Higher Education Institutions as Targets for Cyber-attacks: Measuring Employees and Students Cybersecurity Behaviours in the Estonian Academy of Security Sciences

Kate-Riin Kont

Estonian Academy of Security Sciences

28.09.2023

Cybercrime can never be eliminated, the only way is to educate yourself. People's basic everyday cyber hygiene needs to improve.

It is extremely important that we are able to develop people's cyber security skills in such a way that our human resources are one of the major strongholds of a secure social order.

Grete Kodi, Marki Tihhonova-Kreek (2022)

SISEKAITSEAKADEEMIA

The importance of the topic

- Across Europe, the number and sophistication of cyber- attacks and cybercrime is increasing. While nearly every major industry faces significant cyber security challenges, higher education is particularly vulnerable for several important reasons.
- Collaborating and sharing information with other researchers both inside and outside the university is a security challenge that has not been a problem in various industries or even for the financial sector.
- As a result, they have long been visible targets, and cybercriminals are likely to know their weaknesses very well. A few examples of cyber-attacks on universities show that such an attack can be not only detrimental to relations between countries but even life-threatening.

The importance of the topic

- In recent years, security breaches in higher education institutions have become very frequent. A few of examples of cyber-attacks on universities show that such an attack can be not only detrimental to relations between countries, but even life-threatening:

University of Maryland, USA (2014-2018)

The University of Helsinki, Finland (2019)

Düsseldorf University, Germany (2020)

Tartu University, Estonia (2020)

The Silent Librarian and Mabna Institute Campaigns

The purpose of the study

- Several studies have shown that there is a human dimension to the causes of cyber attacks in universities (Muniandy & Muniandy, 2012; Othman et al., 2020).
- The purpose of this study is to identify the most common characteristics that make users vulnerable, either individually or in groups, and to determine whether there is a relationship between user behaviour and victimisation of a cyber-attack. This research should help characterise people who are more likely to become victims of various phishing and social attacks.

The research methodology

- The five-scale measure developed by Öğütçü et al. was used.
- The **RBS** measures the risk behaviour of Internet users, e.g. whether various security measures are used to protect themselves as well as the people they live or work with.
- The purpose of the **CBS** is to measure the Internet user's actions and actions in protecting his personal information.
- The purpose of the **EOS** is to measure the exposure of users to any cyber security threat, highlighting the user's behaviour in relation to the risks, threats and effects resulting from the events.
- The **RPS** measures the level of risk or threat that befalls the Internet user and is related to the field of trust that the user has in the face of possible cyber-attacks.

The reserach methodology

- The survey consists of five parts:

    1) questions that collect respondents' demographic data,

    2) questions about user profiles related to IT and computer security,

    3) questions dealing with risky issues related to IT behaviour,

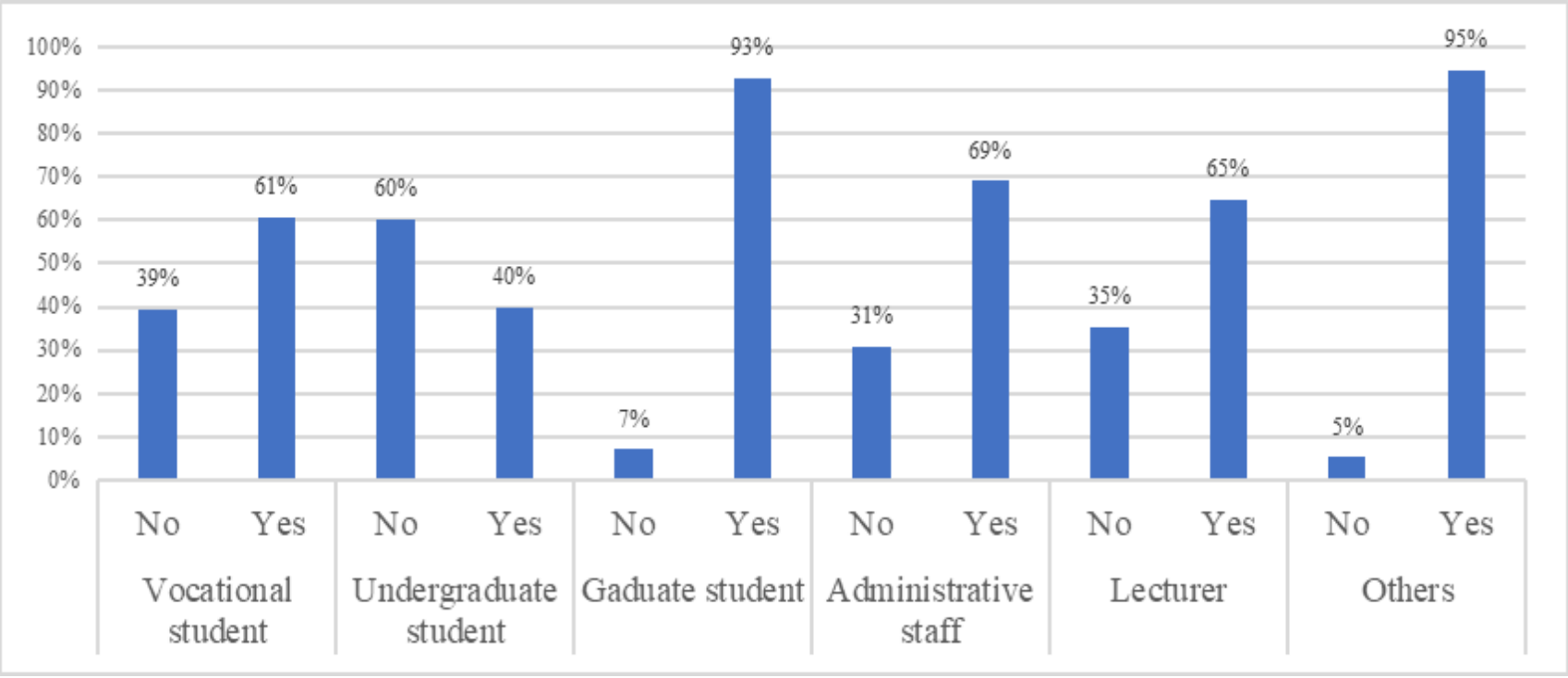
    4) questions about respondents' behaviour regarding information security and threats, and

    5) questions that address users' exposure to cybercrime.

- Answers could be given according to a 5-point Likert scale. The proposed scales were formulated depending on the questions asked.
- The survey was conducted using LimeSurvey and was administered by sending a link to the online survey.

General results

Figure 1. Results of the completed cyber security trainings by position



General results

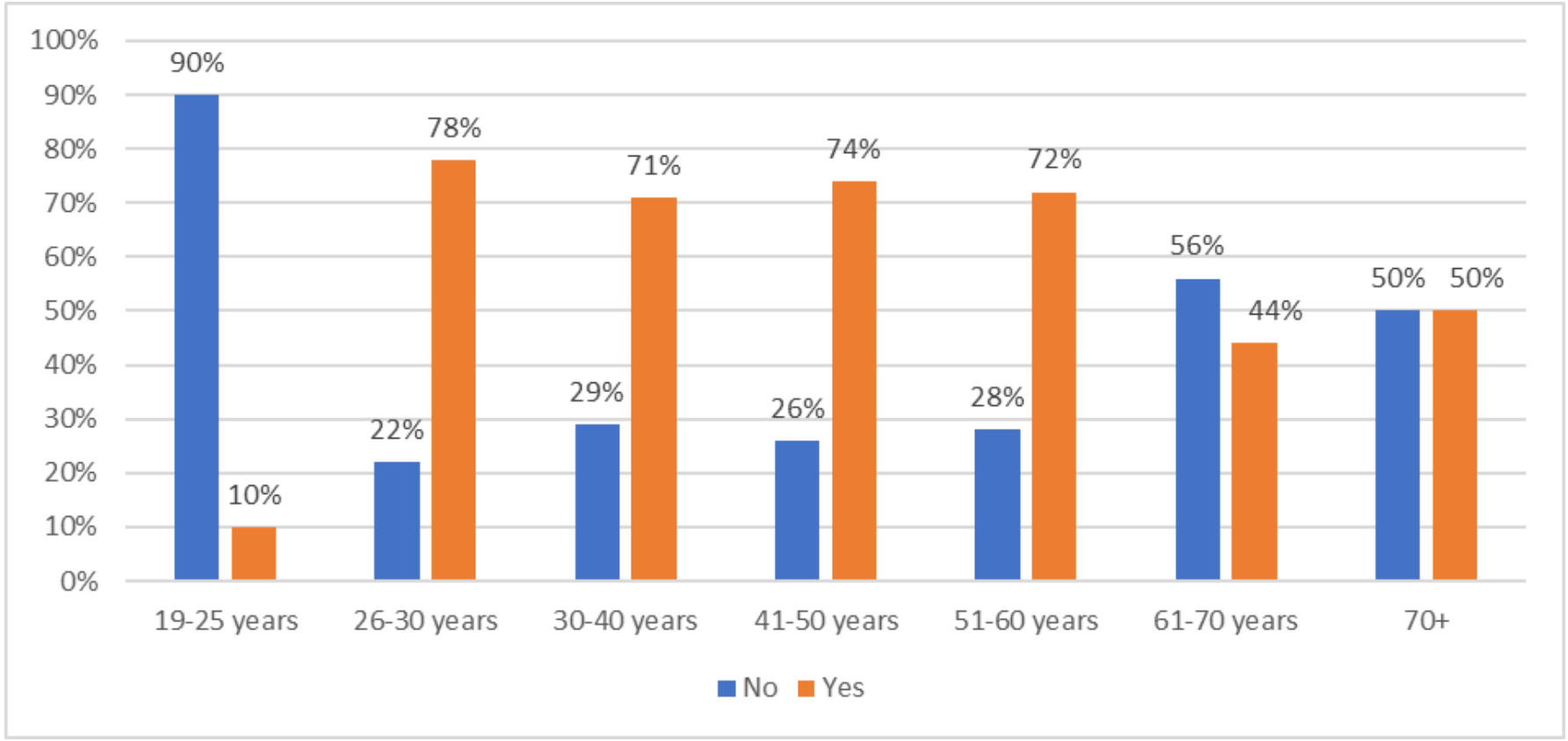
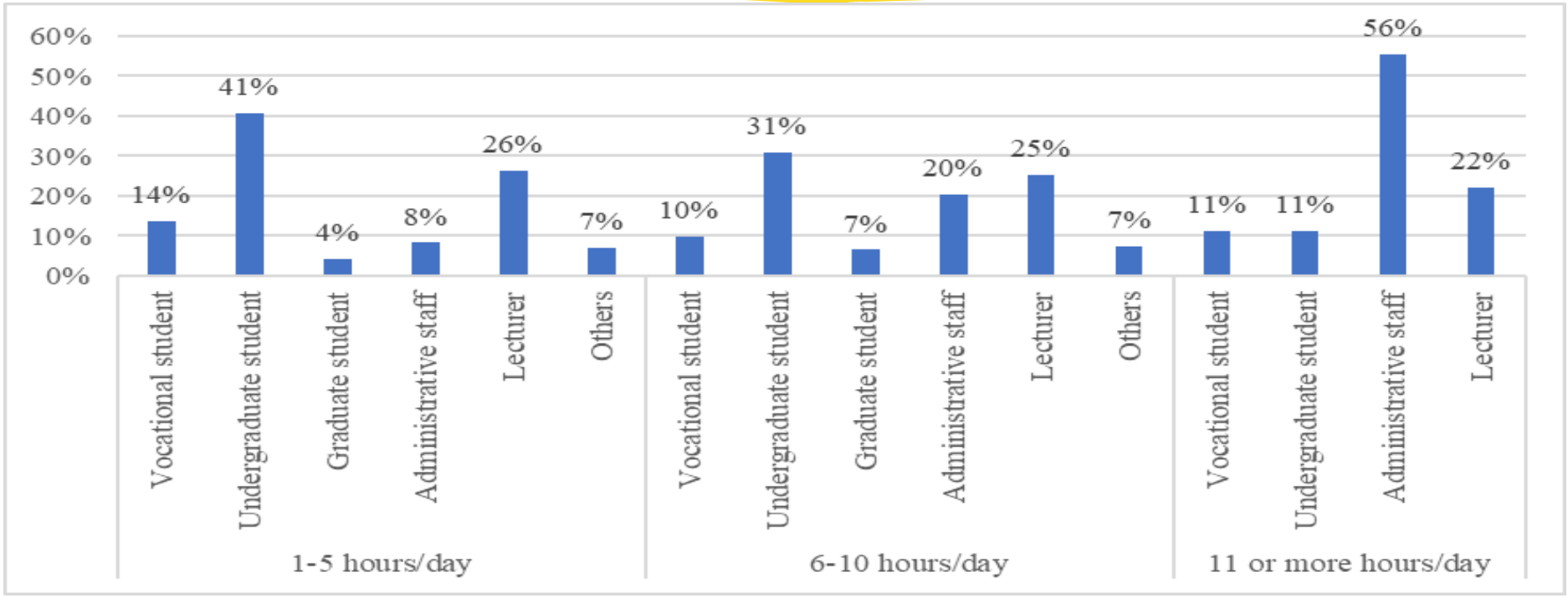


Figure 2. Results of the completed cyber security trainings by age

General results

Figure 3. Time spent on Internet according to the position



General results

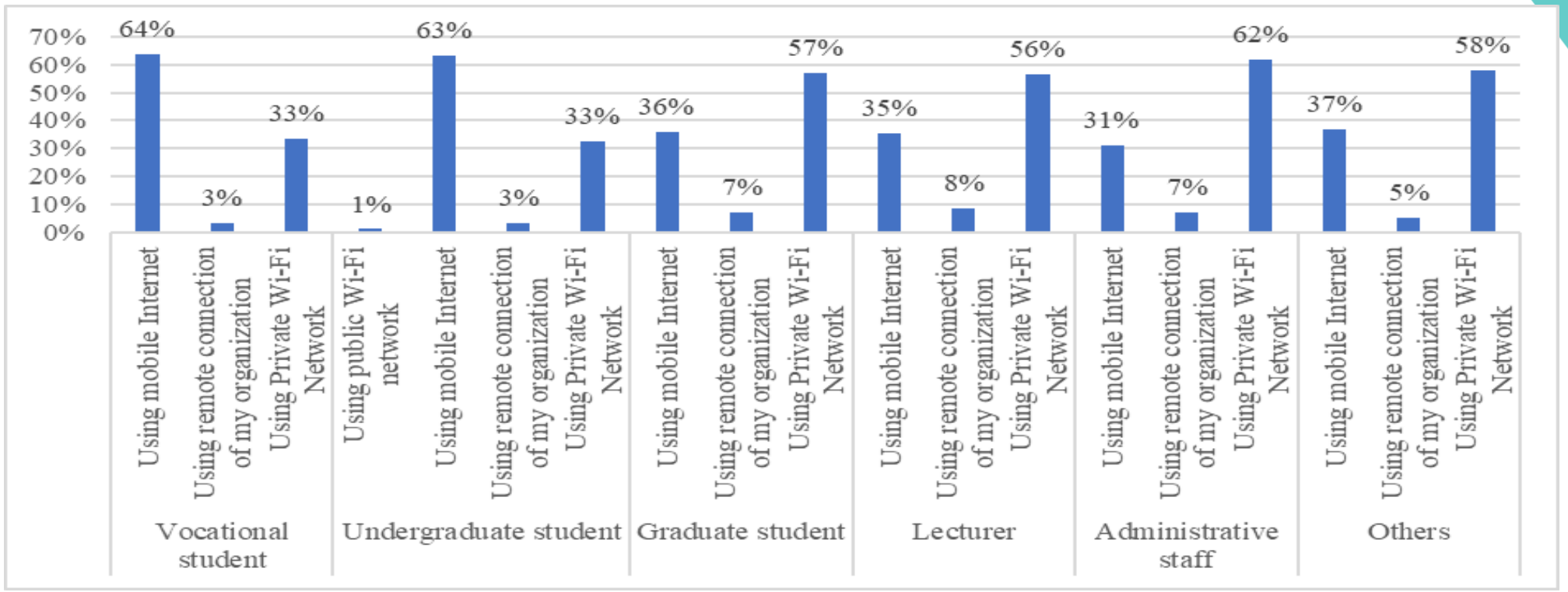


Figure 4. Access to the Internet from outside the respondents' workplace

First results

TABEL 1. NUMBER OF QUESTIONS, AVERAGES AND CRONBACH ALPHA OBTAINED BY SCALE

Scale	Number of questions	Average score	Cronbach alpha
RBS	20	2,610	0,650
CBS	10	4,051	0,702
EOS	7	1,389	0,435
RPS	17	3,498	0,823

First results

Score type	Group	n	Mean	Standard deviation	Min	Max
Risky Behavior Scale (RBS)	Vocational student	33	48,121	7,801	34	65
	Under-graduate student	98	49,898	6,397	33	65
	Graduate student	14	46,928	4,906	39	57
	Lecturers	71	46,084	6,353	34	67
	Administrative staff	42	48,524	5,052	37	59
	Other	19	45,894	6,297	34	57
	TOTAL	**277**	**52,249**	**6,879**	**35**	**72**
Conservative Behavior Scale (CBS)	Vocational student	33	38,485	5,438	25	50
	Under-graduate student	98	38,194	5,076	24	48
	Graduate student	14	43,428	3,673	37	48
	Lecturers	71	42,563	4,191	30	50
	Administrative staff	42	41,524	3,909	31	47
	Other	19	43,947	4,116	37	50
	TOTAL	**277**	**40,513**	**5,082**	**24**	**50**
Exposure to Offence Scale (EOS)	Vocational student	33	10,061	2,076	7	15
	Under-graduate student	98	9,663	2,275	7	22
	Graduate student	14	9,857	1,231	7	12
	Lecturers	71	9,535	1,873	7	16
	Administrative staff	42	10,071	1,980	7	16
	Other	19	9,263	1,881	7	14
	TOTAL	**277**	**9,722**	**2,037**	**7**	**22**
Risk Perception Scale (RPS)	Vocational student	33	60,303	7,892	45	75
	Under-graduate student	98	58,561	9,158	24	85
	Graduate student	14	62,928	6,474	52	75
	Lecturers	71	58,380	9,559	17	81
	Administrative staff	42	60,524	6,259	46	75
	Other	19	61,789	5,360	55	75
	TOTAL	**277**	**59,462**	**8,448**	**17**	**85**

Responents' comments

- *Basically, everything can be dangerous, but some environments need to be used. It would be safest to live offline.*
- *For example, using an internet bank in itself cannot be considered dangerous, but using it on a public Wi-Fi network is. The same can be the case in the view of cloud services, etc.*
- *If you understand where to press and what to share, there are no problems. The more you participate in FB sharing games, the more problems you have.*
- *Online shopping and data entry - if I do it in the safest places I know, I don't consider it a problem, but I never go shopping in a little-known store in Estonia or in a foreign environment.Common sense must be maintained in the internet environment as well as in the normal environment.*
- *Many of the activities can be dangerous, but it is necessary to consider the justification and check the existence of security solutions (e.g. in the case of internet banking, whether there is secure authentication and the correct website, before opening e-mails with advertising content, the authenticity of the sender and to be sure that there is any interest in such e-mails, etc. . On the other hand, the use of public Wi-Fi should be avoided in any case and rather use mobile data*

First conclusions

- In summary it is necessary to emphasise that people's behavior can contribute to making it easier to become victims of cyber-attacks, and it is by raising their awareness that it is possible to mitigate the consequences of cyber-attacks on universities.
- The model proposed can be successfully applied to different higher education institutions – it helps quickly find out the cyber security training needs and develop the training policy which can be implemented at the right level of difficulty. Similarly, this model identifies the knowledge and skills of user groups, to deal with social engineering attacks.

THANK YOU FOR YOUR ATTENTION!

SISEKAITSEAKADEEMIA