

Received June 27, 2020, accepted July 4, 2020, date of publication July 8, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007867

# Factors Related to Cyber Security Behavior

ANA KOVAČEVIĆ<sup>1</sup>, NENAD PUTNIK<sup>1</sup>, AND OLIVER TOŠKOVIĆ<sup>2</sup>

<sup>1</sup>Faculty of Security Studies, University of Belgrade, 11000 Belgrade, Serbia

<sup>2</sup>Laboratory for experimental psychology, Faculty of Philosophy, University of Belgrade, 11000 Belgrade, Serbia


Corresponding author: Ana Kovačević (kana@rcub.bg.ac.rs)

**ABSTRACT** Theoretical and empirical insight notes that cyber security awareness is a topic of particular interest in cyber security. Humans are the central figures in cyber security and the way to reduce risk in cyberspace is to make people more security aware. While there have been numerous studies about various aspects of cyber security awareness, they are both inconsistent and environment-dependent. The main aim of our research is to analyze cyber security awareness in depth, and to try to discover how various factors such as socio-demographics, cyber security perceptions, previous cyber security breaches, IT usage, and knowledge may individually or together impact on cyber security behavior. To prove that we conducted our research on students, as they are the most technologically active part of the society. We discovered that knowledge proved to be the dominant factor for cyber security awareness, and although students are digital natives, they do not feel safe in the cyber environment; they do not behave securely and do not have adequate knowledge to protect themselves in cyberspace.

**INDEX TERMS** Cyber security, cyber security behaviours, cyber security breaches, cyber security perception, knowledge, user awareness.

## I. INTRODUCTION

Today, life can hardly be imagined without information technology; more than half of the world's population (58.8%) used the Internet in 2019 with 73.4% Internet users in Serbia [1]. According to a report compiled by Ratel in Serbia, 99.2 % of those aged between 16 and 24 use computers and 98.2% use the Internet every day or almost every day [2]. Recent technological development has had a great impact on people's lifestyles [3]. However, there is also a dark side to this trend; in 2017 the Ponemon Institute estimated the economic impact of security breaches at nearly half a trillion dollars globally, with the cost of data breaches increasing every year [4]. Security incidents are constantly expanding, and are becoming increasingly sophisticated and more severe. With the wide adoption of information technologies in the last decades, the profile of the end-user also has changed. The average user of information technology is not necessarily technically educated, and has most likely not studied cyber security in his/her previous education. Cyber security is defined as a computer-based discipline, which involves technology, people, information and processes, with

The associate editor coordinating the review of this manuscript and approving it for publication was Sabu M. Thampi .

the goal of securing operations against unauthorized access or attack [5].

Although users are somewhat aware of the security risks, most of them are not sure how they should behave to achieve cyber security (e.g., even if they have heard about phishing, some users are not sure how to recognize the problem or react appropriately). According to numerous reports, human error is seen as the dominant problem for secure information, making it necessary to understand people's behavior towards security technology [6]–[8]. Numerous security breaches are caused by a lack of knowledge or unsafe behavior (e.g., sharing passwords, or clicking on unsecured links in emails). Protecting oneself in cyberspace has become a necessity today.

Security awareness is defined in NIST Special Publication 800-16 as follows: “Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly” [9]. Bada [10] noted that awareness does not only mean being aware of possible threats, but also adopting security behavior.

In this paper, we analyze cyber security awareness in depth, and accordingly, the paper is organized in the following way; the *Background section* reviews and presents relevant work on

cyber security awareness and the proposed research question. *Section III* describes and discusses the adopted methodology. *Section IV* presents the results and provides a discussion of the findings, interpreting them in order to achieve greater clarity. Finally, *Section V* gives our conclusion and future direction of work.

## II. BACKGROUND

Cyber security is a growing and important field involving various research studies [11]. One of the research directions in the field of cyber security is how to improve cyber security awareness, focusing on those factors which are the most significant in achieving this aim. This section briefly presents relevant studies in cyber security awareness, mostly within the education sector.

In their research, Kruger *et al.* [12] describe an exploratory study to test the possibility of using information security vocabulary tests to assess awareness levels and familiarity with security terms so as to identify suitable areas and topics for information security awareness programs. The questionnaire used consisted of two sections: the first section was a vocabulary test and the second evaluated the respondents' behavior. They found the use of the vocabulary test for the assessment of awareness levels to be a useful tool and a significant relationship between knowledge of concepts (vocabulary) and behavior was shown. Al-Janabi and Al-Shourbaji [13] carried out research to analyze information security awareness levels and associated risk, as well as the overall impact on institutions, among students and staff within the educational environment in the Middle East. The results revealed that the participants did not have the required knowledge and understanding of information security awareness. The authors outlined the implications for real-world problems from the identified weakness in this survey, and made recommendation to remedy the situation. Jeske and van Schaik [14] conducted a survey of students' familiarity with different Internet threats. The participants were presented with definitions of threats and were asked to state how familiar they were with each. According to their responses, three clusters were identified; the first cluster included those participants who were knowledgeable about all threats (both new and familiar), the second cluster comprised participants more familiar with new threats, while the third cluster consisted of participants more familiar with well-known threats. The authors showed that time spent on the Internet and the length of Internet experience were predictors of familiarity with Internet threats, which are a further predictor of computer security use.

Gratian *et al.* [15] carried out a survey correlating human characteristics, such as risk-taking preferences, decision-making styles, demographics, and personality traits with cyber security behavior intentions among students and staff at a large public university. They reported that financial risk-taking, rational decision-making, extraversion, and gender are good predictors of security behaviors. Gender was found to predict strength of passwords, with females creating

weaker passwords than males. Their study shows both correlations and contradictions with previous studies (e.g., in line with [16], risk taking preferences did not correlate with security behavior intentions of device securement; contrary to [16], regarding the correlation between individuals willing to take ethical and health/safety risks and poor security behavior intentions), so the authors emphasize the uniqueness of the environment in exploring cyber security.

Moallem [17] carried out a study of cyber security awareness among students in the Silicon Valley in California, USA as the most advanced technology environment. The author reported that although college students believed that they were observed and not secure online, they were not aware of how to protect their data. Besides that, Moallem also stated that educational institutions did not take an active approach to improve awareness among students, to increase their knowledge about threats and to make them safer in cyberspace [17].

Parsons *et al.* [6] surveyed university students by means of their HAIS\_Q instrument (Human Aspects of Information Security Questionnaire), and the same students also participated in an empirical phishing experiment. It was shown that students who had a higher score on the HAIS\_Q performed better in the phishing experiment. The HAIS-Q is based on the Knowledge-Attitude-Behavior (KAB) model, whereby in their previous research the authors demonstrated a strong, positive relationship between knowledge, attitude, and behavior [18], [19]. McCormac *et al.* [19] used the HAIS-Q to measure the relationship between individual differences and information security awareness among working Australians. They reported that conscientiousness, agreeableness, emotional stability and risk-taking propensity are significant, while age and gender have no influence on an individual's information security awareness.

Anwar *et al.* [20] explored how important a factor gender is in terms of cyber security beliefs and behaviors among employees. They found statistically significant gender-wise differences based on computer skills, prior experience, cues-to-action, security self-efficacy, and self-reported cyber security behavior. The women in the study self-reported slightly lower levels of computer skills, lower prior experience with computer security, and lower cues-to-action scores. The greatest difference was noted for self-efficacy, where the women showed significantly lower self-efficacy than the men. The authors also noted that this might have been the consequence of overconfidence among the men or under confidence among the woman in their self-evaluation.

Cain *et al.* [21] analyzed the cyber hygiene knowledge of concepts and threats, and the behaviors of the end-users. In their analysis, they reported that there were statistically significant gender-wise differences in terms of knowledge, where males were more knowledgeable. In addition, there were no statistically significant differences between gender and behavior, previous attacks and behavior, or training and behavior. There was an evident link between self-identified experts and knowledge (and behaviors); self-identified experts had less secure behaviors than

self-identified non-experts and also less knowledge about cyber hygiene. They also concluded that although users should be more knowledgeable in order to improve cyber security, this was not enough in itself, and users should change their behavior. A large majority of the participants (81%) had some security training in cyber hygiene, but it did not improve their behaviors or increase their knowledge. They concluded that more effective training should be provided for all users, and this statement is similar to Bada [10].

The Pew Research Centre conducted research into the perceptions, security breaches and behavior of Americans with regard to cyber security [22]. Their report states that although the majority of Americans had experienced data breaches and did not trust modern institutions to protect their personal data, they themselves did not implement the best practices in cyberspace. In addition, the Pew Research Centre carried out two more studies into the cyber security knowledge of Americans, and their results show that a large number of participants are unclear about certain key cyber security topics, terms, and concepts [23], [24]. It was shown that while the participants are able to identify a strong password or are aware of the danger of using public WiFi, they achieved poorer results in questions with more technical details such as two-factor authentication or page encryption. These Pew Research surveys were quite comprehensive, and the most relevant for our analysis, so most of our questions were based on them.

All of the aforementioned studies, with different focuses and methodologies, but each in its own way - address the complexity of the cyber security awareness phenomenon. Common to all these studies is that they have identified various factors that affect cyber security awareness and tried to explain the interconnectedness of these factors, such as perceptions [14], [17], [22]; security breaches [14], [22]; behavior [6], [12], [14], [15], [21], [22]; knowledge [6], [12], [13], [17], [21], [23], [24]; and socio-demographic characteristics - age and gender [15], [19]–[23].

Although these studies have shown that each of these factors (i.e., socio-demographic characteristics, perception, security breaches, behavior, and knowledge) have an impact on cyber security awareness, there are noticeable inconsistencies in how they affect cyber security awareness. These inconsistencies mostly occur with socio-demographic factors (i.e., gender), perceptions, and previous security breaches, which is in line with the conclusion that cyber security is environment-dependent, as stated in [15].

Hence, our aim was to test the effects of these factors on cyber security awareness, and to attempt to discover how various factors such as socio-demographics, perceived cyber security, previous breach experiences, IT usage, and knowledge may individually or together impact on cyber security behavior. This will serve to expand empirical knowledge about this issue and further contribute to clarifying the dilemma related to the extent of the influence of these factors, without, of course any pretentious intentions to offer conclusive answers.

This led us to our research which focuses on three main areas:

- 1) How are socio-demographic characteristics, such as gender and previous education, related to the behavioral aspects of cyber security?
- 2) How are perceptions of cyber security related to the behavioral aspects of cyber security?
- 3) How is knowledge of cyber security related to the behavioral aspects of cyber security?

In addition, we were also interested in investigating how the assumed factors (socio-demographics, perceived security, and knowledge) are related to each other, and whether they interact in relation to the behavioral aspects of cyber security.

This is the first survey conducted among university students in Serbia to analyze the various factors affecting cyber security awareness.

### III. METHOD

The current study is performed through a survey, on a convenience sample of students. The questionnaire contained adapted items from previous surveys conducted by the Pew Research Centre [22]–[24].

#### A. SAMPLE

Our participants in the survey were students, as it is assumed that this population is very familiar with IT technology [2]. We decided to conduct our research on students at the Faculty of Security Studies, University of Belgrade, as they have chosen to study different aspects of security (i.e., national security, environmental security, crime and criminology, and information security) for their professional vocation and under the assumption that they have a higher degree of security awareness than students from other faculties. In addition, our participants were freshmen at the beginning of their studies and they still do not have specific cyber security expertise, so their current level of knowledge can only be related to the knowledge gained in high school. Our primary idea was to discover the level of security awareness of freshmen when they arrive at the Faculty of Security Studies, and the practical implication is that we can improve our curriculum regarding those findings. The sample consists of 147 participants, 40 (27%) male and 107 (73%) female.

#### B. INSTRUMENTS

The first section of the survey focused on the students' socio-demographic information, such as gender and previous education. Cyber security is quite a complex and broad subject [23], and the second part of the questionnaire analyzed the various dimensions of cyber security. The majority of the questions were adapted from the survey conducted by the Pew Research Centre in 2016 [22]. The third part of the survey measured knowledge, and we chose to use questions from questionnaires [23], [24], which were developed by cyber security experts to measure the general concepts and essential building blocks for online protection. We selected those questions which were relevant for our participants. We chose those

questionnaires because the questions were specific, in the form of a test mostly with only one correct answer, explicitly showing knowledge of lack of knowledge [23], [24].

The tested variables included socio-demographic factors (gender, previous education), IT usage (5 questions), previous cyber security breaches (7 questions), perceptions of cyber security (11 questions), cyber security behavior regarding passwords (11 questions), cyber security behavior regarding cell phones (7 questions), and cyber security knowledge (10 questions).

The items were translated into Serbian by professional translators, and then verified through back-translation procedure. The Pew Research Centre published the original content in English but has not reviewed or approved this translation

### C. PROCEDURE

The Faculty of Security Studies at the University of Belgrade approved the study. A paper-based survey was administered to the students at the same faculty on November 22th, 2019. The survey was completed in a group classroom setting under the supervision of the authors. The participants were briefed about the goal of the study and approximately 20-30 minutes were required to complete it. Participation was voluntary, and all of the students were informed that participation (or refusal to participate) would not affect their course grade.

The Statistical Package for Social Sciences (SPSS) version 22 was used to process the data collected, and to analyze the repossesses of the participants from the survey [25]. Firstly, the descriptive-statistical data were processed, where the parameters of the mean and standard deviations were used for the numerical variables, while the frequencies and percentages were used for the categorical variables. Subsequently, the following methods were used for the purpose of analysis: Principal Component Analysis, T-test, Pearson's correlation coefficient, multiple regression analysis and hierarchical multiple regression analysis, with a significance level of  $p < 0.05$ .

## IV. RESULTS AND DISCUSSION

To provide construct validity to cyber security perceptions, cyber security breach experiences and cell phone and password behaviors, we firstly performed factor analysis- PCA (Principal Component Analysis) on the related questions. Factor analysis with PCA (Principal Component Analysis) was used in order to reveal groups of questions which showed high inter-correlations. This facilitates the detection of so called latent variables, which lie behind the participants' answers to the questions.

### A. CONSTRUCTS

One factorial solution was chosen for each of the examined constructs. For factor structure loadings, we chose only items which showed high saturations ( $> 0.3$ ). The *cyber security perception* factor explains 40% of the variance, and loadings are in the range from 0.309 to 0.824; the *cyber security breach experiences* factor explains 43% of the variance,

and saturation is from 0.452 to 0.824; the *password related behavior* factor explains 17% of the variance and saturation is from 0.313 to 0.677 and the *cell phone related behavior* factor explains 22% of the variance with saturation from 0.507 to 0.706.

In the following step for each of the aforementioned constructs, we calculated the corresponding score as the sum of the individual items. In addition, we also calculated the total score for knowledge and IT usage by summing up all the items related to them. Table 1 shows the descriptive statistics for each construct's score.

TABLE 1. Basic descriptive statistics for each measured construct.

	N	Min.	Max.	Mean	SD	SS	SK
Knowledge	146	0	8	3.77	1.83	1.16	1.43
IT usage	147	3	6	4.65	0.71	1.90	1.52
Cyber security perceptions	147	5	39	21.22	6.24	0.49	1.04
Cyber security breach experiences	147	3	10	4.61	1.60	4.92	0.77
Password related behavior	147	0	6	2.67	1.40	1.78	0.14
Cell phone related behavior	147	0	4	2.34	1.00	1.12	0.59

SD= Standard deviation, SS= Standardized Skewness, SK= Standardized Kurtosis

According to the values of standardized skewness and kurtosis, almost all of the variables have satisfactory values (within  $\pm 1.96$ ), with the exception of cyber security breach experiences, as is shown in Table X1. The skewness value on this score indicated positively skewed distribution, meaning that most of the participants had low breach experience, which is expected. So, we can conclude that most of the variables fulfill the conditions of normality, except for cyber security breach experiences. However, we also decided to use this variable in our analysis since it did show some significant relations.

### B. DESCRIPTIVE RESULTS REGARDING CYBER SECURITY

Almost all of the participants have smartphones (99.3%), and use the Internet on their cell phones (or other mobile handheld devices). Besides that, 99.3% use social media sites such as Facebook, Twitter, or LinkedIn. However, when it comes to online shopping and e-banking, only 17.7% of the participants use online banking services, while 50.3% of the participants do their shopping online.

The majority of the students (73.5%) have never faced a security breach, while 11.6% of them have encountered one, 12.2% less than five times, 2.0% more than 3 times, and just one participant(0.7%) more than ten times. We also analyzed which security breaches the participants had encountered; 4.1% of the participants had experienced a compromised email account, while 22.4% a compromised social media

account. On the other side, almost all of the participants (99.3%) said that they had heard about at least one security breach that had happened to their close friends or family: 34.7% just once, 46.3% between 1 and 5 times, and 18.3% more than five times.

The participants do not feel very confident in various institutions to protect their personal data from unauthorized users, and they show the greatest level of concern (not confident at all) primarily about social media sites (42.8%), government institutions (20%), companies they pay online (20%), or Internet providers (20%). On the other side, they have higher levels of confidence in the university e-service (28%) and online banking (22%). Roughly one third of the participants (30.6%) feel that their personal data is more secure than five years ago, 30.6% think that it is as secure as it was five years ago, while 28% think they are less secure.

Passwords are considered one of the main factors that increase the security of an information system, which increase security especially if they are complex (e.g., a combination of numbers, small/capital letters, and symbols) and not shared with others. Despite the existence of new authentication methods, usernames and passwords are still very popular because of their simplicity [17]. The reuse of passwords is quite common, and in the study from 2007, conducted on more than 500,000 users, it was reported that the average user reuses the same password across 3.9 sites [26]. With the steady increase in the number of web applications since this study was conducted, we can assume that today this number is even higher. In line with this, over half of the participants reported that they had reused passwords for highly important accounts [27]. The reason for reusing passwords may be found in the results that a strong password requires distinctive cognitive processing [28] while reusing it is much easier. We explored whether our students have safe password behavior.

The participants demonstrated self-reported unsafe behavior as 74.1% stated that most of their passwords are the same or very similar. This result is in line with the result in [17]; where it was reported that 78% reuse or sometimes reuse their passwords. Reusing passwords is not a secure behavior, and may put users at risk when a website does not encrypt usernames/passwords. Also, almost half of the participants (47.6%) considered passwords stressful and found it difficult to keep track of their passwords. On the other hand, 54.4% of the participants chose to use less secure passwords, because complicated passwords are too hard to remember. This shows the important fact that the majority of the participants are not aware of how to create good passwords that can be easily remembered. In addition, it is also evident that the majority of these students lack awareness about safe passwords: 54.4% have shared an online account with others and 72.1% have used a social media account to log on to another website.

Although almost all users have smartphones, only 32% of them have installed antivirus protection on their phones. Public Wi-Fi or unfamiliar Wi-Fi networks are very vulnerable and can easily be attacked by hackers, and users should

avoid performing sensitive activities on them [22]. In terms of using public Wi-Fi; 12.2% of the participants make online purchases connected to public Wi-Fi, 6.1% have used public Wi-Fi for online banking, while 60.5% have used it for sending an email. It was shown that although the majority of the participants are aware of threats from public Wi-Fi for online banking and purchasing, they lack awareness when using emails. If we compare this data to the question about https, only 10.9% of the participants know what https is. This led us to the conclusion that while some students use online banking and shopping services, they have insufficient security awareness of the threats posed by using unsecured connections.

If we analyze the results of knowledge, no one had all the correct answers, and the best result was 8 out of 10. The question with the most correct answers was related to creating secure passwords (85.7%), followed by the safety of public Wi-Fi (64.4%), while the least correct answers were for more technical questions such as identifying botnets (3.4%), email encryption (10.2%) or https (10.9%). Such results imply that although the participants spend quite a large amount of time on their digital devices, they are not so aware of security threats in cyberspace.

### C. THE EFFECT OF SOCIO-DEMOGRAPHIC CHARACTERISTICS ON CYBER SECURITY PERCEPTIONS, KNOWLEDGE AND BEHAVIOURS

The T-test for independent samples is used in order to reveal any differences between two groups on certain numerical characteristics. In our paper, we used it for analyzing gender and differences in the type of school attended by the respondents, their cyber security perceptions, knowledge, experiences and behaviors.

The analysis showed that there are significant differences based on gender only for knowledge ( $t=3.505$ ;  $df=144$ ;  $p<0.01$ ): the male respondents had higher scores (4.60) than the females (3.50), as can be seen in Fig. 1. This result is in line with previous research [21]. Also, for cyber security perceptions, the p-value is close to the significance level, so we concluded that males are more convinced of their

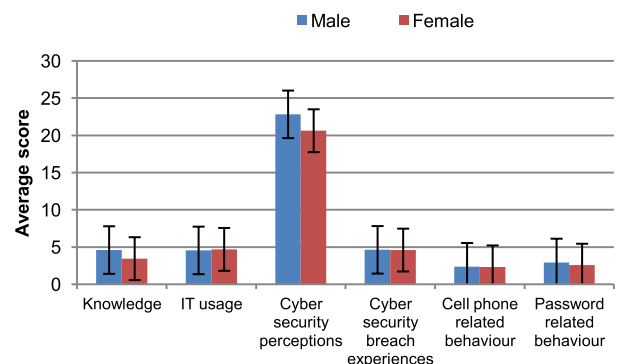


FIGURE 1. Average values and deviations of measured constructs for two genders.

security ( $t=1.919$ ;  $df=145$ ;  $p=0.057$ ). Something is considered significant if it is  $<0.05$ .

In addition, we also used a t-test for independent samples for testing the differences between the type of school attended by the respondents on the aforementioned variables. The analysis showed that there are statistically significant differences between school types (grammar school and vocational school) on knowledge ( $t=2.115$ ;  $df=146$ ;  $p<0.05$ ), cyber security breach experiences ( $t=1.987$ ;  $df=144$ ;  $p<0.05$ ), and cell phone related behavior ( $t=2.914$ ;  $df=144$ ;  $p<0.01$ ). The differences lie in the higher scores recorded for students who attended grammar schools for three constructs; they experienced security breaches more frequently, they know more, and their cell phone related behavior are more security-conscious, as is shown in Fig. 2.

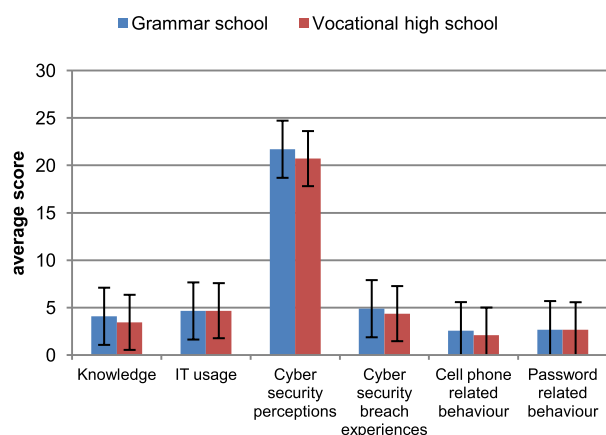


FIGURE 2. Average values and deviations of measured constructs for different school types.

#### D. RELATIONS BETWEEN PERCEPTIONS, KNOWLEDGE, EXPERIENCES AND BEHAVIOURAL ASPECTS OF CYBER SECURITY

Pearson’s correlation coefficient is used to detect the intensity and direction of the relation between numerical characteristics. In this paper, Pearson’s correlation was used between each of the two individual scores to further assess the relationship between cyber security perceptions, knowledge, experiences, and behaviors. There is a clearly significant negative correlation between cyber security breach experiences and password behavior (those who experienced cyber security breaches more often use less secure passwords), as well as a positive correlation between cyber security breach experiences and knowledge (those who were more frequent victims, scored higher on knowledge), as is shown in Table 2. The last claim is consistent with the Protection Motivation Theory [29]. Although, these correlations are significant, their intensity is low (below 0.2), so the relations are weak. As shown in Table 2, there is no significant correlation between cyber security perceptions and the behavioral aspects of cyber security.

Since Pearson’s correlation shows the correlation of individual scores, 2 by 2, (i.e., each one with the other), we tried

TABLE 2. Pearson’s Correlation coefficients between cyber security perceptions, knowledge, experiences and behaviors.

N=146	Know ledge	IT usage	Cyber security breach experiences	Cyber security perceptions
Password related behaviour	-.006	-.024	<b>-.157*</b>	.058
Knowledge		.112	<b>.145*</b>	.032
IT usage			.127	.027
Cyber security breach experiences				-.041

\*significant at the 0.05 level

a somewhat more complex analysis in order to gain a better insight into their interrelationships.

Multiple regression analysis shows the significance of one numerical characteristic prediction based on a set of numerical indicators. Multiple regression analysis was used to predict cyber security behavior based on cyber security perceptions, IT usage, cyber security breach experiences, and knowledge. Password related behavior and cell phone related behavior were used as cyber security behavior indicators. For each of those two cyber security behavioral indicators, we performed separate regressions.

Firstly, the idea behind this analysis was to discover the existence of any combination of predictors that can best explain cyber security behavior regarding passwords. The analysis showed that there is no significant prediction, i.e., password behavior cannot be explained by the previously mentioned predictors ( $r^2=0.028$ ;  $F=1.002$ ;  $df=4, 144$ ;  $p=0.409$ ). We can only note that cyber security breach experiences is close to the significance level ( $p=0.067$ , Table 3). If we consider the previously mentioned correlation between cyber security breach experiences and passwords, it can be concluded that there is a tendency for those who are the victims to have less secure passwords. However, this tendency should be further investigated since it might be mediated or moderated by some other factors which we did not measure.

TABLE 3. Regression coefficients for predicting password related behavior.

	$\beta$	t	p	r
Knowledge	.016	.185	.854	-.006
IT usage	-.010	-.116	.908	-.024
Cyber security breach experiences	-.156	-1.843	.067	-.157
Cyber security perceptions	.052	.625	.533	.058

We also used multiple regression analysis to test the prediction of cell phone related behavior based on cyber security perceptions, IT usage, cyber security breach experiences and knowledge. As in the previous analysis, we tried to discover whether there is any combination of predictors which can best describe how we predict cell phone related behavior. The analysis showed that there is significant prediction, i.e., cell phone related behavior can be explained by some of the aforementioned predictors. It was shown that 13.6% ( $r^2=0.136$ ;  $F=5.353$ ;  $df=4, 141$ ;  $p<0.01$ ) of cell phone

behaviors depend on knowledge and IT usage only. This indicates that although greater knowledge results in better cell phone behaviors, more frequent IT usage leads to less secure behaviors (Table 4). This can be explained by the fact that the participants may feel more confident because they use technology more, but they are not aware of the threats in cyberspace.

**TABLE 4. Regression coefficients for predicting cell phone related behavior.**

	$\beta$	t	p	r
<b>Knowledge</b>	<b>.333</b>	<b>4.183</b>	<b>.000</b>	<b>.301</b>
<b>IT usage</b>	<b>-.196</b>	<b>-2.470</b>	<b>.015</b>	<b>-.168</b>
Cyber security breach experiences	-.064	-.801	.425	-.040
Cyber security perceptions	-.007	-.093	.926	-.008

The finding that increased IT usage is related to less secure behaviors is in line with the research conducted by Ovelgönne et al. [30], who collected data longitudinally from users’ computers about cyber attacks and antivirus software, and reported that software-developers were attacked most often, followed by gamers and professionals, and then “regular” users. In addition, Grimes et al. [31] reported that younger users are less secure than older ones, because they are more confident, and believe that they are more tech-savvy.

Finally, in order to control the effects of the socio-demographic characteristics, we carried out the prediction in two steps, i.e., by means of hierarchical multiple regression analysis. Hierarchical multiple regression analysis also tests the criterion prediction, but allows for the possibility to control for certain effects, such as those related to socio-demographic characteristics. In all the performed analysis we adopted a significance level of 0.05. In the first step we tested the effects of gender and school type, and in the second we added cyber security perceptions, IT usage, cyber security breach experiences, and knowledge. In that way, we could differentiate effects of cyber security perceptions, knowledge, and experiences from socio-demographic characteristics, i.e., we could discover whether individuals behave more securely because of their gender and education, or because of better security knowledge and experiences. Hierarchical multiple regression was used to try to predict cell phone related behavior in two steps:

- 1) In the first step based on gender and type of school
- 2) In the second step, beside gender and school, we added cyber security perceptions, IT usage, cyber security breach experiences and knowledge.

The analysis showed that there is a significant prediction in both steps, with socio-demographics only ( $r^2=0.063$ ;  $F=4.789$ ;  $df=2, 142$ ;  $p<0.05$ ), and with cyber security perceptions, knowledge, and experiences added ( $r^2=0.183$ ;  $F=5.147$ ;  $df=6, 138$ ;  $p<0.01$ ). In the first step only type of school previously attended turned out to be significant (students from grammar schools behave more securely when it comes to cell phones) and it remained significant even after adding new predictors in the second step.

The most important finding is that the difference between the two models also appeared significant ( $r^2_{\text{change}}=0.12$ ;  $F_{\text{change}}=5.05$ ;  $df=4, 138$ ;  $p<0.01$ ). This means that cyber security perceptions, knowledge, and experiences additionally improve the prediction of cell phone related behavior, even after controlling for socio-demographic characteristics. In addition, we could see that the effects of cyber security perceptions, knowledge, and experiences are stronger than the effects of socio-demographics, 12% in comparison to 6.3%. According to the regression coefficients, we could conclude that only IT usage and knowledge about cyber security appear as significant predictors of cell phone related behavior, as shown in Table 5. The effects are such that the more the participants knew about security, and the less they used IT, the more they tended to behave securely with cell phones.

**TABLE 5. Regression coefficients for predicting cell phone related behavior, in two steps.**

	$\beta$	t	p	r
Model 1 Gender	-.014	-.172	.864	-.021
School	-.251	-3.084	.002	-.251
Model 2 Gender	.091	1.107	.270	-.021
School	-.211	-2.656	.009	-.251
Knowledge	.326	3.939	.000	.303
IT usage	-.191	-2.416	.017	-.159
Cyber security breach experiences	-.088	-1.110	.269	-.029
Cyber security perceptions	-.015	-.191	.849	-.013

Hierarchical multiple regression analysis was used in our attempt to predict password behavior in two steps:

- 1) In the first step based on socio-demographic characteristics: gender and school type.
- 2) In the second step, beside gender and school, we added cyber security perceptions, IT usage, cyber security breach experiences, and knowledge.

The analysis showed that there is no significant prediction in either step, i.e., that password related behavior cannot be predicted on socio-demographics ( $r^2=0.013$ ;  $F=0.967$ ;  $df=2, 142$ ;  $p=0.383$ ) or by combined socio-demographics and cyber security perceptions, knowledge, and experiences ( $r^2=0.04$ ;  $F=0.961$ ;  $df=6, 138$ ;  $p=0.454$ ).

Knowledge is a dominant factor in cyber security behavior on cell phones, and is not significant for password behavior, thus providing the answer to our third research question as to how knowledge of cyber security is related to the behavioral aspects of cyber security.

**V. CONCLUSION**

The environment is a very important factor when analyzing cyber security, as stated in [15], and this is the first survey conducted among university students in Serbia (in particular freshmen), which analyzes the factors relevant for cyber security awareness in depth. In addition, our survey also analyzed unreported correlations; how various factors in

particular and together, such as socio-demographic characteristics, cyber security perceptions, cyber security breach experiences, IT usage, and knowledge influence security behavior.

It was shown that the effects of cyber security perceptions, knowledge, and experiences are stronger than the effects of socio-demographics for cell phone related behavior, or in particular, IT usage and knowledge appeared as significant predictors of cell phone related behavior. However, any significant predictors have not been discovered for password related behavior, which will be the focus of our future analysis. Even though our participants perceived that their data were not safe, this did not serve as a trigger for them to learn more about cyber security so as to find out how to behave more securely in cyberspace.

None of the participants answered all of the questions correctly in the part of the questionnaire regarding knowledge, which led us to the conclusion that students do not have the required knowledge or adequate awareness of threats in cyberspace. Although there are considerable resources on the Internet, as well as numerous tutorials, these have not proved to be effective tools for students to learn. So, this can be a signal to educational institutions to take a more active approach to improve cyber security knowledge in a structural way and to teach students to protect themselves against cyber attacks. The practical implications of our research are that in future students should have effective training in high school regarding more secure behavior. Future research should be focused on developing more effective training to encourage young users to behave more securely.

## REFERENCES

- [1] Miniwatts Marketing Group. (2020). *World Internet Users Statistics and 2020 World Population Stats*. [Online]. Available: <https://www.internetworldstats.com/stats.htm>
- [2] Ratel. Belgrade. Serbia. (2018). *Digital Literacy and Internet Security*. (in Serbian). [Online]. Available: <https://www.cert.rs>
- [3] F.-J. Hinojo-Lucena, I. Aznar-Diaz, M.-P. Caceres-Reche, J.-M. Trujillo-Torres, and J.-M. Romero-Rodríguez, "Factors influencing the development of digital competence in teachers: Analysis of the teaching staff of permanent education centres," *IEEE Access*, vol. 7, pp. 178744–178752, 2019, doi: [10.1109/ACCESS.2019.2957438](https://doi.org/10.1109/ACCESS.2019.2957438).
- [4] "Cost of data breach study: Global overview," Ponemon Int. LLC., North Traverse City, MI, USA, Tech. Rep., 2017. [Online]. Available: <https://www.ibm.com/downloads/cas/ZYKLN2E3>
- [5] Joint Task Force (JTF) on Cybersecurity Education, "Cybersecurity curricula 2017-curriculum guidelines for post-secondary degree programs in cybersecurity," Version 1.0, Tech. Rep. ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8, Dec. 2017. [Online]. Available: <https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>
- [6] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017, doi: [10.1016/j.cose.2017.01.004](https://doi.org/10.1016/j.cose.2017.01.004).
- [7] B. D. Sawyer and P. A. Hancock, "Hacking the human: The prevalence paradox in cybersecurity," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 60, no. 5, pp. 597–609, Aug. 2018, doi: [10.1177/0018720818780472](https://doi.org/10.1177/0018720818780472).
- [8] B. K. Wiederhold, "The role of psychology in enhancing cybersecurity," *Cyberpsychol., Behav., Social Netw.*, vol. 17, no. 3, pp. 131–132, Mar. 2014, doi: [10.1089/cyber.2014.1502](https://doi.org/10.1089/cyber.2014.1502).
- [9] D. E. de Zafra, S. I. Pitcher, J. D. Tressler, J. B. Ippolito, and M. Wilson, "Information technology security training requirements?: A role- and performance-based model," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-16, 1998, doi: [10.6028/NIST.SP.800-16](https://doi.org/10.6028/NIST.SP.800-16).
- [10] D. M. Bada, "Cyber security awareness campaigns why do they fail to change behaviour?" Global Cyber Secur. Capacity Centre, Univ. Oxford, Oxford, U.K., Tech. Rep., 2014. [Online]. Available: <http://discovery.ucl.ac.uk/1468954/>
- [11] H. Suryotrisongko and Y. Musashi, "Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective," in *Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA)*, Kaohsiung, Taiwan, Nov. 2019, pp. 162–167, doi: [10.1109/SOCA.2019.00031](https://doi.org/10.1109/SOCA.2019.00031).
- [12] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Inf. Manage. Comput. Secur.*, vol. 18, no. 5, pp. 316–327, Nov. 2010, doi: [10.1108/09685221011095236](https://doi.org/10.1108/09685221011095236).
- [13] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *J. Inf. Knowl. Manage.*, vol. 15, no. 1, Mar. 2016, Art. no. 1650007, doi: [10.1142/S0219649216500076](https://doi.org/10.1142/S0219649216500076).
- [14] D. Jeske and P. van Schaik, "Familiarity with Internet threats: Beyond awareness," *Comput. Secur.*, vol. 66, pp. 129–141, May 2017, doi: [10.1016/j.cose.2017.01.010](https://doi.org/10.1016/j.cose.2017.01.010).
- [15] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018, doi: [10.1016/j.cose.2017.11.015](https://doi.org/10.1016/j.cose.2017.11.015).
- [16] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (SeBIS)," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. (CHI)*, 2015, pp. 2873–2882.
- [17] A. Moallem, *Cybersecurity Awareness Among Students and Faculty*. Boca Raton, FL, USA: CRC Press, 2019.
- [18] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014, doi: [10.1016/j.cose.2013.12.003](https://doi.org/10.1016/j.cose.2013.12.003).
- [19] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Comput. Hum. Behav.*, vol. 69, pp. 151–156, Apr. 2017, doi: [10.1016/j.chb.2016.11.065](https://doi.org/10.1016/j.chb.2016.11.065).
- [20] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Hum. Behav.*, vol. 69, pp. 437–443, Apr. 2017, doi: [10.1016/j.chb.2016.12.040](https://doi.org/10.1016/j.chb.2016.12.040).
- [21] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018, doi: [10.1016/j.jisa.2018.08.002](https://doi.org/10.1016/j.jisa.2018.08.002).
- [22] K. Olmstead and A. Smith, "Americans and cybersecurity," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2017. [Online]. Available: <https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>
- [23] K. Olmstead and A. Smith, "What the public knows about cybersecurity," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2017. [Online]. Available: <https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/>
- [24] M. Anderson and E. Vogels, "Americans and digital knowledge," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2019. [Online]. Available: <https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/>
- [25] *IBM SPSS Statistics for Windows*, version 22.0, IBM Corp, Armonk, NY, USA, 2013.
- [26] D. Florencio and C. Herley, "A large-scale study of Web password habits," in *Proc. 16th Int. Conf. World Wide Web (WWW)*, Banff, AB, Canada, 2007, p. 657, doi: [10.1145/1242572.1242661](https://doi.org/10.1145/1242572.1242661).
- [27] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," in *Proc. 7th Australas. Inf. Secur. Conf. (AISC)*, Wellington, New Zealand, 2009, pp. 71–78.
- [28] A. Adams and A. M. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40–46, Apr. 1999, doi: [10.1145/322796.322806](https://doi.org/10.1145/322796.322806).
- [29] R. W. Rogers, "A protection motivation theory of fear appeals and attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/00223980.1975.9915803>
- [30] M. Ovelgönne, T. Dumitraq, B. A. Prakash, V. S. Subrahmanian, and B. Wang, "Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach," *ACM Trans. Intell. Syst. Technol.*, vol. 8, no. 4, pp. 51:1–51:25, Mar. 2017, doi: [10.1145/2890509](https://doi.org/10.1145/2890509).
- [31] G. A. Grimes, M. G. Hough, E. Mazur, and M. L. Signorella, "Older adults' knowledge of Internet hazards," *Educ. Gerontol.*, vol. 36, no. 3, pp. 173–192, Feb. 2010, doi: [10.1080/03601270903183065](https://doi.org/10.1080/03601270903183065).





**ANA KOVAČEVIĆ** was born in Belgrade, Serbia, in 1969. She received the B.S. degree in electrical engineering and the M.S. degree in software systems from the School of Electrical Engineering, University of Belgrade, in 1993 and 2004, respectively, and the Ph.D. degree in software engineering from the Faculty of Organizational Sciences, University of Belgrade, in 2010.

From 1994 to 2004, she was involved in all phases of the software development in business application systems in “Jugobanka” and the Public Enterprise “Elektroprivreda” Serbia. Since 2004, she has been with the Faculty of Security Studies, University of Belgrade, where she is currently an Associate Professor. She has taught several undergraduate and graduate courses, such as computer science, information security, project management, and analysis and visualisation of data. She has authored three books, several book chapters, and articles published in international journals. Her research interests include information security, data mining, data bases, and information visualization.

Dr. Kovačević is a member of GOOD-OLD-AI, a society for object-oriented design and artificial intelligence.



**NENAD PUTNIK** was born in Belgrade, Serbia, in 1977. He received the B.S. degree in philosophy from the Faculty of Philosophy, University of Belgrade, in 2002, and the M.S. and Ph.D. degrees from the Faculty of Security Studies, University of Belgrade, in 2008 and 2012, respectively.

From 2004 to 2012, he was an Instructor with the Faculty of Security Studies, University of Belgrade, on the following graduate and postgraduate courses: conflict theories, conflict management, and methodology of scientific research. From 2013 to 2018, he was an Assistant Professor on the courses: conflict theories, conflict management, and designing data protection systems. Since 2018, he has been an Associate Professor with the Faculty of Security Studies, University of Belgrade, on the aforementioned courses. He also lectures at postgraduate level studies, where he teaches the course cybercrime and national security. He also teaches cyber security at the Diplomatic Academy of the Serbian Ministry of Foreign Affairs. He has published a number of academic articles, book chapters, and encyclopedic determinants in the field of cyber security, cyber warfare, conflict theories, and human security. He has authored the book *Cyber Space and Security Challenges* (Faculty of Security Studies, University of Belgrade, 2009).



**OLIVER TOŠKOVIĆ** received the Ph.D. degree in anisotropy of perceived space from the Department of Psychology, University of Belgrade.

He is currently an Assistant Professor with the Department of Psychology, University of Belgrade, and also lectures part time at the Faculty of Philosophy, Kosovska Mitrovica. He teaches Statistics in Psychology, Statistics in Educational Research, Multivariate Statistics, Academic Skills, and Perception. He has participated in various projects regarding basic cognitive processes and also projects, such as PISA, TIMSS, the academic motivation of students in Serbia, and the ACE-Serbia project. He has attended additional training in hierarchical linear modeling, dynamical systems in psychology, structural equation modeling, IRT analysis, and multi-level modeling. He has published 44 scientific articles and 138 conference abstracts, which have been cited 277 times (h-index = 7), and has organized ten public exhibitions on experimental psychology topics. His research interests include perception, statistics, and research methodology.

Dr. Tošković was granted the Psychological Society of Serbia Žiža Vasić Award for the popularization of psychology, in 2012. From 2012 to 2018, he was an Action Editor for the international journal *Psihologija* and a Reviewer for many international journals.

...