e-protect

Desk Research

Greece

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

movetia

Table of Contents

Profile of the digital elder society

The breakthroughs that have taken place in the fields of technology and medicine have, as a result, a great increase of life expectancy and consequently a new societal reality, where elder people are a bigger part of the world population. Europe is the continent with the highest percentage of elder people to the total population, mainly because of low birth rate and an increase in life expectancy. On 1st January 2010 the average age in Europe was calculated at 40,9 years. Until 2060 European population's average age is expected to be 47,6 years, 15 years more than one century ago. This fact indicates a major change on the composition of Europe's population.

In Greece the same tendency is observed. The percentage of population that is older than 65 grows higher rapidly, because of a reduction in weddings and births, as well as an increase in life expectancy and the accelerating urbanization. According to a research that took place in 2010, women tend to live more years than men, with an average of 4,4 years, 1,7 more years than in 1950.

Since 2004, the largest pan-European social science panel study is taking place, providing internationally comparable longitudinal micro data which allows insights in the fields of public health and socio-economic living conditions of

European individuals. This study is made possible by SHARE (http://www.share-project.org/home0.html). The Survey of Health, Ageing and Retirement in Europe (SHARE) is a research infrastructure for studying the effects of health, social, economic and environmental policies over the life-course of European citizens and beyond. So far, 380,000 in-depth interviews with 140,000 people aged 50 or older from 28 European countries and Israel have been conducted.

The dataset that was collected in Greece offers a view on the basic aspects of elderly's profile in the country. The sample consists of men and women whose age is 50 plus. One first glimpse at the social characteristics of elderly people in Greece gives us the marital status. In detail, 72,3% were married, 4,9 % divorced, 4,6% unmarried and 18,3% have lost their spouse or husband.

One second important social characteristic is the level of education. In Greece at ages 50-59 the average number of years of education is at 10,67 for men and 9,98 for women. At ages 60-69 the average number of years of education is reduced to 9,26 for men and 7,46 for women. At ages 70-79 the average is reduced even more to 7,53 for men and 5,28 for women and at ages 80 plus the average is 6,04 for men and 4,59 for women. It is observed that the percentages are similar to those measured in Italy.

 Lastly, one feature of major importance is the economic background of elderly people in Greece. In general, European South seems to have low average income. In Greece we meet the lowest price of average after-tax income with 18.870 euros annually. Economic recession becomes clear when the question of how hard it is for them to meet the daily needs arises. In detail, 25% find it almost impossible to cope with daily needs, 45,5% encounter difficulties in coping with daily needs, 20,1% find it fairly easy to cope with the daily needs and a 9,4% have no economic troubles. These troubles that most elderly people have to cope with in Greece seem to have raised largely since 2006-2007.

The use of the internet and digital devices among the elderly (65+)

The SHARE project, in the sixth wave, included questions regarding the use of internet among the elderly residents of Europe. The sample of this study includes 61,202 Europeans aged 50 or older from 17 countries. The results showed that almost half of the respondents (49%) use the Internet for several reasons, mainly for e-mails, browsing information and making purchases. A noteworthy fact though, is that this proportion is not the same at all parts of Europe. On the contrary, the proportion varies from Northern and Western countries, such as Sweden and Denmark, to Southern and Eastern countries, such as Greece, Croatia and Poland. It seems that the first group of countries makes a more extended use of the Internet in relation to the second one. This variation is connected with factors such as country's Gross Domestic Product and quality of the information and communication infrastructure. (SHARE)

In Greece, an extensive research regarding the usage of Internet among the elderly has not yet been conducted. Recently, Hellenic Statistical Authority (ELSTAT) studied the use of information and communication technologies by households and individuals, although it includes the total population for the year 2020, not just the elderly population. The results from this study, showed that 8 out of 10 households have access to the internet from their home (80,4%). The percentage had 73,3% increase in comparison to the results of the year 2010. During the first semester of 2020, 8 out of 10 (78,1%) used the Internet. One out of two (52,9%) used the eGovernment services during the time period between April 2019 and March 2020 for personal purposes. During the first semester of 2020, maybe due to the Coronavirus pandemic, 1 out of 2 (47,8%), who have used at least once the internet, made at least one online purchase or order of retail goods through the internet. (ELSTAT)

In 2017 a survey was published at ERKYNA, an electronic scientific journal with free access of the Panhellenic Pedagogical Society of Secondary Education, that studied the reasons and the level of computers and internet usage by the elderly in Greece, as well as their intention to participate in respective educational programs, in order to improve themselves. This study involved, as sample, 155 people from 60 to 74, that lived at Attica, Rethymno, Ahaia, Evoia, Karditsa, Thessaloniki and Rodopi areas, which were randomly selected.

The results offer an insight on the use of information and communication technologies by the elderly people in Greece. To the question, if they have ever used a personal computer, more than half of them (56,13%) answered negatively. A 58,17% answered that they have never used the internet. Among the respondents, that have used personal computer, 9,68% use it about once a month, a 24,52% about once a week and a 9,68% more than twice a week. The respective percentages for the internet usage are 7,10%, 23,87% and 9,68%.

The survey included questions regarding the reasons that elderly people use a personal computer and the internet. Among the most popular answers were reading the news (78,06%), the acquisition of new knowledge and skills (72,26%), communication with loved ones (61,29%) and fight against loneliness (60,00%). 56,13% of the respondents also use a personal computer and the internet for

entertainment, 45,16% use them to keep up with modern lifestyle and, finally, 36,77% use them in order to maintain their autonomy.

The study also enlightens us about the reasons the elderly people choose not to use a personal computer and the internet. Most of them feel unprepared to handle these technologies without some help (84,78%). It is impressive that a big percentage of the respondents (64,13%) choose not to use them because they are concerned about the cost of buying a computer and the cost of the internet connection. Other reasons are: the belief that they are not necessary (60,87%), the lack of trust regarding the protection of their personal data (58,70%), the physical dysphoria that is caused because of their usage (46,74%). Almost half of them report lack of free time (45,65%) and feelings that their age does not comply with the usage of these technologies (45,65%). Moreover, some of the respondents (36,96%) choose not to use pc and the internet because of the stress feelings that their usage causes to them (Alexandrakis, 2017).

Common threats and problems in using the internet

While using the internet is quite beneficial for the elderly people, it also hides a plethora of dangers for the users. Computer security threats are very common and those who try to exploit the users are very inventive and persistent. The result is continuously evolving threats that can harm the users. According to Norton, a widely known company that provides users antivirus and security software for personal computers, almost 500 million consumers have been the victim of a cybercrime according to 2019 Cyber Safety insights report, with about 350.000.000 of them becoming victims during 2019 (The Harris Poll, 2020).

McAfee another company that provides users with cybersecurity products collects the most common threats, that should all be aware of (Gaffney, 2019):

Malware

The term Malware is derived from the words malicious software. It is very dangerous for any computer that is exposed to it. It refers to any software that has been designed to damage a computer and it comes in several forms: viruses, worms, Trojans etc. Usually, our devices stay protected against malware by using an antivirus software.

Computer worm

Computer worms are very dangerous because they can replicate themselves and spread rapidly in a computer or network without requiring human interaction. Worms usually trick internet users and exploit software security holes. A worm, if it infects a device, can corrupt files, steal data, give access to the device to cybercriminals.

Spam

Spam came to mean Unsolicited Bulk Email. Unsolicited means that the Recipient has not given permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content. Although it is usually harmless, it can also hide malicious software.

Phishing

Phishing schemes take many forms and can trick you into clicking links and/or giving sensitive information such as passwords, account details etc. They do so by sending e-mails, through social media messages or by creating fake web pages that impersonate other legitimate ones, like an easily bank web page.

Botnet

Hackers launch a specific malware to a computer in order to be able to control it remotely without your knowledge. They recruit several devices and form a network of computers, which is called botnet, from the words robot network. With this power hackers can attack corporate or government sites and perform a great number of requests simultaneously, which is also known as a distributed denial of service (DDOS) attack. As a result, the site either goes offline or presents long lag time and consequently cost a lot of money to the corporate by causing loss of customers.

It is important to be aware of online threats and be able to protect yourself from online threats. It may seem like an easy task for the new generations that have grown up using a personal computer

or smartphone to safely use the internet. The truth though is that Millennials, although they spend many hours a day online, they are more likely to expose themselves to online dangers. According to Norton Cybersecurity Insights Report of 2015 44% of US Millennials have confronted online threats in the year before the report was published.

The case is not the same when it comes to the generation of Baby Boomers (Years of birth: 1946-1962). According to the same survey only 16% of Baby Boomers have confronted online threats the same year. It seems that, in contradiction with the widely accepted opinion that older users of the internet, that learned in old age to use these technologies, have safer online behavior than Millennials, as they are more careful and tend to keep their passwords to themselves and use more secure passwords (Norton by Symantec, 2015).

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

movetia
Austausch und Mobilität
Echanges et mobilité
Scambio e mobilità
Exchange and mobility

Current strategies, policies and programs for providing relevant education and training

Research regarding national strategies and synergies in internet safety showed that Greece has designed a National Strategy for Cybersecurity for the years 2020 to 2025. This section Includes the measures that it is expected to be taken, in order to protect, in an effective way, digital governmental infrastructure from online threats, as well as the security of citizens and businesses. (MINDIG)

The interventions planned refer to 5 main aspects:

- ➢ Functional cybersecurity governance system
- ➢ Fortification of critical infrastructure, security and latest technologies
- ➢ Optimization of incident handling, fight against cybercrime and privacy protection
- ➢ Modern investment environment with emphasis on research and development
- ➢ Skill development and promotion of awareness

Regarding the protection of citizens' data, Greece follows the European legislation regarding GDPR. This legislation guarantees the protection of our personal data wherever these are collected and preserved, regardless if they are collected in traditional printed version or online. All private companies and public institutions are obligated to abide these rules if they are based or offer services inside the European Union's borders. Every time a company or institution in European Union asks for, uses, reuses or processes personal data must ask the person, whose data are asked, to give his/her clear permission.

Lastly, desk research revealed that the Greek state, in an effort to educate the citizens to protect themselves in an effective way, while they are using the internet, implements some online courses free of charge that are available to all citizens. Some examples:

Digital citizen's academy: an initiative that is implemented by the Ministry of Digital Government and intends to improve citizen's digital skills.

Edugate: Edugate is a website of the Education Portal of the Ministry of Education and Religions that offers educational material for a variety of subjects. Among them there is material regarding online safety.

Greek Safer Internet Center: This center operates since 2016 under the auspices of Foundation for Research & Technology, a research center founded by the Ministry for Education. The center has a website (SaferInternet4Kids.gr) presenting extensive material regarding the use of internet and online safety.

Challenges on addressing the gaps

As it was already mentioned, a high percentage of the elderly people in Greece are afraid of using the internet without assistance. This is a problem that is identified by the Ministry of Digital Government and is included in the Book of digital transformation for 2020-2025 where it is stated that we should focus on creating co-operations in the fields of education, labor and public affairs with special emphasis in vulnerable social groups (people with disabilities, elderly e.t.c.) as well as in social groups that are in danger of being unable to work (women, unemployed, soldiers e.t.c.).

Today, although there are training programs regarding internet safety, they are more general and not planned and organized having in mind the unique needs of elderly people. This is a necessary addition to the existing programs, because elderly people with no experience on using the internet and they need more specialized guidance and educational material designed according to their pace of learning. Elderly people do have suspicions and distrust regarding their safety when using the internet, but they lack the theoretical knowledge of technical aspects of privacy and data protection, legal framework, practices of institutions and possible threats in order to effectively protect themselves.

Skills validation systems and processes

Research regarding the existence of a national qualification framework about digital literacy showed that the Greek state has not elaborated such a framework, but it is planned to do so in the next years in the context of the strategy to invest on the development of citizen's and employee's digital literacy, in order to achieve the country's digital transformation goals.

Research on validation systems that can assess user's skills regarding online privacy has revealed that this subject has been studied a lot in the recent years, as there is a need to identify user's gaps in knowledge, regarding their safety when using the internet. More recent studies are based less on self-assessment methods and more on objective knowledge testing (Trepte et al., 2015).

On 2017 an online privacy competence scale (OPLIS) has been developed in order to provide "an objective and validated measuring instrument to record online privacy competence" (SITE OPLIS). The development took place in two steps:

➢ Literature review and theory development
➢ Empirical development and validation

The design of this validation assessment took in consideration 5 dimensions:

1. Knowledge about the practices of institutions and online service providers
2. Knowledge about the technical aspects of online privacy and data protection
3. Knowledge about potential privacy threats and risks
4. Knowledge about the laws and legal aspects of data protection in European Union
5. Knowledge about strategies for individual online privacy control

The final scale consisted of four dimensions and was comprised of 20 knowledge questions (five per dimension). The creators however propose to estimate this competence as a bi-factor model, which means taking into account global variance as well as domain specific variance (Masur et al., 2017).

Field research summary of results

Online questionnaires

The online questionnaires were gathered on March and April 2021. The questionnaires were disseminated to professionals working with the elderly. In total we received 20 responses.
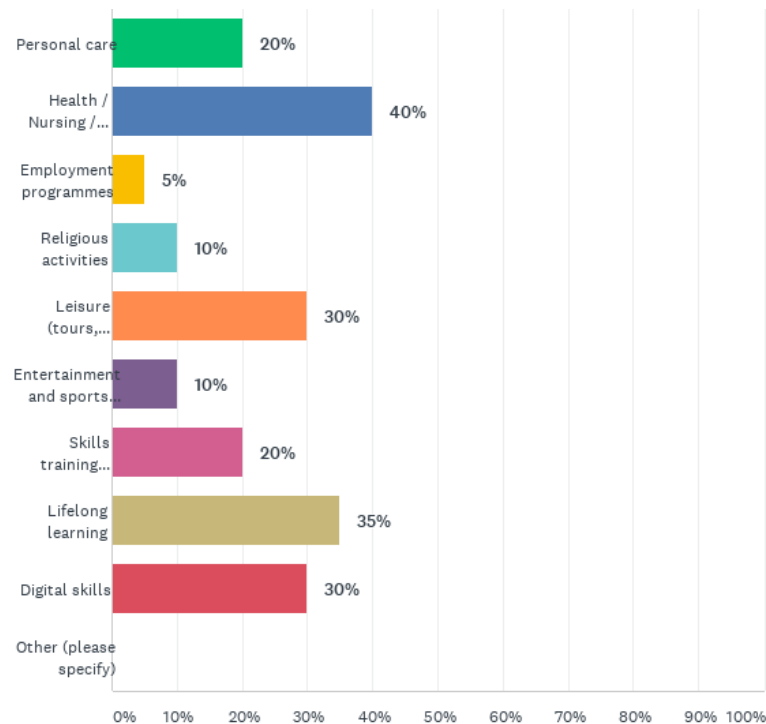

Table 1 What kind of education/training do you offer to the elderly?

Most participants work with the elderly in the areas of health and nursing and in the areas of lifelong learning. As far as the obstacles in the participation of the elderly in digital skills trainings are concerned, the participants provided the following responses:
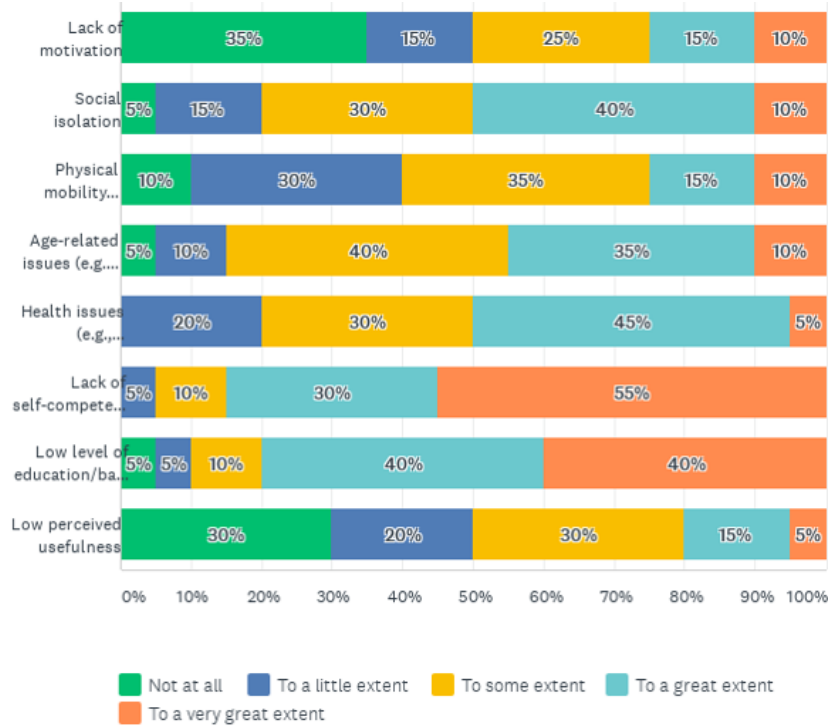
Table 2 To what extent the following challenges affect the participation of the elderly in digital skills training

The most prevalent obstacles are the lack of basic competences and the low level of education/basic skills. Our research also examined the most effective teaching methods, based on the perception of the participants, which could be utilized for the project.
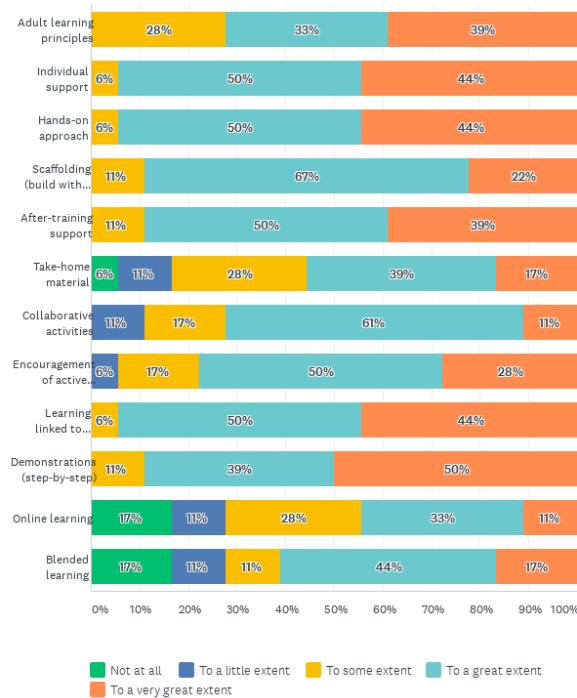

Table 3 To what extent the following teaching techniques/practices respond to the needs of the elderly during digital skills training

All of the methods presented scored high, as most respondents believe that these methods can be effective to a great and a very great extent. However, the top three of methods are the demonstrations, hands-on approach and individual support. It is evident that participants consider the practical experience are one of the most important factors for success in teaching the elderly digital skills.

On the topic of the desired skills, a trainer must have in order to teach digital skills effectively to the elderly, the following table presents the results:
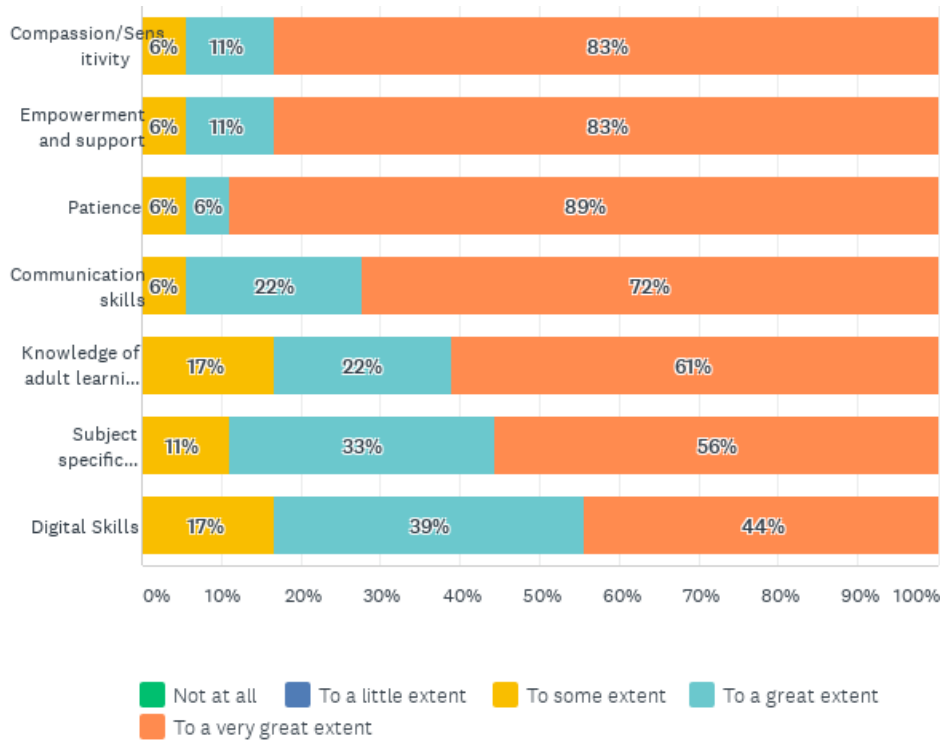

Table 4 To what extent are the following competences of trainers necessary during digital skills training for the elderly

Patience is considered to be the most desired skill for the trainers of the elderly, with compassion/sensitivity and empowerment and support following.
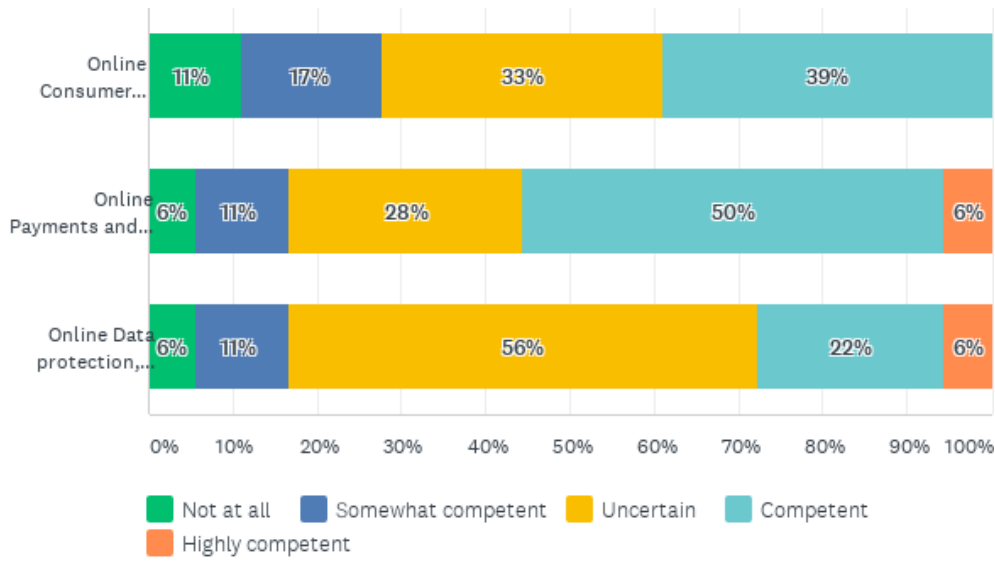
Table 5 How competent are you in

The majority of participants consider themselves competent in online consumer protection and online payments, while the majority is uncertain about online data protection.

On the other hand, participants consider that the elderly are somewhat competent in the presented topics.
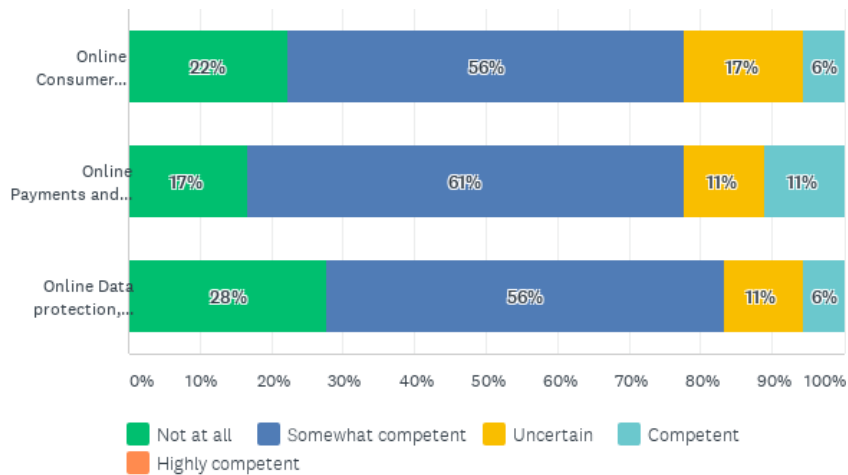

Table 6 How competent do you think elderly are in

Interviews

On March and April 2021 we conducted five interviews with elderly on their perspective on their competencies in consumer and data protection. The results of the interviews are presented in the table below:

Part 1: Familiarity with internet use - Introduction	
Interview 1	*The participant uses the internet on a daily basis for information and social media use. The participant has a tablet and a PC and feels competent in using the internet, due to years of experience.*
Interview 2	*The participant uses the internet daily for studying purposes. The participants has a tablet (most commonly used) and a PC but does not feel very competent.*
Interview 3	*The participant uses the internet on a daily basis to google and communicate with peers. The participant has a laptop and a smartphone and feels quite competent.*
Interview 4	*The participant uses the internet on a daily basis for information, communication and studying. The participant uses a PC and feels somewhat confident.*
Interview 5	*The participant has never used the internet. The participant does not feel competent at all in using the internet and only has a smart TV.*

Part 2: Consumers competence	
Interview 1	*The participant shops online sometimes, in case the price is better online than in a physical store. Before shopping the participant prefers to have communication with the seller in order to get an offer. The participant shops online only from e-shops in Greece and avoids shopping from abroad. The participant does not believe that they are affected by ads.*
Interview 2	*The participant does not shop online, but prefers to "see and feel" the product before buying. The participant does not know the rights of consuments and considers that the threats in online shopping outweigh the benefits.*
Interview 3	*The participant does not shop online. The participant's childrent conduct online shopping on their behalf. The only benefit in online shopping according to the participant are the better prices and the threats are poor quality.*
Interview 4	*The participant does not feel competent enough to shop online and is afraid that their data might be stolen (such as credit card details). The participant knows about the rights of consumers and believes that the main benefits of online shopping is that it is time effective, cheaper and with a wide variety of products.*
Interview 5	*The participant does not shop online and is not competent in online shopping. The participant believes that online shopping offers a bigger variety of products.*

Part 3: Online Payments and Safety	
Interview 1	*The participant uses e-banking services but tries to be carefull with that. Uses a two-step identification procedure to be safe and outlined that the bank has already sent them information on possible dangers in online payments.*
Interview 2	*The participant does not use online payments and e-banking services. The participant stated that is used in the traditional procedure in banking.*
Interview 3	*The participant does not use online payments and e-banking services. The participant considers that it is not safe to make payments through other apps such as facebook and that the only secure app in e-banking.*
Interview 4	*The participant does not use online payments and considers that the biggest threats are hackers, viruses and having the personal data stolen.*
Interview 5	*The participant does not use online payments and considers them dangerous.*

Part 4: Data protection competence

Interview 1	*The participant knows about GDPR and that their personal data is used by third parties and reads the general terms and conditions before accepting. The participant has read about data protection on the internet.*
Interview 2	*The participant has some knowledge about data protection and what terms and conditions means, but is not sure how someone can be protected on the internet and does not know about GDPR.*
Interview 3	*The participant is afraid of accepting terms and conditions and cookies and is not well informed about the topic. The participant is afraid of getting a virus.*
Interview 4	*The participant knows about data protection and terms and conditions but does not believe that there is a way to be safe on the internet no matter what.*
Interview 5	*The participant does not know about data protection on the internet.*

Part 5: Conclusion (areas and competences to be addressed)	
Interview 1	*The participant would like to know more about legal procedures in case of data breach and consider that the basic skill is to know how to be protected in case of an attack.*
Interview 2	*The participant wants to know more about online security, data protection and how data is used by third parties.*
Interview 3	*The participant would like to know more about online payments and security. The main skills someone should have on the internet is to be protected from fake news and false advertising of products.*
Interview 4	*The participant would like to know more about data protection, how data is used by third parties and how to surf safely.*
Interview 5	*The participant would like to know how to use the internet and be safe.*

In conclusion, the majority of participants uses the internet on a daily basis, however only one in five uses it for online shopping and online payments. Most of the participants use the internet to get information and to communicate via social media. Most participants have a basic knowledge on data protection and what terms and conditions mean, but are not very confident on the topic.

Almost all participants agree that they want to know more on data protection and security. Other areas are how data is used by third parties and online payments.

Recommendations

Strategies that are applied on students' education programs regarding online privacy, could be adapted to the project, in order to design more relevant educational material. Online privacy education for children is a popular and sufficiently studied and implemented subject, which could be transferred to learning materials for older populations. Educational practices that target specifically elderly people and their needs could be combined with the designed material.

OPLIS, the privacy competency scale that was analyzed in a previous section could be used as a compass when designing the competence scale, as it includes the basic skills, that are crucial, in order to assess competencies regarding online security and privacy. Nevertheless, the skills mentioned could be further divided in sub-skills, in order to get a detailed picture of privacy competence.

In addition to those skills, the following could also be added:

➢ Knowledge of security tools that are available in the market, such as antiviruses, antimalware, firewalls etc.
➢ Updated knowledge regarding current trends on online threats, for example, passwords known to hackers, common threats, dangerous web-sites etc.
➢ "Healthy" browsing behavior: right practices when using the internet.
➢ In depth knowledge of how their hardware and software work in order to identify weak points and abnormal behavior before it becomes a serious problem.

References

Alexandrakis, D. (2017). Η χρήση των υπολογιστών και του διαδικτύου από ηλικιωμένα άτομα και η πρόθεσή τους για συμμετοχή σε προγράμματα εκπαίδευσης στις ΤΠΕ.

Gaffney, M. (2019). 5 Most Common Types of Threats You Need to Know About | McAfee Blogs. https://www.mcafee.com/blogs/enterprise/5-most-common-types-of-threats-you-need-to-know-about/

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). Diagnostica, 63(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

Norton by Symantec. (2015). NORTON CYBERSECURITY INSIGHTS REPORT. https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt&promocode=DEFAULTWEB%20

The Harris Poll. (2020). 2019 CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS. Norton Life Lock. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?promocode=DEFAULTWEB

Trepte, S., Teutsch, D., Masur, P. K., Eichler, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS) (pp. 333–365). https://doi.org/10.1007/978-94-017-9385-8