e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

FACTORS RELATED TO CYBER SECURITY BEHAVIOR

Solankar Saurav*1, Katade Aditya*2, Kasbe Nikhil*3, Monika Rokade*4

*1,2,3Student, (TE) Department Of Computer Engineering: Shree Gajanan Maharaj Shikshanprasarak Mandal Dumbarwadi's Sharadchandra Pawar College Of Engineering. Junnar Tal, Pune District, Maharashtra, India.

*4Assistance Professor, (TE) Department Of Computer Engineering: Shree Gajanan Maharaj Shikshanprasarak Mandal Dumbarwadi's Sharadchandra Pawar College Of Engineering. Junnar Tal, Pune District, Maharashtra, India.

ABSTRACT

An abstract Theoretical and empirical insight notes that cyber security recognition is a subject of specific hobby in cyber protection. people are the critical figures in cyber security and the manner to lessen risk in our on-line world is to make people greater protection conscious. at the same time as there had been severa research about diverse aspects of cyber safety consciousness, they are each inconsistent and environment-dependent.

Theprinciple aim of our studies is to investigate cyber security recognition intensive, and to try to find out how different factors including socio-demographics, cyber safety perceptions, preceding cyber protection breaches, IT utilization, and know-how might also personally or together effect on cyber protection behavior. To prove that we conducted our research on students, as they may be the most technologically lively part of the society. We determined that understanding proved to be the dominant element for cyber security recognition, and even though students are virtual natives, they do not experience secure inside the cyber environment; they do now not behave securely and do not have adequate expertise to defend themselves in our on-line world.

I. INTRODUCTION

These days, existence can infrequently be imagined with out records era; greater than half of of the sector's populace (fifty eight.eight%) used the internet in 2019 with 73.four% net users in Serbia [1]. consistent with a report compiled with the aid of Ratel in Serbia, ninety nine.2 % of these elderly between 16 and 24 use computers and ninety eight.2% use the net each day or almost each day [2]. latest technological development has had a excellent impact on people's life [3]. but, there's additionally a darkish side to this fashion; in 2017 the Ponemon Institute expected the economic impact of safety breaches at almost half a thousand billion bucks globally, with the cost of statistics breaches increasing every yr [4]. protection incidents are constantly increasing, and are getting increasingly sophisticated and extra excessive. With the wide adoption of records technology inside the ultimate decades, the profile of the cease-consumer also has changed. The common consumer of records generation isn't always technically knowledgeable, and has most probable not studied cyber safety in his/her preceding training. Cyber security is described as a computer-primarily based area, which involves era, people, information and strategies, with the intention of securing operations towards unauthorized access or attack [5]. despite the fact that users are truly aware about the security risks, most of them are not sure how they must behave to achieve cyber safety (e.g., despite the fact that they have got heard approximately phishing, a few customers are not sure the way to recognize the trouble or react accurately). in step with severa reviews, human error is seen as the dominant hassle for at ease facts, making it necessary to recognize humans's conduct towards security era [6], [7], [8]. numerous protection breaches are because of a lack of know-how or unsafe behavior (e.g., sharing passwords, or clicking on unsecured hyperlinks in emails). protective oneself in cyberspace has come to be a necessity today. safety focus is described in NIST unique book 800-16 as follows: "consciousness isn't training. The reason of recognition shows is sincerely to awareness interest on protection. recognition shows are supposed to allow individuals to recognize IT protection concerns and reply for this reason" [9]. Bada et al. [10] stated that focus does no longer only suggest being aware about possible threats, but additionally adopting safety conduct. in this paper, we examine cyber safety recognition in depth, and accordingly, the paper is prepared inside the following manner; the heritage phase opinions and provides relevant work on cyber protection awareness and the proposed research query. phase III describes and discusses the adopted technique. segment IV affords the effects and gives a discussion of the findings,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

interpreting them so one can attain greater clarity. ultimately, segment V offers our conclusion and future path of paintings.

II. BACKGROUND

Cyber protection is a developing and essential discipline regarding numerous research studies [11]. one of the studies instructions within the area of cyber safety is the way to enhance cyber safety cognizance, focusing on those factors which might be the maximum big in reaching this intention. This segment in brief affords relevant studies in cyber safety attention, basically inside the training area. of their research, Kruger et al. [12] describe an exploratory study to test the opportunity of the usage of statistics protection vocabulary assessments to evaluate awareness levels and familiarity with security phrases for you to indentify suitable regions and subjects for data safety focus packages. The questionnaire used consisted of sections: the first section changed into a vocabulary take a look at and the second one evaluated the respondents' behavior. They found using the vocabulary test for the evaluation of attention tiers to be a beneficial tool and a giant dating between information of concepts (vocabulary) and conduct turned into proven. Al-Janabi & Al Shourbaji [13] accomplished studies to analyze statistics safety recognition degrees and related danger, in addition to the standard impact on institutions, among students and team of workers inside the academic environment within the middle East. The outcomes discovered that the participants did now not have the required know-how and know-how of records security focus. The authors mentioned the results for actual international issues from the diagnosed weakness in this survey, and made advice to remedy the situation. Jeske & Van Schaik [14] conducted a survey of students' familiarity with special internet threats. The individuals have been supplied with definitions of threats and have been requested to kingdom how familiar they have been with every. in step with their responses, three clusters have been identified; the primary cluster covered those participants who were knowledgeable about all threats (each new and familiar), the second cluster comprised participants extra familiar with new threats, even as the 1/3 cluster consisted of contributors more familiar with 9aaf3f374c58e8c9dcdd1ebf10256fa5 threats. The authors confirmed that time spent on the internet and the period of net experience have been predictors of familiarity with net threats, which can be a in addition predictor of laptop safety use.

III. METHOD

The contemporary have a look at is achieved thru a survey, on a comfort sample of college students. The questionnaire contained tailored objects from preceding surveys carried out with the aid of the Pew studies Centre [22], [23], [24].

A. pattern

Our members in the survey have been students, as it's miles assumed that this populace could be very familiar with IT era [2]. We determined to behavior our studies on college students on the college of protection studies, university of Belgrade, as they have chosen to take a look at specific aspects of security (i.e., country wide protection, environmental safety, crime and criminology, and information protection) for their expert vocation and underneath the idea that they have a better degree of safety focus than students from other schools. similarly, our contributors had been learners on the starting of their studies and that they nevertheless do no longer have precise cyber security expertise, so their cutting-edge level of know-how can only be related to the expertise gained in high faculty. Our number one concept became to discover the level of safety consciousness of freshmen when they arrive on the faculty of safety studies, and the practical implication is that we will improve our curriculum regarding those findings. The pattern consists of 147 members, 40 (27%) male and 107 (seventy three%) female.

B. gadgets

The first section of the survey centered on the scholars' socio demographic information, inclusive of gender and previous training. Cyber protection is quite a complex and vast concern [23], and the second part of the questionnaire analyzed the diverse dimensions of cyber protection. The majority of the questions have been adapted from the survey conducted by using the Pew research Centre in 2016 [22]. The third part of the survey measured information, and we chose to apply questions from questionnaires [23], [24], which had been developed with the aid of cyber security experts to measure the overall concepts and crucial constructing blocks for on line safety. We decided on the ones questions which have been relevant for our individuals. We

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

selected those questionnaires due to the fact the questions had been precise, within the form of a take a look at ordinarily with handiest one correct answer, explicitly showing know-how of lack of know-how [23], [24].

IV. RESULTS AND DISCUSSION

To offer assemble validity to cyber safety perceptions, cyber protection breach stories and cell telephone and password behaviors, we firstly carried out element analysis- PCA (foremost component evaluation) on the related questions. thing evaluation with PCA (primary factor analysis) became used so as to show corporations of questions which showed high inter-correlations. This allows the detection of so referred to as latent variables, which lie in the back of the contributors' solutions to the questions.

A. CONSTRUCTS

One factorial solution changed into selected for every of the tested constructs. For issue structure loadings, we chose only objects which confirmed excessive saturations (>0.3). The cyber safety belief component explains forty% of the variance, and loadings are in the range from zero.309 to zero.824; the cyber protection 2 breach studies aspect explains forty three% of the variance, and saturation is from zero.452 to zero.824; the password related behavior factor explains 17% of the variance and saturation is from 0.313 to 0.677 and the cellular telephone associated behavior thing explains 22% of the variance with saturation from 0.507 to 0.706.

B. DESCRIPTIVE effects concerning CYBER

Security nearly all of the contributors have smartphones (99.3%), and use the internet on their cell telephones (or different cell handheld gadgets). besides that, ninety nine.3% use social media sites such as facebook, Twitter, or LinkedIn. but, when it involves online purchasing and e-banking, most effective 17.7% of the contributors use online banking offerings, even as 50.three% of the participants do their buying on line. most of the people of the scholars (73.five%) have never confronted a security breach, at the same time as 11.6% of them have encountered one, 12.2% less than 5 times, 2.0% more than three instances, and simply one participant(zero.7%) extra than ten instances. We also analyzed which safety breaches the contributors had encountered; 4.1% of the individuals had professional a compromised e-mail account, whilst 22.4% a compromised social media account. On the alternative factor, nearly all the people (99.3%) said that they had heard about as a minimum one safety breach that had took place to their close to friends or circle of relatives: 34.7% simply as quickly as, 46.three% among 1 and five times, and 18.3% extra than five instances. The members do not experience very confident in numerous institutions to defend their 255fb4167996c4956836e74441cbd507 facts from unauthorized customers, and they show the satisfactory stage of subject (now not confident at all) generally about social media sites (42.8%), government institutions (20%), groups they pay online (20%), or net groups (20%). On the alternative side, they have higher tiers of self assurance inside the university e-company (28%) and 8db290b6e1544acaffefb5f58daa9d83 banking (22%). kind of one 1/3 of the people (30.6%) experience that their 255fb4167996c4956836e74441cbd507 statistics is extra cozy than five years within the past, 30.6% expect that it's miles as relaxed as it come to be five years in the past, even as 28% assume they're plenty much less secure.

C. THE impact OF SOCIO-DEMOGRAPHIC traits ON CYBER protection PERCEPTIONS, information AND BEHAVIOURS

The T-take a look at for impartial samples is used if you want to display any variations among two organizations on positive numerical characteristics. In our paper, we used it for studying gender and differences within the kind of school attended via the respondents, their cyber safety perceptions, knowledge, reports and behaviors. The analysis confirmed that there are large differences primarily based on gender best for information (t=3.505; df=a hundred and forty four; p<zero.01): the male respondents had higher scores (4.60) than the females (3.50), as can be visible in Fig. 1. This result is in line with preceding studies [21]. additionally, for cyber safety perceptions, the p-cost is close to the significance degree, so we concluded that men are extra satisfied of their safety (t=1.919; df=a hundred forty five; p=zero.057). some thing is taken into consideration massive if it's miles <zero.05.

D. members of the family among PERCEPTIONS, understanding, reports AND BEHAVIOURAL components OF CYBER protection

Pearson's correlation coefficient is used to stumble on the intensity and course of the relation between numerical traits. on this paper, Pearson's correlation became used between every of the two person rankings to

similarly check the relationship among cyber safety perceptions, understanding, reviews, and behaviors. there is a simply large negative correlation among cyber security breach stories and password conduct (individuals who skilled cyber safety breaches extra often use less comfortable passwords), as well as a advantageous correlation between cyber protection breach reports and information (people who have been extra frequent victims, scored better on know-how), more than one regression evaluation indicates the importance of one numerical characteristic prediction based totally on a fixed of numerical indicators. more than one regression analysis changed into used to are expecting cyber protection conduct primarily based on cyber protection perceptions, IT utilization, cyber protection breach studies, and expertise. Password related behavior and cell phone related conduct were used as cyber security conduct signs. For every of those two cyber security behavioral signs, we carried out separate regressions.

V. CONCLUSION

The surroundings is a totally crucial element when analyzing cyber protection, as stated in [15], and this is the first survey performed amongst college students in Serbia (specifically inexperienced persons), which analyzes the factors relevant for cyber protection focus extensive. in addition, our survey additionally analyzed unreported correlations; how different factors in particular and together, including socio-demographic characteristics, cyber protection perceptions, cyber security breach studies, IT utilization, and know-how have an impact on protection behavior.

It was proven that the results of cyber security perceptions, information, and reports are stronger than the effects of socio-demographics for cellular cellphone related behavior, or particularly, IT utilization and knowledge 2 regarded as considerable predictors of cellular telephone related conduct. but, any large predictors have now not been located for password related behavior, in an effort to be the focal point of our future analysis. even though our contributors perceived that their statistics have been no longer safe, this did now not serve as a cause for them to learn greater approximately cyber protection that allows you to find out a way to behave extra securely in cyberspace.

None of the participants answered all of the questions effectively in the part of the questionnaire concerning information, which led us to the belief that scholars do not have the desired expertise or good enough awareness of threats in our on-line world. even though there are enormous resources at the internet, in addition to severa tutorials, those have no longer proved to be powerful equipment for college kids to study. So, this can be a sign to educational establishments to take a greater energetic method to enhance cyber safety understanding in a structural manner and to train students to guard themselves towards cyber assaults. The realistic implications of our studies are that in destiny college students must have effective schooling in high college regarding more comfortable conduct. future studies must be centered on growing greater effective education to inspire younger users to act more securely.

VI. REFERENCES

[1] Swapnil Kumbhalkar, Shubham Meshram, Grishma Hedaoo, Raksha Tabhane, Priyanka Thoke, Prof. Mukesh Barapatre, “online challenge management gadget” November- 2018.

[2] B. Persis Urbana Ivy, G Uma Maheswari, Kumar P, JSuganya Pandi.“Android based totally task scheduler and indicator”, January 2014.”

[3] J. A. Larco, J. C. Fransoo, V. C. S.Wiers. Scheduling the scheduling mission: a time-control angle on scheduling”, October 2017.

[4] Dr. Monika Dhananjay Rokade. “Android battery saver machine: an alarm telling the person to pressure prevent or close the apps which can be drawing electricity the usage of ai-based programming” yr 02021.

[5] Dr. Monika Dhananjay Rokade “facts technology: The emerging area in IT” yr 2023.

[6] Dr. Monika Dhananjay Rokade “development of an Android based actual Time Bus tracking machine” 12 months 2021.