SuperCyberKids Learning Framework

SuperCyberKids
Deliverable no. D2.1 (Annex 1)

Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
Project No. 101087250

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Project ref. number	101087250
Project title	SCK - SuperCyberKids
Document title	SuperCyberKids Learning Framework -SCKLF (M7)
Document Type	Deliverable (Annex)
Document version	1.1, 2024-09-25
Previous version(s)	1.0, 2023-12-04 0.1, 2023-07-31
Planned date of delivery	2023-07-31
Language	English
Dissemination level	Public
Number of pages	40
Partner(s) responsible	CRN (WP2 – Leader) UMA (WP2.1 Leader)
Participating partner(s)	CRN; UMA
Author(s)	Dirk Ifenthaler, UMA; Nicolai Plintz, UMA; David Gall, UMA
With contributions by	Flavio Manganello, CNR; Jeffrey Earp, CNR; Manuel Gentile, CNR; Salvatore Perna, CNR; Giuseppe Città; CNR
Keywords	SuperCyberKids, Cybersecurity Education Initiatives, Systematic Literature Review, Skill framework
DOI	https://doi.org/10.17471/54025
How to cite	Gentile, M., Manganello, F., Fante, C., Earp, J., Perna, S., Città, G., Plintz, N., Bassi, G, Callaghan, P., de Vibraye, A., Fabbri, S., Matteucci, I., Vaccarelli, A., (2023). SuperCyberKids Learning Framework - SCKLF. Deliverable 2.1 - SuperCyberKids project (ERASMUS-EDU-2022-PI-FORWARD - ERASMUS-LS - Project No. 101087250). DOI: https://doi.org/10.17471/54025

Annex 1

1.1 Final Version Framework

SCK - Foundation-Framwork	Identify Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.	Protect	Detect	Respond	Recover
	Kids should know...	Kids should be able to...	Kids should be able to...	Kids should be able to...	Kids should...
Malicious code & cyber-attacks	... that malware exists and that there are different types of it. ... that viruses exist. ... how hackers use viruses to damage important data and obtain private information. ... how a virus can reach your PC. ... that a file called a virus can make a computer stop working. ... that worms exist. ... packet sniffing exists. ... there is a danger of packet sniffers on unsecured wireless networks. ... that spyware exists. ... that loggers exist. ... to discuss examples of unsafe content such as popups and malicious links. ... the basic functionalities of the internet/computers. ... the effects of malware (e.g. steal or damage the data). ... that malicious web pages can be used to steal their data or download a malware. ... that an email attachment could also contain malware.	... protect themselves from hackers or attackers, which can cause demage to important data and obtain private information. In this context kids should know how to guard themselves against such attacks by using safe passwords, antivirus software and encryption. ... avoid viruses by deleting supsious mails from the pc and use an anti-virus program. ... protect themselves against malware. ... avoid being hacked. ... recognize unsecured wifi. ... recognize unsecured environments (websites, Apps, Links). ... know to avoid clicking without reading or knowing where it will lead to.	... spot signs of cyber attacks. ... identify if a website is authentificated or not. ... recognize different forms of cyberattacks and cybercrime. ... identify when a network connection is secure or not (HTTPS). ... discuss examples of unsafe content, such as popups and malicious links. ... note alarm messages & security alerts and evaluate them. ... recognize unsecured environments (website, apps, links) and avoid them to recognize 'bait' messages and void them to learn what they agree to by clicking on links or pop-ups.	... report cyber crime. ... respond to potential threats online. ... disconnect their devices from the internet or their home network. ... know basic attacks that they might be victims of and what to do, specifically who to turn to. ... be aware of predators online and should know who to turn to for help. ... respond to malewaare/cyber attacks by consulting a safe/trusted adult. ... know who they should contact and how to react to cyberattacks and cybercrime. ... know basic attacks that they might be victims of and what to do, specifically who to turn to.	... be able to accept negative online experience. ... know how to cope with negative experience and avoid them in the future. ... know how to reset their mobile devices to factory settings.
Data Privacy & Awareness	... personal data protection. ... to keep private data safe. ... the consequences of exposing personal data. ... that passwords can help to protect computer files and information. ... concept of online privacy and that there are different levels of privacy. ... what possibly happens when they post a comment in a social media app. ... how to authenticate. ... the basics of an individual account in an app. ... security risks when streaming. ... that engaging in the illicit downloading of copyrighted materials is not appropriate. ... that a person can be identified by knowing only a few pieces of information about them, and that they must therefore be careful about what information they provide online. ... recognise what forms 'personal information' can take. ... how to identify different types of personal information that may be elicited in the online environment. ... some of the techniques that are used in the online environment to elicit their personal information. ... how to demonstrate an awareness of why it may be unwise to disclose their personal details online. ... about disclosure of personal information and commercial exploitation. ... how to understand and respect their own rights and those of others regarding private information. ... what personal information and safety procedures are. ... how to classify personal data. ... that they shouldn't post their location online. ... the concept of privacy of personal data of third parties. ... the concept of digital footprints. ... that once they post information on the internet it can't ever truly be erased. ... the security issues caused by social media usage. ... about privacy settings and what they entail. ... that someone they don't know can send them a private message or direct message. ... their rights (e.g. on their own picture) ... what information they can share. ... the concept of copyright. ... how copyright relates to fair use. ... examples of how fair use can help protect an author/creator's rights while promoting the sharing of ideas. ... that downloading copyrighted materials e.g. music and films can be risky. ... about sharing and authoring rights	... handle their own personal data responsibly. ... create User-Accounts (e.g. Guest-Account). ... distinguish between private and public information. By discussing grade-appropriate examples of privacy and what is OK to share about themselves and how that relates to confidentiality. ... be aware of creating privacy settings for minimizing SNS risks, and assessing other online risks or cyberbullying. ... not give out personal data and information. ... use a different password for social media and school accounts. ... prevent themselves from share school passwords with classmates. ... regularly check the privacy settings of their social media accounts. ... not post everything on the internet. ... be aware of online privacy and the levels of privacy. ... use passwords. ... update their computer, when a warning from the computer appears. ... use online storage systems to exchange and keep personal or sensitive information. ... distinguish which data to share/provide online or not. ... check privacy- and chat settings to be safe during gaming. ... handle privacy settings to avoid online enticement and sextortion. ... use the privacy settings in SNS for reporting, blocking and saving their data. ... demonstrate an awareness of why it may be unwise to disclose their personal details online. ... clean their browser cache. ... protect their devices and personal information by using strong passwords or MFA) ... set privacy settings. ... decide whether posting information is OK or not. ... manage their online profiles (e.g. privacy) ... not tell or give any private or personal information about themselves or others to strangers. ... destroy/erase information and protect data appropriately. ... use online privacy settings as a preventive coping strategy because it may decrease the likelihood of being cyberbullied in the future. Privacy settings allow social media users to limit who can access the content they share online (e.g., pictures, comments, personal information). ... understand what happens when posting a comment in a social media app. ... limit visibility of posts and comments. ... limit visibility of personal information. ... decide whether to give out personal data without permission from their parents. ... react if a stranger is asking them for personal information. ... protect their personal data in an online context. ... decide whether it is OK to post their location online or not. ... to recognize and use a pseudonym in the online discussion forum to secure their personal data in an appropriate way. ... use personal password-protected accounts. ... protect their digital identity by knowing where and what information to share online and what not to share.	... recognize when websites, apps, programs or e-mails ask for personal data that should not be given out. ... give examples of how copyright can be equated to ownership and other ideas, such as "Who wrote the document," "Anything I create that is new to the world is mine," and "I need to give credit to any content not created by me."	... cope with negative experiences. ... understand how to destroy/erase information and protect their data appropriately.	... know how and who could help them in case of inappropriate content sent to or received from an adult and/or cyberbullying threat. ...know how to react if they sent out an inappropriate picture. ... know how they might help others who are feeling sad or upset because of online threats.
Frauds	... about phishing and what it entails. ... the basics of sodial engineering attacks. ... that email phishing attacks are possible. ... to be aware of about pharming and what it entails. ... that grooming exists. ... the meaning of grooming. ... that using communication technologies can lead to sexual assault and/or child prostitution. ... to be aware of loggers and what they entail. ... about smishing. ... to be aware of botnets and what it entails. ... to be aware of scams (commercial and financial) and what they entail. ... to be aware of identity theft and what it entails. ... to be aware of online predators and what this entails. ... to be aware of spoofing and what it entails.	... maintain integrity and confidentiality against web tracking & phishing. ... check the security information/certification of online payments. ... refrain from clicking on links in emails if they come from strangers. ... know not to open email attachments if the sender is unknown to them. ... change settings on their phone to prevent autoconnection to insecure wireless networks. ... use strategies for downloading suspicious attachments.	... recognize red flags from untrustworthy people in the online world. ... recognize if a website is safe to register. ... identify cyber grooming attempts. ... decide whether or not to pay. ... identify unsafe content online. ... recognize a phishing email. ... detect online enticement and sextortion by discussing online manipulation. ... name the feelings they may experience when dealing with something or someone untrustworthy.	... report an impostor. ... report cyber attacks. ... respond to grooming. ... know that they should change their password after a phishing attack. ... know to contact a trusted adult if a fraud happend to them.	... be able to change passwords after they have fallen victim to a scam. ... know who to ask for help to do a recovery of their device/account. ... know how to reset their mobile devices to factory settings.
Abusive Content	... that inappropriate content could appear online. ... that intolerant content could appear online. ... that hate speech could appear online. ... that violent content could appear online. ... that illegal materials such as images of child abuse could appear online. ... of online gambling services. ... that pornographic content exists online. ... that sexual or harmful content exists online. ... that false & untrue content exists online as well as fake news. ... that bullying via websites, mobile phones or other forms of communication devices is possible. ... that chatrooms on the internet can be an unsafe place. ... that downloading data, like music from unlicensed sources can be dangerous. ... that a stranger can ask them for personal information. ... the meaning of grooming. ... using communication technologies can lead to sexual assault and/or child prostitution.	... classify age-appropriate websites (by adapting the knowledge of the parent's "What is a child-friendly website"). ... create safe content safely. ... decide if a website is age-appropriate. ... self-protect on an individual level in an online environment. (Ignore or retreat to other media) ... decide whether a website is safe or suspicious. ... avoid dangerous chats and internet sites entirely. ... use appropriate privacy settings to minimize SNS risks, asses other online risks or recognize cyberbullying. ... assess the security of websites before entering information. ... handle privacy settings to avoid online enticement and sextortion. ... identify "Red Flags" and malicious intentions of strangers in the field of online enticement & sextortion. ... ask a trusted adult for help to decide if their online activity is age-appropriate. ... ask teachers for guidance when deciding whether a website is age appropriate or not. ... decide if they should respond in cyberspace or not. ... decide if you can believe a piece of information in cyberspace or not. ... recognize and avoid inappropriate material (such as illegal or pornographic content). ... use strategies to prevent cyberbullying.	... recognize inappropriate and harmful media content. ... identify safe and not safe internet sources. ... identify unsafe content online. ... recognize a phishing website. ... detect online enticement and sextortion by discussing online manipulation.	-	... know how to cope with negative online experience. ... know how they might help others who are feeling sad or upset because of online threats.
Safety	... right and wrong online behavior. ... the different motivations that influence right and wrong online behaviors. ... what it means to use a "parent" credit card. ... the reality of payments that are conducted online. ... risks of internet use/digital environments. ... different forms and behaviors of harmful digital actions. ... that they should be nice and polite to other people on the internet. ... about the principle of online etiquette, upstander & bystander. ... how to treat others online. ... about inappropriate and bullying behaviors and consider how these impact the feelings of others. ... the importance of considering the impact on others and society before acting. ... about computer and internet addiction, and health issues that come from the overuse of technology (physical, mental issues). ... what cybersecurity is. ... netiquette, online communication and collaboration. ... that not every sender of an email is trustworthy. ... how online actions have real-world consequences and that laws and regulations may also apply online. ... not to open frivolous email attachments if the sender is unknown to them. ... right and wrong uses of digital devices. ... not to download every and any content. ... not to visit every website. ... that they should asses a website before opening it. ... the importance of considering the negative consequences before posting something on social media. ... that there is danger in social networking. ... that nothing you post on the internet is really safe/secure. ... that people could be manipulative online. ... not to send abusive texts or emails. ... that teachers can help them to stay safe on the internet. ... how to use the internet in a safe way. e.g. not chatting with strangers, not sending personal information and photos, and not meeting people whom they solely know only via the internet. ... not to give personal information out. ... how to anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person). ... how to refrain from activities that harm their health (such as excessive smartphone use). ... what a bystander and an upstander in regards to cyberbullying is. ... the risks of SNS. ... how to protect their computer. ... about the prevention of cyberbullying. ... the expression 'reporting'. ... what the following expression 'online predator' means. ... the possible risks and the negative effects of the internet on their physical and psycho-social development. ... that they are not anonymus while using the internet. ... that their digital and real identities are heavily connected. ... that the internet doesn't forget. ... that dangerous situations can appear during the use of SNS.	... protect themselves from harm on the internet. ... browse safely and securely. ... know basic cyber hygiene: behavior, how to communicate and how to take care of their devices and accounts. ... decide whether a website is safe or suspicious. ... make backups and know the importance of backups. ... avoid dangerous chats and websites entirely. ... not meet up with people from chatrooms. ... not trust what people say on the internet. ... not leave their laptop/iPad/mobile unlocked when they working in the classroom. ... not click on links in messages (email, SNS, Chat), only if they come from someone they know. ... assess the security of websites before entering information. ... not open email attachments if the sender is unknown to them. ... not post everything on the internet. ... understand that downloading data like music from unlicensed sources can be dangerous. ... identify situations in which it is wise to turn to a trusted adult for help. ... understand that their emotions can be a powerful tool to help them assess unsafe situations. ... identify some of the physical sensations that alert humans of unsafe situations. ... anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person). ... understand the importance of checking with an adult before participating in the online environment. ... understand that not everyone they meet (whether in the 'real world' or online) is trustworthy. ... check files with an adult before downloading. ... ask teachers to help them stay safe on the internet. ... decide to follow or click a link or not. ... consider the impact on others and society before acting in an SNS environment. ... understand the meaning of entering into contracts, and never do this by themselves. ... use future-oriented coping strategies, or "preventive coping," like responding to potential stressors before a stressful situation has occurred. ... understand some of the qualities that can be used to assess if a person is trustworthy. ... identify some of the physical sensations that alert us to unsafe situations.	... differentiate between paid and non-paid services online. ... check the security information/certification by online payments. ... name the feelings they may experience when dealing with something or someone untrustworthy.	... know where to ask for help and how to explain their digital safety issues using basic terms, yet proper IT vocabulary (such as phishing, cyberbullying, etc.). ... understand what to do against cyberbullying or help others in the situation. ... understand that it is good to act on their feelings (intuition) in order to avoid or escape from unsafe situations. ... know to report the situation or the person if they feel unsafe. ... know how to document evidence, such as screenshots or saved concersations to support their claims.	... be able to learn from safety issues and how to repsond to possible consequences

1.2 List of used references of cybersecurity skills

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education*, *62*(2), 134–140. https://doi.org/10.1109/te.2018.2877182

Anastasiades, P. S., & Vitalaki, E. (2011). Promoting Internet Safety in Greek Primary Schools: the Teacher's Role. *Journal of Educational Technology & Society*, *14*(2), 71–80. https://www.jstor.org/stable/jeductechsoci.14.2.71

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, *11*(23), 11269. https://doi.org/10.3390/app112311269

Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R., Nordvik, J., Papameletiou, D., Reina, V., Ruzzante, G., Sanchez Martin, J., Sportiello, L., Steri, G. and Tirendi, S., Cybersecurity, our digital anchor, Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., Kounelis, I., Mortara, B., Nordvik, J. and Sanchez Martin, J. editor(s), EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19958-8, doi:10.2760/967437, JRC121051.

Berson, I., Berson, M., Desai, S., Falls, D., & Fenaughty, J. (2008). An Analysis of Electronic Media to Prepare Children for Safe and Ethical Practices in Digital Environments. *Contemporary Issues in Technology and Teacher Education*, *8*(3), 222–243.

Buchanan, L., Scarlatos, L., & Telendii, N. (2021). Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students. *2021 IEEE Integrated STEM Education Conference (ISEC)*. https://doi.org/10.1109/isec52395.2021.9763930

Cranmer, S., Selwyn, N., & Potter, J. (2009). Exploring primary pupils' experiences and understandings of "e-safety." *Education and Information Technologies*, *14*(2), 127–142. https://doi.org/10.1007/s10639-008-9083-7

DeFranco, J. F. (2011). Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers (J1)*, *86*(5), 52–55.

Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, *117*, 105064. https://doi.org/10.1016/j.chiabu.2021.105064

Fujikawa, M., Ikehara, H., & Abe, Y. (2020). SNS Education Game for Upper-Grade Elementary School Students. *Proceedings of the 2020 8th International Conference on Information and Education Technology*, 137–141. https://doi.org/10.1145/3395245.3395248

Fujikawa, M., Ryoya Kanou, Itoh, A., & Abe, Y. (2019). Development of an SNS education game for higher-grade elementary school children. *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning,* 130–134. https://doi.org/10.1145/3306500.3306501

Graafland, J. H. (2018, September 17). New Technologies and 21st Century Children: Recent Trends and Outcomes. *OECD Education Working Papers, No. 179*. *OECD* Publishing, 1–60. https://doi.org/10.1787/e071a505-en.

Hammond, S. P., Polizzi, G., & Bartholomew, K. J. (2022). Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. *Education and Information Technologies,* 28, 3681-3709. https://doi.org/10.1007/s10639-022-11240-z

Hudson, C. C., Lambe, L., Pepler, D. J., & Craig, W. M. (2015). Coping While Connected. *Canadian Journal of School Psychology*, 31(1), 3–16. https://doi.org/10.1177/0829573515619623

Kenny, M. C., Long, H., Billings, D., & Malik, F. (2022). School-based abuse prevention programming: Implementation of child safety matters with minority youth. *Child Abuse Review*, 31 (3). https://doi.org/10.1002/car.2742

Kilavo, H., Kondo, T. S., & Hassan, F. (2022). The impact of teaching computer programming in Tanzanian primary schools. *Interactive Learning Environments*, 1–12. https://doi.org/10.1080/10494820.2022.2115078

Konak, A. (2014). A cyber security discovery program: Hands-on cryptography. *2014 IEEE Integrated STEM Education Conference,* 1–4. https://doi.org/10.1109/ISECon.2014.6891029

Kralj, L. (2014). Children's safety on the Internet-development of the school curriculum. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 593-596. https://doi.org/10.1109/MIPRO.2014.6859637

Kralj, L. (2016). E-safety and Digital Skills as Part of School Curriculum. *Medijske Studije*, *7*(13), 59–75. https://www.ceeol.com/search/article-detail?id=551938

Kritzinger, E. (2015, July 1). Enhancing cyber safety awareness among school children in South Africa through gaming. *2015 Science and Information Conference (SAI)*, London, UK, 2015, 1243-1248. https://doi.org/10.1109/SAI.2015.7237303

Kritzinger, E., & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. *2013 Africon*, Pointe aux Piments, Mauritius, 2013, 1-5. https://doi.org/10.1109/afrcon.2013.6757708

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication*, *29*(3), 271–288. https://doi.org/10.1177/0267323114521045

Martínez-de-Morentin, J.-I., Lareki, A., & Altuna, J. (2021). Risks Associated With Posting Content on the Social Media. *EEE Revista Iberoamericana de Tecnologias del Aprendizaje*, vol. 16, no. 1, pp. 77-83. https://doi.org/10.1109/RITA.2021.3052655

Nicolaidou, I., & Venizelou, A. (2020). Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-Experimental Study. *Multimodal Technologies and Interaction*, *4*(2), 10. https://doi.org/10.3390/mti4020010

Piccolo, L. S. G., Troullinou, P., & Alani, H. (2021). Chatbots to Support Children in Coping with Online Threats: Socio-technical Requirements. *Designing Interactive Systems Conference 2021*, 1504-1517. https://doi.org/10.1145/3461778.3462114

Pooja, P. R. & Shashidhar, R. (2022). EVALUATION OF STUDENTS'AWARENESS TOWARDS CYBER SECURITY. *Phronimos*, *2*(4), 33-40.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2021). A scoping review of child grooming strategies: pre- and post-internet. *Child Abuse & Neglect*, *123*, 105392. https://doi.org/10.1016/j.chiabu.2021.105392

Santre, S. (2023). Cyberbullying in adolescents: a literature review. International Journal of Adolescent Medicine and Health, 35 (1), 1-7. https://doi.org/10.1177/0267323114521045

Standards National Institute of & Technology. (2017). *Digital Identity Guidelines: NIST SP 63a*. CreateSpace Independent Publishing Platform.

Scheibe, M., Skutsch, M., & Schofer, J. (2002). IV. C. Experiments in Delphi methodology. *The Delphi method: Techniques and applications*, 257-281.

Shen, L. W., Mammi, H. K., & Din, M. M. (2021). *Cyber Security Awareness Game (CSAG) for Secondary School Students*. *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Bandung, Indonesia, 2021, 48-53. https://doi.org/10.1109/ICoDSA53588.2021.9617548

Tanrikulu, I., & Erdur-Baker, Ö. (2019). Motives Behind Cyberbullying Perpetration: A Test of Uses and Gratifications Theory. *Journal of Interpersonal Violence*, *36*(13-14), https://doi.org/10.1177/0886260518819882

Toledo, W., Louis, S. J., & Sengupta, S. (2022, October 1). *NetDefense: A Tower Defense Cybersecurity Game for Middle and High School Students*. *2022 IEEE Frontiers in Education Conference (FIE)*, Uppsala, Sweden, 2022, 1-6. https://doi.org/10.1109/FIE56618.2022.9962410

Vinayakumar, R., Soman, K. P., & Menon, P. (2018, July 1). *Digital Storytelling Using Scratch: Engaging Children Towards Digital Storytelling*. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, 2018, 1-6. https://doi.org/10.1109/ICCCNT.2018.8493941

Weeden, S., Cooke, B., & McVey, M. (2013). Underage Children and Social Networking. *Journal of Research on Technology in Education*, *45*(3), 249–262. https://doi.org/10.1080/15391523.2013.10782605

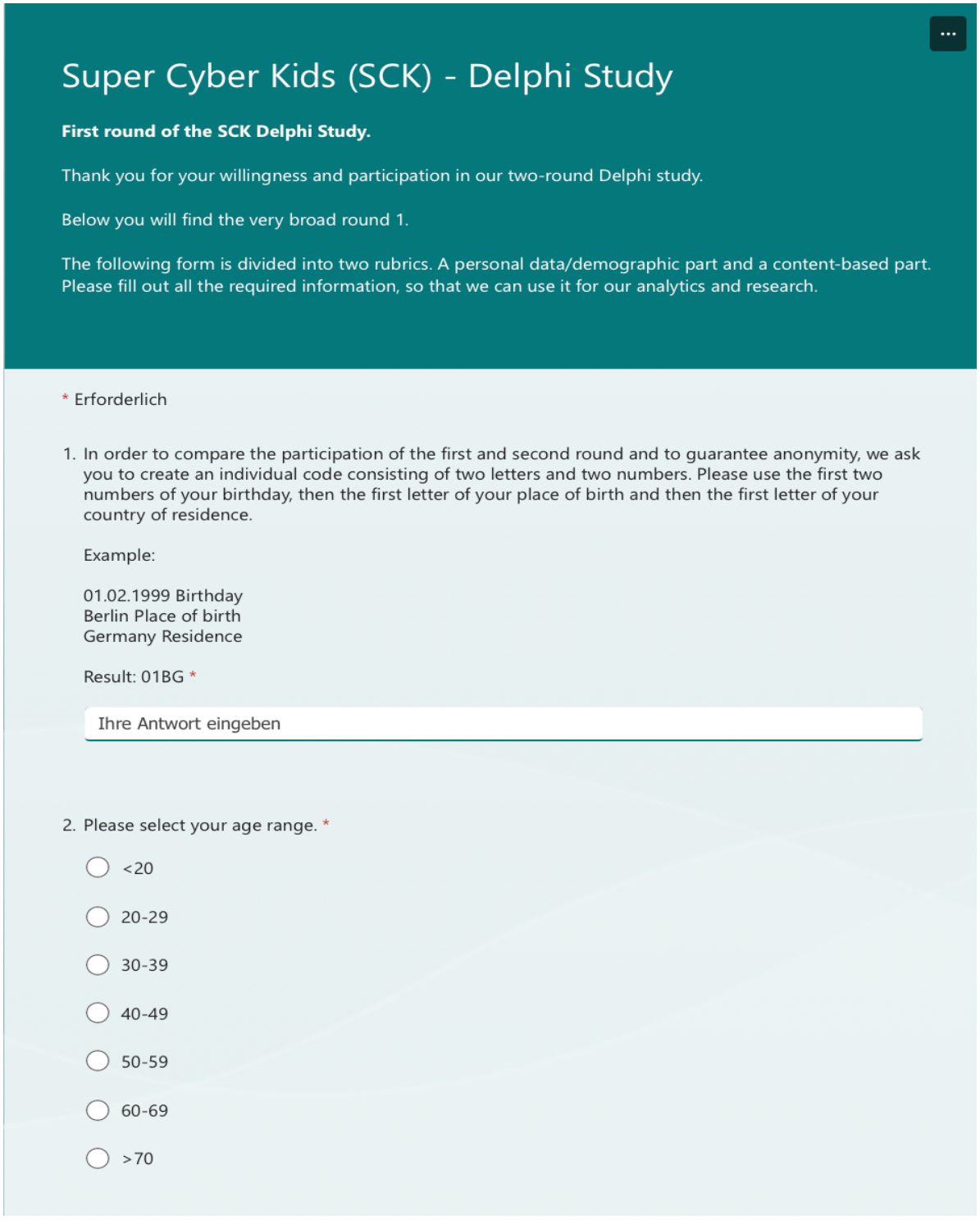
Wishart, J. M., Oades, C. E., & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education*, *48*(3), 460–473. https://doi.org/10.1016/j.compedu.2005.03.003

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

Yu, W. D., Gole, M., Prabhuswamy, N., Prakash, S., & Shankaramurthy, V. G. (2016). An Approach to Design and Analyze the Framework for Preventing Cyberbullying. *2016 IEEE International Conference on Services Computing (SCC)*, 864-867. https://doi.org/10.1109/scc.2016.125

1.3 SURVEY FORM - Delphi Study

1.2.1 Round 1



Super Cyber Kids (SCK) - Delphi Study

First round of the SCK Delphi Study.

Thank you for your willingness and participation in our two-round Delphi study.

Below you will find the very broad round 1.

The following form is divided into two rubrics. A personal data/demographic part and a content-based part. Please fill out all the required information, so that we can use it for our analytics and research.

* Erforderlich

1. In order to compare the participation of the first and second round and to guarantee anonymity, we ask you to create an individual code consisting of two letters and two numbers. Please use the first two numbers of your birthday, then the first letter of your place of birth and then the first letter of your country of residence.

   Example:

   01.02.1999 Birthday
   Berlin Place of birth
   Germany Residence

   Result: 01BG *

   Ihre Antwort eingeben

2. Please select your age range. *

   - <20
   - 20-29
   - 30-39
   - 40-49
   - 50-59
   - 60-69
   - >70

3. What is your gender? *

- ◯ Male
- ◯ Female
- ◯ Prefer not to say
- ◯ Sonstiges

4. What is your highest educational qualification? *

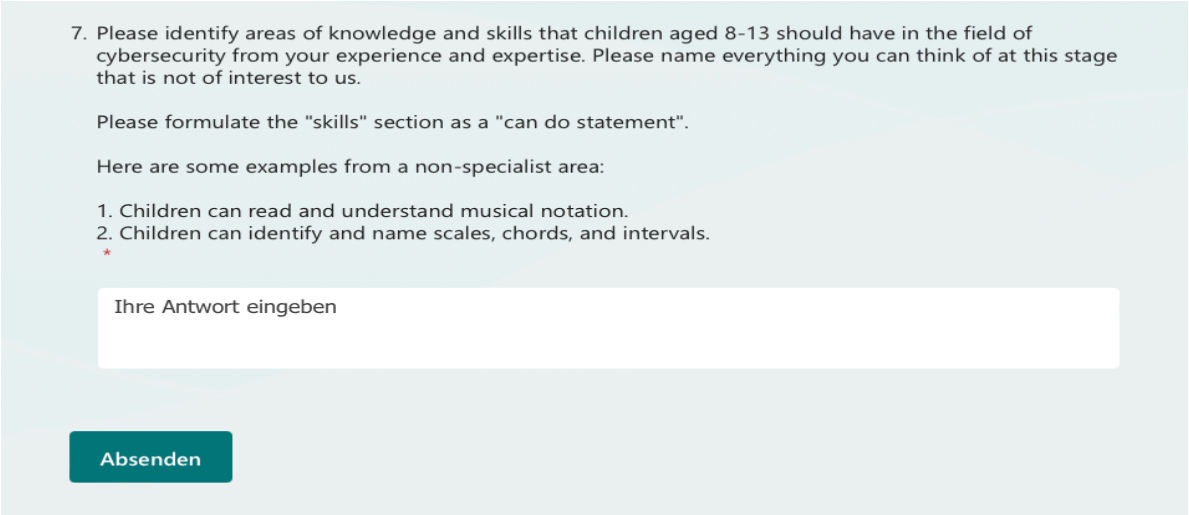
- ◯ No educational qualification
- ◯ Secondary school
- ◯ A-levels
- ◯ University degree
- ◯ Apprenticeship
- ◯ Doctoral degree

5. What is your area of expertise? *

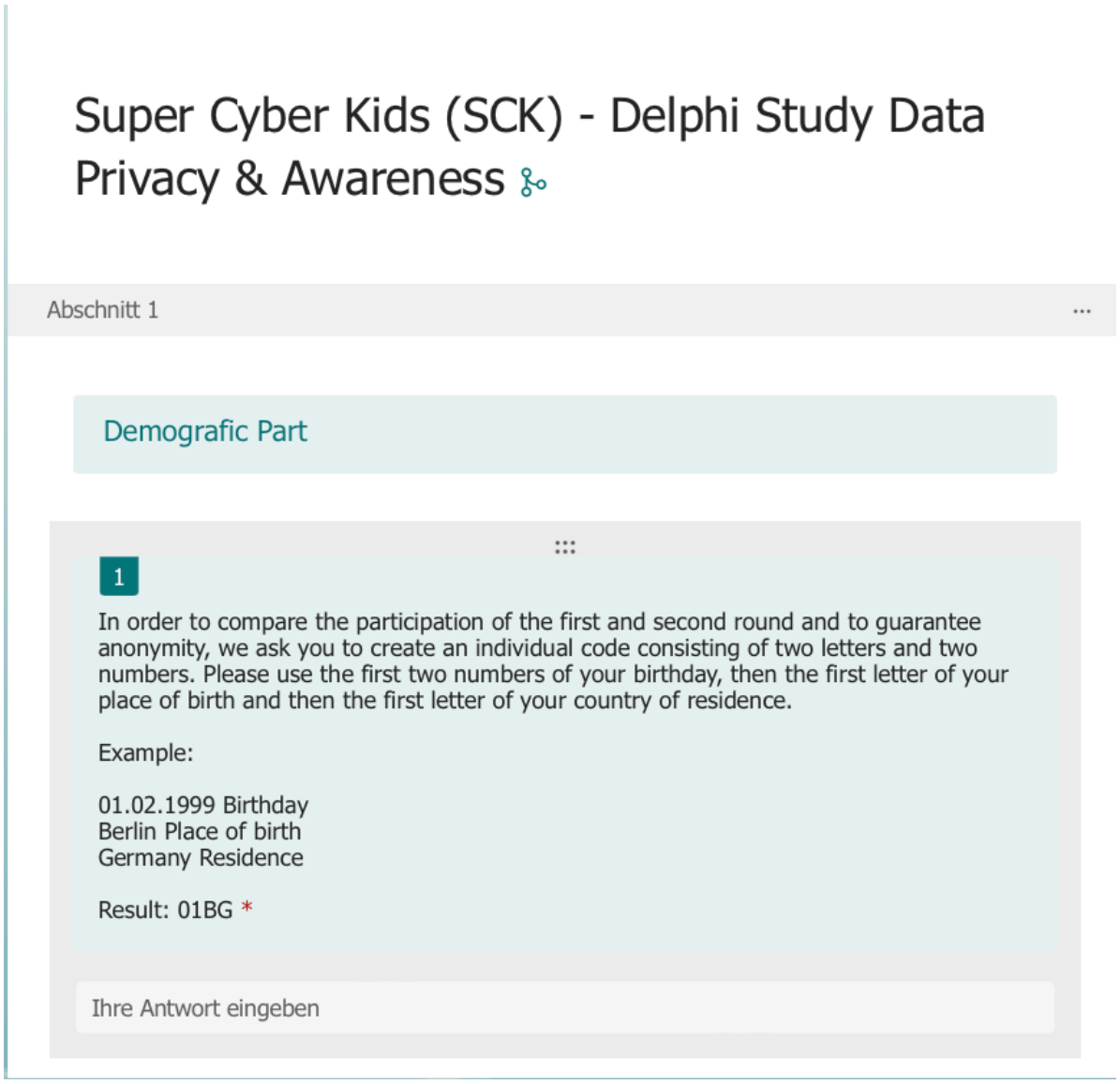
- ◯ Education
- ◯ Cybersecurity
- ◯ Cybersecurity education
- ◯ Sonstiges

6. How many years of expertise do you have in the mentioned area above? *

Ihre Antwort eingeben


7. Please identify areas of knowledge and skills that children aged 8-13 should have in the field of cybersecurity from your experience and expertise. Please name everything you can think of at this stage that is not of interest to us.
Please formulate the "skills" section as a "can do statement".
Here are some examples from a non-specialist area:
1. Children can read and understand musical notation.
2. Children can identify and name scales, chords, and intervals.
*
Ihre Antwort eingeben
Absenden

1.2.2 Round 2


Super Cyber Kids (SCK) - Delphi Study Data Privacy & Awareness
Abschnitt 1
Demografic Part
1
In order to compare the participation of the first and second round and to guarantee anonymity, we ask you to create an individual code consisting of two letters and two numbers. Please use the first two numbers of your birthday, then the first letter of your place of birth and then the first letter of your country of residence.
Example:
01.02.1999 Birthday
Berlin Place of birth
Germany Residence
Result: 01BG *
Ihre Antwort eingeben

Abschnitt 2 ...

Content Part

Below is a brief explanation of how the dimensions were created. You will then be asked to validate each of the 5 fields of the matrix-based framework.

It may be that some fields do not contain any content, if this is the case it is because no skills could be assigned in the scientific literature, in the existing cybersecurity games and in the first Delphi round.

In the cover picture of the section, you will find the dimensions and the categories.

The dimensions Identify, Protect, Detect, Respond and Recover have been taken from the NIST Cybersecurity Framework and then adapted to the age group (8-13-year-olds). The categories in our framework are understood taxonomically. For example, general knowledge is classified in the Identify category. Whereas in the Detect category, application knowledge is required.

Here is a short definition of the categories:

Identify: This category is for basic knowledge and general knowledge about cybersecurity.

Protect: Skills and measures for protection in cyberspace should be classified in this category. Both technical and non-technical skills.

Detect: This category should include skills that children can use to recognize that they are affected by a cybersecurity problem.

Response: This category should include skills for responding to a security incident.

Recover: This component deals with recovery from a security incident.

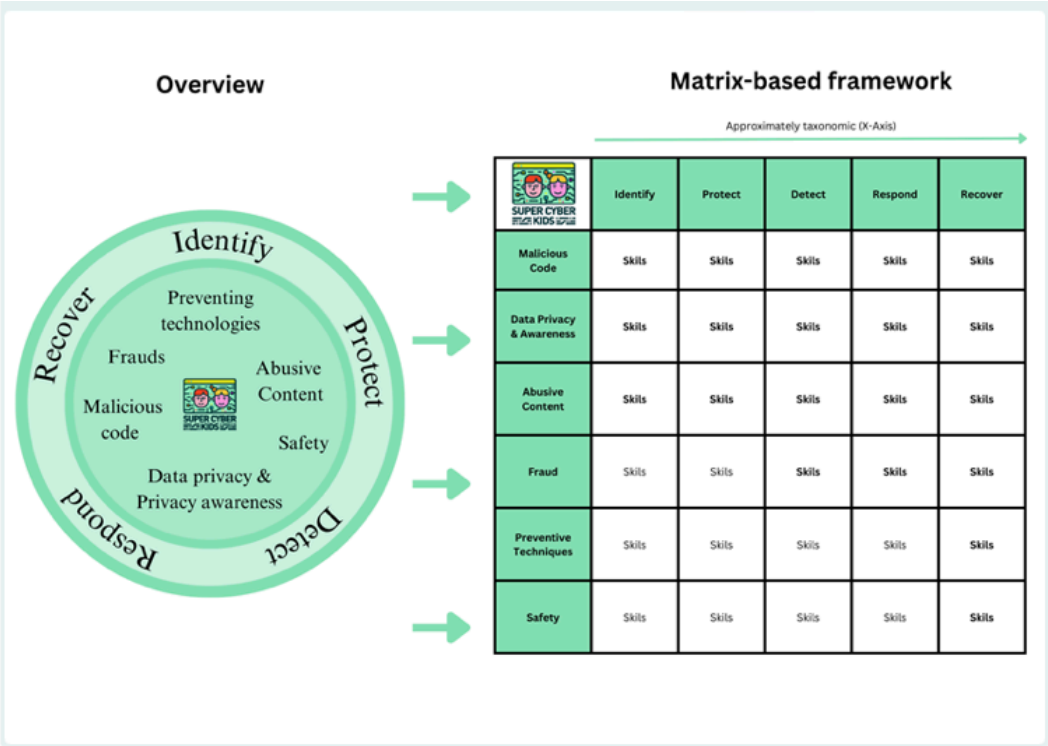
Here is a non-specialist example:

Children know that bacteria exist (Identify).
Children know not to sneeze into their hands but into their elbows (Protect).
Children can recognize unhygienic objects in everyday life, such as door handles in public buildings (Detect).
Children can wash their hands after contact with door handles (Respond).
Children can wash their hands after contact with door handles (Recovery).

For the original version of the NIST framework, you are also welcome to read here:
https://www.nist.gov/cyberframework

In the matrix-based framework, the adapted categories of the NIST Cybersecurity Framework represent the X-axis.

On the Y-axis are categories identified from the scientific literature and existing frameworks (Malicious Code, Data Privacy & Awareness, Fraud, Preventive Techniques, Abusive Content, Security).
Here, the skills are classified in a matrix-based manner.


Overview
Identify
Protect
Detect
Respond
Recover
Preventing technologies
Frauds
Abusive Content
Malicious code
Safety
Data privacy & Privacy awareness
Matrix-based framework
Approximately taxonomic (X-Axis)
Identify
Protect
Detect
Respond
Recover
Malicious Code
Data Privacy & Awareness
Abusive Content
Fraud
Preventive Techniques
Safety
Skils

2

We are in the dimesion Identify and Data Privacy & Data Awareness section.

Kids should know...

... personal data protection.
... to keep private data safe.
... the consequences of exposing personal data.
... that passwords can help to protect computer files and information.
... concept of online privacy and that there are different levels of privacy.
... what possible happens when then post a comment in a social media app.
... how to authenticate.
... the basics of an individual account in an app.
... security risks when streaming.
... that a person can be identified by knowing only a few pieces of information about them, and that they must therefore be careful about what information they provide online.
... recognise what forms 'personal information' can take.
... to identify different types of personal information that may be elicited in the online environment.
... some of the techniques that are used in the online environment to elicit their personal information.
... to demonstrate an awareness of why it may be unwise to disclose their personal details online.
... about disclosure of personal information and commercial exploitation.
... to understand and respect their own rights and those of others regarding private information.
... what personal information and safety procedures are.
... how to classify personal data.
... not post their location online.
... the concept of privacy of personal data of third parties.
... the concept of digital footprints.
... that when they post something on the internet it can't ever truly be deleted.
... the security issues caused by social media usage.
... to be aware of privacy settings and what they entail.
... that someone they don't know can send them a private message or direct message.
... their rights (e.g. on their own picture)
... what information they can share.
... the concept of copyright.
... how copyright relates to fair use.
... examples of how fair use can help protect an author/creator's rights while promoting the sharing of ideas.
... that illicit downloading of copyrighted.
... that downloading copyrighted materials e.g. music and films can be risky.
... about sharing and authoring rights

Do you find the extracted skills adequate and complete?

3

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

4

We are in the dimension Protect and Data Privacy & Data Awareness section.

Kids should be able...

... to handle their own personal data responsibly.
... to create User-Account (e.g. Guest-Account).
... to distinguish between private and public information. By discussing grade-appropriate examples of privacy and what is OK to share about themselves and how that relates to confidentiality.
... to be aware of creating privacy settings for minimizing SNS risks, and assessing other online risks or cyberbullying.
... to not give out personal data and information.
... to use a different password for social media and school accounts.
... to not share school passwords with classmates.
... to regularly check the privacy settings of their social media accounts.
... to not post everything on the internet.
... to be aware of online privacy and the levels of privacy.
... to use passwords.
... to update their computer, when a warning from the computer appears.
... to use online storage systems to exchange and keep personal or sensitive information.
... to use strategies for downloading suspicious attachments.
... to distinguish which data to share/provide online or not.
... to check privacy- and chat settings to be safe during gaming.
... to handle privacy settings to avoid online enticement and sextortion.
... to use the privacy settings in SNS for reporting, blocking and saving their data.
... to demonstrate an awareness of why it may be unwise to disclose their personal details online.
... to clean their browser cache.
... to set privacy settings.
... to decide whether posting information is OK or not.
... to manage their online profiles (e.g. privacy)
... to not tell or give any private or personal information about themselves or others to strangers.

... to destroy/erase information and protect data appropriately.
... to use online privacy settings as a preventive coping strategy because it may decrease the likelihood of being cyberbullied in the future. Privacy settings allow social media users to limit who can access the content they share online (e.g., pictures, comments, personal information).
... to understand what happens when post a comment in a social media app.
... to limit visibility of posts and comments.
... to limit visibility of personal information.
... to decide whether to give out personal data without permission from their parents.
... to react if a stranger is asking them for personal information.
... to protect their personal data in an online context.
... to decide whether it is OK to post their location online or not.
... to recognize and use a pseudonym in the online discussion forum to secure their personal data in an appropriate way.
... to use personal password-protected accounts.
... to protect their digital identity by knowing where and what information to share online and what not to share.

Do you find the extracted skills adequate and complete?

- ○ Yes
- ○ No

5

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

6

We are in the dimension Detect and Data Privacy & Data Awareness section.

Kids should be able...

... to recognize when websites, apps, programs or e-mails ask for personal data that should not be given out.
... examples of how copyright can be equated to ownership and other ideas, such as "Who wrote the document," "Anything I create that is new to the world is mine," and "I need to give credit to any content NOT created by me."

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

7

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

8

We are in the dimension Respond and Data Privacy & Data Awareness section.

Kids should...

... cope with negative experiences.
... understand how to destroy/erase information and protect their data appropriately.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

9

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

10

We are in the dimension Respond and Data Privacy & Data Awareness section.

Kids should...

... know to react if they already sent out an inappropriate picture.
... know how they might help others who are feeling sad or upset because of online threats.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

11

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

12

Any other comments?

Ihre Antwort eingeben

Super Cyber Kids (SCK) - Delphi Study Malicious code

Dear participant,

Thank you for taking part in the second and thus also the last round of the study!

The round will take about 30-45 minutes.

Please fill in all the fields. The second round will again consist of two sections, a demographic section and a content section. If you have already participated in round one, you will automatically be redirected to question 7.

The aim is to validate the Cybersecurity skills from the scientific literature, existing cybersecurity games and your answers from round 1. (Target group: 8-13-years old)

We have classified the skills into a framework. This is briefly presented and explained in the content section. If you have any questions, please do not hesitate to contact Nicolai Plintz (nicolai.plintz@uni-mannheim.de).

Thank you for your participation in advance!

Abschnitt 1 ...

1

Did you participate in the first round?

- ○ I participated in the first round.
- ○ I did not participate in the first round.

2

Please select your age range.

- ◯ <20
- ◯ 20-29
- ◯ 30-39
- ◯ 40-49
- ◯ 50-59
- ◯ 60-69
- ◯ >70

3

What is your gender?

- ◯ Male
- ◯ Female
- ◯ Prefer not to say
- ◯ Sonstiges

4

What is your highest educational qualification?

- ◯ Apprenticeship
- ◯ A-levels
- ◯ Doctoral degree
- ◯ No educational qualification
- ◯ Secondary school
- ◯ University degree

5

What is your area of expertise?

- ◯ Cybersecurity
- ◯ Education
- ◯ Cybersecurity education

6

How many years of expertise do you have in the mentioned area above?

Ihre Antwort eingeben

7

In order to compare the participation of the first and second round and to guarantee anonymity, we ask you to create an individual code consisting of two letters and two numbers. Please use the first two numbers of your birthday, then the first letter of your place of birth and then the first letter of your country of residence.

Example:

01.02.1999 Birthday
Berlin Place of birth
Germany Residence

Result: 01BG

Ihre Antwort eingeben

Abschnitt 2 ...

Content part

Below is a brief explanation of how the dimensions were created. You will then be asked to validate each of the 30 fields of the matrix-based framework.

It may be that some fields do not contain any content, if this is the case it is because no skills could be assigned in the scientific literature, in the existing cybersecurity games and in the first Delphi round.

In the cover picture of the section, you will find the dimensions and the categories.

The dimensions Identify, Protect, Detect, Respond and Recover have been taken from the NIST Cybersecurity Framework and then adapted to the age group (8-13-year-olds). The categories in our framework are understood taxonomically. For example, general knowledge is classified in the Identify category. Whereas in the Detect category, application knowledge is required.

Here is a short definition of the categories:

Identify: This category is for basic knowledge and general knowledge about cybersecurity.

Protect: Skills and measures for protection in cyberspace should be classified in this category. Both technical and non-technical skills.

Detect: This category should include skills that children can use to recognize that they are affected by a cybersecurity problem.

Response: This category should include skills for responding to a security incident.

Recover: This component deals with recovery from a security incident.

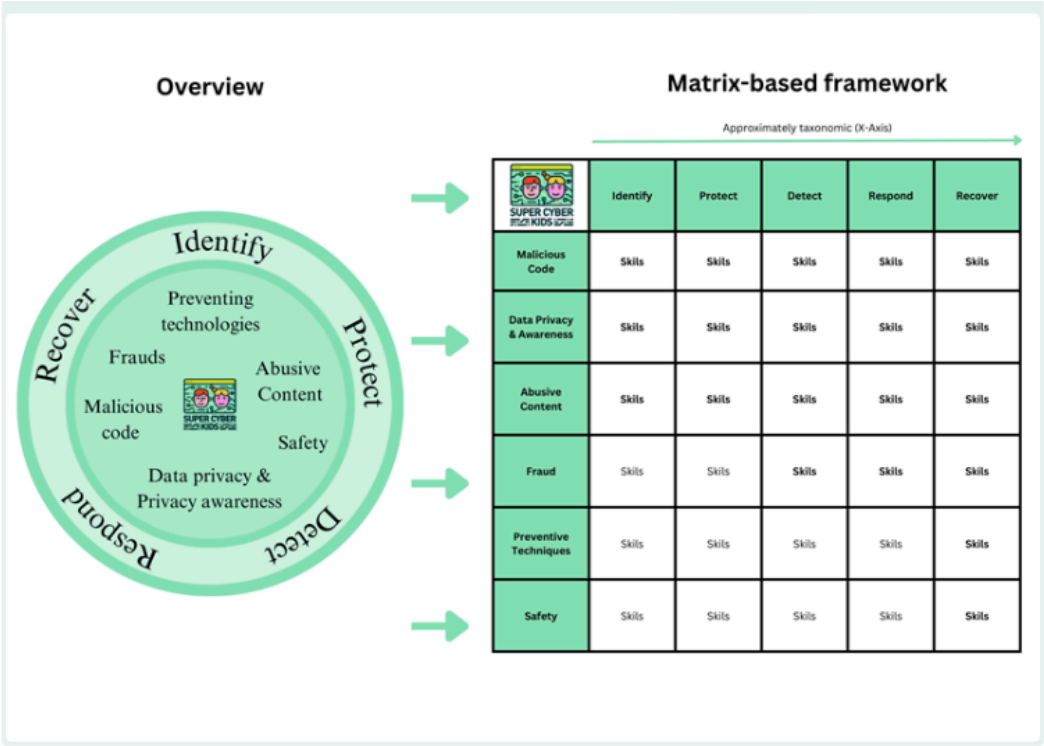
Here is a non-specialist example:

Children know that bacteria exist (Identify).
Children know not to sneeze into their hands but into their elbows (Protect).
Children can recognize unhygienic objects in everyday life, such as door handles in public buildings (Detect).
Children can decide whether it is necessary to wash their hands. (Respond).
Children can wash their hands after contact with door handles (Recovery).

For the original version of the NIST framework, you are also welcome to read here:
https://www.nist.gov/cyberframework

In the matrix-based framework, the adapted categories of the NIST Cybersecurity Framework represent the X-axis.

On the Y-axis are categories identified from the scientific literature and existing frameworks (Malicious Code, Data Privacy & Awareness, Fraud, Preventive Techniques, Abusive Content, Security).
Here, the skills are classified in a matrix-based manner.



8

We are in the dimension Identify and Malicious Code section.

Kids should know...
... that malware exists and that there are different types of it.
... that viruses exist.
... how hackers use viruses to damage important data and obtain private information.
... how a virus can reach your PC.
... that a file called a virus can make a computer stop working.
... that worms exist.
... packet sniffing exists.
... there is a danger of packet sniffers on unsecured wireless networks.
... that spyware exists.
... that loggers exists.
... to discuss examples of unsafe content such as popups and malicious links.
... the basic functionalities of the internet/computers.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

9

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

10

We are in the dimension Protect and Malicious Code section.

Kids should be able...

... to protect themselves from hackers or attackers, which can cause demage to important data and obtain private information. In this context kids should know how to guard themselves against such attacks by using safe passwords, antivirus software and encryption.
... to avoid viruses by deleting supsious mails from the pc and use an anti-virus program.
... to protect themselves against malware.
... to avoid being hacked.
... to recognize unsecured wifi.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

11

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

12

We are in the dimension Detect and Malicious Code section.

Kids should know...

... to spot signs of cyber attacks.
... if a website is authentificated or not.
... to recognize different forms of cyberattacks and cybercrime.
... how hacker can use packet sniffers to snoop on peoples internet traffic in public spaces.
... to identify when a network connection is secure or not (HTTPS).
... to discuss examples of unsafe content, such as popups and malicious links.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

13

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

14

We are in the dimension Respond and Malicious Code section.

Kids should...

... know to report cyber crime.
... able to respond to potential threats online.
... know basic attacks that they might be victims of and what to do, specifically who turn to.
... be aware of predators online and should know who to turn to for help.
...know who they should contact and how to react to cyberattacks and cybercrime.
... know basic attacks that they might be victims of and what to do, specifically who to turn to.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

15

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

16

We are in the dimension Recover and Malicious Code section.

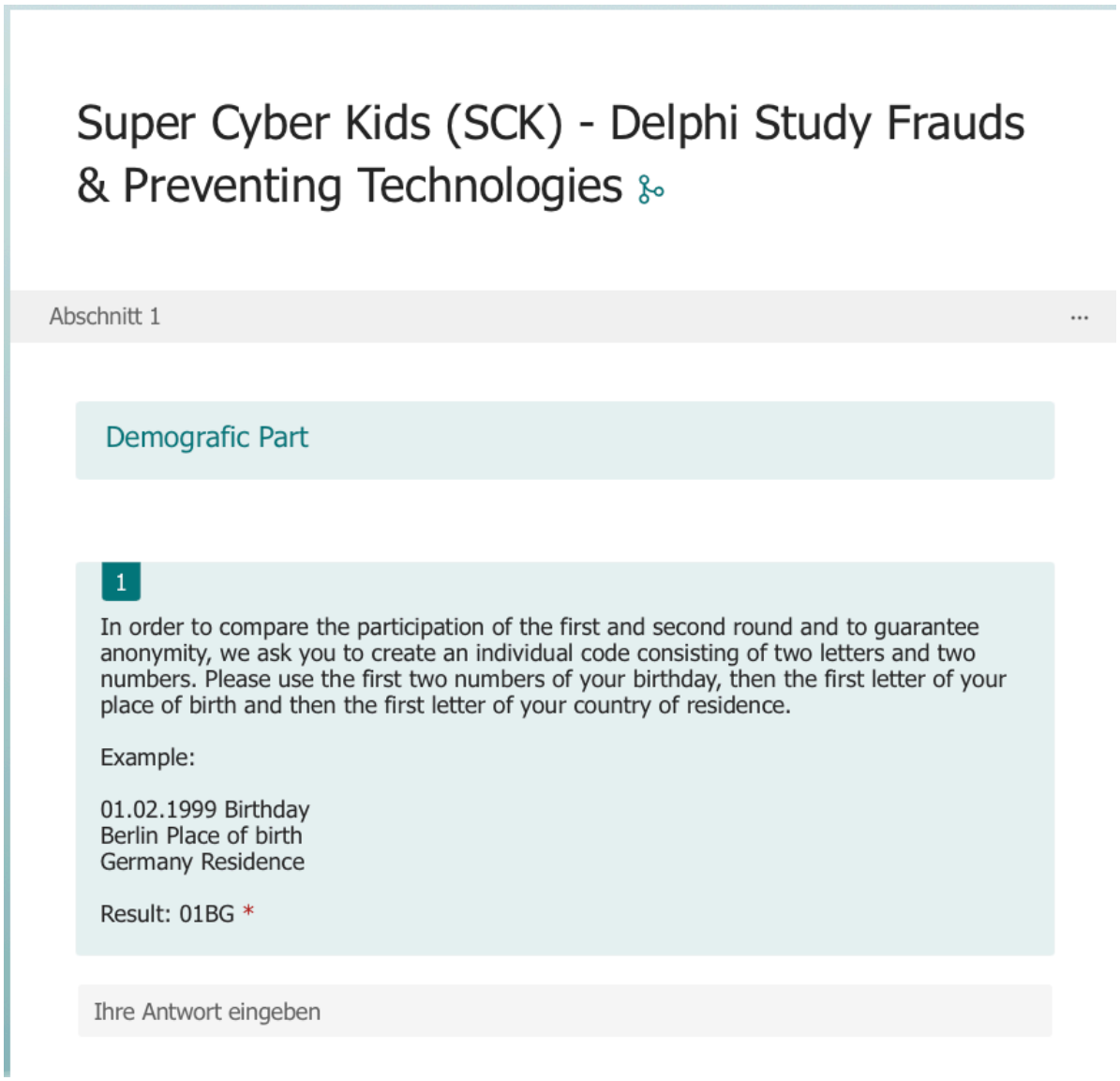
... be able to accept negative online experience.
... Children can restore files after a cyber attack through a backup.

- ◯ Yes
- ◯ No

17

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben



Super Cyber Kids (SCK) - Delphi Study Frauds & Preventing Technologies

Abschnitt 1

Demografic Part

1

In order to compare the participation of the first and second round and to guarantee anonymity, we ask you to create an individual code consisting of two letters and two numbers. Please use the first two numbers of your birthday, then the first letter of your place of birth and then the first letter of your country of residence.

Example:

01.02.1999 Birthday
Berlin Place of birth
Germany Residence

Result: 01BG *

Ihre Antwort eingeben

Abschnitt 2 ...

Content Part

Below is a brief explanation of how the dimensions were created. You will then be asked to validate each of the 5 fields of the matrix-based framework.

It may be that some fields do not contain any content, if this is the case it is because no skills could be assigned in the scientific literature, in the existing cybersecurity games and in the first Delphi round.

In the cover picture of the section, you will find the dimensions and the categories.

The dimensions Identify, Protect, Detect, Respond and Recover have been taken from the NIST Cybersecurity Framework and then adapted to the age group (8-13-year-olds). The categories in our framework are understood taxonomically. For example, general knowledge is classified in the Identify category. Whereas in the Detect category, application knowledge is required.

Here is a short definition of the categories:

Identify: This category is for basic knowledge and general knowledge about cybersecurity.

Protect: Skills and measures for protection in cyberspace should be classified in this category. Both technical and non-technical skills.

Detect: This category should include skills that children can use to recognize that they are affected by a cybersecurity problem.

Response: This category should include skills for responding to a security incident.

Recover: This component deals with recovery from a security incident.

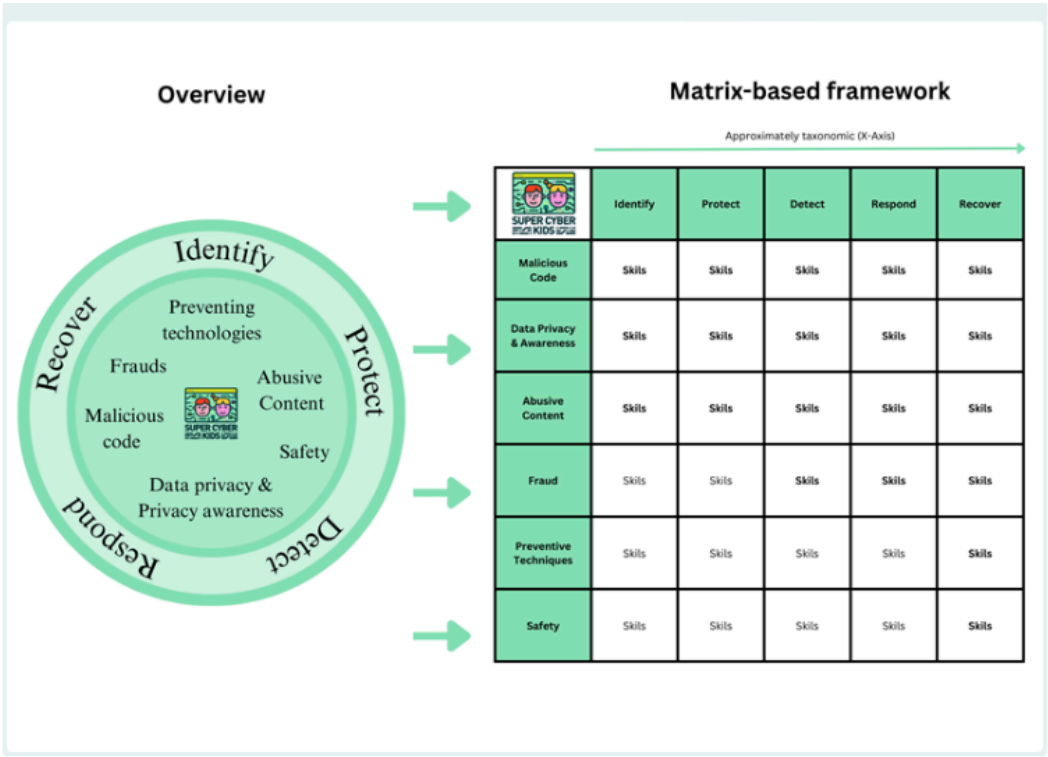
Here is a non-specialist example:

Children know that bacteria exist (Identify).
Children know not to sneeze into their hands but into their elbows (Protect).
Children can recognize unhygienic objects in everyday life, such as door handles in public buildings (Detect).
Children can decide whether it is necessary to wash their hands. (Respond).
Children can wash their hands after contact with door handles (Recovery).

For the original version of the NIST framework, you are also welcome to read here:
https://www.nist.gov/cyberframework

In the matrix-based framework, the adapted categories of the NIST Cybersecurity Framework represent the X-axis.

On the Y-axis are categories identified from the scientific literature and existing frameworks (Malicious Code, Data Privacy & Awareness, Fraud, Preventive Techniques, Abusive Content, Security).
Here, the skills are classified in a matrix-based manner.



2

We are in the dimesion Identify and Frauds section.

Kids should know...

... to be aware of phishing and what it entails.
... the basics of social engineering attacks.
... that email phishing attacks are possible.
... to be aware of pharming and what it entails.
... that grooming exists.
... the meaning of grooming.
... that using communication technologies can lead to sexual assault and/or child prostitution.
... to be aware of loggers and what they entail.
... to be aware of botnets and what it entails.
... to be aware of scams (commercial and financial) and what they entail.
... to be aware of identity theft and what it entails.
... to be aware of online predators and what this entails.
... to be aware of spoofing and what it entails.

Do you find the extracted skills adequate and complete?

- ○ Yes
- ○ No

3

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

4

We are in the dimension Protect and Frauds section.

Kids should be able...

... to maintain integrity and confidentiality against web tracking & phishing.
... to check the security information/certification of online payments.
... create a safe password to avoid phishing attacks.
... to not click on links in emails if they come from strangers.
... to know not to open email attachments if the sender is unknown to them.
... to change settings on their phone to prevent autoconnection to insecure wireless networks.
... to use strategies for downloading suspicious attachments.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

5

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

6

We are in the dimension Detect and Frauds section.

Kids should be able...

... to evaluate the trustworthiness of others they communicate with.
... to recognize if a website is safe to register.
... to identify cyber grooming attempts.
... to decide whether or not to pay.
... how to identify unsafe content online.
... how to recognize a phishing email.
... how to detect online enticement and sextortion by discussing online manipulation.
... the different feelings they may experience when dealing with someone untrustworthy.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

7

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

8

We are in the dimension Respond and Frauds section.

Kids should...

... able to report an impostor.
... able to report cyber attacks.
... able to respond to grooming.
... know that they should change their password after a phishing attack.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

9

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

10

We are in the dimension Recover and Frauds section.

Kids should...

... able to change passwords after they have fallen victim to a scam.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

11

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

12

We are in the dimesion Identify and Preventive techniques.

Kids should know...

... to use passwords.
... to point out secure use of technology (passwords to antivirus)
... ways of enhancing security (e.g. secure passwords, not clicking links).
... security software.
... to be aware of networks and what they entail.
... to be aware of cryptography and how it can be used.
... to be aware of firewalls.
... what a strong password is.
... the dangers of weak passwords.
... that passwords can help protect computer files and information.
... about child-appropriated web browsers and SNS.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

13

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

14

We are in the dimension Protect and Preventive techniques section.

Kids should be able...

... to use and install security software/antiantivirus software.
... to use passwords.
... choose strong passwords.
... to protect their devices mobile and computers.
... distinguish wifi's.
... to secure data on the internet by using secure password creation, hashing and authentication.
... to protect themselves from hackers or attackers, which like to cause damage to important data and obtain private information. In this context, kids should know how to guard themselves against such attacks by using safe passwords, antivirus software and encryption.
... to protect systems from attacks by using encryption techniques.
... to make backups and know the importance of backups.
... how to create a safe password by using use a combination of letters, numbers, and symbols in their school passwords.
... to use online storage systems to exchange and keep personal or sensitive information.
... to know the effects of disabling the anti-virus system.
... to understand the basics of computer networks.
... to understand the important terms of password management.
... to avoid viruses by deleting suspicious mail from their PC and using an anti-virus system.
... to back up their data regularly.
... to use e-safety applications for kids.
... to keep their passwords a secret.
... to block other cyber users.
... to take steps to prevent their PCs or other devices from being hacked (such as setting strong passwords).
... to protect themselfe by using multi factor authentication (MFA).

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

15

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

16

We are in the dimension Detect and Preventive techniques section.

Kids should be able...

... to update security software.
... to decide if a website is authenticated or not.
... how to identifiy a potentially problematic domain by scanning network protocols.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

17

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

18

We are in the dimension Respond and Preventive techniques section.

Kids should...

... know that there is a reporting function for almost all problems.
... know that they should change their password after a phishing-/cyberattack.
... be able to change passwords on their tablets/mobile phones easily.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

19

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

20

We are in the dimension Recover and Preventive techniques section.

Kids should...

... know that they should change their password after a phishing-/cyberattack.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

19

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

20

We are in the dimension Recover and Preventive techniques section.

Kids should...

... know that they should change their password after a phishing-/cyberattack.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

21

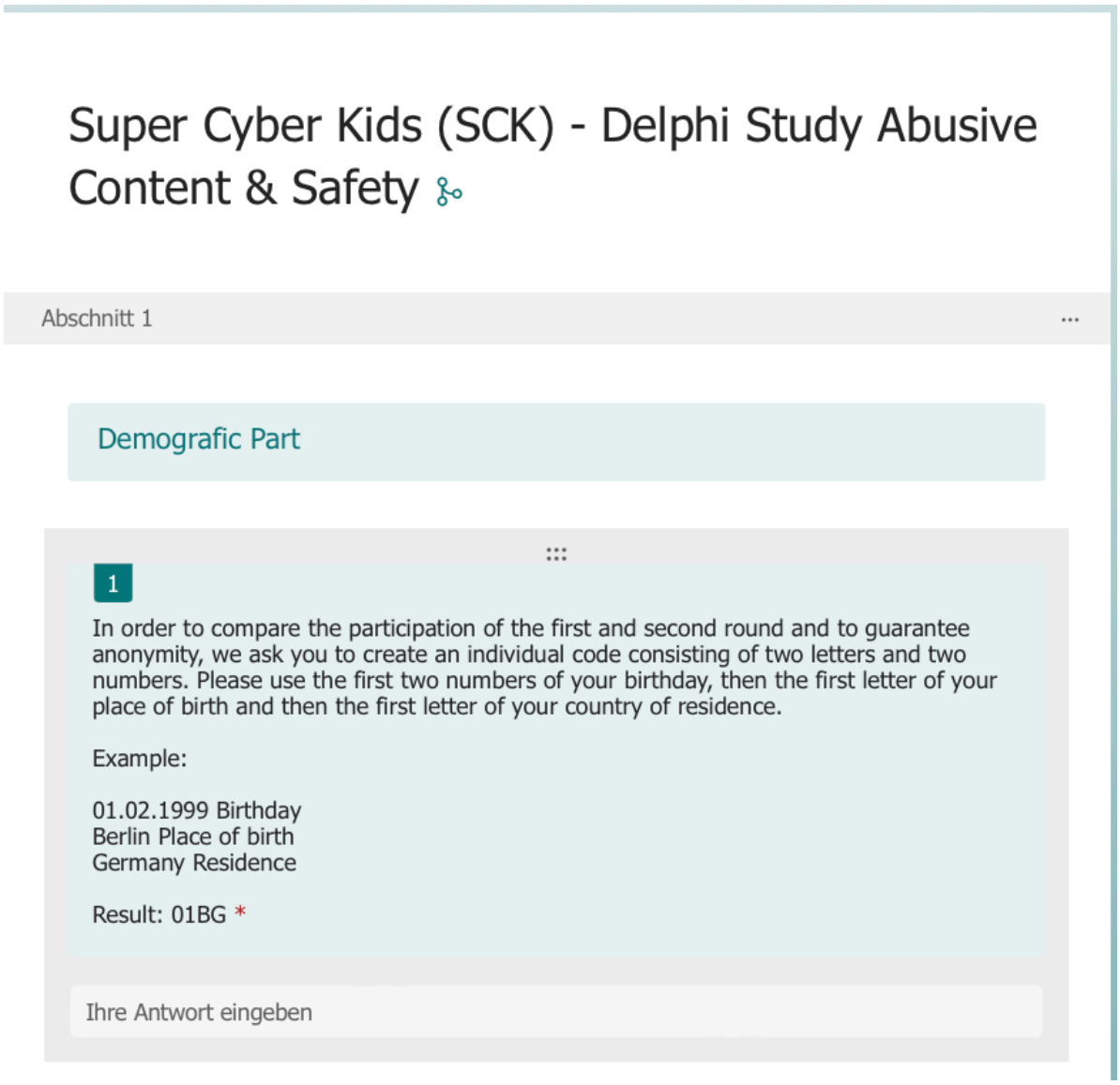
If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

22

Any other comments?

Ihre Antwort eingeben


Super Cyber Kids (SCK) - Delphi Study Abusive Content & Safety
Abschnitt 1
Demografic Part
1
In order to compare the participation of the first and second round and to guarantee anonymity, we ask you to create an individual code consisting of two letters and two numbers. Please use the first two numbers of your birthday, then the first letter of your place of birth and then the first letter of your country of residence.
Example:
01.02.1999 Birthday
Berlin Place of birth
Germany Residence
Result: 01BG *
Ihre Antwort eingeben

Abschnitt 2 ...

Content Part

Below is a brief explanation of how the dimensions were created. You will then be asked to validate each of the 5 fields of the matrix-based framework.

It may be that some fields do not contain any content, if this is the case it is because no skills could be assigned in the scientific literature, in the existing cybersecurity games and in the first Delphi round.

In the cover picture of the section, you will find the dimensions and the categories.

The dimensions Identify, Protect, Detect, Respond and Recover have been taken from the NIST Cybersecurity Framework and then adapted to the age group (8-13-year-olds). The categories in our framework are understood taxonomically. For example, general knowledge is classified in the Identify category. Whereas in the Detect category, application knowledge is required.

Here is a short definition of the categories:

Identify: This category is for basic knowledge and general knowledge about cybersecurity.

Protect: Skills and measures for protection in cyberspace should be classified in this category. Both technical and non-technical skills.

Detect: This category should include skills that children can use to recognize that they are affected by a cybersecurity problem.

Response: This category should include skills for responding to a security incident.

Recover: This component deals with recovery from a security incident.

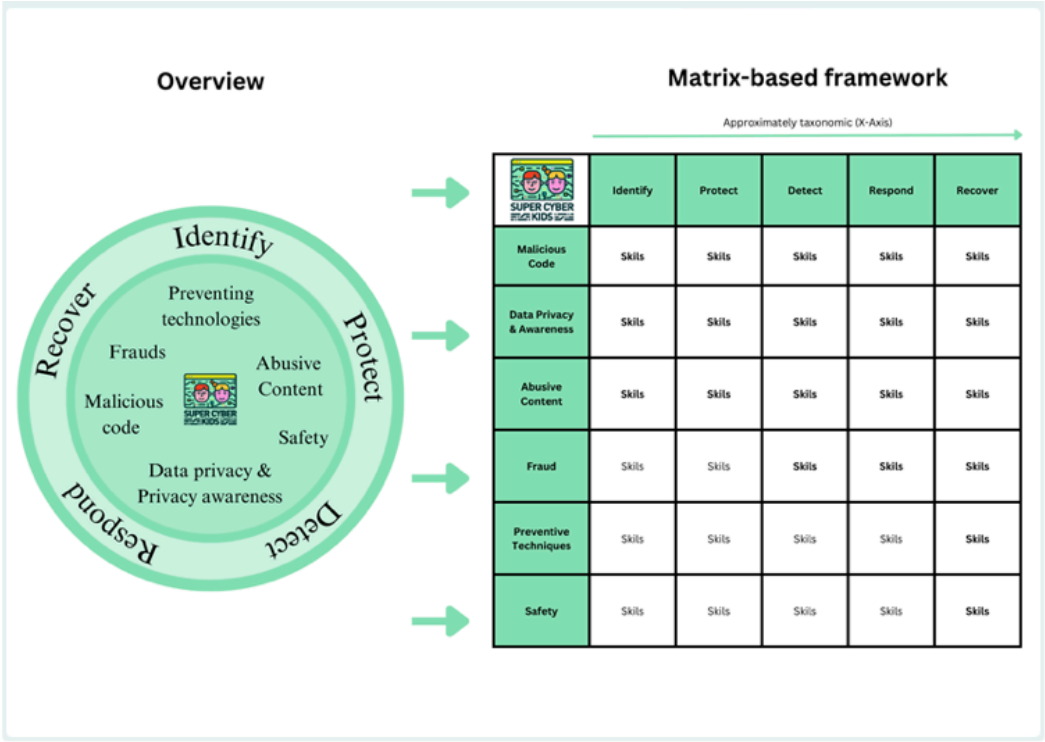
Here is a non-specialist example:

Children know that bacteria exist (Identify).
Children know not to sneeze into their hands but into their elbows (Protect).
Children can recognize unhygienic objects in everyday life, such as door handles in public buildings (Detect).
Children can decide whether it is necessary to wash their hands. (Respond).
Children can wash their hands after contact with door handles (Recovery).

For the original version of the NIST framework, you are also welcome to read here:
https://www.nist.gov/cyberframework

In the matrix-based framework, the adapted categories of the NIST Cybersecurity Framework represent the X-axis.

On the Y-axis are categories identified from the scientific literature and existing frameworks (Malicious Code, Data Privacy & Awareness, Fraud, Preventive Techniques, Abusive Content, Security).
Here, the skills are classified in a matrix-based manner.



2

We are in the dimesion Identify and Abusive Content.

Kids should know...

... that inappropriate content could appear online.
... that intolerant content could appear online.
... that hate speech could appear online.
... that violent content could appear online.
... that illegal materials such as images of child abuse could appear online.
... of online gambling services.
... that pornographic content exists online.
... that sexual or harmful content exists online.
... that false & untrue content exists online as well as fake news.
... that bullying via websites, mobile phones or other forms of communication devices is possible.
... that chatrooms on the internet can be an unsafe place.
... that downloading data, like music from unlicensed sources can be dangerous.
... that a stranger can ask them for personal information.
... the meaning of grooming.
... using communication technologies can lead to sexual assault and/or child prostitution.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

3

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

4

We are in the dimension Protect and Abusive Content section.

Kids should be able...

... to classify age-appropriate websites (by adapting the knowledge of the parent's "What is a child-friendly website").
... to create online content safely.
... to decide if a website is age-appropriate.
... to self-protect on an individual level in an online environment. (Ignore or retreat to other media)
... to decide whether a website is safe or suspicious.
... to avoid dangerous chats and internet sites entirely.
... to use appropriate privacy settings to minimize SNS risks, asses other online risks or recognize cyberbullying.
... to assess the security of websites before entering information.
... to handle privacy settings to avoid online enticement and sextortion.
... to identify "Red Flags" and malicious intentions of strangers in the field of online enticement & sextortion.
... to keep their password a secret, safe and strong.
... to ask teachers for guidance when deciding whether a website is age appropriate or not.
... to decide if they should respond in cyberspace or not.
... to decide if you can believe a piece of information in cyberspace or not.
... to recognize and avoid inappropriate material (such as illegal or pornographic content).
... to use strategies to prevent cyberbullying.

Do you find the extracted skills adequate and complete?

- ○ Yes
- ○ No

5

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

6

We are in the dimension Detect and Abusive Content section.

Kids should be able...

... to recognize inappropriate and harmful media content.
... to identify safe and not safe internet sources.
... to identify unsafe content online.
... to recognize a phishing website.
... to detect online enticement and sextortion by discussing online manipulation.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

7

We are in the dimension Respond and Abusive Content section.

Kids should...

... be able to open up to others about negative things they see/experience in digital environments.
... know what to do when they run into problematic content. Whom to turn to and where to report it. For example, when they run into porn or extreme violence.
... know to report the situation or the person if they feel unsafe.
... know that if they experience something strange online, they share this with a trusted adult (parents/teacher/etc.).
... learn age-appropriate intervention against cyberbullying by discussions focused on age-appropriate intervention.
... know examples of cyberbullying and what to do when someone is mean online, and what behavior should be modeled when online.
... know age-appropriate responses to cyberbullying.
... report users after they have a negative experience with them.
... know to deal with online sexual harassment.
... know to respond to grooming.
... know that they should seek help from a trusted adult if they are being bullied.
... report individuals that are cyberbullying.
... respond to cyberbullying by talking to adults.
... know strategies for responding appropriately to cyberbullying and all kinds of abusive online dangers.
... should know how to handle if someone treats them in a nasty or harmful way.
... know how they should react if they receiving harmful or bullying messages (Reporting)
... know to report the situation or the person if they feel unsafe.
... know how to react if they see a website or post with inappropriate pictures (Sexual or harmful stuff).
... react appropriately when receiving inappropriate pictures.
... respond appropriately if someone harms or cyberbullies them on the internet (e.g. close the game/website and report)

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

8

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

9

We are in the dimension Recover and Abusive Content section.

Kids should...

... accept that negative online experience exists.
... know how they might help others who are feeling sad or upset because of online threats.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

10

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

11

We are in the dimesion Identify and Safety section.

Kids should know...

... right and wrong online behavior.
... the different motivations that influence right and wrong online behaviors.
... what it mean to use a "parent" credit card.
... the reality of payments that are conducted online.
... risks of internet use/digital environments.
... different forms and behaviors of harmful digital actions.
... that they should be nice and polite to other people on the internet.
... about the principle of online etiquette, upstander & bystander.
... how to treat others online.
... about inappropriate and bullying behaviors and consider how these impact the feelings of others.
... to consider the impact on others and society before acting.
... about computer and internet addiction, and health issues that come from the overuse of technology (physical, mental issues).
... what cybersecurity is.
... netiquette, online communication and collaboration.
... that not every sender of an email is trustworthy.
... how online actions have real-world consequences and that laws and regulations may also apply online.
... not to open frivolous email attachments if the sender is unknown to them.
... right and wrong uses of digital devices.
... not download every and any content.
... not to visit every website.
... that they should asses a website before opening it.
... to consider the negative consequences before posting something on social media.
... that there is danger in social networking.
... that nothing you post on the internet is really safe/secure.
... that people could be manipulative online.
... not to send abusive texts or emails.
... that teachers can help them to stay safe on the internet.
... to use the internet in a safe way. e.g. not chatting with strangers, not sending personal information and photos, and not meeting people whom they know only via the Internet.
... not to give personal information out.
... to anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person).
... to refrain from activities that harm their health (such as excessive smartphone use).
... what a bystander and an upstander in regards to cyberbullying are.
... the risks of SNS.
... how to protect their computer.
... about the prevention of cyberbullying.
... knowing the expression 'reporting'.

... the risks of SNS.
... how to protect their computer.
... about the prevention of cyberbullying.
... knowing the expression 'reporting'.
... what the following expression 'online predator'.
... the possible risks and the negative effects of the internet on their physical and psycho-social development.

Do you find the extracted skills adequate and complete?

- ○ Yes
- ○ No

12

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

13

We are in the dimension Protect and Safety section section.

Kids should be able...

... to protect themselves from harm on the internet.
... to browse safely and securely.
... be able to know basic cyber hygiene: behavior, how to communicate and how to take care of their devices and accounts.
... to decide whether a website is safe or suspicious.
... to make backups and know the importance of backups.
... to avoid dangerous chats and websites entirely.
... to not meet up with people from chatrooms.
... to not trust what people say on the internet.
... to not leave their laptop/iPad/mobile unlocked when they working in the classroom.
... to not click on links in emails, only if they come from someone they know.
... to assess the security of websites before entering information.
... to not open email attachments if the sender is unknown to them.
... to not post everything on the internet.
... to understand that downloading data like music from unlicensed sources can be dangerous.
... to identify situations in which it is wise to turn to a trusted adult for help.
... to understand that their emotions can be a powerful tool to help them assess unsafe situations.
... to identify some of the physical sensations that alert humans of unsafe situations.
... to anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person).
... to understand the importance of checking with an adult before participating in the online environment.
... to understand that not everyone they meet (whether in the 'real world' or online) is trustworthy.
... to check files with an adult before downloading.
... to ask teachers to help them stay safe on the internet.
... to decide to follow or click a link or not.
... to consider the impact on others and society before acting in an SNS environment.
... to understand the meaning of entering into contracts, and never do this by themselves.
... to use future-oriented coping strategies, or "preventive coping," like responding to potential stressors before a stressful situation has occurred.
... to understand some of the qualities that can be used to assess if a person is trustworthy.
... identify some of the physical sensations that alert us to unsafe situations.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

14

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

15

We are in the dimension Detect and Safety section section.

Kids should be able...

... to differentiate between paid and non-paid services online.
... to check the security information/certification by online payments.
... the different feelings they may experience when dealing with someone untrustworthy.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

16

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

17

We are in the dimension Respond and Safety section.

Kids should...

... know where to ask for help and how to explain their digital safety issues using basic terms, yet proper IT vocabulary (such as phishing, cyberbullying, etc.).
... understand "what is cyberbullying" and what to do against it or help others in the situation.
... understand that it is good to act on their feelings (intuition) in order to avoid or escape from unsafe situations.
... know to report the situation or the person if they feel unsafe.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

18

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

19

We are in the dimension Recover and Safety section.

Kids should...

No skill was identified.

Do you find the extracted skills adequate and complete?

- ◯ Yes
- ◯ No

20

If no, please explain briefly or make your suggestion.

Ihre Antwort eingeben

21

Any other comments?

Ihre Antwort eingeben