Security Journal (2023) 36:373–405
https://doi.org/10.1057/s41284-022-00343-4

ORIGINAL ARTICLE

Cyber-security and risky behaviors in a developing country context: a Pakistani perspective

Naurin Farooq Khan[1] · Naveed Ikram[1] · Sumera Saleem[1] · Saad Zafar[1]

Accepted: 6 May 2022 / Published online: 29 May 2022

Abstract

Cyber-security behavior research is scant with even scarce studies carried out in developing countries. We examine the cyber-security and risky Internet behaviors of undergraduate students from Pakistan, taking into account the diversity of these students in terms of demographics, socioeconomic status, and the digital divide. Data were collected using a survey questionnaire. A total of 294 students belonging to six different cities of Pakistan were surveyed employing multistage stratified sampling in face-to-face interaction. The results indicated significant differences of cyber-security posture in terms of gender, age and digital divide variables. The profiles of students based on cyber-security and risky Internet behaviors indicate three groups with a majority of them falling into group that exhibits more risk-averse yet low cyber-security behavior. Moreover, proactive cyber-security awareness behavior has a positive impact on high risk-averse behavior. The implications of the findings are studied in terms of providing customized training and awareness. The future directions are laid out for further explorations in terms of cultural differences within and cross-country contexts.

Keywords Cyber-security behavior · Risky behavior · Tertiary institutes · Developing country · Survey

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

Naveed Ikram
naveed.ikram@riphah.edu.pk

Sumera Saleem
sumera.saleem@riphah.edu.pk

Saad Zafar
saad.zafar@riphah.edu.pk

[1] Riphah International University, Main Campus, I-14, Islamabad, Pakistan

Introduction

In the wake of globalization and the complex integration of Information Systems with Information and Communication Technologies (ICTs), cyber-security constitutes an important place. Cyber-security has been defined as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*" (Alahmari and Duncan 2020). Cyber-security being relatively a nascent area of research (Lowry et al. 2017), complex individual behaviors have caught the attention of researchers only recently (Schneier 2015). Cyber-criminals exploit the weak security behavior of individuals to carry out different cyber-crimes. Literature is replete in prescribing technical hardware-software controls to safeguard assets from security threats and consequent breaches (Schneier 2015). Never-the-less, complete reliance on technical cyber-security solutions has been considered insufficient (Abawajy 2014) and various studies are emphasizing the role of non-technical cyber-security interventions in deterring security breaches (Bulgurcu et al. 2010; Haeussinger and Kranz 2013). According to a study within the field of cyber-security research, only 4% of the literature deals with behavioral studies (Gillam and Foster 2020). Moreover, most of the studies from cyber-security behavioral research are from developed countries.

In a connected world, cyber-crimes have a global cost of billions of dollars (Świątkowska 2020) and are not confined by physical borders between nations. Cyber-criminals exploit the rapid increase in the ICTs infrastructure in developing countries (Świątkowska 2020) and inadequate cyber-security behavior (Kshetri 2010) of the citizens to launch attacks on the developed world. There are a few cyber-security behavior studies that have been conducted in developing countries (AlMindeel and Martins 2020) such as Pakistan—a nation that has increased reliance on its ICTs infrastructure and a large number of youngsters fuelling its digital economy ("Payoneer | The Global Gig-Economy Index: Q2 2019, 2020) amid hostile socio-political settings that pose increased cyber-threat to the nation (Shad 2019). Young individuals (Aliyu et al. 2010) indulge themselves in many activities such as sharing passwords and self-disclosure on social media which compromise their cyber-security. These behaviors not only put their personal security at risk but also that of the tertiary institutes they are enrolled in (Al-Janabi and Al-Shourbaji 2016). Various studies have pointed out students' heightened vulnerability to cyber threats compared to other individuals (Jeske and Van Schaik 2017; Mohebzada et al. 2012). Students are regularly exposed to the Internet, have reckless attitudes in using ICTs (Aliyu et al. 2010) and exhibit risky cyber behavior (Sonia Livingstone et al. 2014) as a result of which their exposure to cyber-crimes is comparatively higher (Öğütçü et al. 2016).

With meager cyber-security behavioral contributions in tertiary institutes (Hina et al. 2019), we empirically evaluate the cyber-security practices of university students in the context of a developing country—Pakistan. The survey-based study aims to deepen our understanding of the cyber-security posture of students to further facilitate the development of effective cyber-security policies and practices. In this study, we will first define key terms that are used throughout the paper. Providing definitions to these key terms helps understand the study.

Terminology

Cyber-security behavior is the measure taken and the behavior exhibited by individuals to protect their devices (Zwilling et al. 2020). It is the protective behavior that has positive connotations in which individuals hold cyber-security principles (Stanton et al. 2005).

Cyber-security 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).

Cyber-threat is an event in cyberspace that can potentially cause loss of assets and undesirable consequences as a result (NIST SP 800-160) (Bederna and Szadeczky 2020). According to (Shad 2019), it is the "*action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system*".

Cyber-espionage is defined as collecting classified information without the consent or permission of the owner (Bederna and Szadeczky 2020). Additionally, it is defined by (Paterson and Hanley 2020) as "*the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization*".

Cyber-terrorism is defined as attacks carried out by terrorists using cyberspace (Hua and Bapna 2013). Additionally, it is defined as "*computer attacks intended to cause significant damage in order to coerce or intimidate a government or civilian population*" (Platt 2012).

Phishing is defined as creating a carbon copy of an existing web page to trick users into submitting information that can be of personal or financial nature (Van der Merwe et al. 2005). Additionally, it is defined by (Wang et al. 2020) as the use of spoofed emails by the attackers to trick and lure individuals into sharing sensitive information.

Hacking is defined as gaining unauthorized access to information by malicious actors who use their technical skills to cause harm (Bederna and Szadeczky 2020). It is also defined as "*the attitude and behavior of a group of people who are greatly involved in technical activities which, more commonly today than in previous years, result in gaining unauthorized access*" (Alsunbul et al. 2015).

Malware is a malicious software that is used to exploit computer devices, services and networks (Moser et al. 2007). It is an acronym for malicious software that is a script or a binary code that performs malicious activity and compromises the confidentiality, integrity and availability of the system as defined by (Or-Meir et al. 2019).

Encryption is the process of hiding information utilizing a cipher in such a way that it is not readable to anyone except the one who possesses the cipher key

(Basharat et al. 2012). Additionally, encryption is defined as "the process of translating plaintext message into a form known as ciphertext message". This ciphertext message should not be read by anyone without a process known as decryption (Ahmad et al. 2015).

Multidimensional Poverty Index is the measure of poverty at a national level which is based on three core dimensions of education, health and living standards (Alkire and Santos 2010).

Background

Cyber-crimes and human aspect of cyber-security

Cyber-crimes are growing in both severity and frequency (Bedser 2007). They are predicted to take over traditional crimes (Anderson et al. 2019) in the near future. They are estimated to cost $600 trillion in 2020 which is two times the estimated cost in 2015 (Lallie et al. 2020). At the time of writing of this paper during the current COVID-19 pandemic, the prevalence of cyber-crimes has accelerated at an unprecedented scale (Lallie et al. 2020). Scams and malware attacks have significantly risen with phishing being reported to increase a whopping 600% during march 2020 (Lallie et al. 2020). According to studies, 95% of the cyber-attacks are targeted within home environments (Talib et al. 2010). Existing studies indicated that the majority of computer users lack information security knowledge because of inadequate awareness (Aldawood and Skinner 2018) and do not know how to protect themselves (Kushzhanov and Aliyev 2018). The cyber-security behavior of end-users is more important because regardless of the security of a system, an individual is often a critical backdoor to the network (Bulgurcu et al. 2009; Dodge Jr et al. 2007). Moreover, cyber-security breaches due to human factors are attributed to an individual's act of negligence (Rao and Nayak 2014). Such breaches occur at certain costs to individuals, organizations, and nations. These costs are estimated to be around US$600 to the global economy in 2018. It is for this reason humans are often considered as the weakest link in the cyber-security landscape of any organization and consequently any nation.

Global cyber-security landscape and developing nations

The dependence on ICTs infrastructure and its vulnerability—comprising of both technical and social factors—constitutes the cyber-security landscape of a nation (Shad 2019). With increased development in ICTs and digital transformation, the developing nations are facing cyber threats that may hamper their economic development and disrupt the financial system on a global scale (Świątkowska 2020). Developing nations have crossed the Internet penetration threshold of 10% (Świątkowska 2020) and have started taking necessary steps towards reinforcing the global cyber-security landscape by systematically addressing the related threats. On the other hand, cyber-criminals have started to exploit the lack of inadequate cyber-security awareness and practices of individuals from developing nations (Kshetri 2010) and their national digital infrastructure (Świątkowska 2020) to initiate attacks on the developed nations. Cyber-threats are of concern not only at the regional level but also at the national and international level (Štitilis et al. 2017). Therefore, the weak cyber-security of individuals from developing nations has global implications (Świątkowska 2020). The cyber-security scholarship should be warranted for developing nations particularly those countries that are experiencing increased ICTs development while being the target of increased cyber threats—such as Pakistan.

Pakistan: digital transformation, economic development and cyber-security posture

Amid hostile socio-political environments in domestic as well as regional settings, Pakistan faces increased cyber threats (Shad 2019). With the fast-growing digital economy, the volatile regional conflicts pose cyber threats such as cyber-organized crimes (Shad 2019), cyber-espionage (Rafiq 2020) ("British E-Spy Agency Hacked Network Routers to Access Almost Any Internet User in Pakistan" 2020) and cyber-terrorism. Cyber-crimes like hacking, cyber-harassment and blackmailing on social media are on the rise as per national cyber-crimes agencies (Shad 2019). Similarly, the country had been the target of the highest number of malware attacks in late 2015 (Rafiq 2020). The individuals of the country face being the victims of cyber-terrorism due to the lack of cyber-security practices. Banned outfits operating in the social networks have targeted young individuals to spread their narratives (Salim et al. 2019). Most of the victims of these cyber-crimes are students studying in tertiary institutes. These students are also responsible for the surge in the digital economic development of the country ("Payoneer | The Global Gig-Economy Index: Q2 2019" 2020).

Due to increased unemployment, a large number of young people use digital labor platforms as one of the main sources of income (Berg 2015)—with an average freelancer earning more relative to the average wage in traditional markets (Beerepoot and Lambregts 2015). Pakistan is now ranked 4th in ICT outsourcing (Masood et al., n.d.), bringing home revenue of $1 billion. The limited opportunities in the local labor market in Pakistan has fuelled this growing interest in freelancing (Malik et al. 2020) that is supported by one of the largest young population of under twenty five in the world ("Payoneer | The Global Gig-Economy Index: Q2 2019" 2020). These freelancers are equipped with technically oriented education ("Payoneer | The Global Gig-Economy Index: Q2 2019" 2020) and constitutes 70% of the Pakistani freelance landscape ("Freelancer Salaries & Earnings Income Survey 2020" 2020). Therefore, with students from tertiary institutes being the target of cyber-crimes it is important that they should be the focus of understanding cyber-security posture in Pakistan.

Cyber-security and tertiary institutes

The concerns on the vulnerability of the university environment are as old as 1975 (Kortjan et al 2012). Universities often have high-end and easily accessible but poorly protected digital infrastructure (Zhang and Li 2015). Furthermore, the cyber-security practices/skills and awareness levels among the students are often ignored or not fully addressed in higher education institutes (Moallem 2018). Although students from tertiary institutes are concerned about security (Pramod and Raman 2014), they lack knowledge of cyber-security practices (Chandarman and Van Niekerk 2017). This means that university students may be technologically well informed, but it does not mean that they know how to protect their information and systems effectively (Kim 2014). With this backdrop, this study aims to understand the cyber-security practices rooted in the cyber-security behavior of individuals belonging to tertiary institutes in the context of Pakistan.

Literature review

Cyber-security behavior

Cyber-security behavior research has evolved over the past decade. Authors from a tertiary institute measured the cyber-security behavior of 385 respondents (Öğütçü et al. 2016). The results showed that students were more vulnerable with respect to their risky behavior as compared to academics and staff. Similarly, results from another study (Slusky and Partow-Navid 2012) revealed low cyber-security behavior of students in terms of computer skills, data encryption, data loss, passwords and risks of social networking sites. The study's findings from the survey responses of 397 students showed cyber-security noncompliance behavior of the students, despite their proficiency in security knowledge. A survey of 247 graduate/undergraduate students showed low-security knowledge as well as cyber-security practices (Moallem 2018). The descriptive results highlighted that almost half of the surveyed students self-reported their lack of knowledge in cyber-security and poor password behavior. This entails the inactive role of academic institutes in improving the cyber-security posture of the students. Yet another study surveyed 197 undergraduate students to understand their cyber-security behaviors in five dimensions: web security, email security, cyber-attack prevention, document safety, mobile security, and password security (Kim 2013). A high percentage of students reported their lax attitude in encryption and backup of files, use of anti-virus, frequent change in passwords and keeping their software up to date—which are important security practices. Other studies that were carried out recently also report the poor cyber-security behavior in general users. An online survey consisting of 312 participants revealed users' lack of best practices in password security and against phishing attacks (Cain et al. 2018). Women and younger users kept weaker passwords and exhibited weaker updating software behavior. Moreover, the study finds that those participants who self-reported to be proficient in cyber-security exhibited poor behavior than the non-proficient ones (Cain et al. 2018). The studies described above employed questionnaires that are not validated and thus analysis and consequent findings from such studies may not be valid. Moreover, some of these studies employed cyber-security instruments which only partially examined the security behavior and lacked a holistic measurement of the phenomenon.

The studies that make use of validated instruments to measure cyber-security behavior are also scarce with mostly conducted in industrial organizations. For instance, on a sample of 505 Australian workers (McCormac et al. 2017; Parsons et al. 2014; Pattinson et al. 2015) reported the findings of the cyber-security behavior using the Human Aspect of Information Security Questionnaire (HAIS-Q) and its relationship with gender, personality traits and age. In these studies, age and gender explained the 7% variance in the cyber-security behavior (McCormac et al. 2017) while familiarity with computers was negatively associated with cyber-security behavior (Pattinson et al. 2015). Another study (Gratian et al. 2018) conducted on a sample of 369 participants (including staff, faculty, and students) from a large public university in the USA examined the personality traits, risk-taking preferences and decision-making styles and their correlations with security behavior. The study finds individual differences to account for a 5–23% variance in cyber-security behavior of individuals with females showing weaker password practices and updating behavior (Gratian et al. 2018). The younger participants also exhibited weak cyber-security behaviors in password practices and proactive awareness (Gratian et al. 2018). Another multi-national study from seven countries reported the cyber-security behavior of 3500 participants (Sawaya et al. 2017) using the Security Behavior Intention Scale (SeBIS) instrument. A total of 500 participants (from China, France, Japan, Russia, South Korea, USA and UAE) showed differences in their security behavior with the Japanese exhibiting the least secure behavior. Another empirical study that gauges the cyber-security behavior of health care professionals showed older participants exhibited more secure behavior in some cyber-security aspects (Solic et al. 2019). The scale used in the study was the Users' Information Security Awareness Questionnaire (UISAQ). Another empirical evidence on cyber-security behavior of the 355 secondary school students was reported in (Velki et al. 2017) that showed younger school students to exhibit the least secure password sharing behavior. Similarly, preliminary results from a national sample (Velki and Romstein 2019) comprising of school students and employees from Croatia reported that cyber-security behavior improves when people are in their middle ages.

The limitation of these studies which employ validated scales to measure security behavior is the variances pertaining to different dimensions and/or subscales. Some of these scales are very long containing more than 60 items. This can cause unreliable results due to the lack of interest and motivation of the participants in filling up a great many questions. Another problem with these validated scales is that not all of them are rigorously validated for their content, construct, and criterion validity as well as psychometric properties except SeBIS and HAIS-Q. Secondly, there is a lack of empirical evidence which reflects the experience of cyber-security societal challenge in developing countries (AlMindeel and Martins 2020). As a result, the literature seems to exhibit reporting bias in terms of context and geographical location (Crossler et al. 2013). The findings reported in the context of developed countries may not generalize well to users from less studied regions (Sawaya et al. 2017). There are few notable mentions carried out in developing countries such as Malaysia (Faith et al. 2020) (Muniandy et al. 2017), Oman (Ramalingam et al. 2016) and India (Senthilkumar and Easwaramoorthy 2017) but again these studies lack utilization of proper scales and fail to holistically report the cyber-security behavior.

Understanding the cyber-security posture of developing nations is important since there are differences in the cyber-security behavior of participants from different regions of the world (Sawaya et al. 2017). Findings from the developing countries call for more research in tertiary institutes to better understand the cyber-security posture of students and hence the need for cyber-security training and practices (AlMindeel and Martins 2020).

Risky Internet behavior

Risky behaviors are actions while being online which put people at risk (Milne et al. 2009). These behaviors are negative cyber-security behavior in which there is an increased threat from malicious attacks and the likelihood of a cyber-security breach (Hadlington 2018). Examples of such behavior include sharing personal information and downloading material from illegal websites. Users are not expected to indulge in such activities, but they do so to get short-term gains. Such activities/actions can lead to losses on many fronts (Bechara 2003). People indulge in risky behaviors to get short-term gains that can result in potentially long-term losses (Moore and Gullone 1996). Understanding both cyber-security behavior along with users' engagement in risky online behavior is important and has implications for safe and secure usage of the cyberspace (Hadlington 2018).

Risky behavior by younger users is a well-studied phenomenon (Boyer 2006; Jessor et al. 1977). Studies have shown that compared to other groups, students are more exposed to online risks (Staksrud et al. 2013). Students exhibit many online risky behaviors such as: visits to harmful sites, meeting face-to-face with strangers, being exposed to banned outfits, online abuse and sharing personal information with strangers to name a few (De Moor et al. 2008; Gamez-Guadix et al. 2016; Livingstone and Haddon 2009; Livingstone et al. 2012). Longitudinal studies also report an increase in these risks (Valcke et al. 2011). Studies have also shown a direct relationship between risky behavior and the ratio of exposure to crime/negative online experience (Öğütçü et al. 2016). Most of the studies conducted on risky Internet behavior are from developed countries with very little emphasis given to developing countries (Waheed 2019).

Keeping in mind the gaps in the cyber-security behavioral research, we conduct an empirical study to measure cyber-security and risky Internet behaviors. We conduct this study in Pakistan—a developing country—to understand the cyber-security posture of tertiary institute students along with their risky behavior. We employ (1) demographic variables such as gender, age, languages; (2) socioeconomic variables such as poverty level of the region, urban/rural living and (3) digital divide variables such as frequency of Internet use, multiple places of Internet access to explore the cyber-security posture. There are not many studies that make use of socioeconomic and digital divide variables to demonstrate the cyber-security posture in a national setting. We also make profiles of the students based on their risky and cyber-security behaviors to better understand the phenomenon. Moreover, we try to find the factors in terms of different cyber-security practices that affect risky Internet behavior. Specifically, we try to answer the following research questions:

RQ1 How do students' risky Internet behavior and cyber-security behavior differ across gender, age, socioeconomic status and digital divide?

RQ2 What are the profiles of students in terms of risky Internet and cyber-security behaviors?

RQ3 Do different types of cyber-security behaviors predict students' risky Internet behavior?

Methodology

To measure the cyber-security and risky behaviors of university students, a survey containing two instruments was conducted in January 2020. In the subsections below, we discuss the instruments used, the sampling strategy, workflow, and statistical significance of the results.

Instruments

Security Behavior Intention Scale (SeBIS): It's a validated scale for measuring the computer security attitudes and related behavior of the end-users (Egelman and Peer 2015). It is a 16 items scale that measures the four underlying constructs namely, (1) Device Securement, (2) Password Generation, (3) Proactive Awareness and (4) Updating Behavior. The first construct measures the cyber-security behavior in terms of securing devices (SeBIS items 1–4), the second construct measures the password-related behavior (SeBIS items 5–8) and the third construct measures the overall vigilance of users while browsing different websites (SeBIS items 9–13). The last construct measures the updating software behavior to secure devices (SeBIS items 14–16). The SeBIS is 5 points Likert scale and has been validated by correlating it with existing psychometrics (Egelman and Peer 2015). Its criterion validity has also been established by experimental results to see if the participants' self-reported security intentions coincide with their actual security behavior. High correlations between each of the SeBIS four dimensions and relevant computer security behavior (Egelman et al. 2016) have established the self-reports to be valid. Moreover, Cronbach's $\alpha = 0.81$ is also high which is a very good indicator of its internal reliability. The self-reported data from SeBIS have helped forecast long-term exposure risks and resulted in moderate accurate predictions (Sharif et al. 2018). It's a comparatively short instrument and has the potential to give reliable results thus giving a true image of the human component in cyber-security behavior research compared to other bigger scales (Velki and Šolić 2019).

Risky Behavior Scale (RBS): It's a 16 items Likert scale (Gökçearslan and Seferoğlu 2016). The scale measures the risky behavior on the Internet such as meeting people face-to-face from online sites, accessing sexual content, online abuse and deactivating filter programs. The scale has been adapted from the risky use of Internet communication tools for university students. Factor analysis has been performed to determine the suitability of the scale in the original study and it reported a one-factor structure. The reliability of the scale in the original study is very high with Cronbach's $\alpha = 0.95$. In our sample, the Exploratory Factor Analysis (EFA) was performed with a one-factor structure—it explained 24% of the variance. The *Kaiser–Meyer–Olkin* (KMO) measure had a value of 0.73 and *Bartlett's Test* of Sphericity had a p-value less than 0.001 which showed an adequate sample size. All items loaded onto a one-factor structure with values 0.3 to 0.6. The Cronbach's α for our sample was 0.76.

Variables

Socio-Demographic Variables: The socio-demographic variables for our study consist of gender, age, languages and socioeconomic status. The age is an ordinal variable with the age group of 18–20 years old coded as 1, 21–25 years old coded as 2 and above 25 years old participants coded as 3. The languages variable is categorical with code 1 for national language, 2 for local language and 6 for multiple languages spoken at home.

For socioeconomic status, we take poverty strata as described by Multidimensional Poverty Index (MPI) ("Multidimensional Poverty in Pakistan" 2018). It is a better indicator of socioeconomic status like social class (Goldthorpe et al. 1982) compared to selected years of formal education as a proxy for socioeconomic status (Dodel and Mesch 2019). Based on the MPI, the country is divided into 8 poverty strata. Districts falling in poverty brackets of (1) less than 10%, (2) 10–19.9%, (3) 20–29.9%, (4) 30–39.9%, (5) 40–49.9%, (6) 50–59.9%, (7) 60–69.9%, and (8) more than 70%. The poverty strata variable is ordinal and is coded as 1 to 8, representing the socioeconomic status respectively. We also make use of the distribution of participants belonging to urban and rural areas as a dichotomous variable.

Digital Divide Variables: To assess the inequalities in digital access, we take frequency of Internet access and access of Internet from multiple places variables. The frequency of Internet access is measured as 3 ordered categories coded as 1 to represent multiple times a day, 2 to represent once a day and 3 to represent once a week. Access of Internet from various places is coded as follows: 1 to represent Internet access from home, 2 for school/university, 3 for work, 4 for friends/family and 6 to represent Internet access from multiple places.

Sampling method

The sampling method adopted for the research was stratified multistage sampling (Jain and Hausman 2006) in which multistage sampling is combined with stratification. The advantage of stratification is that it narrows the difference between different types of individuals through classification, which is conducive to extracting representative samples (Shi 2015) and reducing the sample size. (1) At stage 1 of multistage sampling, the stratification of the country population was done by Multidimensional Poverty Index (MPI) into 8 strata ("Multidimensional Poverty in Pakistan" 2018). (2) At Stage 2, the universities were identified which were established in the districts/cities of the MPI-based 8 strata. (3) At stage 3, the Sindh province of the country was chosen based on convenience sampling. The reason for choosing

Sindh is due to an increased number of university students falling victim to cyber-crimes. (4) At Stage 4, one university was chosen from each stratum from Sindh. (5) At stage 5, students from each university were randomly selected. This multistage sampling resulted in the selection of 6 universities. It should be noted here that not all of the cities/districts in 8 MPI-based strata have a recognized operational university. Therefore, in our sampling, only 6 of the MPI-based strata represent the sample in the selected province.

The average time calculated to fill in the survey was 10–15 min. The mode of the survey was traditional paper and pencil format. Doing so allowed the researchers to control the settings and circumvent the undesirable patterns in responses (Johnson 2005). The direct contact with the participants allowed for personalization and face-to-face interaction hence the environmental distractions and attention deficit (Meade and Craig 2012) were controlled. The first and third authors of this research traveled to each of the six universities in different districts of Sindh in a 15-days road trip. The universities were contacted beforehand through the Office of Research Innovation and Commercialization (ORIC) to take permission for the conduction of the survey. Before the survey, the authors explained the purpose of the questionnaire to the students and advised them to ask any question that they fail to understand. Moreover, they were assured of the anonymity of their responses. Any student not willing to take part in the survey was removed from the sample. After completion of the survey, the students were given a small seminar on safe and secure habits to adopt while being online. A counseling session followed the seminar in which the troubled students who became victims of cyber-crimes were given advice.

The responses received via paper and pencil were coded and numbered. A total of 328 participants filled in the questionnaire. The data from the responses were entered into excel by a data entry operator and the validation of the data was also carried out. The cleaning of data followed. Incomplete entries were removed from the sample. A total $\text{response}_{\text{min}} \geq 281$ was recorded for the two scales. A total of ($N=294$) responses were received for Risky Behavior Scale (male = 166) and ($N=281$) for Security Behavior Intention Scale (male = 157).

Descriptive statistics

In order to characterize the sample of this research, demographics (Table 1) show that males constituted more than 56% for both SeBIS and RBS scales. Participants in the age group of 18–20 were approximately 54% and 56% for RBS and SeBIS scales. Almost 60% of the participants spoke the local language at home whereas approximately 8% spoke multiple languages. Similarly, half of the participants (55%) belonged to urban areas in the country. On digital divide variables, 47% of the participants accessed the Internet from their homes and almost 6% of the participants accessed the Internet from their friends/family while 23% accessed from multiple places. Frequencies of poverty strata are detailed in Table 1.

Descriptive statistics for SeBIS and RBS responses are provided in Tables 2 and 3. Students showed low cyber-security in many areas. Almost 90% of the students do not change their passwords unless they have to due to any reason. A total of 13%

Table 1 Frequency analysis of variables

Variables	Responses	SeBIS	%	RBS	%
Gender	Female	124	44	128	43.5
	Male	157	56	166	56.5
Age	18–20 years	157	55.9	159	54.1
	21–25 years	114	40.6	122	41.5
	Above 25	10	3.6	13	4.4
Languages	National	82	29.2	90	30.6
	Local	176	62.6	180	61.2
	Multiple	23	8.2	24	8.2
Frequency of internet access	Multiple times a day	246	87.5	253	86.1
	Once a day	21	7.5	25	8.5
	Once a week	14	5.0	16	5.4
Access of internet from various places	Home	134	47.7	139	47.3
	University	49	17.4	48	16.3
	Work	15	5.3	18	6.1
	Friends/family	17	6.0	19	6.5
	Multiple places	66	23.5	70	23.8
Urban/rural	Urban	155	55.2	162	56.1
	Rural	126	44.8	127	43.9
Poverty strata	Less than 10%	32	11.4	31	10.5
	20–29.9%	25	8.9	35	11.9
	30–39.9%	69	24.6	63	21.4
	40–49.9%	34	12.1	35	11.9
	50–59.9%	94	33.5	103	35
	60–69.9%	27	9.6	27	9.2

of the students do not include special characters in their passwords. Almost 60% of students open links without verifying first where do they go and continue doing work despite discovering a security problem. Similarly, 70% of the students see the look and feel rather than the URL bar to recognize the website they are visiting. In device securement, 26% of the students do not set the computer screen to auto-lock if they don't use it for a prolonged period while 15% don't manually lock their screens when they step away from it. A total of 13% and 6% of students do not lock their computers and mobile phones with a password/pin code.

The students tend to engage in different risky behaviors such as almost 20% share their photos with unknown people, receive emails with sexual content, and visit websites about weapons and explosives and share secrets on the Internet. Similarly, almost 30% of the students reported visiting websites that encourage violence, illegal activities and humiliated a particular group as well as receiving sexual content or joining social media groups that had violent content. Almost 10% of the students reported visiting websites that encourage suicide and drug use. The most intense risky behaviors include: 65% of the students publishing personal photographs on

Table 2 Risky behavior scale descriptive statistics

RBS Questions		Always	Often	Sometimes	Seldom	Never
1. Send photos to unknown people	N	6	11	38	9	230
	%	2.0	3.7	12.9	3.1	78.2
2. Meeting unknown people	N	9	19	46	17	203
	%	3.1	6.5	15.6	5.8	69.0
3. Publishing photograph on social networks	N	66	38	71	12	107
	%	22.4	12.9	24.1	4.1	36.4
4. Visiting websites that encourage violence and illegal activities	N	21	12	39	4	218
	%	7.1	4.1	13.3	1.4	74.1
5. Belong to groups with violent content	N	20	8	35	7	224
	%	6.8	2.7	11.9	2.4	76.2
6. Visit websites with sexual content	N	8	6	51	22	207
	%	2.7	2.0	17.3	7.5	70.4
7. Receive emails with sexual content	N	3	5	39	9	238
	%	1.0	1.7	13.3	3.1	81.0
8. Visit websites whose aim is to humiliate a particular group	N	8	13	45	8	220
	%	2.7	4.4	15.3	2.7	74.8
9. Belong to online groups which humiliate a particular group	N	6	5	33	13	237
	%	2.0	1.7	11.2	4.4	80.6
10. Visit website with weapons and explosives	N	4	9	32	13	236
	%	1.4	3.1	10.9	4.4	80.3
11. Let other know user name and password	N	4	5	23	10	252
	%	1.4	1.7	7.8	3.4	85.7
12. Visit websites that encourage suicide	N	1	0	26	3	264
	%	0.3		8.8	1.0	89.8
13. Visit websites that encourage drug use	N	4	3	16	6	265
	%	1.4	1.0	5.4	2.0	90.1
14. Share secrets over the Internet	N	7	6	27	11	243
	%	2.4	2.0	9.2	3.7	82.7
15. Give personal information on website to win free prizes	N	10	9	63	20	192
	%	3.4	3.1	21.4	6.8	65.3
16. Download illegal material	N	12	17	78	16	171
	%	4.1	5.8	26.5	5.4	58.2

social networking sites and 42% of students downloading illegal material from websites. Similarly, a total of 35% of students reported giving out their personal information in order to win free prizes while 30% meet people they only know online.

Results based on inferential statistics

For inferential analysis, we employ univariate and multivariate analyses. The *Shapiro–Wilk* test for normality with $p < = 0.05$, as well as the normal Q-Q plots showed that the data were not normally distributed. To answer research question 1, the data were analyzed using non-parametric tests (univariate analysis) for both SeBIS and RBS scores. We used *Mann–Whitney's U* test for gender and

Table 3 Security behavior intention scale descriptive statistics

SeBIS Questions		Always	Often	Sometimes	Seldom	Never
1. Set computer lock	N	114	29	53	11	74
	%	40.6	10.3	18.9	3.9	26.3
2. Use of password to unlock	N	210	15	17	2	37
	%	74.7	5.3	6.0	0.7	13.2
3. Manual lock of computer after stepping away	N	150	31	52	5	43
	%	53.4	11	18.5	1.8	15.3
4. Pin/passcode to unlock mobile	N	241	9	10	4	17
	%	85.8	3.2	3.6	1.4	6.0
5. Do not change password unless needed	N	150	41	54	5	31
	%	53.4	14.6	19.2	1.8	11.0
6. Use different passwords for different accounts	N	120	29	58	16	58
	%	42.7	10.3	20.6	5.7	20.6
7. Use of password that goes minimum requirement	N	86	51	77	14	53
	%	30.6	18.1	27.4	5.0	18.9
8. Do not include special characters in passwords	N	84	42	53	15	87
	%	29.9	14.9	18.9	5.3	31.0
9.Opening link without verifying	N	44	37	77	17	106
	%	15.7	13.2	27.4	6.0	37.7
10. Recognize websites based on look and feel	N	62	45	80	18	76
	%	22.1	16.0	28.5	6.4	27.0
11. Submitting information without ensuring its safety	N	42	26	63	28	122
	%	14.9	9.3	22.4	10.0	43.4
12. Mouse over links to see where they go	N	69	47	78	21	66
	%	24.6	16.7	27.8	7.5	23.5
13. Continue doing work despite discovering security problem	N	33	30	90	17	111
	%	11.7	10.7	32.0	6.0	39.5
14. Installing software updates	N	75	44	84	28	50
	%	26.7	15.7	29.9	10.0	17.8
15. Use of updated programs	N	106	51	83	18	23
	%	37.7	18.1	29.5	6.4	8.2
16. Regularly updating anti-virus	N	74	38	97	27	45
	%	26.3	13.5	34.5	9.6	16.0

urban/rural and *Kruskal–Wallis* test for age, languages, poverty strata, frequency of Internet access and access of Internet from different places. The homogeneity of variance was checked using non-parametric *Levene's* test on the rank transform data as described by (Nordstokke and Zumbo 2010). To answer research question 2, we performed a cluster analysis (two-way clustering) on SeBIS and RBS scores to profile the students (multivariate analysis). Moreover, to find the differences among the profiles of students with respect to gender, age, languages, poverty strata, frequency of Internet access and access of Internet from different places—we performed *Pearson's Chi-Square* test. We performed a multiple regression analysis to see the impact of different security behaviors in predicting risky Internet behavior for answering research question 3.

Security behavior intention scale

The total SeBIS score is calculated by adding scores of 16 items. The highest score for the SeBIS scale is 80 while the lowest is 16. Higher SeBIS scores correspond to better security behavior. The reliability of the SeBIS scale was calculated by Cronbach's $\alpha = 0.75$ in our sample. Tables 4 and 5 show the inferential statistics between SeBIS and demographics, socioeconomic status and digital divide variables.

SeBIS and socio-demographic variables

A *Mann–Whitney's U* test was run to evaluate the difference in SeBIS scores across males/females and urban/rural areas (Table 4). The assumption of homogeneity of variance was satisfied with $p = 0.788$. We found no significant difference with $U = 9609$, $Z = -0.185$ and $p = 0.853$ between the males and females. Similarly, no significant differences were found $U = 9665.00$, $Z = -0.148$ and $p = 0.883$ in the SeBIS score between participants belonging to urban and rural areas (Table 4). The homogeneity of variance was satisfied with $p = 0.216$.

We carried out the *Kruskal–Wallis* test to find the statistically significant difference mean SeBIS scores for age, languages and poverty strata (Table 5). There was no statistically significance differences between age groups χ^2 (2, $N = 281) = 1.005$, $p = 0.605$ and language groups χ^2 (2, $N = 281) = 3.176$, $p = 0.204$. Similarly, the *Kruskal–Wallis* test indicated that there were no statistically significant differences in the SeBIS scores across the poverty strata χ^2 (2, $N = 281) = 10.079$, $p = 0.073$.

Table 4 Mann–Whitney's tests for SeBIS and RBS

Variables	N	Mean rank	Sum of ranks	*U*	*p*
SeBIS					
Gender				9609.00	0.853
Male	157	141.80	22,262.00		
Female	124	139.99	17,359.00		
Socioeconomic				9665.00	0.883
Urban	155	140.35	21,755.00		
Rural	126	141.79	17,866.00		
RBS					
Gender				5736.00	0.000***
Male	166	118.05	19,597.00		
Female	128	185.69	23,768.00		
Socioeconomic				9259.00	0.144
Urban	162	151.35	24,518.00		
Rural	127	136.91	17,387.00		

Table 5 Kruskal–Wallis tests for SeBIS scores

Variables	N	Mean	*df*	χ^2	*p*
SeBIS					
Poverty strata			5	10.079	0.073
Less than 10%	32	108.09			
20–29.9%	25	120.28			
30–39.9%	69	155.03			
40–49.9%	34	149.75			
50–59.9%	94	140.40			
60–69.9%	27	154.39			
SeBIS					
Age			2	1.005	0.605
18–20	157	136.94			
21–25	114	145.40			
Above 25	10	154.55			
SeBIS					
Languages			2	3.176	0.204
National	82	134.91			
Local	176	140.20			
Multiple	23	168.80			
SeBIS					
Frequency of Internet access			2	10.510	0.005**
Multiple times a day	246	146.89			
Once a day	21	103.26			
Once a week	14	94.07			
SeBIS					
Internet access from different places			4	0.875	0.928
Home	134	138.07			
University	49	141.46			
Work	15	133.13			
Friends/family	17	140.76			
Multiple places	66	148.46			

SeBIS and digital divide variables

To test the statistically significant differences in access of Internet groups and frequency of Internet access groups, the *Kruskal–Wallis* test was carried out (Table 5). No statistically significant differences were observed between access of Internet from various places groups with ($F(2,278) = 0.114$, $p = 0.978$).

A *Kruskal–Wallis* test indicated that there were statistically significant differences in the SeBIS scores across the frequency of Internet access, χ^2 (2, $N = 281$) = 10.510, $p = 0.005$, $\varepsilon^2 = 0.04$. Dunn's pairwise tests were carried out for the three pairs of groups. There was very strong evidence (p < 0.03, adjusted using the Bonferroni correction) of a difference between the group that accessed the Internet multiple times a day with groups accessing Internet once a day ($Z = 43.630$, $p = 0.054$) and once a week ($Z = 52.821$, $p = 0.054$). There was no significant difference between the group who accessed the Internet once a day and the group that accessed once a week ($Z = 9.910$, $p = 1.00$). The mean rank of the group that accessed the Internet multiple times a day was 146.89 and for groups who accessed Internet once a day was 103.26, and those who accessed Internet once a week was 94.07. Students accessing the Internet more frequently exhibited more secure behavior compared to students who accessed the Internet once a day or once a week.

Risky behavior scale (RBS)

The total RBS score of the participants was calculated by adding scores of 16 items. The highest score for the RBS scale is 80 while the lowest is 16. Higher scores correspond to high aversion towards risky behavior i.e., participants exhibit less risky Internet behavior. The Cronbach's α of RBS in our sample was 0.76. Tables 4 and 6 show the inferential statistics between RBS and demographics, socioeconomic status and digital divide variables.

Risky behavior scale and socio-demographics variables

We ran a *Mann–Whitney's U* test to evaluate the difference in the responses of males/females and those belonging to urban/rural areas (Table 4). The assumption of homogeneity of variance was satisfied with $p = 0.142$ which is greater than 0.05. We found a significant difference between male and female groups. The mean ranks of males and females were 118.05 and 185.69, respectively; ($U = 5736$, $Z = -6.776$, $r = 0.39$) with $p = 0.0001$. Females were more conscious of their behavior and exhibited less risky behavior than males. We found no significant difference with $U = 9259$, $Z = -1.461$ and $p = 0.144$ between RBS and urban/rural. The assumption of homogeneity of variance was satisfied with $p = 0.480$.

A *Kruskal–Wallis* test (Table 6) indicated that there were statistically significant differences in the risky behavior scores across the age groups, χ^2 (2, $N = 294$) $= 7.481$, $p = 0.024$, $\varepsilon^2 = 0.02$. The assumption of equal variances was satisfied with $F(2) = (0.597$, $p = 0.551)$. Dunn's pairwise tests were carried out for the three pairs of groups. There was very strong evidence ($p < 0.033$, adjusted using the Bonferroni correction) of a difference between the group aged 18–20 and the group aged 21–25 with ($Z = 25.44$, $p = 0.038$). There was no significant difference between the group aged 16–20 and the group aged above 25 ($Z = -16.116$, $p = 1.00$) as well as between the group aged 21–25 and the group aged above 25 (Z = -41.560, $p = 0.280$). The mean rank of age group 21–25 was 131.90 and that of age group 18–20 was 157.35. Students aged 18–20 exhibited less risky behavior compared to students aged 21–25. A *Kruskal–Wallis* test indicated that there were no statistically significant differences in the risky behavior scores across the poverty strata, χ^2 (5, $N = 294$) $= 3.223$, $p = 0.666$. Similarly, there were no statistically significant

Table 6 Kruskal–Wallis tests for RBS scores

Variables	N	Mean	*df*	χ^2	*p*
RBS					
Poverty Strata			5	3.223	0.666
Less than 10%	31	152.37			
20–29.9%	35	132.46			
30–39.9%	63	152.72			
40–49.9%	35	137.71			
50–59.9%	103	146.40			
60–69.9%	27	166.11			
RBS					
Age			2	7.481	0.024*
18–20	159	157.35			
21–25	122	131.90			
Above 25	13	173.46			
RBS					
Languages			2	4.715	0.095
National	90	163.01			
Local	180	141.99			
Multiple	24	130.63			
RBS					
Frequency of Internet access			2	0.317	0.853
Multiple times a day	253	147.58			
Once a day	25	140.42			
Once a week	14	137.89			
RBS					
Access of Internet from various places			4	9.450	0.051
Home	139	159.59			
University	46	144.15			
Work	18	151.11			
Friends/family	19	109.92			
Multiple places	70	130.80			

differences in the risky behavior scores across the languages, χ^2 (2, $N=294$) $=4.715$, $p=0.095$.

RBS and digital divide variables

A *Kruskal–Wallis* test in Table 6 indicated that there were no statistically significant differences in the risky behavior scores across the places of Internet access, χ^2 (4, $N=294$) $=9.450$, $p=0.05$. Similarly, there were no statistically significant differences in the risky behavior scores across the frequency of Internet access, χ^2 (2, $N=294$) $=0.317$, $p=0.853$.

Cluster analysis

Cluster Analysis is one of the leading methods for multivariate analysis (Kettenring 2006). It is used to profile the participants by grouping them into clusters based on the similarity or closeness of the measures—the clusters themselves are distinct from each other. It is considered to give more accurate and unbiased results than heterogeneous data (Kayri 2007) and reduces the number of variables for comparison hence interpreting results easier (Johnson 1998). A two-way cluster analysis was carried out to find the profiles of the participants in terms of their security practices and aversion towards risky behaviors (RQ2). The participants best fit into three clusters when clustering was performed on RBS and SeBIS scores considering 1–15 subgroups. The Bayesian Information Criterion (BIC) value for the 3-cluster solution was BIC (276.107) and the ratio of distance measures (2.044) with good silhouette measure of cohesion and separation. The ratio of the largest cluster size to the smallest cluster was 2.8. Figures 1, 2, and 3 depict the three clusters in which the light pink color denotes the overall score distribution among participants and the maroon color denotes the cluster score distribution. Cluster 1 contained 36.3% participants with a median RBS score of 70.97 and SeBIS score of 61.03. The majority of the students were in cluster 2 that contained 47.3% participants with a median RBS score of 72.98 and SeBIS score of 50.97. Cluster 3 contained 16.4% participants and a median RBS score was 54.3 whereas SeBIS score was 54.42.

The participants in cluster 1 have high RBS and SeBIS scores which means that they had good security practices and exhibited low risky behavior with a profile as low risky—good security behavior. The participants in cluster 2 had high RBS scores and low SeBIS scores so they were profiled as low risky—low-security behavior. The participants in the third cluster had low RBS scores and low SeBIS scores; therefore, they were profiled as high risky—low-security behavior (Fig. 4).

Each *Kruskal–Wallis* test, which were ran for SeBIS and RBS, indicated statistically significant differences among the three clusters as shown in Table 7, hence validating the three clusters. To find the differences between profile groups with respect to gender, age, languages, poverty strata, urban/rural living, frequency of

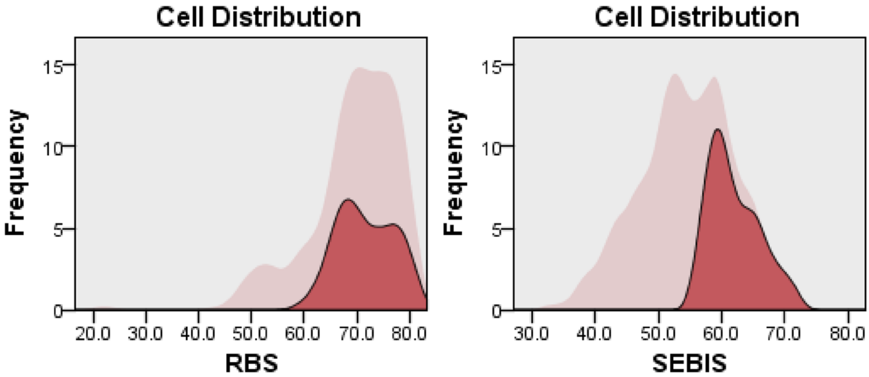

Fig. 1 Cluster 1 score distribution for RBS and SeBIS scales

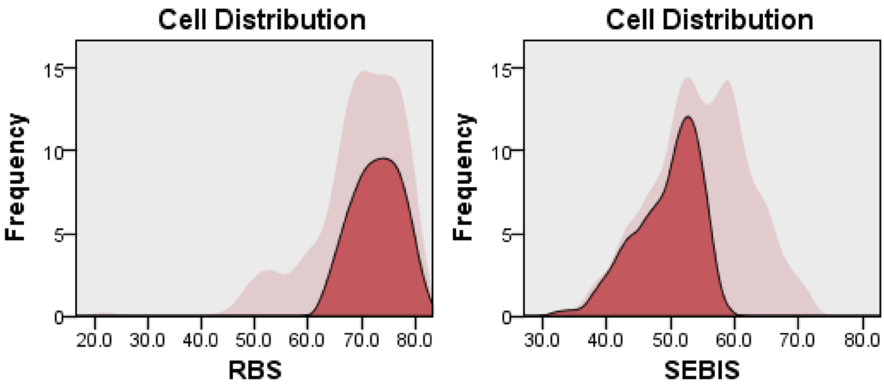

Fig. 2 Cluster 2 score distribution for RBS and SeBIS scales

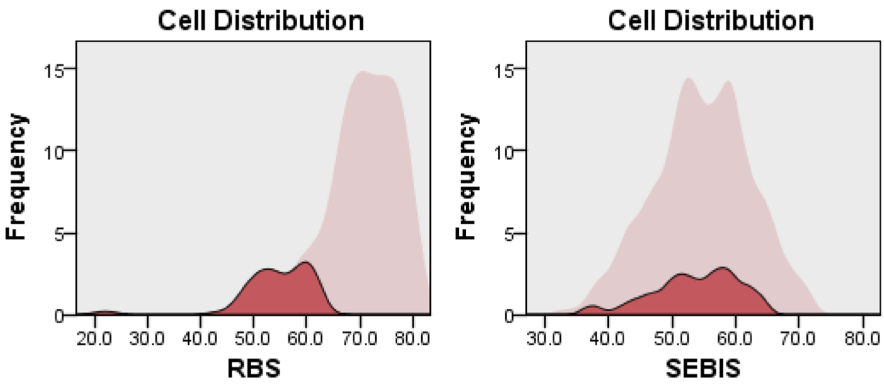

Fig. 3 Cluster 3 score distribution for RBS and SeBIS scales

Internet access and access of Internet from various places, we performed *Pearson's* C*hi-Square*. Where significant results were found, post hoc analysis was carried out using *Bonferonni* correction. The analysis showed significant results for gender χ^2 (3,281) = 16.019, p < 0.001. The post hoc analysis using *Bonferroni* adjustment showed that the percentage of males (82.6) was more in cluster 3 than females (17.4). That means more males exhibited high risky behavior and low cyber-security habits. The analysis also shows significant results for languages χ^2 (4,281) = 9.477, p = 0.050 and for frequency of Internet access with χ^2 (4,281) = 9.183, p = 0.057. However, the post hoc analyses with Bonferroni adjustment did not show significant differences among different clusters. The analysis also shows significant results for poverty strata with χ^2 (10,281) = 18.094, p = 0.097. The post hoc analysis using Bonferroni adjustment showed that the percentage of students in 20–29.9 poverty stratum were more in cluster 3 and exhibited high risky behavior and low cyber-security habits.

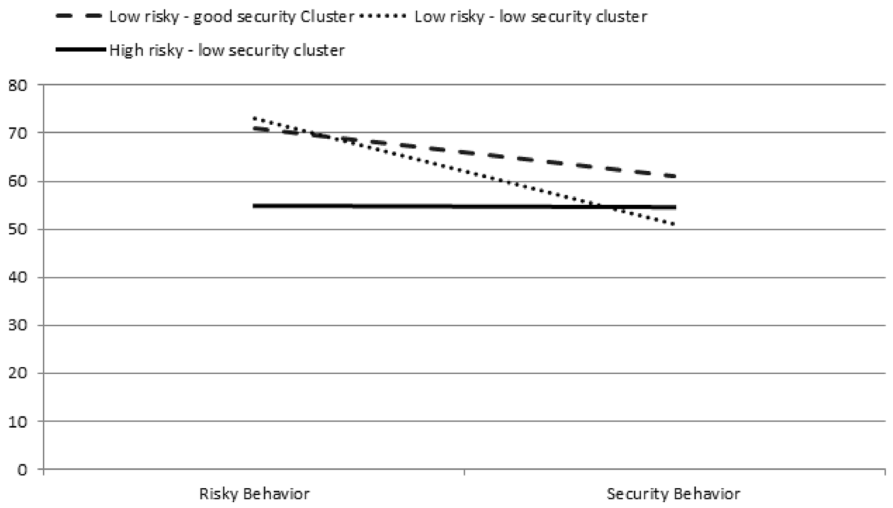

Fig. 4 Three clusters and their RBS and SeBIS median scores

Table 7 Kruskal–Wallis results among SeBIS and RBS

Scale	Profiles of students			χ^2
	Low risky – good security (N = 102)	Low risky – low security (N = 133)	High risky – low security (N = 46)	
RBS	171.12	171.12	23.86	117.024, p = 0.0001
SeBIS	223.40	81.20	131.18	177.902, p = 0.0001

Multiple regression analysis

To answer our research question 3, a multiple linear regression using enter method was carried out to predict risky Internet behavior based on different types of cyber-security behaviors. The dependent variable was RBS and the independent variables were Device Securement, Password Generation, Proactive Awareness and Updating Behavior whereas the control variables constituted demographics, socioeconomic and digital divide variables (gender, age, languages, Internet access from various places and frequency of Internet access). The control variables were converted into dummy variables. The assumptions for carrying out the regression analysis were checked before the process. To ensure that there was no multicollinearity, the values of tolerance (0.4) and variance inflation factor VIF (1.9) indicated that no violation of the assumption took place. A *Durban-Watson* statistics was used to test the assumption of independence of residuals values. The value of 2.1 showed that the assumption was not violated and observations were not correlated to each other. The P-P plots showed that the assumption of residuals to be normally distributed was not violated and scatter plots indicated that the data did not have heteroscedasticity. The value of the cook's distance was found to be less than 1 hence the assumption of bias from any cases was not violated. The Table 8 presents the results of a multiple hierarchal regression analysis which we performed in two steps. The first step contained only demographics, digital divide and socioeconomic variables and in second, Device Securement, Password Generation, Proactive Awareness and Updating Behavior variables were added. The *ANOVA* test of explained and residual variances showed that the Model 1 explained 18% of the variance in risky behavior with $F(17, 276) = 3.546$, $p < 0.000$ and adjusted $R^2 = 0.136$. With addition of SeBIS dimensions, the model 2 also explained the risky behavior when controlling for demographic, digital divide and socioeconomic variables with R^2 of 0.278 and $F(21, 276) = 4.674$, $p < 0.000$. The model 2 explained the additional variance of 9% with $\Delta R^2 = 0.089$ which is a small size effect. The proactive awareness security behavior ($B = 0.654$, $t = 4.886$, $p < 0.000$) contributed significantly to predict RBS (Table 8). Students who exhibited high proactive awareness security behavior were also highly conscious of their Internet risky habits. Standardized estimates of regression coefficients for Proactive Awareness were ($\beta = 0.269$) which indicated that 27% of the variance in RBS was accounted for by proactive awareness security behavior.

Discussion

Overview and findings

This study sheds light on the cyber-security and risky behaviors of university students from a developing country's perspective. Our findings show that although the overall SeBIS and risky behavior scores are above the total average, they cannot be attributed to good cyber-security practices. The low probability and high consequences attributed towards cyber-security breaches entail that cyber-security incidents may be rare but when they do happen, the damage and cost associated with them is quite high. Moreover, the majority of students in our study belong to low risky—low-security cluster. When individual risky behavior in our study is taken into account, we see that 30% of the students agreed to meet strangers in person whom they have known online while 20% received emails containing sexual content. These findings are similar to other studies where students less than 18 years of age tend to show these risky behaviors irrespective of gender, age, frequency of Internet use and places of Internet access (Gamez-Guadix et al. 2016; Staksrud et al. 2013).

Our study shows no significant difference between males and females in terms of cyber-security behavior. This is in line with the findings from (Pattinson et al. 2015) where no gender differences were found in the Behavior component of the HAIS-Q dimensions. Our findings are contrary to (McCormac et al. 2017) where females were reported to show stronger cyber-security behavior in terms of knowledge, attitude, and awareness as a whole. Similarly, other studies also show no gender differences in terms of cyber-security behavior such as (Cain

Table 8 Multiple hierarchical regression analysis on RBS ($N = 281$)

	Model 1		Model 2	
	B	*β*	*B*	*β*
Constant	75.215(1.78)		67.549(3.99)	
Control variables				
Demographics				
Gender	− 5.949(1.06)	− 0.351***	− 6.005(1.01)	− 0.355***
Age—20–25	− 0.373(1.12)	− 0.022	− 0.081(1.07)	− 0.005
Age—> 25	4.494(2.67)	0.104	4.799(2.54)	0.111
Languages—national	− 0.191(1.25)	− 0.010	0.061(1.20)	0.003
Languages—multiple	− 2.713(1.88)	− 0.094	− 3.042(1.80)	− 0.106
Digital divide				
Internet access—work	− 4.701(2.43)	− 0.0118	− 3.656(2.33)	− 0.092
Internet access—university	0.246(1.65)	0.011	0.981(1.58)	0.043
Internet access—friends/family	− 0.629(2.15)	− 0.018	0.219(2.06)	0.006
Internet access—multiple places	0.058(1.38)	0.003	0.105(1.32)	0.005
Frequency of Internet access—once a week	− 2.56(2.23)	− 0.071	− 4.051(2.18)	− 0.113
Frequency of Internet access—once a day	0.815(2.01)	0.024	− 0.329(1.94)	− 0.010
Socioeconomic status				
Urban/rural	− 1.726(1.15)	− 0.101	− 1.276(1.10)	− 0.075
< 10% poverty	0.081(2.09)	0.003	1.235(2.03)	0.046
20–29.9% poverty	− 6.304(2.17)	–	− 5.745(2.07)	–
40–49.9% poverty	− 1.464(2.03)	0.219***	− 0.747(1.98)	0.199***
50–59.9% poverty	− 0.015(1.53)	− 0.055	0.742(1.50)	− 0.028
60–69.9% poverty	− 1.246(2.15)	− 0.001		0.042
		− 0.045	− 1.48(2.07)	− 0.054
Security behavior variables				
Device securement			− 0.156(.12)	− 0.075
Password generation			0.094(.16)	0.033
Proactive awareness			0.654(.13)	0.269***
Updating behavior			− 0.262(.15)	− 0.099
Model fit				
R^2	0.189		0.278	
Adjusted R^2	0.136		0.218	

No. observations 281

Standard errors are in parentheses, ***$p < .001$

et al. 2018; Sawaya et al. 2017). Our findings are also contrary to studies (Gratian et al. 2018; Solic et al. 2019) in which females are reported to have weaker cyber-security behavior (Anwar et al. 2017; Gratian et al. 2018) in some dimensions such as password generation and updating software while having strong cyber-security behavior in other (Solic et al. 2019; Velki et al. 2017) subscales such as backups and usual behavior. On the other hand, females were reported to have a high aversion towards risks in our study similar to (Valcke et al. 2011) where males reflected a significantly higher level of Internet risky behavior when compared to females. The cluster analysis corroborates these findings where more males exhibited high risky behavior yet low cyber-security practices. These findings could be explained by reports that women are more aware of regulations and tend to have superior ethical values (Titi 2003) as well as higher cyber-security awareness (McCormac et al. 2017) than men.

We examined the participants' characteristics such as age to see its impact on cyber-security behavior. The findings suggest no significant differences between age groups of 18–20, 21–25 and above 25. These findings support other studies such as (Cain et al. 2018; Gratian et al. 2018), where the cyber-security behavior of the participants aged 18–24, 25–29, 30–34 and 35–44 had no significant differences. However, the study (Gratian et al. 2018) reported weaker password generation, proactive awareness, updating behavior for participants aged 18–24. Similarly, our findings are consistent with (McCormac et al. 2017) for showing no significant differences between participants aged 18–25 and 30–39. The evidence from the literature (Cain et al. 2018; McCormac et al. 2017; Solic et al. 2019) suggests differences in cyber-security behavior between younger participants who are in the age bracket of (18–25) and older age groups (above 40). Older participants show strong cyber-security behavior. As far as risky behavior is concerned, studies have reported age to have a significant influence (Velki and Romstein 2019). In our study, students aged 18–20 exhibited more risk-averse behavior in contrast to (Velki and Romstein 2019). Older participants show less risky behavior (Velki and Romstein 2019) compared to their younger counterparts.

Our study did not show any significant differences in urban/rural living for cyber-security behavior which is in line with studies conducted in different countries (Sawaya et al. 2017). Similarly, no significant differences (SeBIS and RBS scores) were observed in the socioeconomic status of participants measured as per the MPI of the area where the survey was conducted. However, the results of cluster analysis revealed that students belonging to the low poverty stratum (20–29.9%) had high risky behavior but low cyber-security habits. Other studies which have made use of education as a proxy for socioeconomic status reported a direct impact on cyber-security behavior such as password safety (Dodel and Mesch 2019). Similarly, other findings report significant differences between education level and cyber-security awareness (Öğütçü et al. 2016). The higher education levels are associated with lower risk and higher security behavior (Öğütçü et al. 2016). Since the sample in our study is from the same education level i.e., undergraduate students, it contradicts the use of education level as a proxy for socioeconomic status.

On digital divide variables, there is a significant difference between those participants who used the Internet multiple times a day compared to those who did once a week. The literature on the digital divide argues that digital skills and digital knowledge are the main determinants of online behaviors (Büchi et al. 2017). Participants who accessed the Internet multiple times a day had stronger cyber-security behavior compared to those who accessed Internet once a week. These findings corroborate the indirect effect of the digital divide on cyber-security behavior such as anti-virus engagement and password safety (Dodel and Mesch 2019). Our findings are also in line with the study (Öğütçü et al. 2016) which shows that as the respondents spend more time on the Internet, they have a tendency to protect themselves more.

Our study also reports the effect of proactive security awareness in predicting risky Internet behavior. The findings show that participants who had good security practices—such as being conscious of links before clicking them, submitting information by ensuring its safety and being concerned when discovering a security problem—exhibited high aversion towards risky Internet behavior. Other studies (Öğütçü et al. 2016) and the anecdotal evidence from Pakistan show that risky behavior of youngsters has been associated with various cyber-crimes. The kidnapping case of Mustafa Dossal (*BBC* News 2013) in 2013 was a manifestation of the risky Internet behavior of "sharing personal information" on Facebook and "meeting an unknown person". Similarly, the recruitment of Noreen Leghari—a final-year medical student from Hyderabad—by the terrorist organization may also be attributed to risky Internet behavior. It has been shown from other case studies (Huey and Witmer 2016), that social networking sites allow for opportunities that can expose young students to terrorist ideologies and the information provided on these networks can result in recruitments (Hoyle et al. 2015). Therefore, the direct effect of proactive security awareness behavior on risky behavior has implications for the safety and security of the students.

Practical implications

The empirical findings from our study contribute towards the field of cyber-security behavioral research. We contribute by empirically evaluating the cyber-security and risky behaviors of students belonging to tertiary institutes in a developing country. To the best of our knowledge, this is the first study conducted across Pakistan in the province of Sindh that measures cyber-security and risky behaviors with respect to demographics, digital divide and socioeconomic status of the participants. It is also the first study to the best of our knowledge that profiles the participants based on both risky and cyber-security behaviors and measures the effect of different types of cyber-security practices in predicting risky Internet behavior.

From an application point of view, our work identifies cyber-security areas that can be improved in terms of practices and appropriate policies in tertiary institutes can be enacted. We propose to develop strategies to ensure safe Internet practices (Ion et al. 2015) instead of restricting Internet usage to avert cyber-risks as the limits imposed on the use of the Internet can result in missed digital opportunities by the students (Livingstone and Helsper 2010). In the context of Pakistan, it is critically important to promote safe online behavior not only with respect to its social and psychological cost on the youth but its potential economic impact due to a growing freelance workforce that is mostly comprised of young people (Baitenizov et al. 2019). The cyber-security behavior problems when analyzed in terms of the digital divide may help define a framework applicable for tertiary institutes to address populations at risk and to develop subsequent interventions. By increasing the cyber-security posture of students who are digitally less connected, such interventions can reduce the risks and can contribute towards a safe, secure and productive online experience. Similarly, the profiles of students constructed based on cyber-security and risky Internet behaviors also allow for identifying high risk—low-security populations to prioritize the delivery of educational interventions. The positive effect of proactive awareness on risk-averse behavior shows that many cyber-crimes (such as cyber-terrorism, blackmailing/kidnapping) can be mitigated by improving the risky Internet behavior. This in turn can be explained by good proactive cyber-security practices.

The results of our study can contribute to developing a cyber-security curriculum that is tailored based on the localized factors (Świątkowska 2020). The training programs can be customized to address the higher-risk population groups and contextualize them in the local context and languages. Similarly, a high risky population can be subject to specialized proactive cyber-security trainings to heighten its risky online behavior and consequently lower cyber-crimes. This inclusive way of crafting educational programs at target groups will ensure the digital inclusion of these groups and precludes the disruption of society and the economy. With developing countries maintaining low resources such as budget (Von Solms and Von Solms 2015) for the development of cyber-security controls, customized trainings established for their efficacy (Muronga et al. 2019) hold promise for efficient utilization of these resources.

Limitations

While this study makes important contributions, a number of limitations should be noted. The study makes use of self-report measures which are criticized for measurement errors and boredom effects (Spector 1992). Several factors have been associated with self-report biases such as true state of affairs, the sensitivity of construct, dispositional characteristics and situational characteristics (Donaldson and Grant-Vallone 2002).

Although self-reports are generally criticized for measuring general behavior, cyber-security behavior falls short of their objective assessments due to inadequacy of measuring the actual incidents (Parsons et al. 2014). Another reason to opt for self-report cyber-security behavior is the low probability and high consequences of cyber-security threats. Poor cyber-security behavior does not always lead to security breaches. Therefore, relying on self-report data in assessing cyber-security behavior is a valid alternative. The choice of instrument to measure the cyber-security behavior should also allay the criticism on self-report. SeBIS has been validated for its criterion validity (Egelman et al. 2016). All four SeBIS subscales namely Device Securement, Updating, Password Generation and Proactive Awareness predicted specific behaviors with large to medium effects sizes. On a further note, study by (Workman 2007) has also shown positive correlations between objective measures and subsequent objective behavior. Thus, there is a propensity of 80% variance in cyber-security behavior that can be explained by self-reports.

To reduce the boredom effects, again the choice of instruments makes a valid contribution. The SeBIS is comparatively small to other valid instruments employed in other studies. Fewer questions presented to participants kept them motivated and focused and we can assume results are reliable. Furthermore, the anonymity and confidentiality of the respondents were ensured by forfeiting their Personally Identifiable Information such as name and home address. This removed any situational characteristics that could lead to socially desirable responses. We further explained to the participants that their true response will add value to the research and they were requested to answer as honestly; hence, further removing dispositional characteristics.

Another limitation of the study is the generalizability of the results. Since the study is conducted in one country, it may have suffered from cultural influences. Studies (Lowry et al. 2011) suggest that there have been key differences in the context of Information Technology when Western and Asian cultures are studied. Similarly, other studies (Vroom and Von Solms 2004) have shown that culture has a major impact on an individual's cyber-security breaches.

Future directions

There are two aspects in which future studies will further scholarship in cyber-security behavioral research. (1) Cross-cultural studies. (2) Individualized trainings. Future studies that examine the cultural differences will comprise a national-level sample taken from all four provinces of the country. The cyber-security behavior will be gauged on socio-demographics and digital divide variables across cultural dimensions as per Hofstede's (Hofstede 2011) cultural model. The model's six dimensions; Power Distance, Uncertainty Avoidance, Individualism/Collectivism, Masculinity/Feminism, Long/Short Term Orientation and Indulgence/Restraints have been considered a paradigm for cross-cultural comparisons. International cross-cultural studies will examine the differences in risky and cyber-security behaviors for similar as well as different cultures measured by Hofstede. Studies examining the second aspect of individualized training will take into consideration the digital divide, age and gender variables to develop and evaluate such trainings using program/training evaluation models (Kirkpatrick and Kirkpatrick 2006).

Conclusion

The confluence of technical and behavioral solutions establishes the required cyber-security in any organization. With the dearth of behavioral evidence in organizations specifically tertiary institutes, this study explores the cyber-security behavior of students in a developing country context. Our study augments previous studies by using a valid and comparatively smaller instrument and exploring in terms of socio-demographics and digital divide variables and by constructing profiles of students based on their risky and cyber-security behaviors. The study was conducted on undergraduate students and significant differences in cyber-security and risky behavior were reported for gender, age, and frequency of Internet access. The findings from this study are the result of the participant pool derived through a stratified multistage sampling strategy thus supporting external validity. The cyber-security behavior of participants from tertiary institutes paralleled with previous studies. New insights were brought to light in contrast to previous studies regarding the cyber-security posture of undergraduate students. Given the dearth of similar studies, our findings add solution evidence to the inexorably growing cyber-security problem space. The results of our study and the statistical processing lay a solid foundation for those who are looking for further scholarship. The practical application of this study calls for tailored cyber-security trainings keeping gender, age, digital divide variables and participants' high risky-low cyber-security profiles in mind. Further, establishing the effectiveness of customized training programs before their implementation holds promise for efficient utilization of meager resources kept for cyber-security intervention in developing countries.

Acknowledgements We acknowledge the efforts of Hajra Murtaza, Aslam Asadi, and Muhammad Saud Khan for providing their valuable feedbacks and Sohail Safdar, Khurram Javed and Obaid-Ur-Rehman for logistic support in carrying out this study. We also acknowledge the anonymous reviewers for a series of constructive feedbacks that allowed us to polish the manuscript.

Funding This research was partially funded by an internal grant from Riphah International University.

Declarations

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

Data availability The data and material can be provided on demand.

References

Abawajy, Jemal. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* 33 (3): 237–248.

Ahmad, Jawad, Seong Oun Hwang, and Arshad Ali. 2015. An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wireless Personal Communications* 84 (2): 901–918.

Alahmari, Abdulmajeed, and Bob Duncan. 2020. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1–5. IEEE.

Aldawood, Hussain, and Geoffrey Skinner. 2018. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, pp. 62–68. IEEE.

Aliyu, Mansur, Nahel AO Abdallah, Nojeem A. Lasisi, Dahir Diyar, and Ahmed M. Zeki. 2010. Computer security and ethics awareness among IIUM students: an empirical study. In 2010 *International conference on information and communication technology for the Muslim world (ICT4M)*, pp. A52–A56. IEEE.

Al-Janabi, Samaher, and Ibrahim Al-Shourbaji. 2016. A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management* 15 (01): 1650007.

Alkire, Sabina, and Maria Emma Santos. 2010. Acute multidimensional poverty: A new index for developing countries.

AlMindeel, Raneem, and Jorge Tiago Martins. 2020. *Information security awareness in a developing country context: insights from the Government Sector in Saudi Arabia*. Information Technology & People: Emerald Publishing Limited.

Alsunbul, Saad, Phu Dung Le, and Jefferson Tan. 2015. Deterring hacking strategies via targeting scanning properties. *International Journal of Network Security and Its Applications* 7 (4): 1–30.

Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the changing cost of cybercrime.

Anwar, Mohd, Wu. He, Ivan Ash, Xiaohong Yuan, Ling Li, and Xu. Li. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69: 437–443.

Baitenizov, Daniyar T., Igor N. Dubina, David FJ. Campbell, Elias G. Carayannis, and Tolkyn A. Azatbek. 2019. Freelance as a creative mode of self-employment in a new economy (a literature review). *Journal of the Knowledge Economy* 10 (1): 1–17.

Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. 2012. Database security and encryption: A survey study. *International Journal of Computer Applications* 47 (12)

BBC News. 2013. Pakistan teenager rescued after kidnap by fake facebook friend, May 27, sec. Asia. https://www.bbc.com/news/world-asia-22678603.

Bechara, Antoine. 2003. Risky business: Emotion, decision-making, and addiction. *Journal of Gambling Studies* 19 (1): 23–51.

Bederna, Z., Szadeczky, T. 2020. Cyber espionage through Botnets. *Security Journal* 33: 43–62.

Bedser, Jeffrey R. 2007. The impact of the internet on security. *Security Journal* 20 (1): 55–56.

Beerepoot, Niels, and Bart Lambregts. 2015. Competition in online job marketplaces: Towards a global labour market for outsourcing services? *Global Networks* 15 (2): 236–255.

Berg, Janine. 2015. Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers. *Comparative Labor Law and Policy Journal* 37: 543.

Boyer, Ty. W. 2006. The development of risk-taking: A multi-perspective review. *Developmental Review* 26 (3): 291–345.

British E-Spy Agency Hacked Network Routers to Access Almost Any Internet User in Pakistan." 2020. *Pakistan defence*. https://defence.pk/pdf/threads/british-e-spy-agency-hacked-network-routers-to-access-almost-any-internet-user-in-pakistan.382336/. Accessed July 10

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*, p. 419.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 3: 523–548.

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.

Chandarman, Rajesh, and Brett Van Niekerk. 2017. Students' cybersecurity awareness at a private tertiary educational institution.

Crossler, Robert E., Allen C. Johnston, Paul Benjamin Lowry, Hu. Qing, Merrill Warkentin, and Richard Baskerville. 2013. Future Directions For Behavioral Information Security Research. *Computers & Security* 32: 90–101.

De Moor, S., M. Dock, S. Gallez, S. Lenaerts, C. Scholler, and C. Vleugels. 2008. *Teens and ICT: Risks and opportunities*. Belgium: TIRO.

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.

Dodge Jr., C. Ronald, Curtis Carver, and Aaron J. Ferguson. 2007. Phishing for user security awareness. *Computers & Security* 26 (1): 73–80.

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*, pp. 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*, pp. 2873–2882. ACM.

Faith, B. Fatokun, Suraya Hamid, Azah Norman, O. Fatokun Johnson, and Christopher Ifeanyi Eke. 2020. Relating factors of tertiary institution students' cybersecurity behavior. In *2020 International*

Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS), pp. 1–6. IEEE.

Freelancer Salaries & Earnings Income Survey 2020. 2020. *Payoneer*. https://www.payoneer.com/resources/freelance-income-survey/. Accessed July 11.

Gamez-Guadix, Manuel, Erika Borrajo, and Carmen Almendros. 2016. Risky online behaviors among adolescents: Longitudinal relations among problematic internet use, cyberbullying perpetration, and meeting strangers online. *Journal of Behavioral Addictions* 5 (1): 100–107.

Gillam, Andrew R., and W. Tad Foster. 2020. Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior* 106319.

Gökçearslan, Şahin, and Süleyman Sadi. Seferoğlu. 2016. The use of the internet among middle school students: Risky behaviors and opportunities. *Kastamonu Education Journal* 24 (1): 383–404.

Goldthorpe, John H., A.H. Halsey, A.F. Heath, J.M. Ridge, Leonard Bloom, and F.L. Jones. 1982. Social mobility and class structure in modern Britain. *Ethics* 92 (4): 766–768.

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.

Hadlington, L. J. 2018. Employees attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology.

Haeussinger, Felix, and Johann Kranz. 2013. Information security awareness: Its antecedents and mediating effects on security compliant behavior.

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.

Hoyle, Carolyn, Alexandra Bradford, and Ross Frenett. 2015. *Becoming Mulan? Female Western Migrants to ISIS*. London: Institute for Strategic Dialogue.

Hua, Jian, and Sanjay Bapna. 2013. The economic impact of cyber terrorism. *The Journal of Strategic Information Systems* 22 (2): 175–186.

Huey, Laura, and Eric Witmer. 2016. # IS_Fangirl: Exploring a new role for women in terrorism. *Journal of Terrorism Research* 7(1).

Ion, Iulia, Rob Reeder, and Sunny Consolvo. 2015. ... "... No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices." In *Proc. SOUPS*.

Jain, A. K., and R. E. Hausman. 2006. *Stratified Multistage Sampling*. Encyclopedia of Statistical Sciences.

Jeske, Debora, and Paul Van Schaik. 2017. "Familiarity with Internet Threats: Beyond Awareness." *Computers & Security* 66. Elsevier: 129–41.

Jessor, Richard, Shirley Jessor, S. L. Jessor, and R. Jessor. 1977. Problem behavior and psychosocial development: A longitudinal study of youth.

Johnson, Dallas E. 1998. *Applied multivariate methods for data analysts*. Duxbury Resource Center.

Johnson, John A. 2005. Ascertaining the validity of individual protocols from web-based personality inventories. *Journal of Research in Personality* 39 (1): 103–129.

Kayri, Murat. 2007. Two-step clustering analysis in researches: A case study.

Kettenring, Jon R. 2006. The practice of cluster analysis. *Journal of Classification* 23 (1): 3–30.

Kim, Eyong B. 2013. Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective* 22 (4): 171–179.

Kim, Eyong B. 2014. Recommendations for information security awareness training for college students. *Information Management & Computer Security* 22 (1): 115–126.

Kim, Hyungjin Lukas, HanByeol Stella. Choi, and Jinyoung Han. 2019. Leader power and employees' information security policy compliance. *Security Journal* 32 (4): 391–409.

Kirkpatrick, Donald. 2006. *and James Kirkpatrick*. Evaluating Training Programs: The Four Levels. Berrett-Koehler Publishers.

Kortjan, Noluxolo, Rossouw von Solms, and Johan Van Niekerk. 2012. Ethical guidelines for cyber-related services aimed at the younger generations. In *HAISA*, pp. 205–215.

Kshetri, Nir. 2010. Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly* 31 (7): 1057–1079.

Kushzhanov, N. V., and U. Zh Aliyev. 2018. Changes in society and security awareness. *ҚАЗАҚСТАН РЕСПУБЛИКАСЫ* 94.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2020. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv:2006.11929.

Livingstone, Sonia, and Leslie Haddon. 2009. *Kids online: Opportunities and risks for children*. Policy Press, Bristol.

Livingstone, S., L. Haddon, A. Görzig, and K. Ólafsson. 2012. *EU kids online final report. EU kids online, London School of Economics and Political Science, London*.

Livingstone, Sonia, and Ellen Helsper. 2010. Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society* 12 (2): 309–329.

Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud. 2014. In their own words: What bothers children online? *European Journal of Communication* 29 (3): 271–288.

Lowry, Paul Benjamin, Jinwei Cao, and Andrea Everard. 2011. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27 (4): 163–200.

Lowry, Paul Benjamin, Tamara Dinev, and Robert Willison. 2017. Why security and privacy research lies at the centre of the information systems (IS) Artefact: Proposing a bold research agenda. *European Journal of Information Systems* 26 (6): 546–563.

Malik, Fareesa, Richard Heeks, Silvia Masiero, and Brian Nicholson. 2020. *Digital platform labour in Pakistan: Institutional voids and solidarity networks*. Loughborough: Loughborough University.

Masood, Faiza, Adnan Naseem, Azra Shamim, Aasma Khan, and Muhammad Ahsan Qureshi. n.d. A systematic literature review and case study on influencing factor and consequences of freelancing in Pakistan.

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.

Meade, Adam W., and S. Bartholomew Craig. 2012. Identifying careless responses in survey data. *Psychological Methods* 17 (3): 437.

Milne, George R., Lauren I. Labrecque, and Cory Cromer. 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs* 43 (3): 449–473.

Moallem, Abbas. 2018. Cyber security awareness among college students. In *International conference on applied human factors and ergonomics*, pp. 79–87. Springer, New York

Mohebzada, Jamshaid G., Ahmed El Zarka, Arsalan H. BHojani, and Ali Darwish. 2012. Phishing in a university community: Two large scale phishing experiments. In *2012 international conference on innovations in information technology (IIT)*, pp. 249–254. IEEE.

Moore, Susan, and Eleonore Gullone. 1996. Predicting adolescent risk behavior using a personalized cost-benefit analysis. *Journal of Youth and Adolescence* 25 (3): 343–359.

Moser, Andreas, Christopher Kruegel, and Engin Kirda. 2007. Exploring multiple execution paths for malware analysis. In *2007 IEEE symposium on security and privacy (SP'07)*, pp. 231–245. IEEE.

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

Muniandy, Lalitha, Balakrishnan Muniandy, and Zarina Samsudin. 2017. Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance and Security* 2017: 1–13.

Muronga, Khangwelo, Marlein Herselman, Adele Botha, and Adéle Da Veiga. 2019. An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A Scoping Review. In *2019 conference on next generation computing applications (NextComp)*, pp. 1–6. IEEE.

Nordstokke, David W., and Bruno D. Zumbo. 2010. A new nonparametric Levene test for equal variances. *Psicológica* 31 (2): 401–430.

Öğütçü, Gizem, Özlem Müge. Testik, and Oumout Chouseinoglou. 2016. Analysis of personal information security behavior and awareness. *Computers & Security* 56: 83–93.

Or-Meir, Ori, Nir Nissim, Yuval Elovici, and Lior Rokach. 2019. Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)* 52 (5): 1–48.

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.

Paterson, Thomas, and Lauren Hanley. 2020. Political warfare in the digital age: Cyber subversion, information operations and 'Deep Fakes.' *Australian Journal of International Affairs* 74 (4): 439–454.

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*, pp. 231–241. Springer.

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

Platt, Victor. 2012. "Still the fire-proof house? An analysis of Canada's cyber security strategy. *International Journal* 67 (1): 155–167.

Pramod, Dhanya, and Ramakrishnan Raman. 2014. A study on the user perception and awareness of smartphone security.

Rafiq, Ms Aamna. 2020. Issue brief on 'increasing cyber threats to Pakistan' | institute of stategic studies Islamabad. http://issi.org.pk/issue-brief-on-increasing-cyber-threats-to-pakistan/. Accessed July 10.

Ramalingam, Rajasekar, Shimaz Khan, and Shameer Mohammed. 2016. The need for effective information security awareness practices in oman higher educational institutions. arXiv:1602.06510.

Rao, Umesh Hodeghatta, and Umesha Nayak. 2014. *The Infosec handbook: An introduction to information security*. New York: Springer.

Salim, Asif, Noor Ullah Khan, and Muhammad Kaleem. 2019. Contemporary digital age and dynamics of E-Jihad in the Muslim World: Case study of Pakistan. *Pakistan Journal of Criminology* 11(4).

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*, pp. 2202–2214.

Schneier, Bruce. 2015. *Secrets and lies: Digital security in a networked world*. New York: Wiley.

Senthilkumar, K., and Sathishkumar Easwaramoorthy. 2017. A survey on cyber security awareness among college students in Tamil Nadu. *Materials Science and Engineering Conference Series* 263: 042043.

Shad, Muhammad Riaz. 2019. Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies* 39 (1): 1–19.

Sharif, Mahmood, Jumpei Urakawa, Nicolas Christin, Ayumu Kubota, and Akira Yamada. 2018. Predicting impending exposure to malicious content from user behavior. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1487–1501.

Shi, Fei. 2015. Study on a stratified sampling investigation method for resident travel and the sampling rate. *Discrete Dynamics in Nature and Society*

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. Medicinski fakultet Osijek.

Spector, Paul E. 1992. A consideration of the validity and meaning of self-report measures of job conditions.

Staksrud, Elisabeth, Kjartan Ólafsson, and Sonia Livingstone. 2013. Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior* 29 (1): 40–50.

Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* 24 (2): 124–133.

Štitilis, Darius, Paulius Pakutinskas, and Inga Malinauskaitė. 2017. EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal* 30 (4): 1151–1168.

Świątkowska, Joanna. 2020. Tackling cybercrime to unleash developing countries' Digital Potential.

Talib, Shuhaili, Nathan L. Clarke, and Steven M. Furnell. 2010. An analysis of information security awareness within home and work environments. In *ARES'10 international conference on availability, reliability, and security, 2010*, pp. 196–203. IEEE.

Titi, Khader Muspah. 2003. *Code of ethics, professionalism and responsibilities*. Ardhah, Jordan: Al-Ahliyyah Amman University.

Valcke, Martin, Bram De Wever, Hilde Van Keer, and Tammy Schellens. 2011. Long-term study of safe internet use of young children. *Computers & Education* 57 (1): 1292–1305.

Van der Merwe, Alta, Marianne Loock, and Marek Dabrowski. 2005. Characteristics and responsibilities involved in a phishing attack. In *Proceedings of the 4th international symposium on information and communication technologies*, pp. 249–254.

Velki, Tena, and Ksenija Romstein. 2019. User risky behavior and security awareness through lifespan. *International Journal of Electrical and Computer Engineering Systems* 9 (2): 9–16.

Velki, Tena, and Krešimir Šolić. 2019. Development and validation of a new measurement instrument: The behavioral-cognitive internet security questionnaire (BCISQ). *International Journal of Electrical and Computer Engineering Systems* 10 (1): 19–24.

Velki, Tena, Kresimir Solic, V. Gorjanac, and K. Nenadic. 2017. Empirical study on the risky behavior and security awareness among secondary school pupils-validation and preliminary results. In *2017 40th international convention on information and communication technology, electronics and microelectronics* (MIPRO), 1280–1284. IEEE.

Von Solms, Rossouw, and Suné Von Solms. 2015. Cyber safety education in developing countries. International Institute of Informatics and Systemics.

Vroom, Cheryl, and Rossouw Von Solms. 2004. Towards information security behavioural compliance. *Computers & Security* 23 (3): 191–198.

Waheed, Moniza. 2019. Online threats and risky behaviour from the perspective of malaysian youths.

Wang, Zuoguang, Limin Sun, and Hongsong Zhu. 2020. Defining social engineering in cybersecurity. *IEEE Access* 8: 85094–85115.

Workman, Michael. 2007. Gaining access with social engineering: An empirical study of the threat. *Information Systems Security* 16 (6): 315–331.

Zhang, Peiqin, and Xun Li. 2015. Determinants of information security awareness: An empirical investigation in higher education.

Zwilling, Moti, Galit Klien, Du.šan Lesjak, Lukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. 2020. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems* 62: 1–16.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.