Developing Essential Cybersecurity Skills in the EU: the Cyber Citizen Learning Model

[Document subtitle]

Finland, September 2024

DESCRIPTION SHEET

Publisher	Aalto University, Cyber Citizen project
Title	Developing Essential Cybersecurity Skills in the EU: the Cyber Citizen Learning Model
Keywords	Cybersecurity, digital security, cybersecurity skills, cybersecurity training, cybersecurity learning, European Union
Language versions	English **Pages** 20

Contents

1 Introduction 3
1.1 Background and Objectives 3
1.2 Key Concepts 4
2 Framework for Learning Content 6
3 Cyber Citizen Learning Model: Practice 9
3.1 Learning Methods 9
3.2 Learning Tools 10
3.2.1 Essential Cybersecurity Skills Badge 11
3.3 Learning Content 12
4 Conclusion 13
References 14
Annex 1 16

1 Introduction

Recent crises have accelerated society's digital transformation, with an increasing shift of daily functions and services online. While this brings new opportunities, it also poses significant security challenges. The cybersecurity landscape has evolved rapidly, with threat actors enhancing their capabilities and employing sophisticated techniques like bots and AI.

The Cyber Citizen project seeks to cultivate a safe digital culture in the European Union (EU) by focusing on awareness and training in essential cybersecurity skills. The security of the EU relies on its people—not only cybersecurity professionals but the entire population—who must contribute to making the EU safer. Every individual in the cyber environment should possess essential cybersecurity skills to safely and effectively leverage digital opportunities, enhancing both personal and communal security.

1.1 Background and Objectives

The Cyber Citizen project seeks to strengthen European cybersecurity and develop standard practices and models to improve the essential cybersecurity skills of Europeans. The project draws upon prior experiences, such as lessons learned from various EU-funded projects like Horizon, Erasmus+, and Digital Europe, to inform its approach to cybersecurity education and training. These experiences help ensure continuity, effectiveness, and sustainability of practices.

Developing an EU-wide model and practice for learning essential cybersecurity skills is accompanied by challenges. Firstly, there are significant differences in the quality of cybersecurity education and other digital skills training across the EU. EU Member States hold varying perspectives on what constitutes essential cybersecurity skills and how cybersecurity competence and culture should be developed. Another challenge lies in defining the goals for cybersecurity competence: how skills are currently taught and learned, and how they should be taught to different target groups. (Limnéll et al., 2023.)

As part of the project, a digital learning portal (Secport) has been created to serve citizens across the EU. The initial research phase of the Cyber Citizen project examined the practical applications of cybersecurity education and training. While a wealth of cybersecurity education and training is available in different countries, the challenge is ensuring it is accessible to those who need it and accommodating various learning preferences and learners. On the positive side, there is a clear willingness across all EU countries to develop civic competences in cybersecurity and support lifelong learning. Moreover, many parallel activities are taking place in different countries, suggesting that combining efforts and sharing best practices would be beneficial. (Limnéll et al., 2023.)

The remainder of this document is structured as follows: Section 1 introduces the background, objectives, and key concepts of the report. Section 2 explores the framework for learning content, detailing methodologies and competencies relevant for developing essential cybersecurity skills. Section 3 presents the Cyber Citizen Learning Model, including the portal and gamified elements. Finally, Section 4 provides a conclusion and summarises the insights and future implications of the Cyber Citizen Learning Model.

1.2 Key Concepts

Understanding key terms and ideas is essential to grasp the scope and goals of the Cyber Citizen project. This section provides definitions and explanations of key concepts relevant to the project, organised alphabetically for clarity.

Cybersecurity
According to the European Union Agency for Cybersecurity (ENISA), cybersecurity is a broad and encompassing term that defies a singular definition due to its extensive coverage. ENISA describes cybersecurity as focusing on the security of cyberspace, whereby cyberspace is defined as the network of connections and relationships among objects accessible through a generalised telecommunications network, and as the set of objects with interfaces for remote control, data access, or involvement in control actions. (Brookson et al., 2015, pp. 7, 28.) ENISA states, "cyberspace is the time-dependent set of tangible and intangible assets that store and/or transfer electronic information." Cybersecurity involves all necessary activities to protect cyberspace, its users, and affected individuals from cyber threats. In the context of the Cyber Citizen project, cybersecurity also encompasses information interference. (ENISA, 2017, p. 6.)

Digital Badge
A digital badge represents a shareable credential that provides evidence of a learning achievement. There are two types of digital badges: competency badges and participation badges. Competency badges assess skills and measure achievements, with the badge description detailing the assessed items and required performance to earn the badge. Participation badges indicate that an individual has participated in an event, such as attendance at a workshop or lecture. Competency and participation badges can be offered together when an individual attends a workshop and subsequently completes a skills test to demonstrate learning. (Pike et al., 2020, p. 20.)

Essential Cybersecurity Skills

Essential Cybersecurity Skills refer to the fundamental knowledge, skills, and abilities required when using digital services and devices. These skills facilitate personal development and enable individuals to maintain the knowledge and abilities to exercise deliberation in various situations. Essential cybersecurity skills encompass personal and social responsibility, as well as understanding the importance of this responsibility in cyberspace. The learning model outlines these competencies and their respective sub-skills:

1. Ethics, rules, rights, and responsibilities: understanding norms and rules as well as individual rights and responsibilities.
2. Critical thinking: engaging with a critical mindset and attitude towards events and information.
3. Understanding of value: recognising what is valuable to each party in each situation, e.g., understanding data as a valuable asset similar to money.
4. Emotional competence: acknowledging the influence of thoughts and emotions in different contexts.
5. Secure use of technology: understanding technology principles and using them securely.

Learning Model
Learning models are primarily grounded in cognitive and psychological theories, focusing on the learner's processing and construction of new information. The Cyber Citizen Learning Model integrates theory and practice. The theoretical component is based on different learning theories, values, and supporting frameworks, while the practical element involves selected learning methods, tools, and solutions informed by theory and experience gained throughout the project.

Learning Solution
A learning solution refers to a comprehensive approach designed to address specific learning needs or challenges, involving a combination of strategies, methods, materials, and assessments. It aims to facilitate the learning process effectively, ensuring learners acquire desired skills, knowledge, or competencies. Learning solutions are applied in contexts such as K-12 education, higher education, corporate training, and professional development. (Clark & Mayer, 2016.)

Learning Theory
Learning theory and learning conception are interconnected terms. Learning conception is an individual's understanding of learning, including assumptions about knowledge and its construction. (Lindblom-Ylänne & Nevgi, 2009, p. 194.) Learning theory is scientific, explaining how learning occurs and translates into practice, based on multiple disciplines like pedagogy, philosophy, psychology, sociology, and neuroscience. Examples include constructivism, connectivism, and behaviourism. (Lindblom-Ylänne & Nevgi, 2009, p. 194; Lynne & Denise, 2013, p. 3.)

Learning Tool
A learning tool encompasses any resource, device, or strategy that supports learning, knowledge acquisition, or enhances the educational experience. Tools can range from traditional resources like textbooks to digital tools like learning management systems, educational software, and mobile applications. (Manches et al., 2010; Coates, 2005; Kebritchi et al., 2010; Traxler, 2007.)

Micro-Credential
A micro-credential verifies the learning outcomes achieved by a learner after a short learning experience, assessed against transparent standards. The credential lists the holder's name, achieved outcomes, assessment method, awarding body, qualifications framework level, and credits gained. Micro-credentials are owned by the learner, shareable, portable, and combinable into larger qualifications. They are underpinned by quality assurance following agreed standards. (Futures et al., 2020, p. 10.)

2 Framework for Learning Content

Essential cybersecurity skills, as identified within the Cyber Citizen project, are based on the European Digital Competence Framework for Citizens (DigComp). According to DigComp, “competences are a combination of knowledge, skills, and attitudes. Key competences are developed throughout life. Skills are the ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the European Qualifications Framework, skills are described as cognitive (involving the use of logical, intuitive, and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools, and instruments).” (Vuorikari, 2022, p. 3.)

The European Skills, Competences and Occupations (ESCO) classification identifies, classifies, and describes digital skills, competences, and knowledge concepts relevant to education, training, and the EU labour market (What is ESCO, 2022). ESCO skills and knowledge concepts are labelled and translated based on DigComp 2.2. As part of a comprehensive five-step methodology, ESCO identifies digital skills when aligning with the DigComp definition. The Council Recommendation on Key Competences for Lifelong Learning reinforces DigComp’s definition: “Digital competence involves the confident, critical, and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It includes information and data literacy, communication and collaboration, media literacy, digital content creation (including programming), safety (including digital well-being and competences related to cybersecurity), intellectual property questions, problem solving, and critical thinking.” (European Commission - Employment, 2022.)

ESCO integrates the five competence areas identified in DigComp—information and data literacy, communication and collaboration, digital content creation, safety, and problem solving—into its skills pillars, alongside DigComp’s 21 competences. These are translated into the 23 EU languages, Icelandic, and Norwegian, reflecting an inclusive approach to digital literacy across the EU (European Commission - Directorate-General for Employment, 2022).

Table 2: Translation of DIGCOMP 2.0 competence areas, adapted and modified from Translations of DigComp 2.0 in the European Skills, Competences and Occupations classification (ESCO).

Translation of DIGCOMP 2.0 competence areas			
DigComp 2.0	**ESCO** label	**DigComp descriptor**	**ESCO descriptor**
Information and data literacy	Digital data processing	To articulate information needs, to locate and retrieve digital data, information and content. To judge the relevance of the source and its content. To store, manage, and organise digital data, information and content	Identify, locate, retrieve, store, organise and analyse digital information, judging its relevance and purpose

Communication and collaboration	Digital communication and collaboration	To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity. To participate in society through public and private digital services and participatory citizenship. To manage one's digital identity and reputation	Communicate in digital environments, share resources through online tools, link with others and collaborate through digital tools, interact with and participate in communities and networks, cross-cultural awareness
Digital content creation	Digital content creation	To create and edit digital content To improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied. To know how to give understandable instructions for a computer system	Create and edit new content (from word processing to images and video); integrate and re-elaborate previous knowledge and content; produce creative expressions, media outputs and programming; deal with and apply intellectual property rights and licences
Safety	ICT safety	To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use	Personal protection, data protection, digital identity protection, security measures, safe and sustainable use.
Problem solving	Problem-solving with digital tools	To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments. To use digital tools to innovate processes and products. To keep up-to-date with the digital evolution.	Identify digital needs and resources, make informed decisions on most appropriate digital tools according to the purpose or need, solve conceptual problems through digital means, creatively use technologies, solve technical problems, update own and other's competence.

The European Digital Competence Framework for Citizens (DigComp) significantly influences most EU member states as it provides a structured approach to developing digital competences across Europe. Essential cybersecurity skills identified within the Cyber Citizen project are designed to support the adoption of the DigComp framework, ensuring they resonate with its core areas: information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving. (Limnéll et al., 2023.)

The DigComp framework serves as a guide for building understanding, competence, and capabilities related to digitalisation at the EU level. Future competence goals in cyberspace should be explored within a broader analytical framework, taking into account individual and social resilience, sovereignty, and well-being. These goals are defined based on innovative mapping methods and literature reviews, offering insights that can be further developed through gamification and the utilisation of a digital learning portal. (Limnéll et al., 2023.)

Here are the DigComp competence areas mapped with Essential Cybersecurity Competences sub-skills (skills that need to be mastered in order to master the broader Essential Cybersecurity skills skill sets, e.g. competences) and learning outcomes:

DigComp competence areas	**Essential Cybersecurity skills, sub-skills**
Information and data literacy	• Is able to evaluate the reliability of information and information sources • Is able to analyse, compare and process information • Understands the cyber environment • Develops foresight skills
Communication and collaboration	• Understands rules and their impact on a personal and communal level • Understands the effect of their actions on general security • Manages their digital footprint • Recognizes the importance of different interaction channels in communication
Digital content creation	• Understands copyright principles • Knows how to use current technologies and services
Safety	• Is able to use prevalent technology securely • Is able to protect used information and look after their digital identity • Is able to maintain sense of security and awareness concerning themselves and others
Problem solving	• Is able to solve problems related to the use of services and devices and communicate about problem situations in an understandable manner. • Understands and actively seeks to develop their own competence • Knows what to do if they become a victim of an information security offence or crime

The Cyber Citizen Learning framework outlines the competency areas required to cultivate essential cybersecurity skills and the specific skills needed to master these areas. This framework provides a clear roadmap for developing comprehensive cybersecurity competencies. For a more detailed definition of the skills involved, please refer to Annex 1.

3 Cyber Citizen Learning Model: Practice

The Cyber Citizen Learning Model primarily involves e-learning and self-study, providing content accessible to all EU citizens free of charge, in all official EU languages. This target group includes entrepreneurs, employees lacking adequate workplace cybersecurity training, and citizens outside the workforce seeking information.

3.1 Learning Methods

The Cyber Citizen Learning Model provides citizens with opportunities to learn both broadly and specifically through macro and micro approaches. **Macro-learning** involves comprehensive courses, lectures, and workshops, allowing learners to delve deeply into new information or skills over extended time periods. The Cyber Citizen cybersecurity course exemplifies macro-learning, offering an in-depth exploration of cybersecurity topics.

Conversely, **micro-learning**, or just-in-time training, offers quick, focused learning to address specific questions or problems. This approach includes elements like video clips, infographics, and interactive content within the portal, designed to provide immediate and actionable knowledge. These micro-learning elements support a flexible education that adapts to the fast-paced digital environment. (Kallio et al., 2018, pp. 16-17.)

The learning model acknowledges diverse learning preferences, ensuring content is available across various formats—including text, video, images, and interactive tasks—to maximize engagement and accessibility.

Educational theorist Joseph Schwab identified four commonplaces essential to education: learner, teacher, subject/materials, and environment. This framework informs effective educational practices. Building on this, Novak adds evaluation as a fifth element, emphasizing it as key to understanding and improving educational outcomes. Novak's framework includes: 1) learner, 2) teacher, 3) knowledge, 4) context, and 5) evaluation, interacting to create meaningful learning experiences leading to empowerment and responsibility. (Novak, 2002, pp. 18-20.)

The Cyber Citizen Learning Model effectively incorporates these elements:

1. **Learner**: The target group includes citizens across the EU, providing wide access to cybersecurity education.
2. **Teacher**: The Cyber Citizen portal delivers structured learning pathways and resources for knowledge acquisition.
3. **Knowledge**: Content is curated to ensure relevance to contemporary digital challenges, focusing on essential cybersecurity skills.
4. **Context**: The model fosters an engaging learning environment through a blend of theory, practice, and interactive portal features.
5. **Evaluation**: Learners receive feedback and recognition through tools such as the Essential Cybersecurity Skills Badge, promoting continuous development.

This holistic approach ensures that educational experiences are constructive, integrative, and consistent with the project’s values, particularly the pursuit of meaningful learning. Through

practical implementation, the Cyber Citizen project empowers participants, enriching their engagement with cybersecurity concepts and fostering resilience across the EU.

3.2 Learning Tools

Research highlights the importance of employing diverse learning tools to accommodate varied learning preferences, thereby creating rich educational experiences. The Cyber Citizen project has developed the Secport portal, designed to positively impact digital society by enhancing the safe use of digital services. The portal aims to:

- Empower users with knowledge and skills for effective digital technology usage.
- Educate about online threats, privacy, and cybersecurity to mitigate risks.
- Encourage responsible online behaviour, including respectful communication and lawful internet usage.
- Provide resources and support to address online harassment and bullying.
- Equip users with critical thinking skills to identify misinformation and disinformation.

Accessibility and Audience

The portal is accessible to a wide audience, including students, educators, professionals, managers, and anyone interested in enhancing cybersecurity skills, awareness, and knowledge. Positioned at a European level, it ensures broad and inclusive access to users across different sectors and demographics.

User Categories

- **Students:** Access engaging materials to build cybersecurity skills across various educational levels.
- **People outside the labour force:** Verification of competences useful for job searches.
- **Educators:** Tools and curricula to integrate cybersecurity skills into lessons.
- **Professionals:** Guidance for maintaining a positive online presence and ensuring cybersecurity in their work.
- **Seniors:** Resources to guide online activities and ensure safety.

Learning Methods

The portal employs multiple methods to facilitate learning:

- **Written e-learning modules:** Offer structured knowledge acquisition.
- **Interactive Modules:** Engage users in digital literacy, online safety, and ethics.
- **Videos:** Visually demonstrate digital citizenship concepts.
- **Tests, quizzes, and assessments:** Reinforce understanding of cybersecurity topics.
- **Simulations, scenarios, and case studies:** Highlight real-life examples, best practices, and potential pitfalls.

Engagement and Participation

Users are drawn to the portal by interest in understanding digital practices and benefiting from expert insights into cybersecurity. Motivation is key to attracting users, with certification processes enhancing attendance. Users are encouraged to engage with the portal and its learning solutions, acquiring knowledge and recognition in the form of gratitude and certification.

Target Groups

The portal effectively reaches key target groups through participating actors like:

- Responsible authorities from EU member states.
- Organisations, top management, and staff members.
- Non-governmental organisations.
- Student organisations.
- Higher education institutions and universities.
- Schools and communities catering to the elderly.

Overall, the Secport portal serves as a comprehensive resource addressing the need for cybersecurity skills in the digital age. It equips users with the knowledge, skills, and tools necessary to navigate the digital landscape responsibly, safely, and ethically, ultimately fostering a more informed and empowered digital society.

The learning journey begins with an orientation that highlights the importance and relevance of the topic, while also detailing the portal's purpose. As learners progress, continuous assessments play a crucial role in evaluating whether they are meeting their goals. Initial competency evaluations guide the tailoring of content and help learners establish clear learning objectives. Objectives are defined along with the behaviour changes required to achieve them, and the requisite training is outlined to realise these objectives. The portal is designed around three key components: content delivery, interactive engagement, and hands-on activities. These components are crucial for retaining information, particularly when it leaves an emotional impact, as emotional experiences tend to be more memorable than specific details.

Users are motivated to enhance their knowledge through online courses. The portal’s role in active conceptualisation is reinforced through awareness-raising initiatives. User participation in designing and producing portal content ensures consistent high-quality output, supported by efficient production processes.

3.2.1 Essential Cybersecurity Skills Badge

Open Badges have emerged as a valuable tool for identifying, evaluating, motivating, and credentialing learning and skills acquired in diverse educational contexts, whether formal or informal, online or in a classroom setting (Devedžić & Jovanović, 2015). They are instrumental in assessing competencies, fostering motivation, and stimulating critical thinking (Godshalk, 2021, pp. 27, 39.). Digital badges positively influence the learning process and skill promotion, offering exciting opportunities to demonstrate achievements

beyond the traditional classroom. They can extend cybersecurity learning and forge clear pathways for learners (Pike et al., 2020, pp. 19, 22.).

On 16th June 2022, the Council of the European Union approved a recommendation for a European approach to micro-credentials aimed at lifelong learning and employability. This recommendation promotes equal learning opportunities for all EU citizens by advocating for the development, implementation, and recognition of micro-credentials (A European approach to micro-credentials, n.d.).

Given their ability to motivate learners and support the acquisition of varied skills, such as Essential Cybersecurity Skills, digital badges serve as a key component of the Cyber Citizen Learning Model. Their inclusive nature aligns with the European Union's encouragement of using badges (micro-credentials) to enhance flexible learning opportunities, making them integral to promoting learning for all EU citizens.

3.3 Learning Content

The Secport portal offers a wide array of content designed to foster comprehensive cybersecurity understanding and skills among users. This includes both declarative and procedural knowledge, enabling learners to grasp essential concepts and apply them in practical scenarios. Declarative knowledge—visible explicit information expressible through reading or listening—is delivered through playbooks, databanks, and manuals available on the Secport portal. Procedural knowledge, or know-how, is developed through practical engagement, as learners apply instructions and participate in activities, verifying their control of topics through use and practice.

Completion of a cybersecurity course on the platform leads to earning digital competence badges, showcasing learners' mastery. Interactivity plays a key role in supporting independent learning, with elements such as chatbots providing feedback, allowing learners to reflect on their actions. Exercises further integrate theory into practice, creating meaningful interactions. Content is accessible, diverse, and engaging, adhering to the Cyber Citizen Learning Model. It is organised into sections as follows:

Cybersecurity Course

The course consists of modules aligning with the framework's learning goals. Upon completion of a final test, participants receive a Cyber Citizen Skills Badge. As the core content of the platform, it aims to enhance overall cybersecurity skills.

Course on Influence Operations and Information Interference

This course aims to deepen citizens’ understanding of influence operations and equip them to detect and respond to information interference attempts. Through virtual storytelling, videos, and case studies, it explores concepts like emotional impacts on information security and resilience.

Cybersecurity Game

A business idle tycoon-style game targets users aged 12 and above, focusing on prevalent cyber threats. This interactive experience introduces vital subjects such as fake news, phishing, romance scams, digital hygiene, and device security, enabling skill development in a fun manner.

Other Gamified Elements

Interactive components, including questionnaires, practical exercises, and scenario-based tasks, engage users. Rewards, storytelling, and virtual achievements incentivise continuous learning.

Knowledge Base

The portal includes a knowledge base, consolidating information for easy access and understanding of multidimensional phenomena, thus simplifying the complex topics that concern citizens.

Glossary

The glossary provides clear definitions of common cybersecurity terms, facilitating quick access to relevant information. For further exploration, users can delve into the knowledge base.

Infographics

Infographics deliver relevant information effectively and visually. By raising awareness, they offer quick ways to understand complex subjects, presented in forms such as factsheets, guidelines, and posters.

Videos

Short animated videos creatively explain phenomena, using visualisations, metaphors, and storytelling. The broad target audience makes this an appealing medium to engage diverse backgrounds and enhance cybersecurity awareness.

These varied content offerings ensure the Cyber Citizen platform is equipped to meet diverse learning needs, enhancing user engagement and fostering skill development across the digital society.

4 Conclusion

Cybersecurity covers a broad spectrum of issues essential to maintaining the security of cyberspace. Essential Cybersecurity Skills include the knowledge, skills, and abilities that EU citizens—whether residing permanently or temporarily in Member States—require to safely navigate the cyber environment in various contexts. These skills are structured around five competence areas: ethics, rules, rights, and responsibilities; critical thinking; understanding of value; attitude; and secure use of technology. The Secport portal is designed to teach and enhance these skills, supported by a learning model that aims to improve educational outcomes from individual to EU-wide levels.

The Cyber Citizen Learning Model is tailored to serve a diverse user base across the EU, accommodating geographic, cultural, and demographic differences. It integrates practical learning elements, offering methods that facilitate both micro-learning, such as through video clips and infographics, and macro-learning, examples of which include comprehensive courses. The model employs a range of learning tools, including the portal, AI, and the Essential Cybersecurity Skills Badge. Additionally, it features a wealth of learning content, such as cybersecurity and information interference courses, interactive games and gamified elements.

With this robust model, the Cyber Citizen project equips users to effectively address cybersecurity challenges, promoting safe and responsible digital engagement throughout the European Union.

References

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., Rannenberg, K., Shamah, J., & Górniak, S. (2015). ENISA: Definition of Cybersecurity - Gaps and overlaps in standardisation. 34.

Clark, R. C., & Mayer, R. E. (2016). *E-learning and the science of instruction : proven guidelines for consumers and designers of multimedia learning* (Fourth edition. ed.). Wiley.

Coates, H. (2005). The value of student engagement for higher education quality assurance. *Quality in Higher Education*, *11*(1), 25-36. https://doi.org/10.1080/13538320500074915

Devedžić, V., & Jovanović, J. (2015). Developing Open Badges: a comprehensive approach. *Educational Technology Research and Development*, *63*(4), 603-620. https://doi.org/10.1007/s11423-015-9388-3

ENISA. (2017). ENISA overview of cybersecurity and related terminology.

A European approach to micro-credentials. (n.d.). European Commission: European Education Area: Quality education and training for all. Retrieved 5.9.2023 from https://education.ec.europa.eu/education-levels/higher-education/micro-credentials

European Commission - Directorate-General for Employment, S. a. a. I.-t. E. S. a. t. J. r. C. J. (2022). *Translations of DigComp 2.0 in the European Skills, Competences and Occupations classification (ESCO)*. https://esco.ec.europa.eu/en/about-esco/publications/publication/translations-digcomp-20-esco

European Commission - Employment, S. A. a. I. (2022). *Digital Skills and Knowledge Concepts - Labelling the ESCO classification - Technical Report - October 2022.pdf*.

Futures, H. S., Andersen, T., & Larsen, K. N. (2020). *A European approach to micro-credentials - Output of the micro-credentials higher education consultation group - final report*. Y. European Commission - Directorate-General for Education, Sport and Culture. https://education.ec.europa.eu/sites/default/files/document-library-docs/european-approach-micro-credentials-higher-education-consultation-group-output-final-report.pdf

Godshalk, V. M., Luke. (2021). Digital Badges in a Post-COVID World. *Academy of Business Research Journal*, *3*, 27-51. https://www.proquest.com/scholarly-journals/digital-badges-post-covid-world/docview/2720474349/se-2

Kallio, P., Saarinen, S., Marjanen, J., Kurkipää, T., & Siira, H. (2018). *Jotta jokainen voisi oppia*. HAUS kehittämiskeskus Oy.

Kebritchi, M., Hirumi, A., & Bai, H. (2010). The effects of modern mathematics computer games on mathematics achievement and class motivation. *Computers & Education*, *55*(2), 427-443. https://doi.org/https://doi.org/10.1016/j.compedu.2010.02.007

Koehler, M., & Mishra, P. (2009). What is Technological Pedagogical Content Knowledge (TPACK)? *Contemporary Issues in Technology and Teacher Education*, *9*(1), 60-70.

Limnéll, J., Alasuutari, M., Candelin, N., Cullen, K., Halonen, O., Helenius, M., Hermunen, T., Lappalainen, J., Latvanen, S., Lindroth, M., Matilainen, T., Palonen, O.-P., Riiheläinen, J., Salminen, M., & Virkkunen, P. (2023). *Cyber citizen skills and their development in the European Union*. Aalto University Research Group. https://cyber-citizen.eu/wp-content/uploads/2023/03/Cyber-citizen-skills-and-their-development-in-the-European-Union_EN.pdf

Lynne, H., & Denise, C. (2013). *University Teaching in Focus : A Learning-centred Approach* (Vol. [New ed]) [Book]. Routledge. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=507455&site=ehost-live&authtype=sso&custid=ns192260

Manches, A., O'Malley, C., & Benford, S. (2010). The role of physical representations in solving number problems: A comparison of young children's use of physical and virtual materials. *Computers & Education*, *54*(3), 622-640. https://doi.org/https://doi.org/10.1016/j.compedu.2009.09.023

Mishra, P., & Koehler, M. J. (2006). Technological Pedagogical Content Knowledge: A Framework for Teacher Knowledge. *Teachers College Record*, *108*(6), 1017-1054. https://doi.org/10.1111/j.1467-9620.2006.00684.x

Novak, J. D. (2002). *Tiedon oppiminen, luominen ja käyttö : käsitekartat työvälineinä oppilaitoksissa ja yrityksissä*. PS-kustannus.

Pike, R. E., Brown, B., West, T., & Zentner, A. (2020). Digital Badges and E-Portfolios in Cybersecurity Education. *Information Systems Education Journal*, *18*(5), 9. https://www.proquest.com/scholarly-journals/digital-badges-e-portfolios-cybersecurity/docview/2459007665/se-2

Traxler, J. (2007). Defining, Discussing and Evaluating Mobile Learning: The moving finger writes and having writ. *International Review of Research in Open and Distance Learning*, *8*. https://doi.org/10.19173/irrodl.v8i2.346

Vuorikari, R., Kluzer, S. and Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*.

What is ESCO. (2022). European Commission. Retrieved 14.9.2023 from https://esco.ec.europa.eu/en

Annex 1

CYBER CITIZEN SKILLS

1) CRITICAL THINKING: Cyber citizens think critically and have a critical attitude towards events and available information.
2) SECURE USE OF TECHNOLOGY: They understand the basic principles of the technologies they use and know how to use them securely
3) ETHICS, RULES, RIGHTS AND RESPONSIBILITIES: Cyber citizens understand the significance of norms and rules as well as their rights and responsibilities.
4) UNDERSTANDING OF VALUE: They have know-how that helps them to understand what is valuable to each party in each situation.
5) EMOTIONAL COMPETENCE: Cyber citizens recognise the impact of their thinking and emotions in different situations.

CYBER CITIZEN SKILLS AND SUB-SKILLS	Learning goals/objectives (Basic Level)	Learning goals/objectives (Intermediate & Advanced Level)
CRITICAL THINKING		
Able to search and understand what affects the search results/online experience	1) Aware how algorithms affect online experience (search results, ads, content exposed to on social media) 2) Aware of potential information biases caused by various factors (e.g. data, algorithms, editorial choices, censorship, one's own personal limitations). 3) Aware that algorithms may not provide only the information that the user wants, and the possible negative consequences: They might also embody a commercial or political message (e.g. to encourage users to stay on the site, to watch or buy something particular, to share specific opinions), which can reproduce stereotypes, lead to sharing misinformation). 4) Understands that top search results may reflect commercial and other interests rather than be the most appropriate result 5) Aware that search results, social media activity streams and content recommendations are influenced by geographical location, the device type, local regulations, behaviour of other users, and the user's past online behaviour across the internet. 6) Wary of the reliability of recommendations (e.g. are they by a reputable source) and their intentions (e.g. do they really help the user vs encourage to use the device more to be exposed to advertising). 7) Understands the notion of echo chambers and how it affects users online experience 8) Aware that AI may include biases. Biases can become automated and worsened by the use of AI. 9) Understands AI is neither good nor bad	1) Knows how to analyse and critically evaluate search results and social media activity streams, to identify their origins, to distinguish fact-reporting from opinion, and to determine whether outputs are truthful or have other limitations (e.g. economic, political, religious interests). 2) Knows how to differentiate sponsored content from other content online (e.g. recognising advertisements and marketing messages on social media or search engines) even if it is not marked as sponsored. 3) Able to adapt search methods and settings to navigate digital environments in the age of information operations and manage information overload
Is able to analyse and process information and evaluate and compare the reliability of information sources	1) Aware that online environment contain mis/disinformation and that information may not be accurate 2) Understands the difference between disinformation (false information with the intent to deceive people) and misinformation (false information regardless of intent to deceive or mislead people). 3) Understands what source criticism is and why it is important 4) Knows what deep-fakes are and that they may be impossible to distinguish from the real thing. 5) Aware that AI content may be impossible to distinguish from human content 6) Aware of the role of traditional (e.g. newspapers, television) and new forms of media (e.g. social media, the internet) in democratic societies. 7) Aware of different cognitive biases which affect how we perceive new information 8) Aware of how algorithms can be used in information operations 9) Aware of manipulation techniques used in information operations	1) Can differentiate between fake news and reliable sources 2) Able to fact-check a piece of information 3) Proactive about using the internet and digital technologies to seek opportunities for constructive participation in democratic decision-making and civic activities 4) Asks critical questions to evaluate the quality of online information, and concerned about purposes behind spreading and amplifying disinformation. 5) Knows how to find the author or the source of the information, to verify whether it is credible (e.g. an expert or authority in a relevant discipline). 6) Understands how cognitive biases affect our perception and able to adapt one's own behaviour 7) Understands how algorithms are used in information operations and able to critically examine information in online environments
Understands and actively seeks to develop their own skills and competence related to cybersecurity	1) Aware that being competent in cybersecurity requires responsible use of technologies in work, education, and leisure (in all aspects of life) 2) Aware where to find more information	1) Capable of reflecting one's own level of competence and knows how to improve
Understands mechanisms how our behaviour is guided online	1) Aware that many communication services and digital environments (e.g. social media) use mechanisms such as nudging, gamification and manipulation to influence user behaviour.	1) Knows how to recognise embedded user experience techniques (e.g. clickbait, gamification, nudging) designed to manipulate and/or to weaken one's ability to be in control of decisions (e.g. make users to spend more time on online activities, encourage consumerism).
Knows about the regulatory landscape of digital applications	1) Aware that for many digital health applications for example, there are no official licensing procedures as is the case in mainstream medicine	1) Evaluates information online and assumes responsibility for protecting personal and collective health from potentially dangerous information

EMOTIONAL COMPETENCE		
Is able to maintain sense of security and awareness concerning themselves and others	1) Able to recognise hostile messages, hate speech, and trolling (Intermediate?) 2) Understands what cyberbullying is and aware how to recognise, report and protect oneself from it 3) Aware that vulnerable groups are at higher risk of victimisation to cyber bullying, scams etc. 4) Understands the "online disinhibition effect" 5) Aware of the need to formulate messages in digital environments so that they are easily understandable by the targeted audience or the recipient. (Information influecing & netiquette) 6) Aware how feelings affect our communication on social media	1) Able to manage one's feelings when talking with other people on the internet. 2) Knows how to stop receiving unwanted disturbing messages or emails 3) Can apply and follow protection strategies to fight online victimisation (e.g. block receiving further messages from sender(s), not reacting/responding, forwarding or saving messages as evidence for legal procedures, deleting negative messages to avoid repeated viewing). 4) Able to recognise cyberbullying and knows how and where to report it
Is able to recognize and respond to potential digital security threats.	1) Knows how to identify suspicious e-mail messages that try to obtain sensitive information (e.g. personal data, banking identification) or might contain malware. 2) Aware of how criminals try to trick them	
Understands the impact of digital technologies on personal health and wellbeing.	1) Aware of the importance of balancing the use of digital technologies and their influence on personal health and wellbeing 2) Aware that health applications can have negative impacts (idealised body images)	1) Knows signs of digital addictions 2) Knows how to apply and monitor screentime 3) Knows how to avoid the negative impacts of digital media
SECURE USE OF TECHNOLOGY		
Understands the cyber environment	1) Understands how the Internet works on a basic level (Global system of interconnected computer networks) 2) Aware how local networks (home network & Wi-Fi) work 3) Understands the difference between intranet and internet 2) Knows what the world wide web is 2) Understands the basic functions of web browsing (URL, Pop-ups, Cookies, Browsing history)	
Recognises the importance of security for different interaction channels in communication	1) Safe use of videoconferencing (B/I) 2) Restrict privacy settings on social media (B/I) 3) Knows that many communication services (e.g. instant messaging) and social media are free of charge because they are partly paid for by advertising and monetising user data. 4) Aware which communication tools and services (e.g. phone, email, video conference, social network, podcast) are appropriate in specific circumstances (security & privacy), depending on the audience, context and purpose of the communication. (B/I)	
Knows how to create and manage passwords securely and other sacerity measures to restrict access	1) Knows about measures to protect devices (e.g. password, fingerprints, encryption) and prevent others (e.g. a thief, commercial organisation, government agency) from having access to all data. 2) Knows that using different strong passwords for different online services is a way to mitigate the negative effects of an account being compromised (e.g. hacked). 3) Knows how to adopt a proper cyber-hygiene strategy regarding passwords (strong passwords, don't recycle or share, password manager) 4) Knows how to activate two-factor authentication when available (B/I)	1) Able to encrypt sensitive data stored on a personal device or in a cloud storage service. 2) Aware of mechanisms and methods to block or limit access to digital content (e.g. passwords, geo-blocking, Technical Protection Measures, TPM).
Is able to use prevalent technology securely	1) Knows about the importance of keeping the operating system and applications up-to-date 2) Aware that firewall blocks certain kind of network traffic, but does not mean you can click on everything 3) Aware of outcomes of clicking links. 4) Vigilant not to leave computers or mobile devices unattended in public places (e.g. shared workplaces, restaurants, trains, car backseat). 5) Knows not to use open Wi-fi networks to make financial transactions or online banking. 6) Knows how to apply basic security measures in online payments (e.g. never sending a scan of credit cards or giving the pin code of a debit/payment/credit card).	1) Able to choose appropriate storage location for data based on security needs 2) Knows how to install and activate protection software and services 3) Routinely checks protective measures for devices and Wi-Fi are still secure 4) Knows how to use electronic identification for services provided by public authorities or public services (e.g. filling-in your tax form, applying for social benefits, requesting certificates) and by the business sector, such as banks and transport services. 5) Can choose services (e.g. search engines) that meet their requirements (accuracy, privacy, etc.) 6) Routinely checks for updates to device and applications
Is able to solve problems related to the use of services and devices and communicate about problem situations in an understandable manner	1) Aware where to report incidents to (work --> workplace IT, personal --> police, bank, NCSC) 2) Aware cyberincidents concerning financial transactions should be reported immediately 3) Understands why it is important to report incidents	1) Can respond appropriately to a security breach (i.e. an incident that results in unauthorised access to digital data, applications, networks or devices, the leaking of personal data such as logins or passwords). 2) Knows where to report different incidents to and can guide others 3) Immediately reports cyberincidents 4) Understands why different incidents need to be reported to different authorities 5) Understands the impact of reporting incidents 6) Able to complete measures to recover from incidents
Knows what to do if they become a victim of an information security offence or crime and what preventative actions they can take to protect themselves and others.	1) Aware how to mitigate data loss in case of ransomware (= make back-ups beforehand) 2) Aware of the personal impact of cyberattacks 3) Aware that ransom should never be paid 4) Aware that everyone is a target for cybercriminals and that one's own behaviour influences how at risk one is 5) Aware how to protect social media accounts from being breached 6) Aware that our own behaviour can protect ourself online	1) Retains positive attitude to cybersecurity and strengthening own preparedness 2) Knows how to make routine back-ups 3) Implements routine back-ups as part of their cyberhygiene strategy 4) Understands what kind of behaviour increases the risk of becoming a victim to cybercrimes/scams 5) Able to carry out measures to protect social media accounts

Is able to manage and protect digital identities and privacy.	1) Understands why to use different digital profiles for private and business use 1) Aware that there are ways to limit and manage the tracking of one's activities on the internet, such as software features (e.g. private browsing, deletion of cookies) and privacy-enhancing tools and product/service features (e.g. custom consent for cookies, opting out of personalised ads).	1) Knows how to manage profiles in digital environments for personal purposes (e.g. civic participation, e-commerce, social media use) and professional purposes (e.g. create a profile on an online employment platform). 2) Knows what strategies to use in order to control, manage or delete data that is collected/curated by online systems (e.g. keeping track of services used, listing online accounts, deleting accounts that are not in use). 3) Considers the benefits and risks when managing one or multiple digital identities across digital systems, apps and services.
Is proficient in identifying and mitigating various digital security threats and scams.	1) Aware of different types of scams (romance, vishing, phishing, CEO fraud) 2) Aware of how to recognise romance scams and phishing 3) Aware of online shopping risks 4) Aware of own vulnerability and how criminals try to use them 11) Aware of different types of risks in digital environments, such as identity theft (e.g. someone committing fraud or other crimes using another person's personal data), scams (e.g. financial scams where victims are tricked into sending money), malware attacks (e.g. ransomware) 6) Aware what identity fraud is and where to report it 7) Aware of the most prevalent cybersecurity threats 8) Being wary of connection/message requests from unknown users on social media, linkedin, WhatsApp etc.	1) Understands the different techniques used by different scam operators 2) Able to recognise romance scams and other scam attempts 3) Able to detect online shopping scams 4) Understands the mechanisms criminals use to target our vulnerabilities 5) Knows how to recognise identity fraud and how to mitigate the risks 6) Able to identify and discuss the most prevalent threats and warn others about them
Understands the privacy and security implications of IoT devices and electronic identification.	1) Aware of the privacy risks of IoT devices 3) Aware of vulnerablities in IoT devices and how they may set personal information at risk 3) Aware that secure electronic identification is a key feature designed to enable safer sharing of personal data with third parties when conducting public sector and private transactions.	1) Able to check and select website cookies 2) Knows how to check the type of personal data an app accesses on one's mobile phone and, based on that, decides whether to install it and configures the appropriate settings. 3) Knows how to modify user configurations (e.g. in apps, software, digital platforms) to enable, prevent or moderate the AI system tracking, collecting or analysing data (e.g. not allowing the mobile phone to track the user's location). 4) Able to minimise personal information given to IoT devices
UNDERSTANDING OF VALUE		
Is able to protect used information and look after their digital identity		1) Weighs the benefits and risks of using biometric identification techniques (e.g. fingerprint, face images) as they can affect safety in unintended ways. If biometric information is leaked or hacked, it becomes compromised and can lead to identity fraud. CT? 2) Weighs the benefits and risks before allowing third parties to process personal data (e.g. recognises that a voice assistant on a smartphone, that is used to give commands to a robot vacuum cleaner, could give third parties - companies, governments, cybercriminals - access to the data).
Understands the principles and practices of cybersecurity and data protection	1) Understands what cybersecurity aims to protect 2) Knows that data has different value/secrecy/privacy levels and actions to protect it should be adjusted according to the level	
Manages their digital footprint	1) Aware of what a digital footprint consists of (set of data identifying a user by means of tracing their digital activities, actions and contributions on the internet or digital devices (e.g. pages viewed, purchase history), personal data (e.g. name, username, profile data such as age, gender, hobbies) and context data (e.g. geographical location)). 2) Aware that online services collect and process user data to offer advertisements, recommendations, and services. 3) Aware that many applications on the internet and mobile phones collect and process data 4) Aware of basic means to limit tracking by online services (private browsing, cookie consent etc.) 5) Aware that online content that is available to users at no monetary cost is often paid for by advertising or by selling the user's data. 8) Aware that everything that one shares publicly online (e.g. images, videos, sounds) can be used to train AI systems. 9) Aware that adapting one's behaviour in digital environments depends on one's relationship with other participants (e.g. friends, co-workers, managers) 10) Aware what data points algorithms use (everything = how long the content engaged you, screenshots, etc.) 11) Aware that algorithms and AI are able to profile users based on their online behaviour 12) Aware that seeminly trivial information can be used by cyber criminals 13) Aware why one should minimise the information they share about themselves 14) Aware why old contacts should be removed from mobile device 15) Aware that quizzes, prizes, and competitions can collect data from you or be scam attempts 16) Aware what information you may share about others	1) Can choose between tools designed to protect search privacy and other rights of users (e.g. browsers such as DuckDuckGo). 2) Weighs the benefits and disadvantages of using AI-driven search engines 3) Knows that data collected and processed, for example by online systems, can be used to recognise patterns (e.g. repetitions) in new data (i.e. other images, sounds, mouse clicks, online behaviours) to further optimise and personalise online services (e.g. advertisements). 4) Aware that sensors used in many digital technologies and applications (e.g. facial tracking cameras, virtual assistants, wearable technologies, mobile phones, smart devices) generate large amounts of data, including personal data, that can be used to train an AI system. 5) Able to verify and modify what type of metadata (e.g. location, time) is included in pictures being shared in order to protect privacy. 6) Knows how to keep one's own and others' personal information private (e.g. vacations or birthday photos; religious or political comments). 7) Identifies both the positive and negative implications of the use of all data (collection, encoding and processing), but especially personal data, by AI-driven digital technologies such as apps and online services 8) Carefully consider what information to share online/with services (phone number etc.) --> protect info from cybercriminals 9) Able to minimise the amount of information shared about oneself 10) Routinely removes old contacts from mobile device 11)Understands the implications of partaking in online quizzes, prizes etc.
Understands and exercises digital rights and demands secure online services	1) Knows that in the EU, one has the right to ask a website's or search engine's administrators to access personal data held about you (right of access), to update or correct them (right of rectification), or remove them (right of erasure, also known as the Right To Be Forgotten). 2) Knows that the user has the right to demand secure services from companies. But at the moment all services are not secure.	1) Knows that the "privacy policy" of an app or service should explain what personal data it collects (e.g. name, brand of device, geolocation of the user), and whether data are shared with third parties.

ETHICS, RULES, RIGHTS, RESPONSIBILITIES		
Understands rules and their impact on a personal and communal level	1) Aware that AI can make controversial decision about their life (CV sorting, exam scoring) 2) Aware that all EU citizens have right to be be subject to fully automated decisionmaking 3) Knows that the processing of personal data is subject to local regulations such as the EU's General Data Protection Regulation (GDPR) 4) Aware that different rules (e.g. legal consumer protections) apply when buying online from a company than from a private person. 5) Aware of rights and responsibilities under GDPR	1) Knows how to flag or report disinformation and misinformation to fact-checking organisations and to social media platforms in order to stop it spreading. 2) Able to consider the ethical implications of AI systems
Understands the effect of their actions on general security	1) Aware of situations when not to use AI solutions. i.e. what data to not give them (personal and company data)	1) Aware that certain activities (e.g. training AI and producing cryptocurrencies like Bitcoin) are resource intensive processes in terms of data and computing power.
Demonstrates responsible and respectful behavior in digital environments	1) Aware of the existence of some expected rules about one's behaviour when using digital technologies 2) Understands that inappropriate behaviours in digital environments (e.g. drunken, being overly intimate and other sexually explicit behaviour) can damage social and personal aspects of lives over a long term. 3) Respects others privacy	1) Able to maintain responsible and constructive attitude on the internet and social media channels 2) Open to and respectful of the views of people on the internet with different cultures, and respect for privacy 3) Knows how to adopt information and communication practices in order to build a positive online identity (e.g. by adopting healthy, safe and ethical behaviours, such as avoiding stereotypes and consumerism).