.

Livingstone, Sonia, and Ellen J. Helsper. 2013. Children, Internet and Risk in Comparative Perspective. *Journal of Children and Media* 7 (1): 1–8.

Luker, Mark A., and Rodney J. Petersen. 2003. *Computer and Network Security in Higher Education*, vol. 8. San Francisco, CA, USA: Jossey-Bass.

Malik, Fareesa, Richard Heeks, Silvia Masiero, and Brian Nicholson. 2020. Digital Platform Labour in Pakistan: Institutional Voids and Solidarity Networks. Loughborough University.

McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson. 2017. Individual Differences and Information Security Awareness. *Computers in Human Behavior* 69: 151–156.

McGuire, Mike, and Samantha Dowling. 2013. Cyber Crime: A Review of the Evidence. *Summary of Key Findings and Implications. Home Office Research Report* 75.

Moallem, Abbas. 2018. Cyber Security Awareness Among College Students. In *International Conference on Applied Human Factors and Ergonomics*, 79–87. Springer.

Mohammad, Taufik, Nur Atikah Mohamed. Hussin, and Mohd Heikal Husin. 2022. Online Safety Awareness and Human Factors: An Application of the Theory of Human Ecology. *Technology in Society* 68: 101823.

Multidimensional Poverty in Pakistan. 2018. *UNDP in Pakistan*. January 25. http://www.pk.undp.org/content/pakistan/en/home/library/hiv_aids/Multidimensional-Poverty-in-Pakistan.html.

Nowrin, Shohana, and David Bawden. 2018. Information Security Behaviour of Smartphone : An Empirical Study on the Students of University of Dhaka, Bangladesh. *Information and Learning Science* 119: 444–455.

Öğütçü, Gizem, Özlem Müge. Testik, and Oumout Chouseinoglou. 2016. Analysis of Personal Information Security Behavior and Awareness. *Computers & Security* 56: 83–93.

Parker, Fayyaadh, Jacques Ophoff, Jean-Paul Van Belle, and Ross Karia. 2015. Security Awareness and Adoption of Security Controls by Smartphone Users. In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 99–104. IEEE.

Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security* 66: 40–51.

Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. 2014. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* 42: 165–176.

Pattinson, Malcolm, Marcus Butavicius, Kathryn Parsons, Agata McCormac, and Dragana Calic. 2015. Factors That Influence Information Security Behavior: An Australian Web-Based Study. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 231–241. Springer.

Payoneer | The Global Gig-Economy Index: Q2 2019. 2020. July 11. https://explore.payoneer.com/q2_global_freelancing_index/.

Pofeldt, Elaine. 2019. The Top 10 Fastest Growing Freelance Markets in The World. *Forbes*. https://www.forbes.com/sites/elainepofeldt/2019/08/18/the-top-10-fastest-growing-freelance-markets-in-the-world/.

Redmiles, Elissa, Amelia Malone, and Michelle L. Mazurek. 2015. How i Learned to Be Secure: Advice Sources and Personality Factors in Cybersecurity. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 666–677.

Reyns, Bradford W., Ryan Randa, and Billy Henson. 2016. Preventing Crime Online: Identifying Determinants of Online Preventive Behaviors Using Structural Equation Modeling and Canonical Correlation Analysis. *Crime Prevention and Community Safety* 18 (1): 38–59.

Rezgui, Yacine, and Adam Marks. 2008. Information Security Awareness in Higher Education: An Exploratory Study. *Computers & Security* 27 (7–8): 241–253.

Robinson, Laura, Shelia R. Cotten, Hiroshi Ono, Anabel Quan-Haase, Gustavo Mesch, Wenhong Chen, Jeremy Schulz, Timothy M. Hale, and Michael J. Stern. 2015. Digital Inequalities and Why They Matter. *Information, Communication & Society* 18 (5): 569–582.

Robinson, Laura, Jeremy Schulz, Grant Blank, Massimo Ragnedda, Hiroshi Ono, Bernie Hogan, Gustavo Mesch, Shelia R. Cotten, Susan B. Kretchmer, and Timothy M. Hale. 2020. Digital Inequalities 2.0: Legacy Inequalities in the Information Age. *First Monday*. https://doi.org/10.5210/fm.v25i7.10842.

Saleem, Sumera, Naurin Farooq Khan, and Saad Zafar. 2021. Prevalence of cyberbullying victimization among Pakistani Youth. *Technology in Society* 65 (2021): 101577.

Saleem, Sumera, Naurin Farooq Khan, Saad Zafar, and Najla Raza. 2022. Systematic Literature Reviews in Cyberbullying/Cyber Harassment: A Tertiary Study. *Technology in Society* 70: 102055.

Sarathchandra, Dilshani, Kristin Haltinner, and Nicole Lichtenberg. 2016. College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. In *2016 Cybersecurity Symposium (CYBERSEC)*, 68–73. IEEE.

Sawaya, Yukiko, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2202–2214.

Serrano-Tellería, Ana. 2018. Users' management of mobile devices and privacy. *El Profesional De La Información* 27 (4): 822.

Shad, Muhammad Riaz. 2019. Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strategic Studies* 39 (1): 1–19.

Shah, Pintu, and Anuja Agarwal. 2020. Cybersecurity Behaviour of Smartphone Users in India: An Empirical Analysis. *Information & Computer Security* 28 (2): 293–318.

Shair, Waqas, Abdul Waheed, Muhammad Mubasher Kamran, and Neelam Kubra. 2022. Digital Divide in Pakistan: Barriers to ICT Usage among the Individuals of Pakistan. *Journal of Economic Impact* 4 (3): 196–204.

Siegmann, K. A. 2009. *The Gender Digital Divide in Rural Pakistan: How Wide Is It and How to Bridge It?(ISS Staff Group 3: Human Resources and Local Development). Rotterdam, Netherlands: Sustainable Development Policy Institute (SDPI)*.

Slusky, Ludwig, and Parviz Partow-Navid. 2012. Students Information Security Practices and Awareness. *Journal of Information Privacy and Security* 8 (4): 3–26.

Solic, Kresimir, Mateo Plesa, Tena Velki, and Kresimir Nenadic. 2019. Awareness About Information Security And Privacy Among Healthcare Employees. *Southeastern European Medical Journal: SEEMEDJ* 3 (1): 1.

Sombatruang, Nissy, Lucky Onwuzurike, M. Angela Sasse, and Michelle Baddeley. 2019. Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 203–213.

Sommestad, Teodor, and Henrik Karlzén. 2019. A Meta-Analysis of Field Experiments on Phishing Susceptibility. In *2019 APWG Symposium on Electronic Crime Research (ECrime)*, 1–14. IEEE.

Spector, Paul E. 1992. A Consideration of the Validity and Meaning of Self-Report Measures of Job Conditions. *International Review of Industrial and Organizational Psychology* 7.

Stylios, Ioannis, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. 2016. Users' Attitudes on Mobile Devices: Can Users' Practices Protect Their Sensitive Data? In *MCIS*, 1.

Świątkowska, Joanna. 2020. Tackling Cybercrime to Unleash Developing Countries' Digital Potential. *Pathways for Prosperity Commission Background Paper Series*, 33.

Tabassum, Farhana, Nazia Akram, and Muhammad Moazzam. 2022. Online Learning System in Higher Education Institutions in Pakistan: Investigating Problems Faced by Students During the COVID-19 Pandemic. *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)* 17 (2): 1–15.

Taha, Nashrawan, and Laila Dahabiyeh. 2021. College Students Information Security Awareness: A Comparison between Smartphones and Computers. *Education and Information Technologies* 26 (2): 1721–1736.

Taneski, Viktor, Marjan Heričko, and Boštjan Brumen. 2014. Password Security—No Change in 35 Years? In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1360–1365. IEEE.

TechABU. 2022. Top 10 Countries With The Most Freelancers 2022. *TechABU*. June 12. https://techabu.co/freelancing/top-10-countries-with-most-freelancers/.

Deursen, Van, J.A.M. Alexander, Ellen Helsper, Rebecca Eynon, and Jan AGM. Van Dijk. 2017. The Compoundness and Sequentiality of Digital Inequality. *International Journal of Communication* 11: 452–473.

Van Dijk, Jan AGM. 2005. *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks, CA: Sage Publications.

Van Ingen, Erik, and Uwe Matzat. 2018. Inequality in Mobilizing Online Help after a Negative Life Event: The Role of Education, Digital Skills, and Capital-Enhancing Internet Use. *Information, Communication & Society* 21 (4): 481–498.

Vehovar, Vasja, Pavle Sicherl, Tobias Hüsing, and Vesna Dolnicar. 2006. Methodological Challenges of Digital Divide Measurements. *The Information Society* 22 (5): 279–290.
Witte, James C., and Susan E. Mannon. 2010. *The Internet and Social Inequalities*. New York: Routledge.
Zhang, Peiqin, and Xun Li. 2015. Determinants of Information Security Awareness: An Empirical Investigation in Higher Education. In *36th International Conference of Information Systems*, 4321–4328.
Zhang, Xiao Juan, Zhenzhen Li, and Hepu Deng. 2017. Information Security Behaviors of Smartphone Users in China: An Empirical Analysis. *The Electronic Library* 35 (6): 1177.