# A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education

**Judit Módné Takács, Monika Pogátsnik**

Óbuda University, Alba Regia Technical Faculty
Budai u. 45, H-8000 Székesfehérvár, Hungary,
modne.t.judit@amk.uni-obuda.hu, pogatsnik.monika@amk.uni-obuda.hu

*Abstract: Background: Cybersecurity is an extremely important topic in the 21st Century, especially for students in education. It is essential for career development in technical higher education to know how to defend against digital threats and cyberattacks effectively. Education may enhance digital literacy and security awareness. To measure the success of this development it is essential to have a reliable measurement tool. Objective: This study aims to develop a Hungarian adaptation of the Cybersecurity attitude survey (CS-C), to test the psychometric properties of the survey among students of technical higher education institutions and to analyze the results. Method: The 25-item questionnaire measures cyberawareness on a 5-point Likert scale. A pilot study with 35 participants, who were retested after a few weeks, was conducted in the first round. For a more comprehensive analysis, N=398 participants in higher technical education were included in the second phase of the study. Results: The results of the psychometric analyses demonstrated the internal reliability and validity of the CS-C-H questionnaire and confirmed that it is reliable ($\alpha$ =.858) in its application and interpretation along dimensions of cyberspace-related attitudes, especially among students in education. Respondents' cybersecurity awareness is at an acceptable level, but question-specific differences between groups can be found. Further research into the factors that influence the development of attitudes is, therefore, worthwhile. Conclusion: The use of this diagnostic tool among Hungarian students is justified based on the results of the study.*

*Keywords: cybersecurity awareness measurement; adaptation; validation; engineering; higher education*

# 1 Introduction

Considering the complexity of the cybersecurity landscape, it is worthwhile to recognize that most incidents, specifically 74 percent, are caused by human errors. [1]. The level of cyberfatigue and reluctance to proactively defend against cyber-

attacks is also influenced by this human factor. Cyber threats to businesses have risen by 97% since the start of the Russian-Ukrainian war [2]. The demand for cyber security professionals is growing in parallel with the increasing frequency of cyber-attacks [1]. Cybersecurity jobs, including information security analysts, are predicted to grow by 35% by 2031, highlighting the growing need for more effective threat management [1].

In the 21st Century, where digital technologies and the online space are an integral part of our daily lives, cybersecurity culture encompasses cybersecurity awareness, safe behavior, and cyber hygiene (safe behavior in the digital environment and defense against online threats) [3]. The number of data security incidents is increasing rapidly, according to current cybersecurity trends and statistics [1, 4]. Cyberattacks are not only aimed at companies but also at individuals who work from home or take part in online meetings [5]. Remote working increases the average cost per incident and contributes to data breaches [1]. Training and awareness, not just for cybersecurity professionals, but for everyone working in cyberspace, has therefore become critical. Addressing this growing threat must be prioritized in training curricula and awareness processes.

Cyberawareness includes understanding online identity, online privacy practices, improving cybersecurity, using social networks wisely, and protecting digital assets, so it covers a broad spectrum [6]. Also, part of this awareness is the increasing importance of Internet use and the understanding of Internet skills. In terms of pedagogy, this shows a certain integration of knowledge transfer.

## 1.1 Assessment and Measurement of Cyberawareness

Two viewpoints exist when examining security awareness. One focuses on technological control, emphasising continuous external monitoring and applying technological restrictions. Another view focuses on individual training and raising awareness. Development is not driven by knowledge alone, but also by motivation, emotion, attitude, culture and interest [7]. Education is of great importance, especially in higher education institutions, as a participant in the development of awareness and the transfer of knowledge. These institutions have a direct link with the industrial sector, which is especially vulnerable to cyberattacks and employs a significant number of people.

Inadequate response to existing problems and attacks, as well as failure to prevent or mitigate damage, is often a key challenge in managing cyberincidents. Many question the effectiveness of annual training, e-learning materials, or exams, as they may not be sufficient to develop real cybersecurity awareness [8]. An important area is the development of cybersecurity skills, together with the enhancement of key competencies that positively influence the reinforcement of attitudes. By expanding users' knowledge and translating it into easily applicable practical skills, educational programs can contribute to the formation of effective

cybersecurity behaviors. The term ISA (Information Security Awareness) refers to Information Security Awareness. It is a field that aims to increase the awareness and knowledge of users, employees, or other stakeholders concerning issues of information security. ISA is defined as having two main aspects: one is Knowledge and Awareness, and the other is Activities and Compliance. Most validated measurement tools used in real-world scenarios approach measurement from the perspective of knowledge and awareness, while the analysis of activities and compliance has been less prominent. This indicates that ISA measurement is still a relatively young area of research, with many appropriate measurement tools emerging in the international context over the last seven years. [9]

Several quantitative studies have been carried out in Hungary using a variety of measurement tools. However, in contrast to our study, these studies did not investigate young people's cybersecurity awareness. In 2022, Gyaraki [8] investigated elements of social media users' internet safety awareness, focusing on password choice and application awareness, the use of public Wi-Fi, and the different levels of attention to internet safety at work and home. Nyikes [10] demonstrated the relationship between cybersecurity awareness and digital literacy in his 2017 study, which covered the entire Hungarian population. Palik and colleagues [11] used two online surveys to survey the general population - civil servants and employees of business enterprises. The survey was conducted using the European Commission's EUSurvey web platform, which is also used by the European Union Agency for Cybersecurity (ENISA). The study of specific young people, i.e. the cybersecurity awareness of schoolchildren, is lacking in previous national studies. These studies generally addressed cybersecurity awareness in general or specific groups. The surveys were based on self-designed questionnaires tailored to the characteristics of the target groups or were conducted on the EUSurvey web platform operated by the European Commission. The questionnaires were aligned with the European Union's cybersecurity standards. However, the school environment has different characteristics that could be considered when adapting a universal measurement tool. Based on these reasons, a validated tool to measure cybersecurity awareness in Hungarian could help obtain more accurate and relevant results among students. In addition, it allows for the assessment and development of the specific needs and knowledge of young people in the cybersecurity field.

## 1.2 Aim of the Study

The study aims to adapt the Cybersecurity awareness Scale (CS-C) to the Hungarian context and to test the psychometric properties of the Hungarian version of the survey (CS-C-H) on a population of students in higher education. Figure 1 shows the process of adapting and validating the questionnaire.

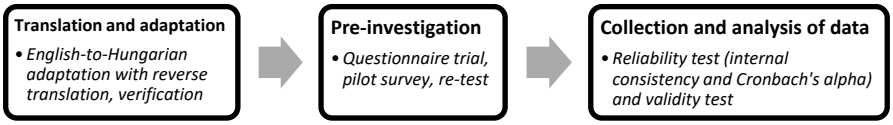


Figure 1

The process of adapting and validating the CS-C questionnaire in Hungarian

Source: Author's construction

# 2 Methods

## 2.1 Sampling and Data Collection Procedures and Instruments

To be representative of the population, the sample was limited to Fejér County and within it Székesfehérvár. A total of 398 engineering students from the Alba Regia Technical Faculty of Óbuda University and the Székesfehérvár Campus of Corvinus University participated in the study. Engineering students predominated in the study population. Two subsamples were used in the study. The first round included a pilot measurement with N=35 participants who were retested after 3 weeks, and the second round included a survey with N=398 participants. Between September 2022 and May 2023 data were collected. Participating was voluntary and anonymous. The eligibility criteria were students had to be in an active semester at a higher education institution in Székesfehérvár, studying full-time or part-time. Data were collected using traditional paper-based questionnaires, then recorded, digitized, and coded by the researcher. Those who did not fill in the questionnaires in full, or who gave incorrect answers to certain questions, were excluded from the survey and their item number was no longer considered.

## 2.2 Survey Adaptation and Validation: Development and Testing of the Questionnaire

The adaptation and validation process of the CS-C questionnaire followed a systematic six-step procedure, defined according to international standards and guidelines as shown in Figure 2 [12, 13].

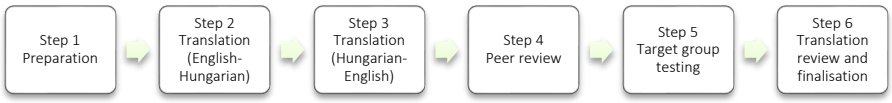


Figure 2

The translation and adaptation process of the CS-C questionnaire into Hungarian

Source: Author's construction

The first step was the preparation of the questionnaire. This included a review of similar Hungarian-language awareness measurement tools to avoid duplication. Following the preparation of the questionnaire, the CS-C was independently translated from English to Hungarian by two computer science educators, native Hungarian speakers with professional familiarity with cybersecurity concepts. In the next step, an independent person translated back and interpreted the questionnaire and compared it with the original version. Finally, the original version was compared with the two translated versions by a group of three computer science teachers from different educational institutions at different levels. The group identified inappropriate terms or expressions and worked on a common version, considering conceptual and cultural equivalence. They reached a consensus on a Hungarian version for the pre-test. Six students from three different levels of education (primary, secondary and university) piloted this version. Minor feedback was incorporated into the final version.

### 2.2.1 Introduction to the CS-C Cybersecurity Awareness Questionnaire

The 25-question, 5-subscale Cybersecurity Scale (CS-C) was developed by Arpaci et al. [9] in 2021. The CS-C questionnaire has good validity and reliability in measuring users' cybersecurity practices and perceptions. The overall scale has a Cronbach's alpha of .887, and the six subscales have good internal consistency ($.735 < \alpha < .810$). The questionnaire is based on the NIST Cybersecurity Framework [14] and the Parkerian Hexad model [15]. NIST focuses on cybersecurity practices and risks, while the Parkerian Hexad model identifies critical security features that influence users' perceptions and practices. The questionnaire follows the principles of the basic security framework, the CIA (Confidentiality, Integrity, Availability) triad [14], and examines users' cybersecurity practices, knowledge, and awareness across six dimensions. The dimensions are as follows: dimension 1 - confidentiality or secrecy which relates to privacy and information security, dimension 2 - integrity or inviolability which relates to unauthorized modification of data, dimension 3 - availability or accessibility which relates to access to information, dimension 4 - authenticity or authenticity which relates to the authenticity of the source of information, dimension 5 - possession or control which relates to the state of controllability or quality of information, dimension 6 - utility or usability which relates to the usefulness of the information and Internet services. Beyond these aspects, there can be of course other key cybersecurity attributes such as anonymity, privacy and resilience that can affect users' perceptions and practices of cybersecurity. Questions were answered on a five-point Likert scale from 1-5, where 1 is 'strongly disagree' and 5 is 'strongly agree', indicating how each statement describes the individual's experience, attitude and practice. Higher scores indicate higher levels of cyberawareness [9]. A translated, adapted version of this term will be referred to as CS-C-H.

# 3 Analysis of the Survey Data

SPSS 24.0 software was used to code, categorize, and analyze the data collected. For the socio-demographic data, descriptive statistics were used to check the mean and standard deviation. When the dependent variable was ordinal or continuous, the Mann-Whitney U test was used to compare differences between two independent groups. The Kruskal-Wallis H test (one-way ANOVA) was used to analyze comparisons between more than two groups for continuous variables. A P value <.05 was statistically significant [16].

Internal consistency and reliability are estimated and measured using Cronbach's alpha [17, 18, 19]. The recommended threshold for Cronbach's alpha is 0.7 [20], but a threshold between 0.6 and 0.8 is acceptable [21]. Pearson's correlation coefficient is used to check the reliability of the retest [19]. The internal consistency of the items is then established based on the correlation between each item and the other scale totals [19]. There are different types of validity, such as construct validity, which is assessed along the relationship between the test form, purpose, and target population [19]. Construct validity refers to the extent to which a particular measurement tool or test measures what they are intended to measure, in other words, if it is consistent with the theoretical construct they are using [22]. To examine questionnaire construct validity, we use principal component analysis (PCA) with varimax rotation. The KMO and Bartlett tests are used as a preliminary check of the appropriateness of the variables. The recommended criterion/value for the KMO is > 0.60, the Bartlett chi-square must be significant at < 0.05, and the correlation matrix must contain elements with a value > 0.30 [23,24]. These results are described in the following sections.

## 3.1 Sociodemographic Characteristics

Sociodemographic variables included age, gender, generation, current school type, education type, specialization, place of residence, parents' highest education level, and average daily time spent online. Data were coded and recorded as categorical or continuous variables. Of the N=398 respondents, 79.1% are male and 20.9% female. Gen Z comprised most of the sample at N=325, Gen Y at N=69, and Gen X at only N=4. The results for non-Generation Z (i.e. Y and X) were not examined separately due to the small size of the sub-sample. Generation Z currently dominates BSc programs, while Generation X and Y dominate engineering distance learning. Students from two higher education institutions in Székesfehérvár participated in the survey according to the inclusion criteria. The campus of Corvinus University in Székesfehérvár, mainly for the range of economic education, with N=58 students, 14% of the total sample, and the Alba Regia Technical Faculty of Óbuda University, for the range of engineering education, with N=340 students, 86% of the sample. Three types of education are represented in the sample: 94% of the students have a BSc, 2-2-2% have an MSc, a higher education vocational training and a further education. This result is also in line with the proportion of participants of

Székesfehérvár training types [25]. In terms of training orientation, real training was represented in 81% of the cases, while humanities-related training in 19%. Within this, when looking at the specializations, three major groups were formed with the following distribution: engineering n=173, IT n=149, and economics n=76.

The personal details of the participants were also examined. Concerning the place of residence, the majority of the students came from the surrounding villages and small towns, with a total of n = 253. The proximity of the capital and the characteristics of the county capital allow the two faculties to include students from the capital, n = 32, in addition to the local students, n = 113. Part of the research was an analysis of the family background data of the students in the study, with a particular focus on the highest level of parental education. The results show that 88% of the students have at least one parent with a school-leaving qualification (n=165) or a university degree (n=185). n=44 have a vocational qualification and n=4 have a primary school qualification.

The average time spent online is defined by the category and shows the average amount of active time spent online per day. The categories were stored and processed according to their average value, with 0-1 hours being stored and processed with a value of 0.5, 2-3 hours with an average value of 2.5, 4-5 hours with an average value of 4.5, 6-7 hours with an average value of 6.5 and more than 7 hours with an average value of 8.5. 40% of respondents reported 4-5 hours of active Internet time, and 1.5% reported 0-1 hours. Based on the coded mean, the average daily time spent on the internet is 5.11 hours (mean=5.11 ± 2.09, N=398). The average daily time spent on the internet varies between students.

# 4 Results

## 4.1 Results of the Adaptation and Validation

### 4.1.1 Pilot Measuring and Re-Testing Results - Pre-Validation

Before surveying the larger population, we conducted a pre-test in two rounds. In the first round, followed by the second round three weeks later, a total of N=35 university students participated. There were 87% males and 13% females in the N=35 sample. More than half of the respondents, 54%, reside in the city, while 20% each live in county seats or villages, and 6% in the capital city, indicating that only one-fifth of the sample is residents. Participants had the opportunity to evaluate and suggest the content, clarity, and administration of the test after completing the survey. Based on their feedback, minor changes have been made to the introductory text and the list of studied specialisations has been extended and made school type specific to facilitate future comprehensive assessments aimed at the secondary and primary school levels.

As shown in Table 1, the reliability test of the pilot and retest measurements of the CS-C-H questionnaire indicates a high degree of internal consistency in both cases. The Cronbach's alpha values obtained are 0.772 and 0.836, which are slightly different from the value of 0.887 for the original questionnaire.

Table 1
Assessment of internal consistency of the CS-C-H pilot and retest questionnaire (N=35)

| | Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|---|
| Pilot | .772 | .788 | 25 |
| Re-test | .836 | .828 | 25 |

The alpha value remained high in both the pilot survey (0.74-0.79) and the re-test (0.81-0.84) when some items were deleted. A Pearson correlation was applied to the cyberawareness scores of the pilot and re-test participants, with a positive statistically significant correlation ($r = .512$, $n = 35$, $p = .002$). The Cronbach's alpha of +0.072 for the pilot survey and +0.136 for the re-test exceeds the recommended threshold of 0.7 [20], indicating high internal consistency. The reliability of the retest was confirmed by the statistically significant correlation, allowing the adapted questionnaire to be tested on a large sample.

### 4.1.2 Internal Validity - Qualitative Assessment of Responses

The reliability test of the CS-C-H questionnaire (N=398) measures indicates a high level of internal consistency, with Cronbach's alpha values of .858, close to the value of the original questionnaire ($\alpha = .887$). The alpha value would remain high ($.848 < \alpha < .863$), also with the deletion of each item, but would not increase too much so that no item is deleted. The analysis also included an examination of the internal validity of each dimension. The subscales and dimensions showed good internal consistency ($.621 < \alpha < .795$).

The confidentiality subscale has a Cronbach's alpha of .790, indicating a reasonable level of internal consistency, close to the original questionnaire ($\alpha = .784$). The items of the subscale (CSC01, CSC02, CSC03, CSC04) have adequate internal item convergence ($r > 0.3$), with varying degrees of inter-item correlations. The results of the internal item convergence for dimension 1 are shown in Table 2.

Table 2
Reliability assessment of the Confidentiality dimension 1 - Inter-Item correlation matrix (N=398)

| | CSC01 | CSC02 | CSC03 | CSC04 | Mean | Std. Deviation |
|---|---|---|---|---|---|---|
| CSC01 | | .589 | .544 | .368 | 4.28 | .972 |
| CSC02 | | | .611 | .442 | 4.51 | .863 |
| CSC03 | | | | .461 | 4.37 | .884 |
| CSC04 | | | | | 3.81 | 1.131 |

There are strong correlations between CSC02 and CSC03 (r = .611) and weaker correlations between CSC01 and CSC04 (r = .368). The mean value of CSC04 is lower and more variable than the other three questions (mean = 3.81 ± 1.13, N = 398), so the distribution of personal information is more variable among students.

The control/possession dimension has a Cronbach's alpha of .621, which indicates a lower, but acceptable level of internal consistency [21], well below the original questionnaire value ($\alpha$ = .810). The internal item convergence of the subscale items (CSC05-CSC09) is not good for all items (r > 0.3), the correlations between items vary, and the results of the internal item convergence are shown in Table 3.

Table 3
Assessment of the reliability of the Control dimension - Inter-Item correlation matrix (N=398)

| | CSC05 | CSC06 | CSC07 | CSC08 | CSC09 | Mean | Std. Deviation |
|---|---|---|---|---|---|---|---|
| CSC05 | | .425 | .237 | .164 | .269 | 4.55 | .898 |
| CSC06 | | | .330 | .268 | .222 | 4.08 | 1.121 |
| CSC07 | | | | .354 | .089 | 4.04 | 1.307 |
| CSC08 | | | | | .202 | 3.85 | 1.314 |
| CSC09 | | | | | | 4.00 | 1.234 |

The mean value of the CSC05 item is outstanding (mean=4.55 ± .898, N=398), so the students are homogeneous in their opinion about sharing passwords with other people and, therefore, do not share their passwords with anyone.

The integrity dimension has a Cronbach's alpha value of .718, which indicates a sufficient level of internal consistency, slightly lower than the original questionnaire ($\alpha$ = .795). Internal item convergence of the subscale items (CSC10-CSC13) is adequate (r > 0.3), with varying degrees of inter-item correlations. The results for the internal item convergence of dimension 3 are shown in Table 4.

Table 4
Assessing the reliability of the Integrity dimension - Inter-Item correlation matrix (N=398)

| | CSC10 | CSC11 | CSC12 | CSC13 | Mean | Std. Deviation |
|---|---|---|---|---|---|---|
| CSC10 | | .369 | .477 | .471 | 2.94 | 1.216 |
| CSC11 | | | .227 | .231 | 3.68 | 1.148 |
| CSC12 | | | | .564 | 2.04 | 1.229 |
| CSC13 | | | | | 2.70 | 1.416 |

There is a moderately strong correlation between items CSC12 and CSC13 (r = .564), while some items are slightly below the expected threshold (CS11 to CS12 r = .227; CSC11 to CSC13 r = .231). The mean value of items in this group is much lower and more variable than the results for items in the previous dimensions. Thus, there is greater variation among survey respondents in the extent to which they share data in cyberspace and have third-party access to information stored there.

The Cronbach's alpha value of the authenticity dimension is .795, which indicates a proper level of internal consistency, close to the original questionnaire value ($\alpha$ = .784). Internal item convergence of the subscale items (CSC14-CSC18) is adequate (r > 0.3), with varying degrees of inter-item correlations. The results for the internal item convergence of dimension 4 are shown in Table 5.

Table 5
Reliability assessment of the authenticity dimension - Inter-Item correlation matrix (N=398)

| | CSC14 | CSC15 | CSC16 | CSC17 | CSC18 | Mean | Std. Deviation |
|---|---|---|---|---|---|---|---|
| CSC14 | | .446 | .508 | .457 | .478 | 4.37 | 1.037 |
| CSC15 | | | .374 | .270 | .321 | 3.83 | 1.103 |
| CSC16 | | | | .508 | .437 | 4.12 | 1.139 |
| CSC17 | | | | | .629 | 4.55 | .932 |
| CSC18 | | | | | | 4.31 | 1.032 |

There are moderately strong correlations between some items (r = .629 between CSC17 and CSC18), and only one case is slightly below the expected threshold (r = .270 between CSC15 and CSC17). The mean value of item CSC17 is outstanding (mean = 4.55 ± .93, N = 398), so most participants tend to ignore emails sent to them that indicate social engineering attacks. This may indicate that participants are confident and aware of recognizing and avoiding these types of threats.

The availability dimension has a Cronbach's alpha value of .779, indicating a reasonable level of internal consistency, close to the original questionnaire value ($\alpha$ = .795). Internal item convergence of the subscale items (CSC19-CSC22) is adequate (r > 0.3), with varying degrees of correlation between items, and the results of internal item convergence are shown in Table 6.

Table 6
Reliability assessment of the availability dimension - Inter-Item correlation matrix (N=398)

| | CSC19 | CSC20 | CSC21 | CSC22 | Mean | Std. Deviation |
|---|---|---|---|---|---|---|
| CSC19 | | .667 | .384 | .473 | 3.56 | 1.396 |
| CSC20 | | | .363 | .532 | 3.20 | 1.394 |
| CSC21 | | | | .360 | 4.12 | 1.175 |
| CSC22 | | | | | 3.15 | 1.371 |

Some items are moderately correlated (r = .667 between CSC19 and CSC20). The mean for item CSC21 is slightly higher than the values within the scale and less variable (mean = 4.12 ± 1.17, N=398), indicating that most respondents use firewalls on their devices. However, this dimension can be characterised as an area of concern due to the low mean values for the group and the sample.

The Cronbach's alpha of the utility dimension is .653, which indicates a poor but still acceptable level of internal consistency [21], lower than the original

questionnaire ($\alpha$ = .735). The subscale items (CSC23-CSC25) have a good internal item convergence (r > 0.3), the correlations between the items vary, and the results of the internal item convergence are shown in Table 7.

Table 7
Utility dimension reliability assessment - Inter-Item correlation matrix (N=398)

| | CSC23 | CSC24 | CSC25 | Mean | Std. Deviation |
|---|---|---|---|---|---|
| CSC23 | | .335 | .302 | 3.60 | 1.219 |
| CSC24 | | | ,552 | 4.24 | 1.012 |
| CSC25 | | | | 3.72 | 1.106 |

Some items have a stronger correlation (r = .552 between CSC24 and CSC25). The mean score for item CSC24 is higher and less varied across the group (mean = 4.24 ± 1.01, N = 398), indicating that most participants actively use online services in problem-solving.

### 4.1.3 Construct Validity and Factor Analysis

Before analysis, the data were checked for eligibility for principal component analysis, and the results are shown in Table 8.

Table 8
Provisional diagnoses before principal components

| **KMO and Bartlett's Test** | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy | | .850 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 3340.778 |
| | df | 300 |
| | Sig. | .000 |

These results provide evidence that the data are adequate for principal component analysis. The Kaiser-Meyer-Olkin (KMO) value, which measures the sampling adequacy of the data, reaches a value of 0.850, which is highly satisfying and indicates the dataset is suitable for factor analysis. The significantly high value of the Bartlett's test ($\chi^2$ = 3340.778, df = 300, p < 0.001) provides further confirmation of significant correlations between variables.

Six dimensions of cyberawareness are assessed in the CS-C-H questionnaire. To test the construct validity of the questionnaire, we used Principal Component Analysis (PCA) with varimax rotation. PCA aims to reduce the 25-item variable set into "principal components" that account for most of the variance in the original variables. The components of the rotated component matrix resulting from the factor analysis, the questions assigned to the components and the original dimensions of the questions are shown in Table 9. Based on this analysis, six main components were identified, each being related to different questions or sets of questions. The subscales of the six-factor structure obtained by exploratory analysis

fully reflected the content of the original theoretical constructs for five subscales (Confidentiality, Authenticity, Availability, Integrity, Utility) and partially for one subscale (Control) (except for the three questions CSC05, CSC06, CSC09).

Table 9

Results of principal component analysis (PCA) rotated component matrix

**Rotated Component Matrix**

| CS-C-H dimenzió | | Component 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| **confidentiality 1** | **CSC02** | **.777** | | | | | |
| | **CSC03** | **.768** | | | | | |
| | **CSC01** | **.731** | | | | | |
| | **CSC04** | **.683** | | | | | |
| *control/possession* | CSC05 | *.566* | | | | | |
| *control/possession* | CSC09 | *.498* | | .330 | | | |
| *control/possession* | CSC06 | *.352* | | | | | |
| **authenticity 2** | **CSC16** | | **.787** | | | | |
| | **CSC17** | | **.722** | | | | |
| | **CSC14** | | **.689** | | | | |
| | **CSC18** | | **.667** | | | | |
| | **CSC15** | | **.561** | | | | |
| **availability 3** | **CSC20** | | | **.806** | | | |
| | **CSC22** | | | **.758** | | | |
| | **CSC19** | | | **.754** | | | |
| | **CSC21** | | .408 | **.458** | | | |
| **integrity 4** | **CSC12** | | | | **.815** | | |
| | **CSC13** | | | | **.779** | | |
| | **CSC10** | | | | **.772** | | |
| | **CSC11** | | | | **.498** | | .476 |
| **utility 5** | **CSC24** | | | | | **.715** | |
| | **CSC25** | | | | | **.710** | |
| | **CSC23** | | | | | **.702** | |
| ***control/possession 6*** | **CSC08** | | | .313 | | | **.557** |
| | **CSC07** | | | .317 | | | **.534** |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 9 iterations.

Most of the items assigned to each component are highly correlated with the factor, with a few items having lower values, but these are also at a reasonable level ($.458 < r < .815$). These subscales represent the factors and their associated sets of questions, which reflect the dimensions of the original questionnaire.

## 4.2 Analysing CS-C-H Results for the Sampled Population

Based on the mean score of the respondents, the CS-C-H has a mean score of 95.61 (mean=95.61 ± 13.76, N=398), weighted mean ($mean_w$=3.82 ± 1.14, N=398), so the sample generally scored high in completing the questionnaire, but the standard deviation value shows that the results are variable, not all participants have a high level of cybersecurity awareness (maximum score available 125). Detailed results for each dimension are shown in Table 2-7. The Integrity factor is at the lowest level (mean=2.84 ± 1.25, N=398). The lower mean and higher variance together may indicate that the assessment of integrity, i.e. data security and integrity, is heterogeneous and that there are different opinions and experiences among the participants in this area. The Confidentiality factor was found to have the highest level and lowest standard deviation (mean=4.24 ± 0.96, N=398), suggesting that participants may be more confident in managing and preserving confidential information in general. When analysing each item, we examined which questions had below-average and above-average standard deviation values as critical points of cybersecurity for individuals (Table 10).

Table 10
Table of questions with below average performance (N=398)

| Dimension | Question num. | Question | Mean | Std. Deviation |
|---|---|---|---|---|
| Confidentiality | CSC04 | I do not share my contact information in cyberspace. | 3.81 | 1.31 |
| Integrity | CSC10 | It is safe to store data in cyberspace. | 2.94 | 1.21 |
| | CSC12 | Sharing data in cyberspace does not involve any risk. | 2.04 | 1.22 |
| | CSC13 | Information and documents stored in cyberspace cannot be accessed by third parties. | 2.70 | 1.41 |
| Availability | CSC19 | I use an up-to-date antivirus program on my devices. | 3.56 | 1.39 |
| | CSC20 | I regularly scan my devices with an antivirus program. | 3.20 | 1.39 |
| | CSC22 | I do not open the files I downloaded from the Internet without scanning with an anti-virus program. | 3.15 | 1.37 |
| Utility | CSC23 | I use social media applications to share information in cyberspace. | 3.60 | 1.21 |
| | CSC25 | I use the services provided in cyberspace for information management (information acquisition, storage, sharing and application). | 3.72 | 1.10 |

The results show that young people feel challenged in certain areas of cyberspace. Sharing and safely storing confidential information is an area of concern. Their perception of security in cyberspace is not satisfactory, and this may be due to a lack of information and knowledge to be able to defend themselves with confidence

against threats. Regular virus scanning and online protection measures are also lacking. This suggests that young people are not adequately protecting their computers and devices from cyberthreats online. Meanwhile, youth seem relatively confident in using social media and online services, suggesting that a sense of security on these platforms is either unrealistic or unaware of potential threats. Taken together, the results suggest that young people need to develop their cyberawareness, especially regarding online safety. The results suggest that a range of educational measures and awareness campaigns are necessary to support the development of safe and conscious online behavior among students in higher education.

## 4.3 Analysis of the Differences between the Groups

The Mann-Whitney U test was used to compare differences between gender groups. Examination of the gender differences and the questionnaire results suggests that there is a statistically significant difference ($U = 10388.5$, $p = 0.004$) in the total scores of the CS-C-H test Availability dimension for the male (mean rank 190.98) and female (mean rank 231.84) groups based on gender identity. Within the deeper analysis of the dimension, two questions (CSC20 and CSC22) show statistically significant differences. The results show that there is a significant difference in the ranking of the overall score for the CSC20 item between the male and female groups. The average rank for men (189.67) is lower than that for women (236.80) and this difference is statistically significant ($U = 9976.5$, $p = 0.001$). Thus, women take more care to secure their devices (e.g., perform regular virus checks) than men. For CSC22, the average rank for men (191.29) is lower than for women (230.67) and this difference is statistically significant ($U = 10485.5$, $p = 0.005$), indicating that women are more aware than men of security measures when it comes to checking files downloaded from the internet.

Examining further dimensions, the following results can be highlighted in terms of gender differences. The items of the control/possession dimension CSC05 and CSC09 also show gender differences. For CSC05, the average rank of females (178.11) is lower than that of males (205.14) and this difference is statistically significant ($U = 11297$, $p = 0.015$), indicating that males share their passwords with other people less than females. For the CSC09, the average rank of males (193.00) is lower than females (224.16) and this difference is statistically significant ($U = 11025.5$, $p = 0.018$), indicating that females are more cautious than males and do not allow their credit card information to be saved when shopping online. For the Integrity dimension CSC11 item, the average rank of females (177.87) is lower than that of males (205.20) and this difference is statistically significant ($U = 11277.5$, $p = 0.045$), indicating that males are more confident about their stored information and documents not being lost or deleted in cyberspace compared to females. For the Utility dimension CSC23 item, the average rank for males (193.59) is lower than that of females (221.92) and this difference is statistically significant

(U = 11212, p = 0.039), indicating that females use social media applications more to share information in cyberspace compared to males.

Generation, place of residence, educational specializations and parents' highest educational qualifications are compared between groups using the Kruskal-Wallis H test. Statistically significant results are reported below.

The results of the Kruskal-Wallis H test indicate a statistically significant difference between the total scores of the Utility dimension of the CS-C-H questionnaire by generation, $\chi^2(2) = 19.905$, $p < 0.01$, with mean rank values of 211.34 for Generation Z (N=325), 149.74 for Generation Y (N=69) and 96.13 for Generation X (N=4). These results suggest that Generation Z members use cyberspace services for problem-solving and information management to a greater extent than Generation Y and Generation X members. There is no statistically significant difference in the overall score for the level of cyberawareness for the groups of residence, educational specialization, and highest educational level of parents.

A deep analysis of each item and group reveals the following relationships. The results of the Kruskal-Wallis H test indicate a statistically significant difference between the CSC01 item scores by place of residence, $\chi^2(2) = 9.307$, $p = 0.025$, with mean rank values of 220.05 for the capital city (N=32), 213.00 for villages (N=122), 204.38 for county seats (N=113) and 177.70 for cities (N=131). According to the results, the respondents' attention to sharing personal information in cyberspace varies according to their place of residence. Respondents living in the capital are more cautious in this area, while this attention is less prominent for those living in cities. There is also a significant difference between the scores of CSC05, CSC08, and CSC23 by specialization studied. For CSC05, $\chi^2(2) = 7.764$, $p = 0.021$, with mean rank scores of 211.25 for the IT specialization (N=149), 198.49 for Engineering (N=173), and 175.85 for the Economics specialization (N=75). There are significant differences in this pattern of behavior between the different specializations in terms of sharing passwords with others. Students in IT or engineering are more aware of sharing passwords than students in economic specialization. For CSC08, $\chi^2(2) = 5.993$, $p = 0.050$, with mean rank values of 225.05 for economics (N=75), 195.89 for IT (N=149), and 189.95 for engineering (N=173). The results show that students in economics are generally more confident in their ability to correctly answer security questions to recover their account passwords compared to students in IT or engineering. $\chi^2(2) = 6.959$, $p = 0.031$ for CSC23, with mean rank values of 226.05 for the economic specialization (N=75), 200.80 for the IT specialization (N=149), and 185.72 for the engineering specialization (N=173). The results show that students specializing in the economic field have a higher tendency to use social media applications to share information. Significant differences can be further identified between the scores of the items CSC02, CSC03 and CSC08, in addition to the items CSC23, CSC24 and CSC25, which are already mentioned in the Utility dimension. For CSC02, $\chi^2(2) = 6.319$, $p = 0.042$, with mean rank scores of 204.24 for Generation Z (N=325), 181.99 for Generation Y (N=69), and 116.25 for Generation X (N=4). The results suggest that

members of Generation Z may be sharing less information in cyberspace compared to members of Generation Y and X which they would not want to share in real life. For CSC03, $\chi^2(2) = 10.717$, $p = 0.005$, where the average rank values are 207.13 for Generation Z (N=325), 168.24 for Generation Y (N=69), and 119.13 for Generation X (N=4). The results show that Generation Z is more concerned about digital privacy and controlled data sharing in cyberspace than Generation Y and Generation X. For CSC08, $\chi^2(2) = 10.799$, $p = 0.005$, where the average rank values are 224.00 for Generation X (N=4), 207.46 for Generation Z (N=325), and 160.57 for Generation Y (N=69). Generation Z participants are consequently more aware of and able to correctly apply measures related to the security of their accounts than Generation Y participants.

**Discussion**

The results of the 2020 research [26] emphasize the necessity of cybersecurity training programs, especially for cybersecurity awareness. Most participants demonstrate acceptable cybersecurity behaviors, but there are challenges with the use of passwords. Although users have a basic understanding of cyberawareness terms and are familiar with how to create secure passwords when choosing a password, their use of these terms varies. Concerning password management, Gyaraki [8] found that less than 20% of respondents adhere to the basic principles of using a combination of upper- and lower-case letters when choosing a password, using a different password for each user account, and not reporting any misuse of their passwords. In a recent survey, a higher number, 48% of respondents, reported using strong, secure passwords. The results reveal, no significant differences between gender, generation, place of residence, studied specialization, and responses on the use of strong passwords.

Furthermore, 68.2% of the respondents indicated that they pay attention to website security and feel safe online [8]. Based on the results of the current survey, only 34% of the respondents pay special attention to website security, for these participants the presence of a security certificate is a decisive factor in assessing the authenticity and security of websites. 49% of the respondents consider that data protection and restrictions on third party access are not implemented in cyberspace, so their personal information and data are not secure. Thus, sharing and storing confidential information securely is seen as a problem area, and their perception of security in cyberspace is not satisfactory.

Palicz and colleagues [11] in 2020 found that males, members of the older generation (X and BB), with a university degree, living in large cities and using multiple devices read IT news more regularly, use different passwords more often and were more aware of the concept of ransomware. In our research, Generation Z members are more aware of cybersecurity issues than the older generation.

In the light of the cybersecurity challenges caused by human error, the gap between knowledge and awareness, and the gaps in their implementation, are closely linked to the digital security problems of users. The noticeable lack of knowledge and good

cybersecurity practices further highlights the need for cybersecurity education programs for users. Based on these conclusions, cybersecurity education has a critical role to play in developing awareness levels and secure behavioral practices.

The sample size of the survey is considered optimal to achieve statistically significant results and to achieve higher factor loadings and more stable scaling. Although a minimum sample size of 300 is generally recommended in the literature, there is no consensus among researchers on the optimal sample size. [27, 28]

**Summary**

The research focuses on the cybersecurity challenges of the 21st Century and aims to develop a Hungarian-language cybersecurity attitude questionnaire (CS-C-H) and to test its psychometric properties. The 25-item questionnaire measures cyber awareness on a Likert scale along six dimensions (confidentiality, control/possession, integrity, authenticity, availability, and utility). The results of pilot studies and extended analyses confirm the reliability and validity of the questionnaire. Reliability test scores for the CS-C-H questionnaire N=398 measurements indicate a high-level of internal consistency [29], with Cronbach's alpha values of .858, close to the original questionnaire ( $\alpha = .887$). The study also included an examination of the internal validity of each dimension. The subscales and dimensions also showed adequate internal consistency ($.621 < \alpha < .795$). Principal component analysis (PCA) with varimax rotation was used to examine construct validity. As a result of the factor analysis, it was found that the subscales are representative of the factors and their associated sets of questions that reflect the dimensions of the original questionnaire.

Based on the results, the level of cybersecurity awareness among participants varies. Participants have different perceptions and attitudes towards cybersecurity issues [30]. They reflect different opinions and experiences with data security. Participants are generally confident in handling confidential information, but perceptions of security and the sharing and storage of confidential information emerged as an area of concern [31]. Gender differences are also evident in several areas, for example, women are more concerned about the security of their devices and more aware of security measures in the online space. There are also interesting differences by generation, with Generation Z members, compared to Generation X and Y members, being more concerned about digital privacy. Differences in password management and information sharing between business and engineering/IT students can also be observed. The results suggest that further research is needed to gain a deeper understanding of cybersecurity attitudes and behaviors.

The validated CS-C-H questionnaire is a reliable and meaningful measure of students' cybersecurity attitudes in educational institutions. The results show that the questionnaire is a useful diagnostic tool among Hungarian students.

## References

[1] Varonis: "*Cybersecurity Statistics and Trends*", 2023 [Online] https://www.varonis.com/blog/cybersecurity-statistics/ (last reviewed 2023.11.20.)

[2] ISC: "*Cybersecurity Workforce Study: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.*", 2022 [online] https://www.isc2.org/Research/Workforce-Study# (last reviewed: 2023.02.10)

[3] Maennel K., Mäses S., Maennel O.: "*Cyber Hygiene: The Big Picture*", In: Gruschka N. (eds) Secure IT Systems. NordSec. Lecture Notes in Computer Science, Vol. 11252, 2018, https://doi.org/10.1007/978-3-030-03638-6_18

[4] So W.-H., Kim H.: "*A Study on the Online School Violence of Teenagers in Cyberspace*", Asia-Pacific Journal of Convergent Research Interchange, Vol. 7, No. 1, pp. 105-114, 2021

[5] Baraković S., Husic J. B.: "*Cyber hygiene knowledge, awareness, and behavioral practices of university students*", Information Security Journal: A Global Perspective, pp. 1-24, 2022, doi: 10.1080/19393555.2022.2088428

[6] Thiyagu K., & Santhosh T.: "*Cyber safety and security education*", Lulu Publication, 2019

[7] Butler-Bowdown T.: *"Psychology in a nutshell 50 basic psychological works (Pszichológia dióhéjban 50 pszichológiai alapmű)"*, HVG Könyvek, 2007

[8] Gyaraki R.: *"The role of security awareness, or questions about cybersecurity (A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról)*", Magyar Rendészet, Vol. 22, No. 2, pp. 245-261, 2022, doi: 10.32577/mr.2022.2.16

[9] Arpaci I., Sevinc K.: *"Development of the cybersecurity scale (CS-S): Evidence of validity and reliability"*, Information Development, 38(2), pp 218-226, 2022, https://doi.org/10.1177/0266666921997512

[10] Nyikes Z.: *"The results of the examination of the digital competence and security awareness of the Central and Eastern European generations (A Közép-Kelet európai generációk digitális kompetencia és biztonságtudatosság vizsgálatának eredményei)"*, Hadmérnök, XII. Évfolyam 4. szám, 2017, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar. ISSN, 1919, 159-173, 2017

[11] Palicz T. G. et al.: *"Security awareness within the cyberspace–results of the 2020 national survey among the population. (Biztonságtudatosság a kibertérben–a 2020-as országos lakossági felmérés eredményei)"*, Belügyi Szemle: A Belügyminisztérium szakmai tudományos folyóirata (2010-), 70(2), 395-418, 2022

[12] Hall D. A. et al.: *"A good practice guide for translating and adapting hearing-related questionnaires for different languages and cultures"*, International Journal of Audiology 57:3, pp. 161-175, 2018, doi: 10.1080/14992027.2017.1393565

[13] Ohrbach R. et al.: *"Guidelines for establishing cultural equivalency of instruments"*, University at Buffalo, 2013

[14] National Institute of Standards and Technology: *"Framework for Improving Critical Infrastructure Cybersecurity"*, National Institute of Standards and Technology, 2018, https://doi.org/10.6028/NIST.CSWP. 04162018

[15] Parker DB: *"Fighting Computer Crime: A New Framework for Protecting Information"*, New Jersey, ABD: John Wiley and Sons, 1992

[16] Laerd Statistics 2023 [online] https://statistics.laerd.com (last reviewed: 2023.12.20)

[17] Orehek Š. and Petrič G.: *"A systematic review of scales for measuring information security culture"*, Information and Computer Security, Vol. 29, No. 1, pp. 133-158, 2021, https://doi.org/10.1108/ICS-12-2019-0140

[18] Cronbach LJ.: *"Coefficient alpha and the internal structure of tests"*, Psychometrika, 16: 297-334, 1951

[19] Hajjar S. T.: *"Statistical analysis: Internal-consistency reliability and construct validity"*, International Journal of Quantitative and Qualitative Research Methods 6.1, pp. 27-38, 2018

[20] Rohan R. et al: *"How gamification leads to continued usage of MOOCs? A theoretical perspective"*, IEEE Access. 9: 108144-108161, 2021, https://doi.org/10.1109/ACCESS.2021.3102293

[21] Wim J. et al.: *"Marketing Research with SPSS. Prentice Hall"*, Pearson Education, ISBN: 978-0-273-70383-9, 274-275, 2008

[22] William M. K. T.: *"Convergent & Discriminant Validity"*, Research Methods Knowledge Base 2023 [online] URL: http://www.socialresearchmethods.net/kb/convdisc.php (last reviewed: 2023.10.16.)

[23] Carpenter S.: *"Ten steps in scale development and reporting: a guide for researchers"*, Commun. Methods Meas. 12: 25-44, 2018, https://doi.org/10.1080/19312458.2017.1396583

[24] Henson R. K., Roberts J. K.: *"Use of exploratory factor analysis in published research: common errors and some comment on improved practice"*, Educ. Psychol. Meas. 66: 393-416, 2006, https://doi.org/10.1177/0013164405282485

[25] Oktatási Hivatal: *"Higher education statistics: 2.2 Statistics on the number of students by type of maintenance, institution, faculty, place of training,*

*work organisation and level of training (Felsőoktatási statisztikák: 2.2. A hallgatók statisztikai száma fenntartó típusonként, intézményenként, karonként, képzési helyenként, munkarendek és képzési szintek szerint)"* 2020 [online] URL: https://dari.oktatas.hu/firstat.index (last reviewed: 2023. 12.20.)

[26] Legárd I.: *"Building An Effective Information Security Awareness Program"*, Central and Eastern European e|Dem and e|Gov Days 2020, Wien, Ausztria: Österreichische Computer Gesellschaft (ÖCG) pp. 189-200, 12 p., 2020

[27] Morgado F. F. R. et al.: *"Scale development: ten main limitations and recommendations to improve future research practices"*, Psicol. Reflexão Crítica. 30: 1-20, 2017, https://doi.org/10.1186/s41155-016-0057-1

[28] Boateng G. O. et al.: *"Best practices for developing and validating scales for health, social, and behavioral research: a primer"*, Front. Public Health. 6: 1-18, 2018, https://doi.org/10.3389/fpubh.2018.00149

[29] Tavakol M. and Dennick R.: "*Making sense of Cronbach's alpha*" International Journal of Medical Education, Vol. 2, pp. 53-55, 2011, doi: 10.5116/ijme.4dfb.8dfd

[30] Arató B.: *"Norm clarity in the light of Hungarian case law"*, Magyar Nyelvőr 46 : pp. 81-90, 10 p., 2022

[31] Kresimir S. et al.: *"Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire,"* Acta Polytechnica Hungarica, Vol. 21, No. 4, pp. 49-68, 2024