DIGITAL SECURITY FOR SENIOR CITIZENS

2020-1-PL01-KA204-082121

Framework of Digital Security Competences

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Co-funded by the
Erasmus+ Programme
of the European Union

Contributors

Cuiablue Ltd, UK

CWEP, Poland

FyG Consultores, Spain

eSeniors, France

Innovation Hive, Greece

Contents

Background

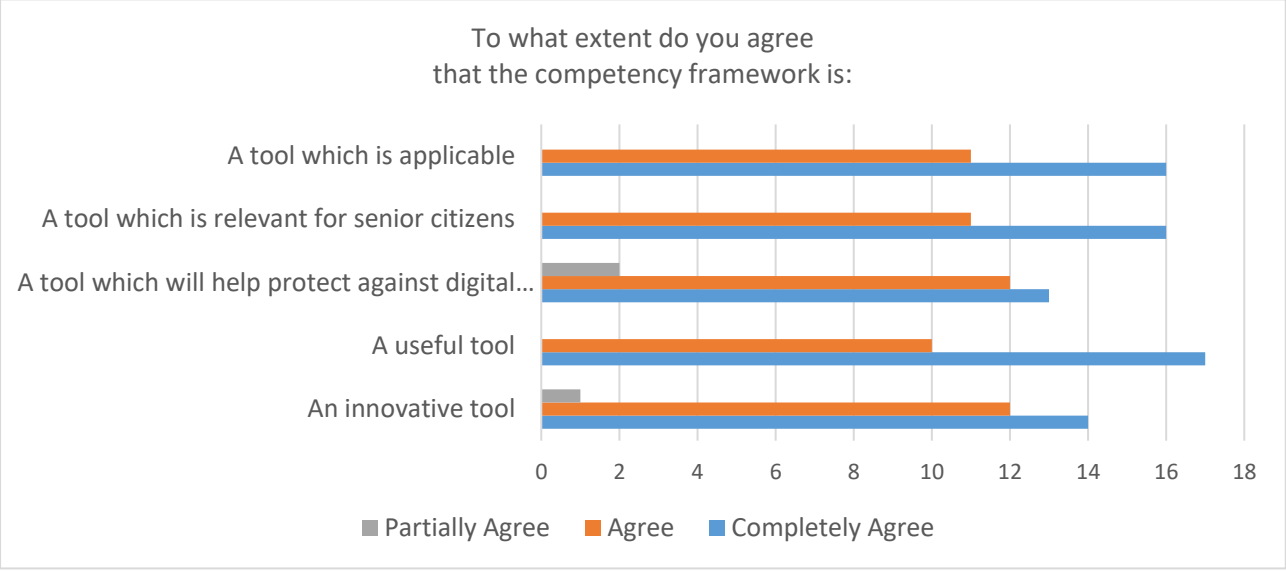
This framework has been developed as part of Intellectual Output 1 of the DiSC (Digital Security for Senior Citizens) project. Within the wider scope of the DiSC project, this output aims to support the project in building the digital capacity of senior citizens to recognise and proactively adapt to digital security threats and scams, and to lay the foundations for the implementation and uptake of targeted digital security policies at European level. This framework is one small step towards both of those objectives.

Methodology

The consortium discussed and agreed on the methodological approach to the development of the framework during the project kick-off meeting in December 2020. Firstly, a set of questionnaires for the stakeholder consultation meetings and template for the desk research was developed, tweaked, and amended accordingly so that partners were able to begin gathering information in the state of the art on current digital security information, advice, guidance, and policy at national level in each represented country. While the consortium undertook desk research, the initial draft of the framework was developed. After summarising and analysing the results of the desk research and taking into consideration the feedback received from the stakeholder consultation meetings, the second iteration of the framework was developed for comments and feedback by the consortium. After comments and input have been incorporated, the finalised version of the framework was translated and piloted with wider stakeholder groups and end users.

Stakeholder Consultation

As part of the DiSC project's co-creation approach to the project outputs, below is a summary of the relevant input gathered from the first stakeholder consultation meetings in early 2021 by all project partners. The statements relating to the competence framework are summarised below, after which stakeholders were invited to comment on their decision or add any thoughts about the framework.



The stakeholders were then asked to follow up on the quantitative responses by answering the question, "Do you have any comments or recommendations that would help us improve the Framework for Digital Security Competences?" and were provided with an open text box to give any comments, thoughts, or general impressions of the concept they had.

Specific recommendations included ensuring relevant vocabulary for older people to understand and a focus on basic, achievable requirements to ensure accessibility and uptake. Another such recommendation was to provide users with the means the resources to develop each competence, which support the need for IO2 and IO3.

The most frequent recommendation received was that the framework considers the most recent and fast-paced technological developments and the associated cyber security issues; cryptocurrency and the hundreds of continually evolving, creative approaches cybercriminals employ to attempt to steal such currencies being a good example. It is within this context that the DiSC consortium faces the biggest challenge in devising the framework: it must be comprehensive enough to cover the wide range of different skills and knowledge required, but also flexible enough to adapt to future innovations.

Desk Research

The second phase undertaken by the consortium focused on gathering relevant information, advice, guidance, and national policy documents which would help frame the context within which the digital security competence framework sits both at national level in each of the partner countries, but also at European level. In total, the consortium analysed 10 pieces of relevant documentation, two each from Poland, the UK, Greece, France, and Spain; these are summarised below. All desk research can be found as an annexe at the end of this document.

Greece's National Cybersecurity Strategy 2020 – 2025: consists of a national plan for the period 2020-2025 including the strategic objectives, priorities, policy, and regulatory measures to ensure a high level of security for digital communication and information systems at national level. The Greek Cyber Crime Division's cyber security campaign about mobile malware presents relevant information and ideas about forms of digital threats and how hackers could breach the personal data of citizens.

In France, the two documents reviewed were the Cyber Malveillance Website, published in 2021 by the French government, and a concise document from the CNIL (National Commission on Informatics and Liberties) entitled '10 Tips from the CNIL to stay clean on the Web'. Both documents are published with the purpose of raising awareness and building the capacity to cope with cyber threats among all citizens. The two documents differ in terms of design and the level and depth of information they relay, and therefore align well with the DiSC project in terms of what we aim to achieve and how DiSC project consortium will engage and present information to end users.

In Poland the research focused on an official cybersecurity guide for citizens, developed and published by the Polish government 'How to protect yourself from the cyberattacks'. The document provides a baseline what could be considered essential knowledge about using the internet and especially social media and therefore could be taken into consideration when developing the framework and potentially adapted and included. The second is a guide developed through another EU project. The document provides guidance around the essential knowledge and awareness that all citizens could have at the basic level so these could be taken into consideration when developing the framework and potentially adapted and included. The information in both contains relevant content which has value in the DiSC application and is relatable to many different individual and familial contexts.

The Spanish research led the partners to the National Cybersecurity Strategy 2019 published by the National Securirty Council of the Spanish Government, which sets directives within the general lines of action to tackle the challenge that cyberspace vulnerability represented for the country. The second publication within the research is "Live a safe Internet: It's never too late to enjoy a safer internet" by Organización de Consumidores y Usuarios (OCU). It contains a series of practical guides for different members of society including children, parents, adults, and seniors. For seniors the guide offers recommendations to learn to enjoy all the advantages of the Internet, without prejudice to their age.

The UK research focused on the UK National Cyber Security Centre's National Advice and Guidance Website. The information provided is set within the broader objective of protecting the UK, and therefore is aimed at all citizens, which is reflected in the content. The second document is the UK Government' National Cybersecurity Strategy 2016-2021 which provides a comprehensive overview of the strategic threats to govt, businesses and the public and so while it is of relevance to the DiSC project, it only marginally covers the areas this project addresses. The comprehensive list of types of threats is highly pertinent for the framework and project as a whole.

In summary, the desk research has informed the development of the framework by presenting the cybersecurity issues, threats and terminology used in each of the national contexts. The presentation and analysis of the various forms of information delivery used for different target groups has also had a strong bearing on the direction of the competence framework, as certain terminology and the presentation of information matters significantly to senior citizens; evidenced in similar material at national level. All partner countries deliver some type of information to senior citizens within the national context, either specifically, or within a larger awareness raising campaign for societal groups, and yet, once completed the framework will stand alone in terms of providing a set of applicable competences required to increase personal capacity to mitigate against cyber threats.

Introduction to the Framework

A competence framework is an effective method to assess, maintain, and monitor the target groups' knowledge, skills, and attributes relating to cybersecurity awareness, reactivity, and proactivity. The DiSC framework was designed to build on the Digcomp Digital Competence Framework which does not explicitly cover security from aggressive cyberattacks, spam and scam tricks used to steal people's data and information online.

More broadly, these competences and skills are based on sections 4.1 and 4.2 of the DigComp 2.1 framework:

4.1 Protecting devices - To protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have due regard to reliability and privacy.

4.2 Protecting personal data and privacy - To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.

The DiSC project consortium have broken down 4.1 protecting devices, and 4.2 protecting personal data and privacy, to five sub-sections, which have been used to classify the relevant digital security competences:

1. Threat Awareness: awareness of the different types of digital security threats
2. Threat Understanding: knowledge of the risks associated with digital security threats
3. Mitigation Planning: preparation against
4. Threat Detection: application of critical and analytical thinking to potential digital security threats
5. Countering Threats: problem solving to counteract threats and breaches

The establishment of the digital security competency framework will allow DiSC project to define the cybersecurity knowledge and skills required to deal with potential threats, identify specific cybersecurity competencies, in the form of sets of topics, and support the development and proposal of specific personal and professional training courses and opportunities for the target groups based on the framework.

The intended end users of the competence framework are senior citizens aged 55+. The framework is also expected to be relevant and of interest to pre-service and in-service ICT teachers, trainers and educators and practitioners working in the field of technological capacity building of senior citizens.

The Framework of Digital Security Competences aims to define the skills, knowledge and attitudes of key competences needed by senior citizens to effectively integrate digital security protocols into their localised contexts, as well as to provide an EU reference framework for developing and evaluating digital security competences.

Scope

For defining the scope of the framework, the partners have identified the device, the approach and the methods considered when applying the Digital Competence Framework. This will help differentiate between other types of criminal activity which are not covered by the competencies within the framework.

Devices: the device used to contact the victim

- Mobile and Smartphones
- Computers and Laptops
- Tablets

Approach: the technique used to scam the victim

- Phishing: A fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.
- Vishing (Voice Phishing): Voice phishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward.

- Smishing (SMS Phishing): An activity which enables criminals to steal victims' money or identity, or both because of a response to a text message. Smishing uses your mobile phone (either a smartphone or traditional non-internet connected handset) to manipulate innocent people into taking various actions which lead to being defrauded.
- Software Fraud: An activity in which the fraudster uses fake or copycat software such as an app or a program to gain access to the data on a digital device, which they then use to steal victims' money or identity.
- Social Engineering: A term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Method: the intended scam

- Phishing email scam
- Wealthy "prince" scam
- Greeting card scam
- Bank loan or credit card scam
- Lottery scam
- Extortion scam
- Romance / online dating scam
- Fake antivirus software
- Facebook impersonation/hijacked profile scam
- "Make money fast!" scams
- Travel scams
- Cryptocurrency scams
    - Fake Bitcoin exchanges
    - Ponzi schemes
    - Everyday scam attempts
    - Malware
- Fake news scam
- Fake shopping websites
- Job offer scams
- SMS Scamming (Smishing)
- Overpayment Online Scam
- Tech Support Online Scams

Note: digital threats are always changing and evolving, and by their nature, it is impossible to write up a comprehensive list. To keep up to date with the threats, DiSC recommends subscribing to a cybersecurity organisation or network, such as Heimdal Security, for example, which posts regular updates on cybersecurity issues, approaches and methods, or Europol's crime trend areas page.

The Framework

Fundamental competences	Levels of proficiency		
Descriptors	Fundamental The individual understands the basic concept, skills, and knowledge requirements of digital security, and is prepared to achieve the highest level of competence that they are capable of.	Intermediate The individual displays critical thinking related to digital security, can differentiate digital threats across all devices and is able to independently plan and successfully carry out mitigation actions to protect from them.	Advanced The individual displays analytical thinking towards digital security and can respond to threats in real time by assessing and choosing the most effective response in a high-pressure situation.

1. Threat Awareness

Threat Awareness	Fundamental	Intermediate	Advanced
Awareness of specific threats which target digital devices.	I am aware of the common approaches used by digital security threats.	I am aware of less common approaches used by digital security threats.	I keep up to date with new digital security approaches as they evolve.
	I am aware of common methods used by digital security threats.	I am aware of the less common methods used by digital security threats.	I keep up to date with new digital security methods as they evolve.
	I am aware of basic social engineering activities in the context of digital security.	I am aware of more complex social engineering techniques.	I am aware of different combinations of social engineering techniques, approaches and methods.

2. Threat Understanding

Threat Understanding	Fundamental	Intermediate	Advanced
Knowledge of the features and functions of each of the threats. Evaluating digital threats and their level of risk. Understanding the changing nature of digital threats. Being aware of the importance of reliable, up-to-date and accurate security information sources.	I understand the key features and functions of the most common digital security threats.	I understand the key features and functions of the rarest and most unusual digital security threats.	I actively refresh my knowledge of digital threats through reliable, up-to-date, and accurate security information sources.
	I understand the level of risk and potential consequences associated with simple digital security threats.	I understand the level of risk and potential consequences associated with multifaceted digital security threats.	I understand the level of risk and potential consequences associated with complex digital security threats.

3. Mitigation

Mitigation	Fundamental	Intermediate	Advanced
Skills and experience which enable informed decisions regarding digital threat protection.	I can identify suitable digital protection tools based to mitigate digital security threats.	I can use my past experiences and skills to inform my decisions on digital security threat protection.	I can use my experience and skills to analyse the potential impacts of different risks and choose suitable protection strategies accordingly.
Knowledge and understanding of different tools and resources to protect against threats.	I can follow basic digital security instructions to mitigate digital security threats.	I can decide on the most appropriate basic digital security tools to mitigate digital security threats.	I can analyse and assess digital security threats and adapt my protection strategy according to the digital security threat.
	I know how to set up a digital device to ensure protection against basic digital security threats.	I know how to check and update a digital device to ensure appropriate protection against the most common digital security threats.	I know how to install protection tools and software on digital devices to mitigate against digital threats.

4. Threat Detection

Threat Detection	Fundamental	Intermediate	Advanced
Ability to recognise digital threats and the specific risks posed	I can recognise and identify the most common digital security threats to my personal data and information.	I can recognise and identify most rare and unusual digital security threats to my personal data and information.	I actively remain aware of the digital security threats through reliable, up-to-date, and accurate security information sources.
Knowledge to be able to categorise digital threats by level of risk	I can recognise clear and obvious risks and threats in digital environments.	I can recognise obscure digital security threats.	I can recognise complex risks and threats in digital environments.
	I can use my knowledge assess potential security threats and decide if they are suspicious.	I can use my analytical approach to digital security to highlight digital threats.	I can use my critical thinking skills to analyse, compare and evaluate the extent of a digital threat and the associated level of risk.

5. Countering Threats

Countering Threats	Fundamental	Intermediate	Advanced
Taking positive effective decisions whilst remaining calm under pressure. Mental strength to cope with uncertainty and stress and difficult situations.	I am flexible and well prepared for digital security threats.	I use adaptability to counter digital security threats.	I actively anticipate digital security threats and their risks and practice being adaptable to counter them.
	I remain positive when facing digital security threats or breaches.	I can use my own experiences to approach potential threats and breaches optimistically and confidently.	I can explain how positive attitude, behaviours, and actions towards digital security have contributed to my digital security.
	I can reflect on past digital threat encounters to take lessons from them.	I can reflect on past encounters and change my behaviour and attitude towards digital threats them to make myself more resilient to them.	I can reflect on past digital threat encounters and change my behaviour and attitude in life to make myself a more resilient person.