# Measuring cyber secure behavior of elementary and high school students in the Netherlands

Witsenboer, Jacob Willem Abraham; Sijtsma, Klaas; Scheele, Fedde

*Published in:*
Computers & Education

*DOI:*
10.1016/j.compedu.2022.104536

*Publication date:*
2022

*Document Version*
Publisher's PDF, also known as Version of record

*Citation for published version (APA):*
Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, [104536]. https://doi.org/10.1016/j.compedu.2022.104536

Computers & Education 186 (2022) 104536

Contents lists available at ScienceDirect

Computers & Education

journal homepage: www.elsevier.com/locate/compedu

# Measuring cyber secure behavior of elementary and high school students in the Netherlands

Jacob Willem Abraham Witsenboer, MSc [a,*], Klaas Sijtsma, MSc PhD [b], Fedde Scheele, MD PhD [c]

[a] *University of Amsterdam, Spui 2, 11012, WX, Amsterdam, the Netherlands*
[b] *Tilburg University, School of Social and Behavioral Sciences, Warandelaan 2, 5037, AB, Tilburg, the Netherlands*
[c] *VU University Amsterdam, Athena Institute of the Faculty of Science, De Boelelaan 1085, 1081, HV, Amsterdam, the Netherlands*

ARTICLE INFO

*Keywords:*
Cyber secure behavior
Information security behavior
Cyber security education

ABSTRACT

School systems may pay attention to the fact that individuals and companies using smart devices are increasingly at risk of becoming victims of cybercrime. The literature on how effective students in developed countries such as the Netherlands are taught about cyber security skills during their school career is scarce. Although curriculum materials are available, scaling up computer science education is behind. Therefore, this study explores to what extent Dutch students develop cyber secure behavior at elementary and high school. A questionnaire was used for self-assessment of cyber security behavior. After the questionnaire was completed, two group interviews were conducted to improve the interpretation of the questionnaire results. The study findings revealed that the Dutch school curriculum hardly pays attention to this topic and that students acquire their online behavior mainly through experience, instructions on the internet, through parents, and through siblings. In addition, many students developed more reckless behavior over time. We recommend that cyber security education should start at elementary school as soon as children begin to use online equipment. A subject that deserves special attention is recognizing phishing emails and phishing websites. The learners should be convinced that risky behavior on the internet may turn against them and against the organization to which they belong.

## CRediT author statement

**Jim Witsenboer**: Conceptualization, Methdology, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization, Project administration; **Fedde Scheele**: Conceptualization, Methdology, Formal analysis, Writing - Original Draft, Writing - Review & Editing, Visualization, Supervision; **Klaas Sijtsma**: Methdology, Formal analysis, Writing - Original Draft, Writing - Review & Editing.

* Corresponding author.
*E-mail addresses:* jimwitsenboer@protonmail.com (J.W.A. Witsenboer), K.Sijtsma@tilburguniversity.edu (K. Sijtsma), f.scheele@olvg.nl (F. Scheele).

https://doi.org/10.1016/j.compedu.2022.104536
Received 19 October 2021; Received in revised form 27 April 2022; Accepted 4 May 2022
Available online 7 May 2022

## 1. Introduction

Cyber security has become increasingly important. A company can spend hundreds of thousands of dollars on cyber security systems, but one employee's risky behavior may open the door for an attacker (Hart et al., 2020; Öğütçü et al., 2016a). The cyber security threats affect not only companies but also individuals that use smart devices (Arachchilage & Love, 2014).

Cyber secure behavior, also called cyber hygiene, is often mentioned in the scientific literature and by policy makers. However, there is no clear definition of this term in academic research (Vishwanath et al., 2020). The present research is based on an adapted version of the definition of Vishwanath et al. (2020, ): Cyber secure behavior concerns "the cyber security practices that online consumers should adopt to protect the safety and integrity of their personal information and their employer's information on their internet-enabled devices from being compromised in a cyber-attack".

Cyber security is a broad concept. In addition to a technical perspective, there are ethical, cultural, and political perspectives to cyber security. In this research, the focus is on human actions with respect to cyber security, because cyber criminals nowadays mainly target the users of systems. Previously, cyber criminals focused on the systems that users use. However, the greatest problem is not the security of the technology but the risky behavior of information systems users (Öğütçü et al., 2016b). Research showed that human errors played a role in 95% of security incidents (Parsons et al., 2017). This is because employees are encouraged to use technology both at home and at work but are not adequately trained to understand what the potential risks are and how to reduce or avoid those risks.

Users rarely pay attention to security notifications of their browser, but look for characteristics that the website could be safe (Kirlappos & Sasse, 2012). An example is that users judge websites on their appearance, but do not realize that they can be counterfeited (Sheng et al., 2010). Research shows that users do not understand the security notifications of browsers, which may be the reason that users do not pay attention to them. When a cyber-attack is aimed at users in organizations, cyber security systems are often in place to protect employees. These systems are managed by cyber security experts, but at home users are responsible for managing their own cyber security (Mashiane & Kritzinger, 2019). In addition, home users usually do not have the IT infrastructure or the policies to protect themselves against cyber-attacks (Arachchilage & Love, 2014). It is therefore important that employees adopt cyber secure behavior, so that they can better protect themselves against attacks.

In a letter, Krutz and Richards (2017) asked the editor of the *Journal of the Association of Computer Machinery*: "Cyber Security Education: Why Don't We Do Anything About It?" In this letter, the authors referred to the lack of proper education. Despite the availability of measurement techniques, there is a lack of published measurements of cyber security behavior. Therefore, the current magnitude of the problem has not been sufficiently assessed. Most literature is about opinions; for example, 96% of a student sample claimed that cyber security in companies is "very important", while 60% said that their own risk behavior is substandard (Teer et al., 2016). Even though the magnitude of the problem has not been extensively substantiated, literature often presents solutions to the supposed problem. Some authors advocated 'just in time' learning in companies, while others made a plea for a culture of cyber security behavior starting at a young age (Kortjan & Solms, 2014; Venter et al., 2019). Another dispute in the literature is the approach to solving the alleged cyber security problem. For example, Venter et al. (2019) claimed that the fundamental problem is knowledge and argued that cyber security skills can be trained (Arachchilage & Love, 2014; Hart et al., 2020; Teer et al., 2016; Venter et al., 2019). Other authors focused on addressing general risk behavior (Öğütçü et al., 2016a).

A literature appraisal showed the need for proper measurement of the present cyber security behavior in Western countries. In the scientific field of evidence-informed education in information technology, it is important to study the current state of learning cyber security behavior at school and to substantiate the design of new curricula for acquiring cyber secure behavior. We attempted to provide a first answer the following question: To what extent do Dutch students develop cyber secure behavior at elementary school and high school?

## 2. Literature review on cyber security curricula

Someone may mainly find literature about cyber security curricula for children in local and National search machines, like the digital library of the Association for Computing Machinery (ACM Digital Library, n. d.). For a school which is planning computer science education in a country like the Netherlands, this literature provides a rich source of information. For example, the CSTA K-12 CS Standards (Computer Science Teachers Association, 2017) lists the competencies primary and secondary students should have to claim computing proficiency. These standards have informed curricula in multiple countries (Duncan & Bell, 2015). For children above elementary school age, the freely available Code. org's CS Discoveries curriculum covers topics such as programming, physical computing, HTML/CSS, and data (Code.org CS Curricula, 2018). For children at a later stage of education, the AP CS Principles course expands the knowledge to basic computing concepts (Cuny, 2015). The K–12 Computer Science Framework emphasizes the need for young students to engage in varied types of computing (K–12 Computer Science Framework, n. d.). The K-12 CS framework offers a comprehensive source for curriculum development, for implementation at the various school levels, for continuous development of teaching staff and numerous resources to be used in the practice of CS education. Besides the availability of all these resources, there is a vivid exchange of innovations and experiments at the digital library of the Association for Computing Machinery (Bernd, Garcia, Holley, & Johnson, 2022; Fleenor et al., 2019; Riel & Romeike, 2020). Also experience with game-based educational tools for cyber security is available (Maqsood & Chiasson, 2021). Although cyber security education is only part of computer science education, it is evident that any school or organization looking for educational resources to teach computer science does not need to reinvent the wheel. The question remained how effective cyber security education was implemented in a western country like the Netherlands and how that reflected in cyber security behavior. As far as we know, quantitative knowledge of cyber security behavior of children and its development through time is absent.

## 3. Method

We performed a quantitative assessment based on a questionnaire measuring the behavior of elementary and high school students and studied the differences between the two groups. Subsequently, group interviews were conducted to improve the interpretation of the results.

### 3.1. Development questionnaire

The questionnaire was developed based on an evaluation of the questionnaires used in previous relevant studies. No studies targeting the cyber security behavior of children were found. Table 1 provides an overview of the examined security awareness (ISA) questionnaires. Six characteristics are highlighted. These characteristics are how many items the questionnaire contains, whether the questionnaire is based on a theoretical framework, whether the questionnaire has been made public for use, in which year the questionnaire was published, what the questionnaire measures, and what the target audience of the questionnaire is.

After careful consideration of the questionnaires, it was decided to mainly use the validated Human Aspects of Information Security Questionnaire (HAIS-Q) of Parsons et al. (2017) and to use the validated questionnaire of Arachchilage and Love (2014) for additional items. The HAIS-Q is the only questionnaire that clearly measures the behavior dimension of ISA and is publicly available. Since the scope of the present study only includes the behavior dimension of the HAIS-Q, we only used the behavior items.

Not all items in the behavior dimension of the HAIS-Q were relevant for our study. For example, “I leave print-outs that contain sensitive information on my desk when I’m not there” was categorized as ‘not relevant’, because it did not apply to the researched age group. As the items of the HAIS-Q are focused on office work, the wording of the relevant items was changed from “work” to “school”. For example, “I use a different password for my social media and work accounts” was changed to “I use a different password for my social media and school accounts”. Afterwards, the modified items were categorized into focus areas, using the defined focus areas of the HAIS-Q. After grouping, four focus areas of the HAIS-Q remained: password management, email use, internet use and social media use. The questionnaire of Arachchilage and Love (2014) was used to add additional items about phishing to the focus areas email use and internet use. After this addition, each focus area had four items, resulting in a total of 16 items. Next, all items were translated into correct Dutch. After all items were translated, minor adaptations were made to improve the items’ readability. Two demographic questions about gender and age were added to the questionnaire, increasing the total number of items to 18.

The reliability and validity of the new questionnaire were studied using the cognitive hybrid model. (Collins, 2003; Ryan et al., 2012). Using the hybrid model, we asked elementary school students whether the items were formulated clearly and unambiguously.

A description was added to the two items about phishing to make sure that the students understood the concept of phishing. Negative words such as “not” and “nothing” were written in bold and capitalized to make sure the negative form was noticed. In addition, two items were rephrased more clearly. The questionnaire can be found in Table 3.

### 3.2. Procedure questionnaire

The surveys were conducted in the final year groups of elementary schools (students aged 4 to 13) and high schools (students aged 12 to 19). Depending on the level of education, high school takes 4–6 years. Students are between 16 and 19 years old when they graduate from high school. Vocational education or higher education can take place after graduating from high school. Dutch law obliges children in the Netherlands to follow education up to the age of 18. For the surveys, the Google Forms application was used to avoid copying errors. The students received a link from their teacher to complete the survey in the classroom. This way, the researcher did not see the names of the students. The data were stored that could identify the students. To ensure that the data collection went well, the researcher (i.e., first author) was physically or virtually present during the survey. Upon arrival, the researcher gave a short

**Table 1**
Summary of the Information Security Awareness questionnaires.

| Characteristics | UISAQ | BCISQ | OSBBQ | Four scales | HAIS-Q |
|---|---|---|---|---|---|
| Measures | The level of security awareness | Information security and awareness | Cyber security awareness, attitudes, behaviors, and beliefs. | Personal information security behavior and awareness | Information security awareness |
| Theoretical framework | None | None | Health belief model and the protection motivation theory | None | KAB model |
| Target group | Students | Everyone | Employees | University staff and students | Employees and students |
| Availability | No | No | No | Yes | Yes |
| Items | 33 | 17 | 75 | 89 | 63 |
| Year published | 2014 | 2019 | 2019 | 2016 | 2017 |

UISAQ = Users’ Information Security Awareness Questionnaire; BCISQ = Behavioral- Cognitive Internet Security Questionnaire; OSBBQ = Online Security Behavior and Beliefs Questionnaire; HAIS-Q = Human Aspects of Information Security Questionnaire; KAB = Knowledge, Attitude and Behavior.

introduction outlining the subject of the survey and the focus areas. He informed the students that the survey was anonymous. While completing the survey, students were not allowed to interact. If they did not understand an item, they could ask the researcher for an explanation.

### 3.3. Questionnaire analysis method

The survey results from the different schools were combined in Microsoft Excel. Separate columns for school type and school name were added to the spreadsheet, so that it was easy to distinguish between elementary schools and high schools. Before the data were transferred to SPSS 27, the data quality was checked using the content non-responsivity method (Parsons et al., 2014). In SPSS, the variable view properties of the columns were defined, such as label, decimals, and data type. The six questionnaire items indicating negative behavior were converted to reverse scoring.

The Likert scale was used to determine the level of agreement between the items. To ensure that the analysis was as accurate, the Likert scale data were analyzed both with a parametric and a nonparametric test, consistent with de (de Winter & Dodou, 2010). These authors compared Type I and II error rates of the *t*-test versus the Mann-Whitney-Wilcoxon test for five-point Likert items and found that the power of the two tests was equal in most cases.

During the analysis, for each item the median and the mean were calculated for each school type. A mean of smaller than 3.5 was rather arbitrarily considered insufficient cyber security behavior. Next, the differences between the two school types were analyzed.

The questionnaire was analyzed per item. The null hypothesis was that there is no difference between the cyber security behavior of elementary school students and high school students. To calculate the significance level for each individual test in this multiple test situation, the initially chosen 5% level was divided by the number of items, known as Bonferroni correction, and resulting in $\alpha = 0.05/16 = 0.003125$. If the *p*-value of an item was smaller than $\alpha = 0.003125$, the difference was significant. The effect size was interpreted for the significant differences using Cohens' *d* (Norman & Streiner, 2003). Following Cohen, effect size *d* was interpreted as follows: *d* between 0.2 and 0.5 is small, between 0.5 and 0.8 medium and above 0.8 large.

The formulation of the interview questions was based on the results of the questionnaire analysis. During the interviews, the aim was to clarify certain findings. Interviews were only conducted with high school students because they can look back on their elementary school period and compare the two school types. The high schools who had invited their students to complete the questionnaire received an email about conducting interviews with the students. One of the three high schools responded. The interviews took place at that high school. The teacher randomly selected several students for the interviews and asked their consent for being interviewed. If consent was given, they were interviewed in a separate room to avoid distractions. The students were interviewed as a group to create the dynamic of a conversation and to make the student feel more at ease.

Before the interview, the students were asked for approval to record the conversation. They were informed that the interview was anonymous and that their teachers would not hear the recording. After approval, an introduction was given about the study goals and the structure of the interview. If students did not have any questions, the recording was started, and the interview could begin. The interview was conducted in such a way that a statement was read aloud and was then discussed with the students. After discussing the prepared statements, it was examined which emerging questions had to be discussed, and finally the interviewed students were asked if they wanted to add anything or had any comments. If this was not the case, the recording was stopped. The number of interviews was extended until saturation was achieved.

### 3.4. Content analysis of the interviews

The audio files of the interviews were uploaded in Amberscript, a web application that can convert audio files into a transcript. After uploading, the researcher indicated how many speakers participated in the interview and the language spoken. In this case, the language was Dutch. The transcript was exported and imported into Atlas TI, a program that can analyze qualitative interview data. Content analysis was performed to identify the themes that were important for the development of cyber behavior.

To create a theme, the content was coded in two ways. First, labels were assigned to content fragments to indicate the topics of these fragments (open coding). During coding, it was also checked whether existing labels could be assigned to overlapping content (axial coding). Second, it was examined which axial codes form building blocks for themes with attention for the level of consensus.

### 3.5. Ethical considerations

After introducing consent and strict privacy regulations in our research proposal, ethical approval and access to the participants was granted by the schools, which is the common procedure in Dutch school research. There is discussion about the site and rigor of ethical approval in different kinds of research, in which the authors took the stance of local approval for protection of the participants (Schutte et al., 2021). This choice was made since the questionnaire served as a teaser for a lesson subsequently provided and participants were not at risk in the opinion of the authors and the school officials.

## 4. Quantitative results

### 4.1. Participants

The questionnaire was distributed among 140 elementary school students and 96 high school students. Among the elementary school respondents, the mean age was 11.31, age ranging from 9 to 13 years. (Age in elementary school ranges from 4 to 12/13 years; we included the older grades because of their greater reading ability and computer literacy). The gender split was 43.6% male and 56.4% female. The questionnaire was also conducted at three high schools, two of which located in Amsterdam and one in Den Helder. The mean age of the high school participants was 16.29, age ranging 15–19 years. (Depending on school type, age ranges from 12/13 to 18/19 years; we included the older grades because we looked for a learning curve starting with participants leaving elementary school). The gender split was 60.4% male and 39.6% female. Table 2 shows participant characteristics. Based on the class size and the number of responses, the response rate was at least 80% (exact number unknown).

### *4.2. Quantitative analysis results*

The results are shown in Table 3. The items are a re-translation of the final Dutch version, which closely resembles the original English version of the items.

#### *4.2.1. Elementary school*

Table 3 shows that elementary school students are cautious in their online behavior. For example, they do not share passwords with classmates, do not click on links in emails, or do not open email attachments without thinking about the potential risks. In addition, they do not look up everything they want on the internet at school. When they experience something strange online, most participating elementary school students discuss the event with their parents. However, they do download everything they need for school assignments and do not lock their electronic devices sufficiently. They score even lower on regularly checking their privacy settings of their social media accounts. In terms of password behavior, elementary students score well, they use strong passwords, and they generally have different passwords for social media and school accounts. They cannot sufficiently recognize either phishing emails or phishing websites. They also do not adequately assess the security of websites before entering their information. They indicate that they do not post everything they want about school but score insufficient for considering the negative consequences before posting on social media.

#### *4.2.2. High school*

High school students scored well on items about password behavior. They have strong passwords, use different passwords for social media and school accounts and do not share their passwords with classmates. High school students also score well on items about e-mail behavior. They do not just click on links in emails and do not just open email attachments. In addition, they indicate that they can recognize phishing emails and phishing websites. However, they do not sufficiently assess the security of websites before entering information, and they download everything they need for school assignments. They do not post everything they want about school and consider the negative consequences before posting on social media. In addition, they leave their electronic devices locked when they work in the classroom. On the other hand, high school students look up everything they want at school and do not regularly check the privacy settings of their social media accounts. In addition, they hardly share with their parents experiencing something strange online.

#### *4.2.3. Difference between elementary school and high school*

High school students were better at recognizing phishing websites and emails. Both items showed a significant difference, and the differences had a medium effect size. What high school students do better as well is locking their electronic devices. This item also had a medium effect size.

On the other hand, high school students performed worse than elementary school students on certain items. For the item "looking

**Table 2**
Participant demographics in the questionnaire main study.

| Characteristics | Total |
|---|---|
| Sample size | 236 |
| *Gender* | |
| Male | 119 |
| Female | 117 |
| *Elementary school* | |
| Sample size | 140 |
| Gender | |
| Male | 61 |
| Female | 79 |
| Average age | 11.31 |
| Standard deviation | 0.551 |
| *High school* | |
| Sample size | 96 |
| Gender | |
| Male | 58 |
| Female | 38 |
| Average age | 16.29 |
| Standard deviation | 0.874 |

**Table 3**
Comparing behavior of elementary and high school students, parametric and nonparametric tests.

| Items | Elementary | Highschool | Parametric | Nonparametric | Cohen's d | Cohen's d |
|---|---|---|---|---|---|---|
| | Mean | Mean | p-value | p-value | Point estimate | Effect size |
| I use a different password for my social media and school accounts. | 3.59 | 3.63 | .854 | .435 | −0,024 | |
| I share my school passwords with classmates. * | 4.42 | 4.40 | .836 | Unable to compute | .027 | |
| I use a combination of letters, numbers, and symbols in my school passwords. | 4.05 | 4.27 | .115 | .296 | -.210 | |
| I leave my laptop/iPad/mobile unlocked when I am working in the classroom. * | 3.31 | 4.16 | <.001 | .008 | -.590 | Medium |
| I don't click on links in emails, only if they come from someone I know. | 3.88 | 4.04 | .320 | .959 | -.132 | |
| If an email from an unknown sender looks interesting, I click on the link in the email. * | 4.31 | 4.14 | .212 | Unable to compute | .166 | |
| I do not open email attachments if the sender is unknown to me. | 3.52 | 3.69 | .365 | .935 | -.120 | |
| I can recognize a phishing email. | 3.07 | 4.02 | <.001 | <.001 | -.793 | Medium |
| I download all the files on my school computer that I need for my assignments. * | 2.54 | 1.97 | <.001 | <.001 | .482 | Small |
| When I have access to the Internet at school, I visit all the websites I want. * | 3.67 | 2.26 | <.001 | <.001 | 1.139 | Large |
| I assess the security of websites before entering information. | 3.24 | 3.47 | .183 | .073 | -.177 | |
| I can recognize a phishing website. | 3.07 | 3.69 | <.001 | <.001 | -.530 | Medium |
| I regularly check the privacy settings of my social media accounts. | 2.71 | 2.35 | .026 | .024 | .296 | |
| I consider the negative consequences before I post something on social media | 3.46 | 3.69 | .200 | .739 | -.170 | |
| I post everything I want about my school on social media. * | 4.19 | 3.88 | .058 | Unable to compute | .253 | |
| If I experience something strange online, I share it with my parents. | 4.07 | 2.80 | <.001 | <.001 | 1.043 | Large |

Note" * indicates that the grading was reversed because these items describe negative behavior.

up everything you want on the internet at school", high school students were more likely to look up everything they want. The effect size was large. In addition, with the item "downloading everything needed for school assignments", the high school students reported worse behavior. The differences between elementary school and high school students are summarized in Fig. 1.

#### 4.2.4. *Gender differences*

The results hardly show differences between boys and girls (Table 4). In elementary school, significant differences between the answers of boys and girls were absent. Among high school students, boys scored higher at recognizing phishing websites and emails. Girls score higher in telling their parents experiencing something strange online.

#### 4.2.5. *Summary of quantitative results*

The findings for the qualitative part of the research are summarized in Table 5. These findings concern the most important differences between elementary and high school students and the items for which both groups score insufficiently. These findings were used as input for the group interviews.

## 5. Qualitative results

### 5.1. *Participants*

Two group interviews were conducted. Both interviews were conducted at a high school in Den Helder. In the first interview, two boys and a girl were interviewed, and in the second interview, three girls and a boy were interviewed. The participants' ages ranged from 15 to 17 years.

### 5.2. *Qualitative analysis results*

#### 5.2.1. *Two themes emerged during the content analysis of the group interviews. These themes were 'sources for acquiring secure behavior' and risky behavior*

Sources for acquiring secure behavior.

Overall, learning from experience emerged most frequently (6 out of 7) in the development of cyber secure behavior. For example, as a source for learning to recognize phishing, most respondents mentioned experience, although some also mentioned parents'

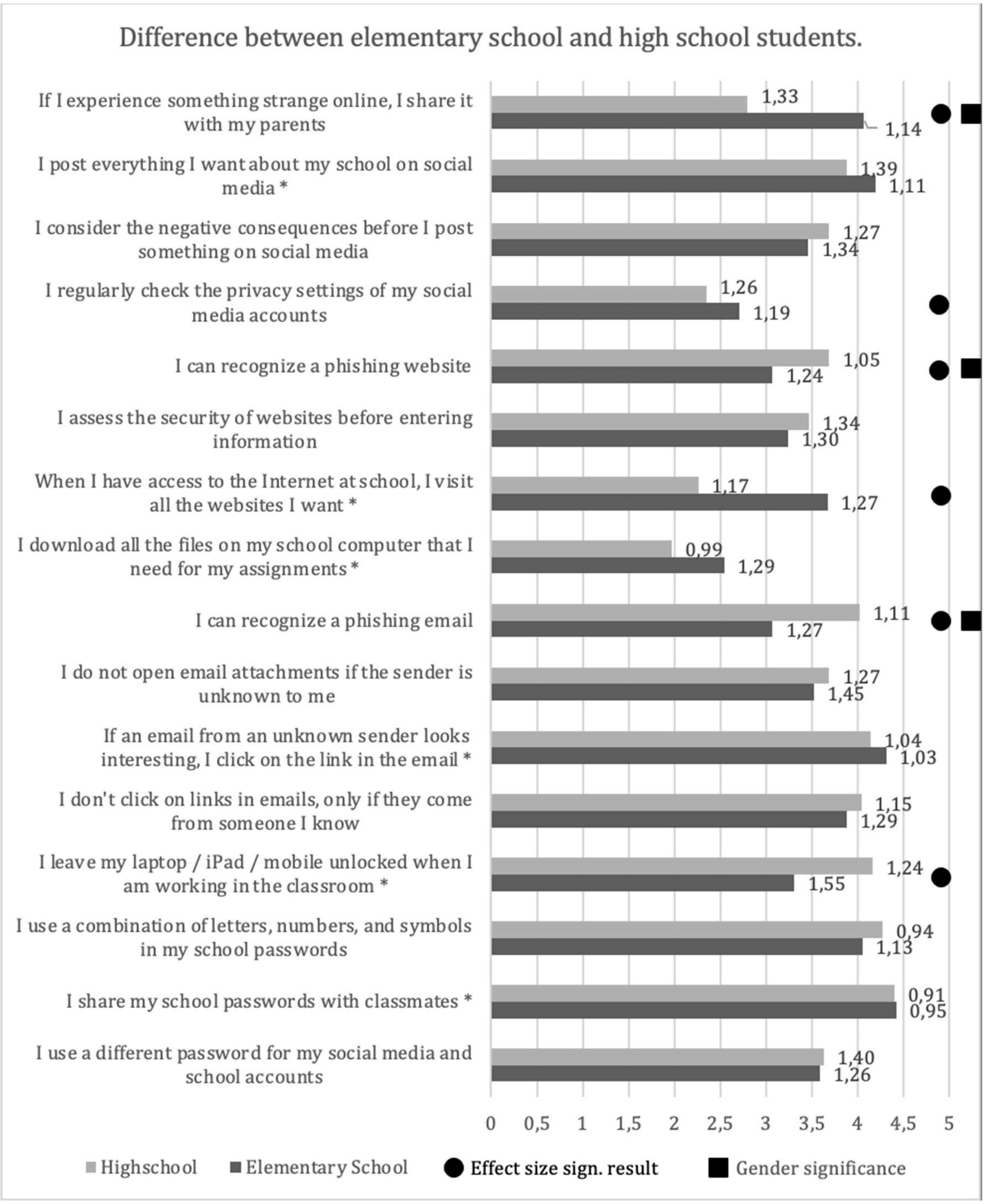

**Fig. 1.** Difference between elementary school students and high school students. Standard deviations are displayed at the end of the histogram bars.

influence, and one participant also mentioned school. In addition, regarding locking devices, five students mentioned experience, indicating that they locked their devices because of what they experienced in school.

Parents and siblings were also often mentioned as sources for developing cyber secure behavior (6 out of 7).

> “My mother has quite a large platform on Instagram, so she regularly receives emails and messages with links, and then she asks me if it is reliable and all that. And then I just look up information about it. And now, when I get such a message on my Instagram, I just know that it is not reliable”.

In addition, the internet was mentioned several times. An example of an internet source are YouTubers who give tips on how to

**Table 4**
Differences between boys and girls in elementary school and high school.

| Items | Elementary school | | Highschool | | Elementary school | High school |
|---|---|---|---|---|---|---|
| | Boys | Girls | Boys | Girls | 2-tailed | 2-tailed |
| | Mean | Mean | Mean | Mean | p-value | p-value |
| I use a different password for my social media and school accounts. | 3.52 | 3.65 | 3.79 | 3.37 | 0.574 | 0.147 |
| I share my school passwords with classmates. * | 1.41 | 1.71 | 1.52 | 1.74 | 0.063 | 0.251 |
| I use a combination of letters, numbers, and symbols in my school passwords. | 4.07 | 4.04 | 4.34 | 4.16 | 0.886 | 0.340 |
| I leave my laptop/iPad/mobile unlocked when I am working in the classroom. * | 2.36 | 2.94 | 1.78 | 1.95 | 0.030 | 0.499 |
| I don’t click on links in emails, only if they come from someone I know. | 3.79 | 3.95 | 4.02 | 4.08 | 0.462 | 0.799 |
| If an email from an unknown sender looks interesting, I click on the link in the email. * | 1.70 | 1.68 | 1.84 | 1.89 | 0.904 | 0.820 |
| I do not open email attachments if the sender is unknown to me. | 3.36 | 3.65 | 3.64 | 3.76 | 0.251 | 0.638 |
| I can recognize a phishing email. | 3.20 | 2.97 | 4.31 | 3.58 | 0.308 | 0.001 |
| I download all the files on my school computer that I need for my assignments. * | 3.48 | 3.46 | 3.91 | 4.21 | 0.929 | 0.152 |
| When I have access to the Internet at school, I visit all the websites I want. * | 2.44 | 2.24 | 3.79 | 3.66 | 0.357 | 0.583 |
| I assess the security of websites before entering information. | 3.05 | 3.38 | 3.69 | 3.13 | 0.135 | 0.046 |
| I can recognize a phishing website. | 3.30 | 2.90 | 4.00 | 3.21 | 0.060 | 0.000 |
| I regularly check the privacy settings of my social media accounts. | 2.59 | 2.81 | 2.50 | 2.13 | 0.277 | 0.164 |
| I consider the negative consequences before I post something on social media | 3.31 | 3.58 | 3.72 | 3.63 | 0.236 | 0.728 |
| I post everything I want about my school on social media. * | 1.77 | 1.85 | 2.21 | 2.00 | 0.681 | 0.480 |
| If I experience something strange online, I share it with my parents. | 3.98 | 4.14 | 2.50 | 3.26 | 0.426 | 0.005 |

**Table 5**
Summary of quantitative results.

| Findings | Description |
|---|---|
| Recognizing phishing emails | High school students can recognize phishing emails better than elementary school students. |
| Recognizing phishing websites | High school students can recognize phishing websites better than elementary school students. |
| Entering data online | The students do not sufficiently assess the security of websites before entering information. |
| Social media privacy settings | The students hardly check the privacy settings of their social media accounts |
| Reporting strange situations | Elementary school students share it with their parents if they experience something strange online. High school students don’t do this sufficiently. |
| Locking mobile devices | The high school students leave their laptop/iPad/mobile locked in the classroom. Elementary school students do not lock their devices appropriately. |
| Downloading files | High school students download all the files they need on their school computers and visit any website they want. |

handle online situations safely.

One of the participants said that he developed online secure behavior at school. This student had received an extensive lesson about online safe behavior in elementary school. When the role of school in the learning process was specifically asked for, two more participants said that they had received information about online secure behavior in the form of a presentation at school.

Participants in both groups indicated that school had little or no influence on their learning process. One of the participants indicated that school hardly had an influence on her safe online behavior and if it had an influence, it was a negative influence. This was due to the classmates who exhibited risky online behavior.

The participants indicated that they were no longer interested in education about safe online behavior, because they felt that they no longer needed it (5 out of 7). They would have liked education in the last years of elementary school. One of the participants indicated that he would have liked someone to come by one morning a week to explain more about safe online behavior. Others indicated that one or two lessons would have been useful when receiving their first laptop or iPad from school (4 out of 7).

### *5.2.2. Risky behavior*

During the interviews, it became evident that most of the students were overconfident. Almost all participants indicated that they no longer needed education about safe behavior online, because they already knew enough (6 out of 7). However, the interviews also suggested that participants lacked knowledge in some areas. For example, when recognizing phishing emails and websites, participants mentioned certain aspects to check the legitimacy but the number of aspects they mentioned was incomplete. They did not appear to possess procedural knowledge, which according to Arachchilage and Love (2014) is important in recognizing phishing attacks. One participant indicated that she judged the security of websites by intuition and did not know how to assess a website properly.

> “Well, it is a bit hard to explain, I act on intuition, I think, just as soon as I don’t trust something, then I don’t do it and then it always goes well”.

Others had more knowledge, for example, they checked whether the prices of online stores differed too much from those of the competitors, they looked at reviews, at the security indicator and at the web address (4 out of 7). Another participant indicated that she just accepts the risk.

> "I know it [is a malicious website] but sometimes I just really want to [visit it]".

During the interviews, no one indicated that they looked at privacy settings of social media regularly. Some indicated that they did not care what their privacy settings are (2 out of 7).

> "It doesn't matter much. I just make sure I pay attention to what I'm doing on [social media]."

Several students gave the impression that they are thinking about the consequences of privacy settings (3 out of 7).

> "When I'm on Snapchat, for example, there is a map. I see so many people on the map and think they all have their location turned on and I can literally see where everyone lives, because they are there very often. So I think either they don't check [their settings] or they think it is normal."

## 6. Discussion

### 6.1. Summary of results

The aim of this study was to determine to what extent Dutch students demonstrate cyber secure behavior in elementary school and high school. A questionnaire completed by elementary school students and high school students and group interviews with high school students revealed that on average the high school students perform better in the areas of safe email behavior, password behavior, phishing awareness, and physical locking of devices. On the other hand, students become more reckless over time when using the internet and hardly share experiencing something strange online with their parents. Neither elementary school students nor high school students regularly check their privacy settings. Among high school students, boys score higher at recognizing phishing websites and emails. Girls score higher in telling their parents when they experience something strange online. Given the fact that cyber security issues are daily news in the media, we were surprised to find that the school system lags behind in such an important domain of knowledge. The importance of the subject combined with the fact that children are already exposed to online risks should make a proper cyber security curriculum at their school mandatory. Teaching at a younger age will likely result in thoroughly skilled adults.

### 6.2. Relationship with other research

We did not retrieve studies with a focus like ours. Hence, we could not compare our findings with the results of previous studies. However, literature about specific cyber security skills in children at a certain age reported low levels of competence (Choong et al., 2019; Quayyum et al., 2021). The present research suggests that the school curriculum hardly pays attention to the development of cyber secure behavior. The students develop their online behavior mainly by learning from experience, from instructions on the internet, through parents, and through siblings. This is partly in line with the research on the online behavior of university students (Schaffer & Debb, 2019). Other research suggested that young adults tend to be more cautious than older adults in their cyber security behavior, but that they are nevertheless more susceptible to cyberattacks due to the fact that they are more active online (Rainie et al., 2013). This was also found by an earlier study of online behavior of young adults: while they were aware of cyber security risks, especially for the individual as the weakest link, they still engaged in risky online behaviors (Zhang, 2005).

The existing research about adults stresses the importance of our findings that suggest that structured learning of cyber security behavior lags behind. In the Global Information Technology Report of 2016, the Netherlands was sixth out of 143 countries on the Networked Readiness Index, which consists of 53 individual indicators that assess the readiness of countries to apply emerging information and communication technology for greater prosperity (Baller, Dutta, & Lanvin, 2016). The Netherlands scored well on the Networked Readiness Index but still pays hardly any attention to cyber security education. We do not have figures about other countries that score lower on the index, but we hypothesize that their attention for cyber security behavior corresponds with this index. As already described in the literature review section, some institutions developed cyber security curricula, of which the PICSAR is a good example (Chase et al., 2020). The PICSAR project is helping to build a foundation for high school study of cyber security by working with K-8 faculty. Together they develop age-appropriate Science, Technology, Engineering, Arts and Math (STEAM) lesson plans integrating cyber security topics at all grade levels. The PICSAR project proposed a K-12 cyber security framework including cyber hygiene, cyber security fundamentals, security administration, network security, offensive security, and cyber competitions. Despite a shortage of teachers with adequate competencies, there are examples of schools offering a K-12 curriculum. However, most courses are used by self-selected small groups of students interested in computer science (Chase et al., 2020).

### 6.3. Strengths and limitations

The present study has several limitations, such as the small sample size and the potentially limited generalizability based on the limited number of participating schools. Also, the fact that the interviews were conducted at only one school may have a negative influence on the generalizability of the study. Extension of the study in the Netherlands, but also in other countries is desired.

The questionnaire was conducted at the beginning of a lesson about cyber security. We approached ethical questions from a utilitarian perspective and decided that, as a first line of defense, the research had almost no risk for participants. Therefore, we left the final ethical clearance to the school officials, who had no interest in the research, and would suffice as second line of defense protecting the participant (Schuwirth & Durning, 2019). An approach from a deontological stance would demand ethical clearance from a centralized ethical board as a third line of defense. And in such a situation, it might be better to be safe than sorry.

Another potential limitation is that the questionnaire that was used for this study has 16 items, whereas the validated questionnaire on Information Security Awareness that was used to develop our questionnaire has 21 items for the behavior dimension (Parsons et al., 2017). It can be argued that an abridged version of the validated questionnaire does not provide a holistic picture of information security behavior. However, shortening the questionnaire was essential because not all the original items were relevant for elementary and high school students. Ultimately, 14 relevant items remained, and two more items were added based on another questionnaire on phishing threat avoidance (Arachchilage & Love, 2014). The items were then translated into Dutch and worded differently, which may have led to a change in the meaning of the items. To ensure that this would not hinder the research, a validity test was performed. Both in the original and abridged versions items like 'strong password' and 'regularly checking security settings' leave room for interpretation and may need a more unequivocal definition in future research. The current formulation of the items was copied from the original validated questionnaires. However, this formulation introduces a flaw in the study because it leaves more room for inadequate self-assessment.

All respondents completed the questionnaire online, to avoid copying errors. The data were checked for content non-responsivity to assess the data quality. The questionnaire and the group interviews were conducted anonymously to ensure that the students answered honestly without having to think about the consequences of their answers. Besides, anonymity reduces the chance of biases (Parsons et al., 2014). However, the fact that we used a self-assessment questionnaire may have led to the Dunning-Kruger effect, which implies that incompetent people tend to overestimate themselves and people who are competent underestimate themselves. The extent to which the Dunning-Kruger effect has occurred is difficult to estimate (Schlösser et al., 2013).

### 6.4. Recommendations

We recommend that cyber security behavior should be learned early on as an integral part of basic school education. As the students themselves indicated in the interviews, it is important that when students receive their first school device (such as a laptop or an iPad) they should receive repetitive lessons about cyber secure behavior, probably in the second half of elementary school. Extra attention should be paid to recognizing phishing emails and websites. The students should be convinced that risky behavior on the internet may turn against them and against the organization to which they belong. An example of identity theft and the dramatic effect on someone's life must be taught convincingly. Just like reading, writing and arithmetic, cyber security should be a part of basic education. The use of well-known curricula like PICSAR should be explored.

### 6.5. Future research

First, a repetition of the current study with a larger sample size and executed in a multi-national context is desirable. More detailed research about terms in the questionnaire that leave room for interpretation, like the use of 'strong passwords' and 'regularly checking security settings' may reveal important behavioral flaws. The outcomes of such more detailed research may be important for adequate future curriculum design. Elaborating on the work of Falkner et al. (2019), who compared curricula used in different countries and based on published K-12 curricula a feasible international core curriculum for children may be developed to be adapted for use in various cultures and countries. In addition, it would also be interesting to investigate why currently available curricula experienced serious delays in scaling up (Rutstein et al., 2019). This research could also be extended to students attending higher education to see whether attention is being paid to cyber security after high school. Ultimately, some students are almost ready to start their careers and therefore need to be well prepared for potential cyber-attacks. Studying cyber secure behavior of teachers in schools could provide more insight into current role model behavior.

## 7. Conclusion

The results of the present study tentatively suggest that students do not effectively develop cyber secure behavior in elementary school and high school in the Netherlands. Students reported cyber secure behavior concerning emails, passwords, phishing and physically locking their devices, but many students also developed overconfident and reckless behavior in the areas of internet use and reporting online incidents Students indicated that school played hardly any role in the development of their cyber secure behavior. They acquired their online behavior mainly through experience, instructions on the internet, through parents, and through siblings. We advocate scaling up of feasible cyber security programs.

## References

ACM Digital Library. (https://dl.acm.org)/.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Baller, Silja, Dutta, Soumitra, & Lanvin, Bruno (2016). The Global Information Technology Report 2016. *World Economic Forum*. https://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

Bernd, Julia, Garcia, Dan, Holley, Buffie, & Johnson, Maritza (2022). Teaching Cybersecurity: Introducing the Security Mindset. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2 (SIGCSE 2022).* (p. 1195). https://doi.org/10.1145/3478432.3499160.

Chase, J., Uppuluri, P., Denny, E., Patterson, B., Eller, J., Lane, D., Edwards, B., & Onuskanich, R. (2020). STEAM powered K-12 cybersecurity education. *Journal of The Colloquium for Information Systems Security Education, 7*, 1–8.

Choong, Theofanos, M. F., Renaud, K., & Prior, S. (2019). Passwords protect my stuff'-a study of children's password practices. *Journal of Cybersecurity (Oxford), 5*(1). https://doi.org/10.1093/cybsec/tyz015

Code.org. (2018). *CS Discoveries curriculum Guide 2018-2019*. https://curriculum.code.org/csd-18/.

Collins, D. (2003). Pretesting survey instruments: An overview of cognitive methods. *Quality of Life Research, 12*(3), 229–238. https://doi.org/10.1023/A:1023254226592

Computer Science Teachers Association. (2017). *CSTA K-12 computer science standards*. Revised 2017 http://www.csteachers.org/standards.

Cuny, Jan (2015). Transforming K-12 computing education: AP® computer science principles. *ACM Inroads, 6*(4), 58–59. https://doi.org/10.1145/2832916

de Winter, J., & Dodou, D. (2010). Five-Point Likert Items: t test versus Mann-Whitney-Wilcoxon (*Addendum added October 2012*). *Practical Assessment, Research, and Evaluation, 15*. https://doi.org/10.7275/bj1p-ts64.

Duncan, C., & Bell, T. (2015). In *A pilot computer science and programming course for primary school students. Proceedings of the Workshop in Primary and Secondary Computing Education (WiPSCE'15)* (pp. 39–48). New York, NY: ACM. https://doi.org/10.1145/2818314.2818328.

Education, V. (2016). *2 (SIGCSE 2022)*. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3478432.3499160

Falkner, Sentance, S., Vivian, R., Barksdale, S., Busuttil, L., Cole, E., Liebe, C., Maiorana, F., McGill, M., & Quille, K. (2019). In *An international Comparison of K-12 computer science education Intended and Enacted curricula. Proceedings of the 19th Koli calling international Conference on computing education research* (pp. 1–10). https://doi.org/10.1145/3364510.3364517

Fleenor, H., Peker, Y., & Cutts, E. (2019). In *Collaboration: Developing and Piloting a Cybersecurity curriculum for Middle school. In Proceedings of the 50th ACM technical Symposium on computer science education (SIGCSE '19)* (p. 1275). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3287324.3293824.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security, 95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security Privacy, 10*(2), 24–32. https://doi.org/10.1109/MSP.2011.179

Kortjan, N., & Solms, R. V. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal, 52*. https://doi.org/10.18489/sacj.v52i0.201

Krutz, D. E., & Richards, T. (2017). Cyber security education: Why don't we do anything about it? *ACM Inroads, 8*(4), 5. https://doi.org/10.1145/3132217

K–12 Computer science framework. *https://k12cs.org/*.

Maqsood, S., & Chiasson, S. (2021). Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Trans. Priv. Secur., 24* (4), 37. https://doi.org/10.1145/3469821. Article 28 (November 2021).

Mashiane, T., & Kritzinger, E. (2019). Cybersecurity behavior: A conceptual taxonomy. In O. Blazy, & C. Y. Yeun (Eds.), *Information security theory and practice* (pp. 147–156). Springer International Publishing. https://doi.org/10.1007/978-3-030-20074-9_11.

Norman, G. R., & Streiner, D. L. (2003). *PDQ Statistics*. USA: PMPH.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016a). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016b). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*. https://doi.org/10.1016/j.ijcci.2021.100343

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online. Pew research center: Internet*. September 5. Science & Tech https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/.

Riel, M., & Romeike, R. (2020). IT security in secondary CS education: Is it missing in today's curricula? A qualitative comparison. In *Proceedings of the 15th Workshop on primary and secondary computing education (WiPSCE '20)* (pp. 1–2). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3421590.3421623. Article 35.

Rutstein, D. W., Xu, Y., McElhaney, K., & Bienkowski, M. (2019). Developing implementation measures for K- 12 computer science curriculum materials. *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 321–327. https://doi.org/10.1145/3287324.3287424

Ryan, K., Gannon-Slater, N., & Culbertson, M. J. (2012). Improving survey methods with cognitive interviews in small- and medium-scale evaluations. *American Journal of Evaluation, 33*(3), 414–430. https://doi.org/10.1177/1098214012441499

Schaffer, D. R., & Debb, S. M. (2019). Validation of the online security behaviors and Beliefs questionnaire with college students in the United States. *Cyberpsychology, Behavior, and Social Networking, 22*(12), 766–770. https://doi.org/10.1089/cyber.2019.0248

Schlösser, T., Dunning, D., Johnson, K. L., & Kruger, J. (2013). How unaware are the unskilled? Empirical tests of the "signal extraction" counterexplanation for the dunning–kruger effect in self-evaluation of performance. *Journal of Economic Psychology, 39*, 85–100. https://doi.org/10.1016/j.joep.2013.07.004

Schutte, T., Scheele, F., & van Luijk, S. (2021). Roses and balances: A paradigm for constructive ethical review of health professions education research. *Advances in Medical Education and Practice, 12*, 529–535. https://doi.org/10.2147/AMEP.S305094, 2021.

Schuwirth, L. W. T., & Durning, S. J. (2019). Ethics approval for health professions education research: Are we going too far down the barrel? *Medical Education, 53* (10), 956–958. https://doi.org/10.1111/medu.13942

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382. https://doi.org/10.1145/1753326.1753383

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2016). Empiracal study of students' computer security practices/perceptions. *Journal of Computer Information Systems*. https://www.tandfonline.com/doi/abs/10.1080/08874417.2007.11645971.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's. *Heliyon, 5*(12), Article e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). A19-Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Zhang, X. (2005). What do consumers really know about spyware? *Communications of the ACM, 48*(8), 44–48. https://doi.org/10.1145/1076211.1076238