education sciences

MDPI

Article

Generational Inclusion: Getting Older Adults Ready to Own Safe Online Identities

Chiara Zanchetta [1], Hannah Schiff [1], Carolina Novo [1], Sandra Cruz [1] and Carlos Vaz de Carvalho [2,*]

[1] Virtual Campus, 4350-151 Porto, Portugal
[2] GILT—Instituto Superior de Engenharia do Porto, 4200-072 Porto, Portugal
* Correspondence: cmc@isep.ipp.pt

Abstract: This article presents an initiative that addresses the problem of the digital literacy generational gap, targeting older adults that struggle to integrate the digital world and are unaware of the dangers of the online environment. The article has a European scope but with a special attention to the Portuguese context. The methodological approach started with a theoretical research on digital and online literacy of adults, followed by the design of an innovative training program specifically designed for this target group and finished with the results of the evaluation of the impact of the training. The overall conclusion, based on the achieved results, leads us to think that it is possible to improve the digital literacy of older adults so that they become effective online users while being alert to the dangers of the online world. Therefore, the work conducted is expected to contribute to a greater awareness of the importance and socio-economic possibilities that arise from the digital and technological investment for stimulating the integration of the older generation in the digital context.

Keywords: adults; cybercrime; online identities; digital exclusion; age digital gap

Citation: Zanchetta, C.; Schiff, H.; Novo, C.; Cruz, S.; Vaz de Carvalho, C. Generational Inclusion: Getting Older Adults Ready to Own Safe Online Identities. *Educ. Sci.* **2022**, *12*, 715. https://doi.org/10.3390/educsci12100715

Academic Editors: Marta Montenegro-Rueda and José María Fernández-Batanero

Received: 10 August 2022
Accepted: 13 October 2022
Published: 18 October 2022

1. Introduction

The digital transformation of the society is an inexorable reality pushed by economical and social factors. In Europe, more than EUR 20 billion have been allocated to finance the digital sector just in the 2014–2020 period. As an example, the Digital Europe Program (with EUR 9.2 billion in funding) had the goal of ensuring that all Europeans had the skills and the infrastructure needed to meet a wide range of digital challenges [1] (p. 10). European Union policymakers also frequently expressed their support for the achievement of the Digital Single Market (DSM), an agreement under which individuals and companies could seamlessly access and engage in online activities, in fair competition, with a high level of consumer and personal data protection, irrespective of their nationality or place of residence.

It is therefore not surprising that more and more people worldwide have online access and spend more time online [2]. The same source indicates that, since 2011, the time spent online per capita (either through a desktop or a mobile device) has more than tripled and is now close to 192 min per day. Adding to this, the change in the socio-economic context caused by the global coronavirus pandemic, has resulted in an even more significant increase in online data movement worldwide in the past few years.

According to the World Health Organization [3] (p. 1), the number of people aged 60 years and older was 1 billion in 2019, and the expectancy was that this number would increase to 1.4 billion by 2030 and to 2.1 billion by 2050. Not only is this growth occurring faster than ever before, but it is even more accelerated in developed countries. Europe, in particular, is already facing a visible populational aging. Therefore, experts in aging and health are focused on the factors that promote successful aging, such as technologies that enable older adults to connect, create and contribute to society for a longer time [4–6]. They point out that aging, health and technology will be inextricably linked in the future and seniors will increasingly depend upon technology because the number of available

caregivers will not keep pace with the social demand. Yet, and although more and more people recognize digital technology as a useful tool for maintaining the seniors' autonomy and independence, only few investments have been effectively made to understand more about aging and the specific needs of this group in terms of technology adoption [7].

To live in a society mediated by digital technology in its cultural, economic and social levels means that people affected by digital exclusion have a reduced ability to fully participate in the society, and consequently, have less independence to manage their own life decisions. Particularly, the exclusion of the elderly from the digital world will have consequences because they will feel left behind and not a part of the modern world [8,9]. Additionally, even if the digital environment expands the offer of new opportunities by democratizing the access to open information, many older adults still lack the skills, confidence or the opportunities to learn about how to use digital technologies, and consequently, a considerable percentage of the adult population lives either excluded from the online world or are not aware of the dangers lurking in the Internet, becoming susceptible targets for a wide range of cybercrimes.

In fact, the access to information and communication technologies by itself does not promote the inclusion of people who are excluded from the "technical skills, status markers, and content structures that are fast becoming key institutional features on the Internet age" [10]. Additionally, due to the rising use of the Internet and the change in the Internet use paradigm where users are now creators of information, an increasing amount of personal data is constantly being transmitted online, which raises the attractiveness for online criminal acts. This trend affects the vulnerable adult population, making them more targetable by cybercriminals because they do not understand the importance of keeping personal data private or because they believe too easily on the truthfulness of the data provided by others, thus being targeted by a third party who is disguised by a false identity.

1.1. Internet Security

The Special Eurobarometer 480 regarding Europeans' attitudes towards Internet security [11], a compilation of the main findings on the topic, found that the daily use of the Internet has increased consistently since 2013, achieving, in 2018, a mark of 73% of the entire population. A more recent analysis showed that in 2020, this percentage increased even more to 79% [2].

The same research showed that most Europeans thought that cybercrimes were serious offenses but just over half of respondents knew someone who had been a victim of cybercrime in the previous three years. Most of the respondents expressed at least some degree of concern about becoming a victim of this type of crime and nearly 8 in 10 said that they believed that there was an increasing risk of being a victim of cybercrime (79%). Around 7 in 10 respondents expressed concern about falling victim to the infection of devices with malicious software, identity theft, bank card or online banking fraud. Slightly fewer were concerned about the possibility of encountering child pornography (67%), hacking of online social networks or email accounts (67%) or online material promoting racial hatred or religious extremism (65%). Around six in ten respondents were concerned about the prospect of becoming a victim of a cyberattack which could shut them out of online services (61%), a demand for payment in return for regaining control of a device (60%), fraudulent emails or phone calls (60%) or online fraud where bought goods are not delivered, are counterfeit, or are not as advertised (58%).

A new concern with online security derives directly from the new web paradigms, where the online environment turned to be a collaborative and co-creation place where people connect, produce, share, and consume information. People are encouraged to upload their data online in social networking or social media sites. This means that, nowadays, a significant amount of personal data is at the disposal of online companies and individuals that through advanced data mining and machine learning technologies are capable of extracting information and exploiting it for different purposes. A major concern is related to the use of such data without the users being informed or even aware of that use. So, the

misuse of personal data is already amongst the most significant concerns of Internet users and more than 4 in 10 (43%) respondents are concerned about the possibility that their data might be misused by a third party.

A major problem with cybercrime is the difficulty in gathering precise and reliable statistics as most victims do not report when they are attacked (sometimes they do not even realize they have been attacked or they just discover it some time after) for personal or commercial reasons (in the case of organizations) [12]. Security services report that only 12% of the victims of cybercrime reach out for help from specialized companies or public security forces. Reep and Jonger conducted a meta-analysis of different cybercrime surveys in Europe and came to conclude that the prevalence of online shopping fraud (mostly addressed at individuals) ranges from 1 to 3% and less than 1% of the population are victims of other types of cyber fraud—"Phishing and social engineering are the main vectors for payment fraud and are still increasing in both volume and sophistication" [13]. Online bullying affects about 3% of the population and up to 6% are victims of hacking. Malware can reach 15% of the online users according to the most extreme surveys [12]. For companies and public institutions, ransomware affiliate programs are becoming a major issue following business email compromise [13]. The yearly total estimated cost of cyberattacks (both to individuals and companies) in Europe is estimated to reach the value of 100 billion (10^9) euros [14].

The European Union's General Data Protection Regulation (GDPR), launched in May 2018, represents a common EU approach to the protection of personal data, trying to reinforce trust by putting individuals back in control of their personal data and at the same time guaranteeing the free flow of personal data between the EU Member States. Over two thirds (67%) of Europeans have now heard about the GDPR and more than half (57%) know that there is a dedicated public authority in their country that is responsible for protecting their data and personal rights surrounding it, however, only one in five know which public authority is specifically responsible and dedicated to protecting them.

In summary, it seems that there is a small majority of Internet users that do know that the use of online environments does carry some risks. However, the number of people that are unaware of these risks is still very high and most of the older adults fall into this category. On top, even for those that are aware of the dangers, there still seems to be some relaxed feeling that this will only happen to others so they do not take adequate precautions while using the Internet.

1.2. The Portuguese Perspective

In terms of digitalization, Portugal ranks among the best countries on the EIBIS Digitalisation Index [15] because the adoption rate of digital technologies is above the EU and US averages in the infrastructure and services sector. Almost 60% of Portuguese digital companies report having increased the number of employees in the last three years, compared to 50% of non-digital firms, and the median wage per employee is slightly higher for digital than non-digital firms, but still below the EU average. In the latest Hootsuite report on Internet, mobile, and social media stats for Portugal [16], there were 8.58 million Internet users in Portugal in January 2021 (roughly 84% of the population), and the number of social media users in Portugal was equivalent to 76.6% of the total population in January 2021.

The National Communications Authority estimates that the state of emergency due to the COVID-19 pandemic led to a 49% increase in the Internet data traffic compared to the period prior to the mandatory confinement [17]. Regarding mobile broadband Internet access traffic, there was also an increase of 25.6% compared to the third quarter of 2019. Most recently, in 2021, there was also an increase of 25.1% compared to the same period of the previous year in the average monthly traffic per active mobile Internet user [18]. Unfortunately, this does not mean that the online population is actually prepared to deal with the dangers and uncertainties of the online world, and this also does not mean that all the population has the same level of access. In Portugal, the senior population still

has strong numbers of digital exclusion [19] (p. 1). According to the Portuguese Statistics Institute, 99% of people 16 to 24 years old and 98% of people between 26 and 34 years old use the Internet while these number fall dramatically for people between 55 and 64 years old (53%) and between 65 and 74 years old (33%) [18]. Additionally, 52% of the Portuguese population between 55 and 74 years old never used the Internet [20].

2. Theoretical Framework and Key Terms

The Adults, Data, and Emerging IDentities (AUDID) project, co-funded by the European Commission, was organized by a consortium composed by 7 partners from 6 countries: Portugal, Croatia, Greece, Italy, Slovenia and The United Kingdom. The nature of the Internet which operates with no borders made it necessary to bring together a range of multinational actors to achieve the project objectives accounting for different national and cultural perspectives and circumstances.

The project was born in the context of the increasing demand for methods to deal with the adult population (with a focus on 55+) who face social exclusion and/or vulnerability when it comes to the use of digital tools and Internet safety. The aim was to enhance their awareness about online identities through the development of practical, motivating, and comprehensible training, as well as learning tools so they can protect themselves against dangers emerging from online presence and cybercrime. The project therefore contributed to the fight against senior exclusion by improving their quality of life, social participation, and cohesion, and consequently, increasing their online confidence and trust. Adults, especially those aged 55 or older, need to learn to appreciate the relevance of data that they provide and receive. They need to learn how to validate incoming data—checking the accuracy and quality of the sources before using, importing, or otherwise processing it, and to assess when to provide and validate outgoing data, understanding the relationship with their online identity.

Often, it is hard for adults to grasp this relation, as the identity emerges from ever more validated data, therefore they should not only be taught what to do and what not to do but they should internalize the reasons behind each practice. Through the internalization process, the learner allows the information to affect them, therefore, shaping their values and character to later manifest the content learned in their beliefs and behaviors. Accordingly, the consortium designed and delivered an innovative experiential pedagogical approach and a set of interactive digital learning tools to enhance the understanding on the subject and the development of related competences, such as critical thinking, together with a structure for the recognition of skills and achievements through Open Badges.

To design the approach, the consortium conducted a research identifying the existing practices carried out on online identity and related safety measures so that it would be possible to develop content with the specific features required to supply the needs of adults in vulnerable situations. The final implementation structure derived from three main resources; (i) the methodological framework—studies aiming at understanding the emergent place the Internet has in adults' lives and the potential consequences of its use, (ii) the investigation between individual characteristics and Internet use, and (iii) national feedback—identification of the best practices carried when using the Internet and its effects regarding online identity. In addition to desk research, partners conducted field research through an online anonymous survey that questioned different aspects of online identities such as information that users might have created to be represented in a particular situation (e.g., on social media), information that companies provided in relation to the collection of data, information they had on the data that companies kept on them, attitudes, emotions, and symptoms that people might have because of excessive Internet usage, including Internet Addictive Behavior (IAB) and concerning potential risks in situations such as viewing pornography and content that encourages hate and violence, cyberbullying, abuse of online personal information, etc.

In Portugal, respondents were between 32 and 55 years old (73%) and over 55 years old (9.8%). For most of them, false online identities were the biggest problem while Internet

addiction was not a major issue. They considered themselves to be reasonably prepared to deal with situations in which excessive Internet use could interfere with normal life and to deal with misused online identities. Half of the respondents considered that fraudulent online identities could be a cause for losing job opportunities. The most frequent pieces of information put in their online profile was their name (90%), their real age, and personal photos. The name was also the most used information respondents shared when they played online games. Most of them answered that they were not worried about becoming the victim of online bullying or harassment. Most respondents thought that profiling is a good idea and they did not felt worried, nervous, panicky, tense, keyed up or anxious when they could not use the Internet.

After analyzing the answers in all the countries, the user model was adapted to meet the researched needs, to increase the accessibility and impact of the content and tools towards ensuring an active engagement with as many adults and educators as possible, with close attention to the conclusion that online identities were the biggest problem on the Internet (even if, in most of the countries, were considered as reasonably prepared to deal with misused and misinterpreted online identities). As adults should understand the significance of data provided and received, incoming and outgoing data knowledge should be validated by applying critical thinking. The approach used by the project is to make adults understand how seemingly random data fragments could make up parts of an identity.

3. Methods

The solution to support the encountered needs of the adult population was implemented in three vertices. The first two were related to the creation of a new interactive multimedia curriculum for adults and adult educators which could empower a conscious, creative and critical stance by adults as responsible civilians towards online behavior by means of training in essential skills and providing essential knowledge, and the provision of tools to facilitate the understanding of risks associated with emerging online identities and to demonstrate in visual and effective ways how random data manifests to building blocks of an identity. The last one related to supporting tools by means of practical exercises providing essential knowledge to adult educators who could later implement the training by themselves, adopting the key role of facilitator. The solution relied on interactiveness, that is, was based on experience rather than theory; facilitating learners' engagement; linking to the growing importance of visual information, and with a dual implementation feature—within a classroom but also online.

The first part was implemented in the form of a Curriculum and Trainer's Guide composed of 5 modules:

- The first module concerns the Online Identity Theory and approaches the idea that the Internet may be defined as a socio-technical system that relies upon the necessary infrastructure machines, protocols and programs as well as social groups and social shifts. The first topic within this module is about how the online world formats itself in and creates a parallel social structure where every user builds his/her online identity. The second topic defines that the representation of social structures is recreated in the ecosystem through social media. The online presence, specifically on social networks, brings a plethora of benefits to the user, for instance, easy and immediate access to services and information, fast communication and communicability as well as emotional and social presence. Nevertheless, being an online actor does not come cost-free: risks and threats related to security, ethics, privacy, legacy, and psychological well-being are always a reality. The third part of this module deals with the identity theories developed within a specific set and wide framework: online gaming. Starting from the definition of who may be named as gamer and which characteristics define this identity, the module analyzes the impact of online games on the gamer construction.
- The second module regards Online Identities and Profiling, describing the multiple viewpoints addressing identity as more than just a collection of data. Although digital

identity may be completely disconnected from real-life perceptions that are a part of offline communication, the concept of 'fixed identities' undergoes corrosion and authenticity, and accountability might need new consideration. This module aims to increase awareness about online identities and has 3 main topics, namely, identities and online profiling, online profiling how and why, and profiling tools and techniques.

- The third module approaches an Online Safety and Prevention theme and discusses the fact that the Internet offers a plethora of benefits, and it is completely impossible to escape its presence. However, despite the benefits that it provides, it can also provide a multitude of risks and so one has to be aware of them and the general safe practices in regard to Online Security, Malware, and Social Media. To achieve the development expected, the content was divided into 4 topics: The first related to safe online behavior, the second topic is about the protection against malware software, while the third approaches safe social media practices, and the fourth and last topic regards online identity management.
- Module number four addresses Good Practices Regarding Interactive Didactics and introduces new participatory approaches towards a blended learning experience. More specifically, it explains how digital tools can personalize learning in adult education. In addition, serious games and mentor-based learning are also examined from the point of view of the trainers. The content of the module is divided into four topics, namely, educators and adult learners as co-learners, personalization of learning by using digital content and tools, how to learn through play and serious games, and introducing mentor-based learning platforms.
- The last module regards Educational Technology and Good Practices. This module addresses 3 different examples of educational technologies: blended learning, flipped classroom, and eLearning. In the module, the user obtains basic information on definitions, advantages, and disadvantages of all three above-mentioned educational technologies. It offers steps to follow when creating a blended learning module, flipped class module, or eLearning module.

Content delivery relies on video lessons and interactive material complemented with textual material for reference. All modules include a glossary of relevant terms to make it easier for adults to understand the content. Assignments are provided to allow learners to write essays on different topics related to the contents which can later be uploaded to social media channels. A quiz with multiple questions is also provided at the end of each lesson for the learners to test their acquisition of knowledge.

To apply the acquired knowledge in the real world and relate it with daily situations, the project has developed a dynamic demonstrator, that is, an interactive web-based digital tool based on real-life scenarios. This tool is available in all national languages and includes 28 different scenarios. These scenarios are a translation of real situations that people face online, related to the topics addressed in the modules. In each scenario, the user assumes a role in a situation where characters are performing actions, which must be labeled as correct or incorrect, considering its level of security or adequacy. This dynamic tool serves as a valuable, indispensable methodological instrument for adult learners to use during any education program, to empower their learners' transversal skills, thereby extending and developing their professional competences on the issue.

All the previously mentioned features are integrated in a delivery environment configured as a Learning Motivation Environment (LME) that supports social and peer learning, the interactive multimedia curriculum, and the dynamic demonstrator. LMEs deliver the training, capitalizing on motivational workflows and gamification mechanics for engaging learners in a social learning environment which motivates learners. To deliver the training, educators will themselves be trained on the LME which also features a content creation tool which they can use to prepare their own content. The LME integrates the Open Badges API that provides certification based on metadata principles: issuer, earner, criteria, and evidence to create a 'network of trust' for the visibility, recognition, and validation by the community, local authorities, etc. In this way, participants are engaged in completing

all levels of skills acquisition. Through the introduction of this method, verification is made possible, as well as the validation and the awarding of the online identities' skills, furthermore, achieving transferability, credibility, and transparency of the non-formal learning and permeability in formal education through the online verification of the skills and achievements of the participants in the form of portable digital badges. In total, there are 9 badges:

1. Online Identity Theories Expert Badge—earned after having skills evaluated in Module 1 "Online Identity Theories".
2. Social Networking Literate Badge—earned after having evaluated skills in Topic "Social Networking: Risks and Benefits".
3. Online Identities and Profiling Expert Badge—earned after having evaluated skills in Module 2 "Online Identities and Profiling".
4. Location Tracking Aware Badge—earned after having evaluated skills in Topic 3 "Profiling Tools and Techniques", this badge ensures that the learner has acquired the knowledge of how to avoid revealing personal data.
5. Online Safety and Prevention Expert Badge—earned after having evaluated skills in Module 3 "Online Safety and Prevention", this badge ensures that the learner knows how to adopt a generally safe online behavior.
6. Malware Prevention Aware Badge—earned after having evaluated skills in Topic 2 "Protection against Malware Software", this badge ensures that the learner has acquired information about malware security, protection, and prevention.
7. Interactive Didactics Expert Badge—earned after having evaluated skills in Interactive Didactics.
8. Educational Practices Expert Badges—earned after having evaluated skills in Educational Technology and Good Practices.
9. Finally, the AUDID Master Badge—earned after having evaluated skills in all the modules, this badge ensures the acquisition of the highest level of skills in Online Identities.

The Academy is multilingual and all the features are free. It includes trainers' guides so that adult trainers can manage hands-on workshops for classroom-based or online training of adults using the curriculum, delivery environment, and supporting tools (i.e., demonstrator), and also how to create and issue Open Badges for recognition of the skills and achievements. The Academy is complemented with support for newcomers through the networks of educators, users, and enthusiasts supported by dedicated social media groups and powered by the resources made accessible through the website.

The Academy serves as an online active community sharing knowledge and experiences in the wider area of Online Identities and Internet Safety. Moreover, it offers an assistance request functionality in which anyone can submit issues and questions to the community using the ticket manager and that is expected to be answered in the maximum period of 48 h. There is also the possibility to arrange real-time online help for the solution of any problem or for assistance. By registering on the forum, the learners have access to the collective wisdom of the online community of the project and the chance to place opinions, doubts, or to help others with the training program.

To validate the project's outcomes with the target group, a pilot testing phase was implemented, which consisted in a presentation of the project and its resources, followed by a practical training activity.

In Portugal, and due to the pandemic situation at the time, the number of persons able to participate locally was restricted, therefore the two pilot training workshops were organized in a combination of face-to-face (6 persons) and online (20 persons). Most participants (17) were over 55 years old, the others were between 25–35 years old (1), 35–45 years old (3), and 50–55 years old. Nine of them were adult educators. After the workshop, participants were asked to fill a survey with quantitative and qualitative questions to assess the effectiveness of the tools and of the training. A short collective discussion followed to gather additional qualitative information.

4. Results

In general, participants considered the organization of the training very positive, and all the participants were willing to be involved in a similar activity in the future. The only less positive item was the duration of the training which some participants considered short (Figure 1).

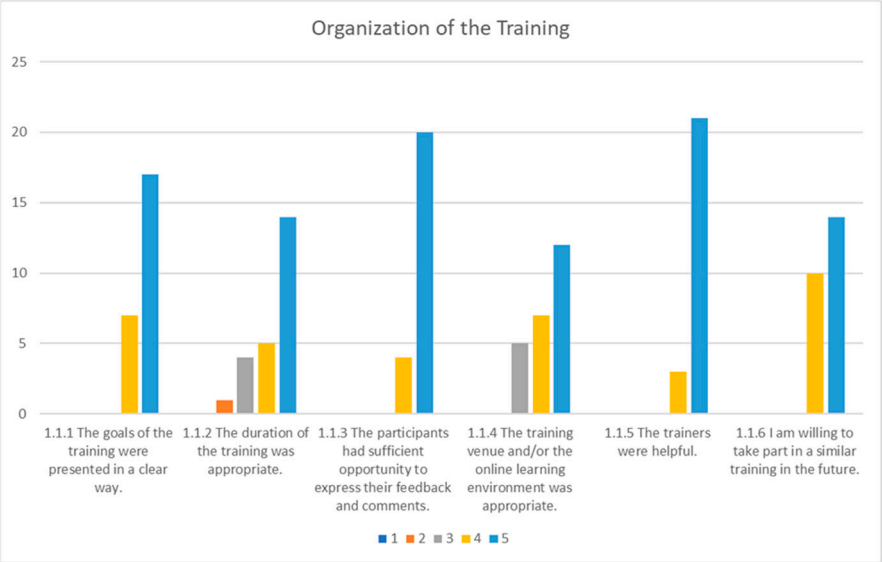

Figure 1. Participants' perception on the organization of the training.

In relation to the specific modules, participants had diverging opinions. When asked about the "Online Identity Theory" module, the participants said that they liked it very much and they considered that the training improved their knowledge and contributed to their confidence. However, some participants did not feel that the goals were clear enough and some did not like the self-assessment exercises. Regarding the second module "Online Identities and Profiling", the participants liked it but some participants mentioned that it was not as relevant for them. The module on "Online Safety and Prevention" was, by far, the one considered more relevant for the participants. The module about "Interactive Didactics" was not so well regarded, which is natural considering that it was targeted mostly at trainers. The subsequent module on "Educational technology" was considered not so relevant for them. There were also many neutral opinions in relation to the contents, exercises, and knowledge acquired.

Participants reported that the event allowed them to have more knowledge about safety on the Internet (70% of respondents) and that they would change their behavior online (52% of respondents). They also mentioned that they wanted to further improve their knowledge about safety on the Internet (73% of respondents). Participants expected to use project results in their personal life (83% of respondents) and in their work life (52% of respondents). They would be interested in participating in future similar events (74% of respondents agreed completely).

The supporting tools were, in general, positively considered as can be seen in Figure 2. Some participants had experience with online platforms, so it was easier for them to understand how to use it but for others, it was a bit more complex to understand the operations (e.g., registration process).

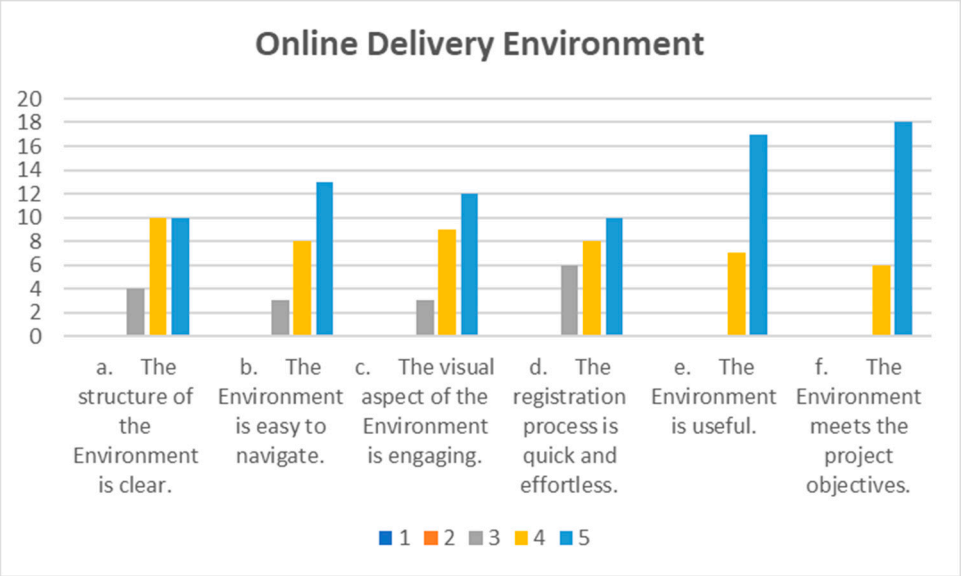

Figure 2. Participants' perception of the online environment.

Participants liked the Dynamic Demonstrator very much, and considered that it had a clear structure, and it was relatively easy to use, therefore the scenarios were useful (Figure 3).

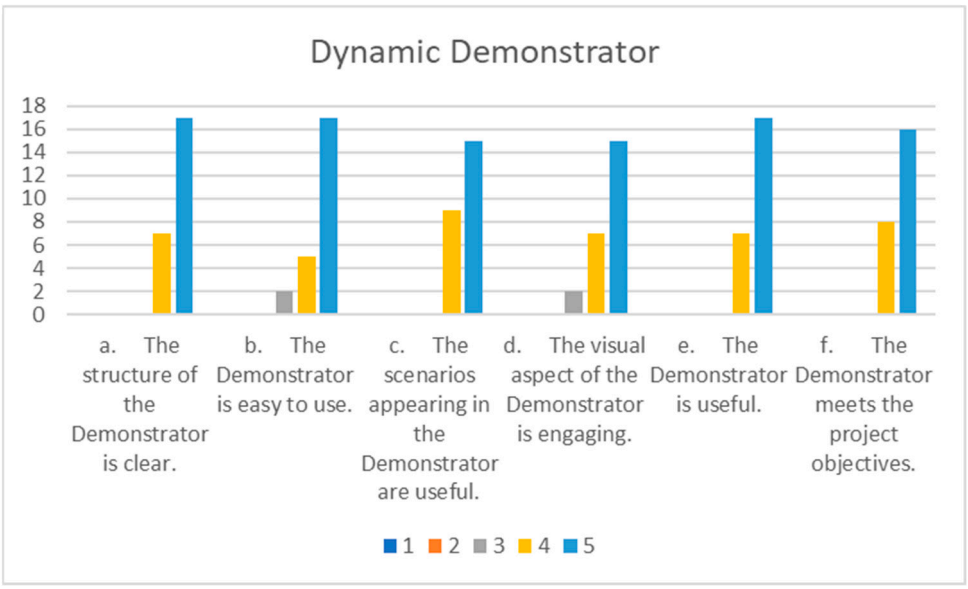

Figure 3. Participants' perception of the Dynamic Demonstrator.

Some participants liked the concept of Open Badges, but others were uncertain about it and did not feel that it motivated them (Figure 4).

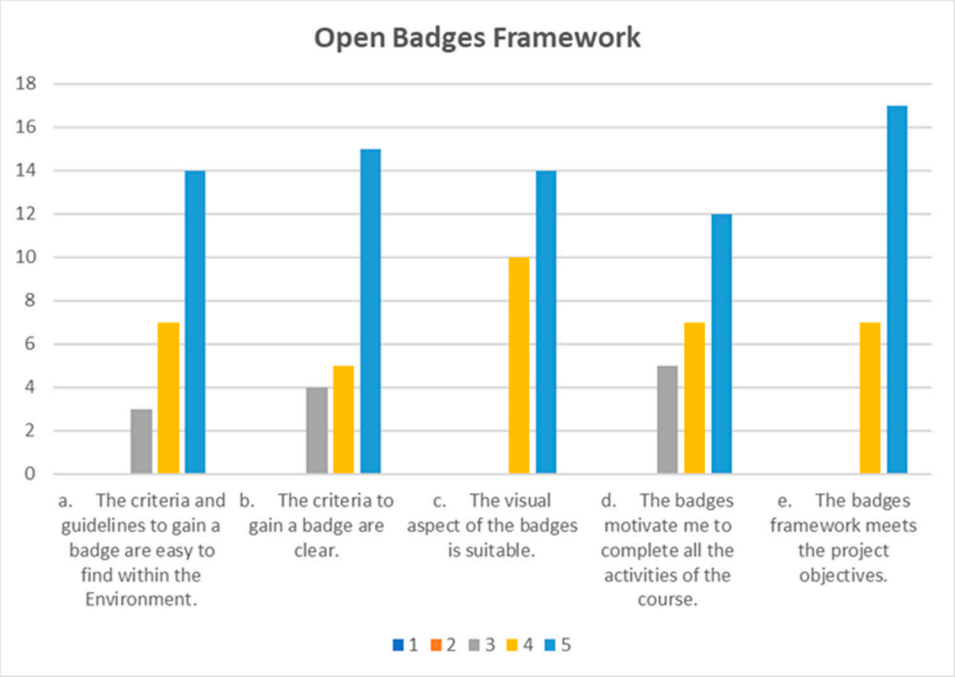

Figure 4. Participants' perception of the Open Badges Framework.

All the participants wrote that they were interested in further using the products after the completion of the study, would use the Academy in the future, and that they would recommend it to others. Some comments provided interesting clues for future improvements:

- "Correct some Portuguese language mistakes",
- "Add more information and contents about Online Safety",
- "Fake news is a very important topic today",
- "More depth in some topics as they are too vague",
- "Have a more complete and longer course based on this one",
- "Prepare a more advanced edition for some of the contents".

5. Discussion and Conclusions

Two major trends that affected the European society relate to the evolution and diffusion of digital technologies and the aging of the population. The need for the use of technological resources has been growing and making computers a symbol of contemporary culture, regardless of age group. In the elderly, one of the risks suffered is the stagnation of the learning process and their difficulty in developing a level of digital literacy that not only ensures their access to information, but that allows them to place themselves in the right position to use this information adequately.

The AUDID project expected to remove the barrier of the unknown for older people, as they would see themselves integrated in the modernized world. That is, the project hoped to promote awareness among adults regarding the risks of online identities and making the Internet a safer place for them, while increasing the trust of adult consumers in online activities and subsequently facilitating the growth of e-Commerce. It was clear from the early days of the project that apart from the functionality and the facilitation provided by the project's tools, the most important aspect of the project was its success in providing an innovative and interactive learning environment for the trainees. Through this effort, an increase in the skills level and self-confidence of the adults could be seen, consequently enhancing the older learners' self-efficacy and motivation to learn.

The outputs are still available and completely accessible (upon request to the authors). Some curriculum changes have been introduced in the meantime due to the technological

evolution of some of the addressed tools and also to changes in the forms of cyberattacks. The commitment of this resource made it possible for the partner to sustain for a substantial amount of time past the life of the project, and further expectations are for the network to grow, as other enthusiasts who are already using the outcomes of the project volunteered to help others, newcomers, to use the results. Therefore, experienced users are encouraged to become volunteers in the network and frequently intervene to assist newcomers.

Older people are important consumers of government services and are a growing market for commercial products and services. Therefore, the project shores up the economic benefits of the expansion of the elderly technological market with more and more elderly finding their footing in the digital world. They are adding fuel to the already booming silver economy and walking toward the mitigation of the digital gap for the elderly.

Author Contributions: Conceptualization, C.V.d.C.; methodology, C.V.d.C.; validation, C.V.d.C.; formal analysis, C.N., C.Z. and S.C.; investigation, C.N., C.Z. and S.C.; resources, C.N., C.Z. and S.C.; data curation, H.S., C.N., C.Z. and S.C.; writing—original draft preparation, C.Z.; writing—review and editing, C.N.; supervision, C.V.d.C.; project administration, C.V.d.C.; funding acquisition, C.V.d.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Commission grant number 2018-1-HR01-KA204-047433 and the APC was funded by the GILT R&D group.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Negreiro, M.; Madiega, T. *Digital Transformation*; EPRS—European Parliamentary Research Service: Brussels, Luxembourg, 2019; p. 10.
2. Eurostat. Data Explorer. Available online: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_ifp_fu&lang=en (accessed on 22 March 2021).
3. World Health Organization. Decade of Healthy Ageing 2020–2030. Available online: https://www.who.int/docs/default-source/documents/decade-of-health-ageing/decade-ageing-proposal-en.pdf?Status=Temp&sfvrsn=b0a7b5b1_12 (accessed on 22 March 2021).
4. Dahlke, D.; Lindeman, D.; Ory, M. 70% of seniors are now online and using technology. In Proceedings of the World Economic Forum, Davos, Switzerland, 22–25 January 2019.
5. Gilhooly, M.; Gilhooly, K.; Jone, R. Quality of Life: Conceptual Challenges in Exploring the Role of ICT for Ageing. In *Information and Communication Tecnologies for Active Ageing in Europe*; Cabrea, M., Malanowski, N., Eds.; IOS Press: Amesterdam, The Netherlands, 2013.
6. Sixsminth, A.; Sixsmith, J. Smart home technologies: Meeting whose needs? *J. Telemed. Telecare* **2000**, *6*, 190–192. [CrossRef] [PubMed]
7. Vaz de Carvalho, C.; Cano, P.; Roa, J.M.; Wanka, A.; Kolland, F. Overcoming the Silver Generation Digital Gap. *J. Univers. Comput. Sci.* **2019**, *2*, 1625–1643.
8. Khvorostianov, N.; Elias, N.; Nimrod, G. Without it I am nothing': The internet in the lives of older immigrants. *New Media Soc.* **2012**, *14*, 583–599. [CrossRef]
9. Vaz de Carvalho, C.; Cano, P.; Roa, J.M.; Wanka, A.; Kolland, F. Digital Information Access for Ageing Persons. In Proceedings of the 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), Mumbai, India, 9–13 July 2018; IEEE: Picataway, NJ, USA, 2018; pp. 345–347.
10. Witte, J.C.; Mannon, S.E. *The Internet and Social Inequalities*; Routledge: London, UK, 2010.
11. European Commission. *Directorate General for Migration and Home Affairs. & Kantar. Europeans' Attitudes towards Cyber Security*; Publications Office of the European Union: Luxembourg, 2020.
12. Reep-van den Bergh, C.M.M.; Junger, M. Victims of cybercrime in Europe: A review of victim surveys. *Crime Sci.* **2018**, *7*, 5. [CrossRef]
13. Europol. *Internet Organised Crime Threat Assessment (IOCTA)*; Publications Office of the European Union: Luxembourg, 2021. [CrossRef]
14. McAfee. Economic Impact of Cybercrime No Slowing Down. 2021. Available online: http://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (accessed on 22 March 2021).

15. Ambrosio, F.; Rückert, D.; Europäische Investitionsbank. Who is Prepared for the New Digital Age? *Evidence from the EIB Investment Survey*. 2020. Available online: https://www.eib.org/en/publications/who-is-prepared-for-the-new-digital-age (accessed on 22 March 2021).
16. Kemp, S. Digital in Portugal: All the Statistics You Need in 2021. DataReportal—Global Digital Insights. 2021. Available online: https://datareportal.com/reports/digital-2021-portugal (accessed on 22 March 2021).
17. ANACOM. COVID-19 Continua a Impulsionar o Aumento do Tráfego de Voz e de Internet Móvel no 3.° Trimestre de 2020. Available online: https://www.anacom.pt/render.jsp?contentId=1584500 (accessed on 22 March 2021).
18. INE (Instituto Nacional de Estatística). *Inquérito à Utilização de Tecnologias da Informação e da Comunicação Pelas Famílias*; INE (Instituto Nacional de Estatística): Lisbon, Portugal, 2020.
19. Rebelo, A.C. *Seniores em Rede: Motivações para o Uso da Internet e do Facebook Pelos Mais Velhos*; ISCTE-IUL: Lisboa, Portugal, 2013.
20. European Commission. Europe's Digital Progress Report 2017—Profile of Portugal. 2017. Available online: https://ec.europa.eu/digital-single-market/en/scoreboard/portugal (accessed on 22 March 2021).