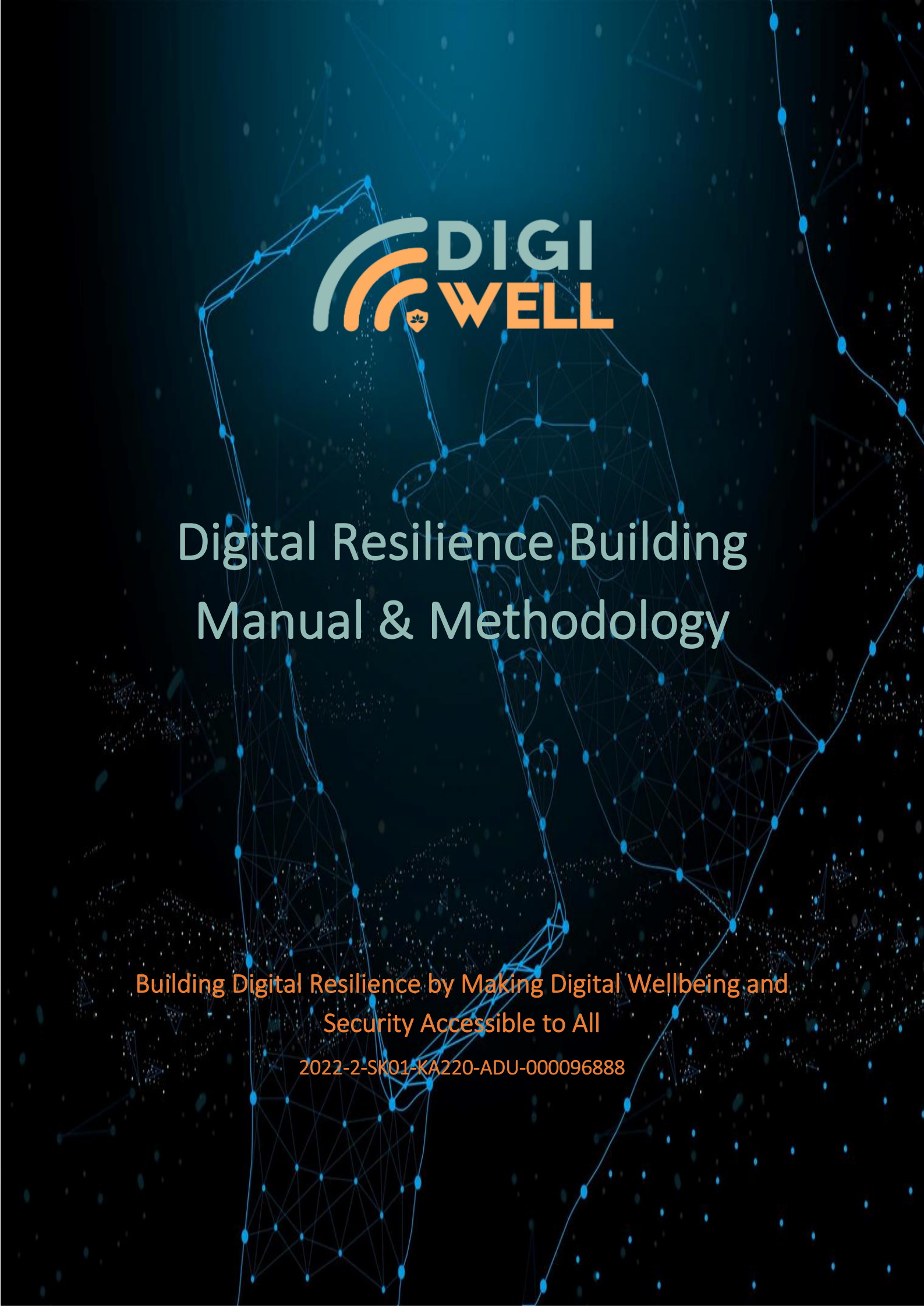

Digital Resilience Building Manual & Methodology

Building Digital Resilience by Making Digital Wellbeing and Security Accessible to All

2022-2-SK01-KA220-ADU-000096888

Co-funded by the European Union

Erasmus+ project KA220 Cooperation partnerships in adult education

Building Digital Resilience by Making Digital Wellbeing and Security Accessible to All

2022-2-SK01-KA220-ADU-000096888

DigiWELL

Digital Resilience Building Manual & Methodology

September, 2023

Co-funded by the European Union

This publication was prepared as the result of the project “Building Digital Resilience by Making Digital Wellbeing and Security Accessible to All” (Project No: 2022-2-SK01-KA220-ADU-000096888), which is implemented in the frame of the Erasmus+ KA220 Cooperation partnerships in adult education.

DigiWELL Consortium

Slovak University of Agriculture in Nitra, Slovakia

Muğla Sıtkı Koçman University, Turkey

Czech technical university in Prague, Czech

Innovation, Training, and Employment Association for Sustainable Development (AIFED), Spain

European Institute for Innovation – Technology (EIfI-Tech), Germany

Foundation Maker's Place Private Company (Found.ation), Greece

Syzigia Skopje Foundation (SYZYGY), Macedonia

Faculty of Economics and Management
Slovak University of Agriculture in Nitra |
Tr. Andreja Hlinku 2 | 949 76 Nitra | Slovakia | email: digiwell@uniag.sk

Website: www.digiwell.sk

Disclaimer:

Work Package 2: **Digital Resilience Building Manual & Methodology**

List of Contributors: *Murat Sümer, Czech Technical University,*

David Vaneček, Czech Technical University,

Martina Hanová, Slovak University of Agriculture in Nitra, Slovakia

Marcela Hallová, Slovak University of Agriculture in Nitra, Slovakia

Eva Oláhová, Slovak University of Agriculture in Nitra, Slovakia

Eyüp Şen, Muğla Sıtkı Koçman University, Turkey

İlker Yorulmaz, Muğla Sıtkı Koçman University, Turkey

Maria Martinez, AIFED, Spain

Jesus de Haro Martinez, AIFED, Spain

Chris Ashe, Elfl-Tech, Germany

Mattia Ferrari, Elfl-Tech, Germany

Maria Kandilioti, Found.ation, Greece

Roula Mourmouri, Found.ation, Greece

Suzana Trajkovska, SYZYGY, Macedonia

Aleksandar Kochankovski, SYZYGY, Macedonia

Table of contents

Summary

After the COVID-19 pandemic, some needs have become vital due to the use of digital technologies and internet, which are very much in our lives. The most important of these is to be able to transact safely in the digital world without being damaged. Especially adults need digital security measures and some competencies to protect themselves from cyber threats. Also, internet and digital technologies not only make life easier, but also create some negative psychological problems. For example, cyberbullying has become a difficult problem to deal with. Accordingly, ensuring well-being in the digital world has now become a necessity in current conditions. Again, in relation to this issue, the increasing use of digital technology and the point reached by digital transformation have brought some issues such as digital fatigue to people's agenda.

In this regard, the DigiWELL project aims to incorporate digital well-being principles into adult education. Its initiatives are towards contributing to overall practices of adult education organizations, networks, and initiatives. The project understands how crucial it is to address how technology is affecting adults' mental health, productivity, and general well-being in the digital age. DigiWELL's main goal is to provide adult learners with the information, abilities, and resources necessary to navigate the digital world ethically and conscientiously. The DigiWELL project also involves the creation and execution of additional adult learners' empowerment initiatives. The goal of these activities is to provide a supportive environment where adults can share their experiences, difficulties, and triumphs in promoting digital well-being. DigiWELL project presents many opportunities for individuals and adult organizations to become aware and enlightened on the importance of digital wellbeing and on how to promote digital wellbeing of adult individuals and adult educators and trainers. Enabling digital wellbeing with a holistic approach is much more possible if all relevant parties take actions to support digital wellbeing needs of individuals. Consequently, the information, tips and good practices presented in this manual invite people and interested organizations to take initiatives so that more of us have better digital wellbeing and stronger digital lives.

1 Introduction

1.1 Aim of the Method & Manual

- To contribute enabling digital wellbeing and digital security accessible to all by encouraging and informing adults about the digital wellbeing and digital security and the necessary competences for them.
- To introduce digital resilience, digital wellbeing and digital security, the framework of terminology, and best practices of digital wellbeing and digital security among all people.
- To ensure multiculturality, adapting the developed outputs to relevant organizations in partner countries.

1.2 EU DigComp Framework

In DigComp, 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 is defined as a combination of knowledge, skills, and attitudes." (Council Recommendation on Key Competences for Life-long Learning, 2018).

The DigComp framework identifies the key components of digital competence in 5 areas. The areas are summarized below:

Information and data literacy: 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 organize digital data, information, and content.

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 presence, identity, and reputation.

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 licenses are to be applied. To know how to give understandable instructions for a computer system.

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.

Problem solving: 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.

One of the key competences in the Safety area is protecting health and well-being. Protecting health and well-being means; (a) to be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies, (b) to be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying) and (c) to be aware of digital technologies for social well-being and social inclusion.

1.3 Why should M&M be a Good Resource for Adults

As it was mentioned above, after the COVID-19 pandemic, some needs have become vital due to the use of digital technologies and internet, which are very much in our lives. The most important of these is to be able to transact safely in the digital world without being damaged. Especially adults need digital security measures and some competencies to protect themselves from cyber threats. Also, internet and digital technologies not only make life easier, but also create some negative psychological problems. For example, cyberbullying has become a difficult problem to deal with. Accordingly, ensuring well-being in the digital world has now become a necessity in current conditions. Again, in relation to this issue, the increasing use of digital technology and the point reached by digital transformation have brought some issues such as digital fatigue to people's agenda.

This manual uses as many real-world examples as possible and let adults' learners figure some concepts out themselves to support adult learning based on Knowles (1968).

1.4 Why should M&M be a Good Resource for Adults Trainers

Training and education play a crucial role in enhancing awareness on digital security by empowering individuals with the knowledge, skills, and best practices needed to protect themselves and their organizations against cyber threats. Additionally, training and education for digital security are essential components of building a strong cybersecurity culture. By designing training programs that are tailored to the specific needs and roles equip adults with knowledge and skills needed to identify and respond to cyber threats effectively.

Training helps individuals understand the various types of cyber threats, such as phishing, malware, social engineering, and ransomware. By recognizing these threats, individuals can be more vigilant and cautious while using digital platforms. Education can teach individuals how to identify phishing emails, messages, or websites. They learn to spot suspicious elements and avoid clicking on malicious links or providing sensitive information. At the same time, training includes guidelines on securing mobile devices, protecting them with passcodes, using encryption, and being cautious with app downloads while ensures that individuals are aware of relevant cybersecurity regulations and compliance requirements, which helps maintain legal and ethical practices. Finally, through education, individuals understand that cybersecurity is a shared responsibility and that everyone's active involvement is necessary to maintain a secure environment, whereas instills good cybersecurity habits, encouraging individuals to implement security measures both at work and in their personal lives.

The DigiWELL project aims to address the digital security and well-being needs of adults who were not born into the Internet Era. It will achieve this by creating and developing flexible learning opportunities that cater to the specific learning requirements of adults. The project will focus on enhancing digital resilience through a blended learning approach. Especially this manual contributes to the above aim as it creates a security-aware culture that actively defends against cyber threats and protects digital assets and sensitive information.

In other words, a manual with a session devoted on digital security can play a significant role in equipping adults with the necessary skills and knowledge to protect themselves in the digital age, fostering a safer and more secure online experience for individuals and communities alike. The DigiWELL is a valuable resource for adults as educates adults about potential risks, helping them understand the importance of cybersecurity and how to protect themselves online. Finally, offers practical guidance on implementing digital security measures and empowers adults to navigate the digital world with confidence and serves as a reference guide that adults can revisit whenever they encounter new digital security challenges or need a refresher on certain topics.

1.5 Dictionary of the DigiWELL Project and How to Use it

Dictionary aims to introduce adult users of digital technologies with basic terms and definitions related to digital well-being, digital security, and digital resilience.

Classification of Terms

In terms of content, the dictionary contains 3 basic categories of terms.

1. Terms and definitions from the field of information and communication technologies (digital technologies according to the project).

2. Terms and definitions from the field of information, cyber and digital security (digital security according to the project).
3. Terms and definitions defined by the project objectives: digital wellbeing and digital resilience. These terms are relatively new, and they are part of the desk research of project teams. It should be emphasized that there is no uniform definition of these terms. This category also includes terms from the field of mental and physical health, e.g. digital addiction, digital fatigue/burnout, digital detox, etc.

Notice: In a dictionary's text database, a term may have more than one definition for many reasons: the original definition has evolved over time, the broad definition is tailored to a specific area, the definitions of terms are similar but with subtle differences, etc.

Terms and Definitions

Digital Resilience: 1. Digital resilience means having the awareness, skills, agility, and confidence to use new technologies and to adapt of changing digital skills requirements. Digital resilience improves the capacity to solve problems and upskills, and capacity to navigate digital transformations. 2. Digital resilience is the ability of young people to develop a critical mind-set when accessing digital information to reduce their vulnerability to potentially harmful information. 3. Digital resilience means "the process of adapting well to digital sources of stress and developing skills to manage the impact of ever-changing digital environments and applications".

Digital Security: Digital security is the protection of digital identity, as it represents a physical identity on the network or internet services. Digital security is a set of best practices and tools used to protect personal data and online identity in the online world. Examples of tools are web services, antivirus software, smartphone SIM cards, biometric and secure personal devices, password managers, parental control, etc.

Digital Wellbeing: 1. Digital wellbeing describes the ability of a person to effectively manage the negative impacts of technology on their professional and personal lives. The aim of digital wellbeing is to promote the healthy use of technological devices and digital services. 2. A state of personal wellbeing experienced through the healthy use of digital technology. 3. Digital wellbeing spans the ways information technology – including communications and sensors – can help people live long and healthy lives.

Digital Competence: Confident, critical, and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It is defined as a combination of knowledge, skills, and attitudes.

Digital Addiction: Digital addiction is a harmful addiction on digital media, devices and the internet characterized by their excessive use in a way that has a negative impact on the user's life.

Digital Skills: Digital skills are as a range of abilities to use digital devices, communication applications, and networks to access and manage information. They enable people to create and share digital content, communicate, and collaborate, and solve problems for effective and creative self-fulfillment in life, learning, work, and social activities.

Cyber Threat: Any circumstance or event with the potential to adversely impact organizations/individuals via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. The goal is to steal/damage data or disrupt the digital well-being.

Cyberbullying: A term for various forms of bullying in online space in which one or more individuals use digital technology to harm another person intentionally and repeatedly (e.g. sending emails or instant messages, posting comments on social networks or public forums).

Cybersecurity: Cybersecurity is a subset of information security, its goal is to protect cyberspace (i.e. networks, intranets, servers, information and computer systems and infrastructure) from unauthorized access, cyber-attacks, or damage. Cybersecurity focuses on the protection of information in electronic/digital form located in computers, storage, and networks (in cyberspace).

Digital Privacy: Digital privacy is the ability of an individual to control and protect the access and use of their personal information as and when they access the internet. Digital privacy helps individuals stay anonymous online by safeguarding personally identifiable information such as names, addresses, social identification number, credit card details, etc.

Digital Security vs. Cyber Security vs. Information Security: Information security: protects information (in any format and form) and information systems from unauthorized access and use to secure and preserve the privacy of important data. Cyber security: protects entire networks and communication systems, computer systems, and other digital components and the digital data stored therein. Digital security: protects online presence (identity and associated sensitive information, assets.

Best Practice: A proven method or procedure that offers the most effective solution in each area, that is proven to lead to optimal results and is established (suggested) as an appropriate standard for widespread adoption. In digital security, these are defined procedures to ensure the protection of an individual/organization in the digital space (e.g. recommended techniques, programs, instructions, manuals).

2 Digital Wellbeing

2.1 What is Wellbeing?

The term "**wellbeing**" describes the condition of being pleased, joyful, and healthy. It includes a person's physical, mental, and emotional well-being, among other areas of their existence. Beyond just being free of disease or discomfort, wellbeing focuses on overall happiness and quality of life.

Physical well-being is the state of one's body, considering things like physical fitness, diet, and the absence of illness or disease. It entails upholding a healthy lifestyle through consistent exercise, nutritious food, enough sleep, and stress management.

The cognitive and emotional health of a person are related to their ***mental wellbeing***. It entails having a good outlook, experiencing fulfillment, and being able to handle stress and the difficulties of life. Activities like practicing mindfulness, taking up a hobby, asking for support from loved ones, and getting professional assistance, when necessary, may all help nourish one's mental wellbeing.

Having a good understanding of and capacity to control one's emotions is referred to as ***emotional wellbeing***. It entails cultivating resilience, upholding good relationships, and having a positive sense of oneself. Self-awareness, emotional control, effective communication, and the development of supportive relationships all contribute to emotional wellbeing.

The quality of a person's connections and sense of community belonging are all parts of ***social well-being***. It entails fostering enduring bonds with close loved ones, close friends, and a larger social network. Participating in social activities, giving back to the community, and upholding a feeling of connection and belonging may all improve social wellbeing.

Overall, **wellbeing** is a comprehensive idea that considers how different facets of a person's life are interrelated. It entails actively seeking a balanced and satisfying existence, caring for one's bodily and mental health, cultivating wholesome relationships, and finding meaning in one's life.

2.2 Wellbeing and Digitalization

By enabling communication, boosting efficiency, and enhancing access to information, technology and digitalization have the potential to improve wellbeing. To manage digital usage, safeguard privacy and security, and strike a good balance between technology and other facets of life, it's crucial to be aware of the possible drawbacks and take the necessary precautions.

Technology and digitalization have greatly enhanced access to information and services, which has a positive effect on wellbeing. People now have easy access to digital tools for personal development, healthcare information, online support groups, and educational resources. Through seamless communication and connection over distances, technology promotes social connections and lessens feelings of loneliness. People may keep in touch with friends, family, and communities thanks to digital platforms, social media, and messaging applications, which improve social welfare. Many facets of life have become more efficient and convenient thanks to digitalization. Through the use of digital tools and services, tasks that once required a lot of time and effort may now be completed swiftly and effortlessly. This can help with general welfare by freeing up time and lowering stress. Moreover, digital abilities are becoming more and more crucial in the work market as technology develops. The employability and socioeconomic well-being of a person can be improved by acquiring and using these talents. The digital gap, which occurs

when some people or groups lack access to technology or digital literacy, can, nevertheless, worsen already-existing disparities.

While using technology improperly or excessively can have harmful effects on one's mental health, it can also have good effects. Anxiety, despair, and low self-esteem may all be influenced by too much screen time, social media comparison, and online abuse. To safeguard mental health, it is crucial to maintain a healthy balance and practice mindful technology use. Also, the digital environment has some privacy and security issues. Cyber threats, data breaches, and online fraud can put people's financial security and personal information in danger. Maintaining overall welfare in the digital age requires protecting digital security and privacy.

2.3 What is Digital Wellbeing?

Digital resilience development and adoption of security procedures lead to a condition of optimal health and general well-being in the digital sphere, which is referred to as ***digital wellbeing***. Digital wellbeing originates from the wellbeing concept, and it has to do with digital lives of individuals. The capacity of people to adapt, manage, and prosper in the digital world while successfully managing both their well-being and security is referred to as ***digital resilience***, which is a mix of digital wellbeing and security. The cornerstone of digital resilience is digital wellbeing, which emphasizes preserving a positive and sensible connection with technology. It entails limiting screen time, placing a high priority on mental and emotional health, creating supportive online communities, and learning digital literacy. In the context of wellbeing, digital resilience helps people handle online difficulties like cyberbullying, online harassment, or exposure to dangerous content while preserving their general well-being. Individuals may build a strong digital resilience that enables them to move through the digital world with assurance and responsibility by integrating digital wellbeing with digital security. They are better able to manage the challenges of the digital world, adjust to changing dangers, make wise judgments, safeguard their personal information, and maintain their mental, emotional, and physical health while using the internet. Digital resilience ultimately encourages a safer, healthier, and more fulfilling online experience for people.

2.3.1 Mental Health, Wellbeing and Digital Wellbeing

Our whole quality of life is influenced by the deep connections between our mental health and overall wellbeing. Our psychological and emotional well-being, including aspects like our thoughts, feelings, and behaviors, is referred to as our mental health. It is fundamental to our total health, just as important as physical wellness. Contrarily, well-being is a comprehensive state of balance, fulfillment, and contentment in life. The relationship between the two is based on how one's mental health has a significant impact on their physical health and vice versa. Our total well-being increases when we cultivate positive mental health by controlling stress, overcoming obstacles, and building healthy relationships, which results in a more fulfilling and meaningful living. On the other hand, a sense of well-being can greatly improve mental health by encouraging resilience, emotional stability, and a higher ability to deal with challenges in life. We may create a happy and prosperous living by placing a focus on the relationship between our mental health and well-being.

Due to the rapid improvements in technology and its pervasive integration into our daily lives, mental health assumes a complex and dynamic nature in the digital age. In the context of the digital age, one's mental and emotional well-being is referred to as having "digital mental health." It includes social media, online interactions, the psychological effects of digital technologies, and the continual connectedness that

defines modern life. Although technology has created many advantages and opportunities, it has also created significant difficulties for mental health. Despite ongoing virtual contact, the digital age can result in problems like internet addiction, cyberbullying, information overload, social comparison, and feelings of isolation. However, it also provides cutting-edge approaches to managing mental health, like as mental health applications, online therapy, and virtual support groups. Maintaining a healthy balance between our online and offline lives, being aware of how much digital media we consume, and actively looking for digital tools that can improve our mental well-being while guarding against potential traps are essential as we traverse the intricacies of the digital age.

In the present day, there is a complex relationship between mental health and digital well-being. Individuals' psychological and emotional well-being, which includes factors like mood, thoughts, feelings, and behavior, is referred to as their mental health. On the other hand, digital well-being describes the equilibrium and harmony one feels when using technology and engaging in digital relationships. The digital era has many benefits, enabling connectivity, information access, and chances for personal development. The excessive use of technology, continual notifications, social media pressure, and information overload, however, can have a negative impact on mental health by causing tension, worry, and a sense of separation from reality. On the other hand, it can have a beneficial impact on mental health when digital well-being is prioritized by setting limits, taking regular breaks from screens, and being attentive of digital consumption. For fostering both mental health and digital well-being and guaranteeing a harmonious coexistence between our virtual and real lives, it is essential to strike a healthy balance between digital involvement and offline activities. A more meaningful and well-balanced life in the digital age can be achieved by deliberately embracing technology and using digital tools to enhance mental health.

2.3.2 Why Do We Need Digital Wellbeing?

The key drivers of digital wellbeing are quality of life, communication, productivity and success, mental and physical health. Because it includes one's whole state of being healthy, happy, and content, digital wellbeing is important. It refers to the overall health of people and communities, taking into consideration their social, psychological, and physical aspects. The use of cellphones, social media, and video games in excess or unhealthily can be detrimental to mental health. Anxiety, despair, loneliness, and poor self-esteem can all be exacerbated by excessive screen time, frequent comparisons to others on social media, or cyberbullying. In this regard, digital wellbeing is the way to have control over our own life. It's crucial to have a healthy connection with technology to support good mental health and digital wellbeing. Setting limits for gadget use, engaging in digital detoxes, participating in offline activities, and giving self-care and face-to-face interactions top priority may all be part of this. We must be aware of the impact that digital technology has on our mental health and take proactive measures to ensure its sensible usage.

Digital wellbeing has become an essential human need in the digital age, particularly in the wake of the Covid-19 pandemic. Our reliance on digital platforms has grown as technology continues to invade every part of our everyday lives, from communication and education to employment and entertainment. The epidemic has caused digitalization to advance at an unprecedented rate, demanding distant labor, online schooling, and more virtual relationships. As a result, maintaining our digital well-being is crucial for leading a fulfilling and healthy life. We may utilize technology in a conscientious and responsible manner to ensure that it improves our lives rather than poses a threat to our general well-being in this quickly changing digital environment by acknowledging digital well-being as a fundamental human need.

2.3.3 Good and Poor Digital Wellbeing

Digital wellbeing is a comprehensive term that covers a variety of aspects from the digital world. It deals with both individuals' being physically, psychologically, and socially healthy and their feeling digitally aware, balanced, safe, satisfied and healthy on the other hand. As seen, the meaning attributed to the term "digital wellbeing" is mostly towards the favorable side of digitalization, which refers to good digital wellbeing. The opposite way round, individuals experiencing a lack of digital wellbeing refers to poor digital wellbeing. Considering this, the following aspects could be asserted to be among the main indicators of good digital wellbeing:

- Digital security: Ensuring digital security provides a remarkable contribution to one's digital wellbeing. It covers protecting your online presence including your identity, data, and assets.
- Digital safety: It includes individuals' being aware of potential risks in the digital world and it has to do with individuals' capability to critically identify and manage various threats in the digital environment.
- Digital balance: It refers to purposefully benefiting from technology and the digital world. Digital balance has to do with using the digital world, digital tools and equipment for areas of life, not for everything. A regular and consistent online/offline balance and avoidance from being heavily reliant on technology are signs of a good digital balance.
- Digital independence: It is the capability to control the time spent online and to avoid centering the digital world to one's daily life. Spending too much time online and planning fewer social activities due to excessive internet usage are some signs of digital dependence.
- Digital satisfaction: It refers to reaching contentment and feeling pleasure while employing digital tools and equipment and intertwining with technology.
- Digital opportunity: It deals with benefiting from technology and digitalization to open up any new possibilities related to dissemination of digital technologies and to acquire newer competencies to build up new opportunities.
- Critical and responsible use of technology: Along with its opportunities, technology requires users to act responsibly by protecting one's own rights and respecting the rights of others, to act in an accountable and cautious manner, and to think critically towards any content in the digital world.

These aspects could also be considered among the dimensions of digital wellbeing. If one has or ensures a relatively higher-level digital security, safety, balance, independence, satisfaction, opportunity and / or critical and responsible use of technology while using digital tools and equipment, s/he could be considered to have a good digital wellbeing. On the contrary, if one lacks some of the above components, it signifies that s/he has poor digital wellbeing. It is noteworthy to remember that one's being physically, psychologically, and socially healthy also refers to a good digital wellbeing and further aspects have a potential contribution to individuals' digital wellbeing and overall wellbeing.

2.3.4 Fostering Digital Wellbeing of Individuals: Potential Profits for All and for Adult Education

Promoting digital wellbeing in adult education or empowering adults' wellbeing and digital wellbeing provides many opportunities. First and foremost, wellbeing is a basic human need. Especially after COVID-19, most people spend a lot more time online and they are more exposed to technology together with its

risks and threats. If people intentionally desire or not, they bring their whole selves to work, namely there is a clear connection in people's own wellbeing and the atmosphere in the work environment. So, the potential actions to foster wellbeing and digital wellbeing of individuals both contribute to them as human-beings and to the organizations they work for. From an organizational perspective, fostering workers' digital wellbeing contributes but is not limited to team performance, commitment, innovation, and satisfaction. Digital wellbeing enables individuals to become more focused, engaged, and productive, which contributes to healthier lives both inside and outside of the work environment. Employees' adopting digital wellness practices enables them to become less exhausted and distracted. Promoting supporting actions for digital wellbeing empowers the work-life balance of individuals. Furthermore, it eliminates the negative impacts of overexposure to digitalization, which enables experiencing less anxiety, despair, stress, and so on.

The idea of well-being in the context of adult education goes beyond conventional ideas of academic accomplishment and includes students' overall health and fulfillment. The concept of "digital well-being" has grown in importance with the advent of the digital era, especially for digital nomads who largely rely on technology while living a mobile lifestyle. In adult education, the term "digital well-being" refers to providing students with the abilities and information they need to use the internet sensibly and ethically. Promoting digital well-being is crucial to creating a successful learning environment since digital nomads frequently encounter difficulties like juggling their personal and professional lives and overcoming emotions of loneliness. Integrating digital well-being into adult education entails teaching students how to properly control their screen time, build positive online communities, and maintain awareness of their digital usage. It also covers topics including cybersecurity, digital weariness, and data privacy. In today's digitally driven world, educators can ensure a positive and enriching learning experience by addressing the obvious need for digital well-being empowerment in adult education and providing digital nomads and other learners with the tools to maintain a healthy balance between their digital interactions and overall well-being.

It takes a careful and thorough strategy to successfully integrate digital well-being into adult education because it is a complicated and continuing process. The first and most important step is to give adult learners training, so they are aware of the value of digital well-being and how it affects their general health and productivity. They gain the necessary practical skills to navigate the digital world sensibly and safely thanks to this instruction. The second stage is to modify the course material such that the curriculum reflects the concepts of digital wellbeing. This entails incorporating ideas like controlling digital distractions, online privacy, digital etiquette, and digital literacy. Adult learners can have a greater grasp of the advantages and disadvantages of technology and learn how to use it effectively by incorporating these features into the courses. A supportive environment is created where learners may share experiences, swap techniques, and reaffirm their commitment to digital well-being by designing additional empowerment events, such as seminars and conversations. To be relevant and effective in fostering well-being in the digital era, adult education must continuously evolve to keep up with the rapidly changing digital landscape.

3 Digital Security

3.1 Digital Security and Cybersecurity

According to the Organization for Economic Cooperation and Development (OECD) **digital security** is essential for trust in the digital age. The OECD has been facilitating international co-operation and developing policy analysis and recommendations in digital security since the early 1990s. The work in this area aims to develop and promote policies that strengthen trust without inhibiting the potential of

information and communication technologies (ICTs) to support innovation, competitiveness, and growth. Digital security refers to the economic and social aspects of cybersecurity, as opposed to purely technical aspects and those related to criminal law enforcement or national and international security. The term "digital" is consistent with expressions such as digital economy, digital transformation, and digital technologies. It forms a basis for constructive international dialogue between stakeholders seeking to foster trust and maximize opportunities from ICTs[1].

Digital security and **cybersecurity** are related but not the same. They both involve protecting digital assets and information from unauthorized access, use, or damage, but they differ in scope and focus.

Digital security refers to the practice of safeguarding digital data, information, and assets from unauthorized access, theft, or damage. It encompasses a broader range of security measures that protect data and information across various digital platforms and devices, including computers, smartphones, tablets, and other digital technologies.

Digital security measures may include:

- Password protection: Creating strong and unique passwords for online accounts and devices.
- Data encryption: Encoding data to prevent unauthorized access or data breaches.
- Secure communications: Using encryption protocols for secure data transmission.
- Access controls: Implementing permissions and restrictions to limit access to sensitive data.
- Device security: Utilizing features like screen locks and remote wiping for lost or stolen devices.

Cybersecurity is a subset of digital security and focuses specifically on protecting digital assets from cyber threats and attacks. It involves the defense against unauthorized access, damage, or disruption of digital systems, networks, and infrastructures.

Cybersecurity measures may include:

- Firewall protection: Setting up barriers to prevent unauthorized access to a network.
- Intrusion detection systems: Monitoring networks for suspicious activities and potential threats.
- Malware protection: Using antivirus software to detect and remove malicious software.
- Incident response planning: Developing protocols to respond to cybersecurity incidents effectively.
- Cyber threat intelligence: Gathering and analyzing information to anticipate and prevent cyber threats.

Digital security covers a broader range of practices that protect data and information in the digital realm, while cybersecurity is a specialized area focused on defending against cyber threats and attacks in digital systems and networks. Both are crucial components in ensuring the overall security and protection of digital assets and information.

[1] HTTPS://WWW.OECD.ORG/DIGITAL/DIGITAL-SECURITY/

3.2 Cybersecurity Threats Faced by Adults

Adults face a wide range of cybersecurity threats in today's digital world. Here are some common cybersecurity threats that adults often encounter:

- ***Phishing Attacks:*** Phishing is a technique used by cybercriminals to trick individuals into providing sensitive information, such as login credentials, credit card numbers, or personal data. Phishing emails, messages, or websites may appear to be from trusted sources, but they aim to deceive users into divulging their information.
- ***Malware:*** Malware is malicious software designed to infiltrate, damage, or gain unauthorized access to computer systems. Types of malwares include viruses, ransomware, spyware, and Trojans. Malware can be spread through malicious email attachments, infected websites, or compromised software.
- ***Identity Theft:*** Cybercriminals can steal personal information, such as Social Security numbers, birthdates, or financial data, to commit identity theft. This information is often obtained through data breaches or phishing attempts.
- ***Online Scams:*** There are numerous online scams targeting adults, such as lottery scams, romance scams, fake tech support scams, and fraudulent investment schemes. Scammers use various tactics to manipulate individuals into sending money or providing personal information.
- ***Data Breaches:*** Data breaches occur when sensitive information held by companies or organizations is exposed or stolen. As an adult, you may be impacted by data breaches if your personal information is stored by affected entities.
- ***Social Engineering:*** Social engineering involves manipulating individuals to disclose confidential information or perform certain actions. Cybercriminals may use social engineering techniques to gain unauthorized access to systems or accounts.
- ***Password Attacks:*** Weak passwords or password reuse can lead to password attacks, such as brute force attacks or dictionary attacks, where cybercriminals attempt to guess or crack passwords to gain unauthorized access.
- ***Public Wi-Fi Risks:*** Using public Wi-Fi networks can expose adults to security risks, as these networks may lack proper encryption and are susceptible to eavesdropping by attackers.
- ***Insider Threats:*** Insider threats involve employees or individuals with authorized access to systems or data intentionally or unintentionally causing harm or leaking sensitive information.
- ***IoT Vulnerabilities:*** The increasing adoption of Internet of Things (IoT) devices can create cybersecurity risks, as many of these devices may have inadequate security measures and can be exploited by cybercriminals.

To protect against these threats, adults should practice good cybersecurity hygiene, including using strong and unique passwords, enabling multi-factor authentication, keeping software and devices up to date, being cautious of suspicious emails and links, and being mindful of the information they share online. Regular cybersecurity awareness training can also help individuals stay informed about emerging threats and best practices for staying safe online. The next section presents in detail some of the most essential digital security practices for adults to reduce the risk of falling victim to cybersecurity threats and protect their digital identities and assets.

3.3 Digital Security Practices for Adults

Digital security practices are essential for adults to protect their personal information, data, and online accounts from cybersecurity threats. Here are some important digital security practices that adults should follow:

- ***Use Strong and Unique Passwords:*** Adults should create strong and unique passwords for their online accounts. Avoid using easily guessable passwords like "123456" or "password." Consider using a password manager to generate and store complex passwords securely.
- ***Enable Multi-Factor Authentication (MFA):*** Whenever possible, enable multi-factor authentication on your online accounts. MFA adds an extra layer of security by requiring a second form of verification, such as a one-time code sent to your mobile device, in addition to your password.
- ***Keep Software and Devices Updated:*** Regularly update your operating system, web browsers, and software applications. Updates often include security patches that address known vulnerabilities.
- ***Be Cautious with Emails and Links:*** Exercise caution when opening emails from unknown senders or clicking on suspicious links. Be especially wary of emails that ask for sensitive information or direct you to log in on a fake website.
- ***Secure Your Home Network:*** Change the default password on your home Wi-Fi router and enable WPA2 or WPA3 encryption to protect your wireless network. Avoid using public Wi-Fi networks for sensitive activities unless you use a virtual private network (VPN).
- ***Regularly Back Up Data:*** Regularly back up your important files and data to an external hard drive, cloud storage, or a secure backup service. In case of data loss or ransomware attacks, having backups ensures you can recover your files.
- ***Use Secure Wi-Fi and HTTPS:*** When accessing sensitive websites, ensure they use HTTPS encryption. Look for the padlock symbol in the browser's address bar to verify the website's security.
- ***Be Mindful of Social Media:*** Be cautious about the information you share on social media platforms. Avoid posting personal details like your address, phone number, or travel plans, as this information can be used for social engineering attacks.
- ***Install Antivirus and Security Software:*** Use reputable antivirus and security software on your devices to protect against malware and other threats. Keep the software up to date to ensure optimal protection.
- ***Educate Yourself About Cybersecurity:*** Stay informed about the latest cybersecurity threats and best practices by reading reputable sources, attending webinars, or participating in cybersecurity awareness programs (Please see the digital security resources available for adults.).

By incorporating these digital security practices into their daily routines, adults can significantly reduce the risk of falling victim to cybersecurity threats and protect their digital identities and assets.

3.4 Digital Security Resources Available for Adults

The Cybersecurity Education Hub[2] (CEH) at the California State University San Marcos offers resources and direction for campus and community efforts to increase digital security education and awareness. The CEH is a collaborative effort of the campus Information Security Office, the Colleges of Science and Math, and Business Administration.

The CEH works to ensure that campus digital security educational programs address broad issues related to current events in the field of digital security, and it provides opportunities for digital security topics to be incorporated into courses taught across the university. The CEH also offers resources to students, student organizations, and the public. It promotes and facilitates communication and collaboration with digital security education throughout the community. They provided learning materials on topics such as privacy and social media, cybersecurity safety for students, cybersecurity today, and cybersecurity concepts.

Besides, in 2008, ENISA[3] Cyber Security Training materials were introduced. It has since been expanded with new sections containing critical information for success in the field of Cyber Security. ENISA contains training materials such as teacher handbooks, student toolkits, and virtual images to supplement hands-on training sessions.

4 Best Practices of Building Digital Security for Adults

Digital security is increasingly important in our connected society, and older people are one of the most vulnerable groups online. As technology advances, so do cyber threats. It is therefore important to establish measures and guidelines to protect older adults in the digital environment. Below are some good practices and successful actions implemented in several countries that can serve as a reference for others.

Cybersecurity Strategy of the European Union represented in the reports that are all available on the official website of the European Commission and provide valuable insights into best practices for improving digital security in Europe.

4.1 Key Issues to Build Digital Security

This section may appear to be a repetition of Section 3.3. Digital Security Practices for Adults, but it contains more real-world scenarios and examples.

Strong Passwords: Help them create strong and unique passwords for each account. Passwords must be long and contain upper- and lower-case letters, numbers, and special characters. Passwords must be long (at least 8 characters), contain upper- and lower-case letters, numbers, and special characters. Avoid using predictable personal information, such as names or dates of birth. Remind them not to share their passwords with anyone and to change them regularly.

[2] https://www.csusm.edu/cybersec-hub/index.html

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

For example, a strong password could be “P@ssw0rd2023!” which combines uppercase letters, lowercase letters, numbers, and special characters. Avoid using predictable personal information like names or dates of birth, such as “John1980” or “MarySmith123.”

Education and Awareness: *Inform* them about online risks and threats such as phishing, malware, and identity theft. Help them understand how to recognize and avoid these situations. It is important to educate them about online risks, such as phishing (attempts to obtain confidential information fraudulently), malware (malware) and identity theft. Learn to recognize these warning signs and avoid falling into these traps. Explain possible negative effects and how to protect yourself.

For instance, explain that phishing emails may appear to be from legitimate sources, asking them to click on links and enter sensitive information. Show them examples of suspicious emails and how to identify them. Provide information on common types of malwares, like fake antivirus software or pop-ups, and how to avoid them.

Two-factor Authentication (2FA): Help them implement two-factor authentication whenever possible. This adds an extra layer of security to your accounts. Two-factor authentication adds an extra layer of security. Help them enable this feature in their accounts if possible. 2FA requires another authentication method in addition to a standard password, such as a text message code, authenticator, or fingerprint.

For example, after entering their password, they will receive a text message with a verification code that they need to enter to access their account. This adds an extra layer of security and makes it harder for unauthorized users to access their accounts.

Safe Use of Mobile Devices: *Help* them set up screen locks, facial recognition, or fingerprints to protect their mobile devices. Remind them not to share their devices with people they don't know and to be careful when downloading apps from unreliable sources.

For example, show them how to enable a PIN or use their fingerprint to unlock their smartphone. Remind them not to share their devices with people they don't know and to be cautious when downloading apps from unreliable sources.

Software Updates: Make sure your devices (computers, tablets, smartphones) have the latest security patches and updates installed. Updates often include fixes for known vulnerabilities, so keeping your devices up to date helps protect them.

Online Shopping: Remind them to shop only on reliable and secure websites and to use secure payment methods. Teach them to look for a lock in the address bar and to use secure payment methods, such as credit cards with extra security measures.

Secure Use of Email: Warn them about phishing and advise them to avoid clicking links or downloading attachments from unknown senders. Warn them about email phishing, where scammers try to get sensitive information by posing as legitimate senders. This highlights the importance of not clicking

links or downloading attachments from suspicious emails or unknown senders. It urges you to verify the legitimacy of emails with the sender before sending confidential information.

Social Media: Help them adjust the privacy settings on their social media to control who sees their posts and avoid sharing sensitive personal information. Teach them to avoid sharing sensitive information, such as phone numbers, addresses, or financial information publicly on social media.

For example, guide them through the privacy settings on Facebook to restrict who can view their posts to friends only. Emphasize the importance of being cautious about sharing information like phone numbers, addresses, or financial details on social media platforms.

Safe Browsing: Learn to recognize these secure websites ("https" and "lock") and avoid clicking on suspicious links or downloading unknown files. Teach them to distinguish between secure websites by checking their address bar for a lock and whether they are started. "http" instead of "https". Explain the importance of avoiding clicking on suspicious links or downloading files from unknown sources, as they may contain malware or redirect you to fraudulent websites.

Wi-Fi Security: Make sure they use strong passwords on their home Wi-Fi network and avoid connecting to public or unknown Wi-Fi networks. Explain the importance of using strong passwords on your home Wi-Fi network and avoid connecting to public or unknown Wi-Fi networks. Unsecured Wi-Fi networks can potentially be attacked or intercepted for data espionage.

Inactive Accounts: Help them close or delete online accounts they no longer use to reduce security risk. Inactive accounts can be vulnerable to attacks, especially if they contain personal information.

Beware of Suspicious Calls and Messages: Teach them not to disclose personal or financial information to unexpected calls or messages. Teach them to be careful when revealing personal or financial information to unexpected calls or text messages. Encourage the sender to verify their identity before sharing sensitive information. For example, provide examples of common scams, such as fake tech support calls or lottery win notifications.

Supervision and Support: Offer to help with regular checks of your online accounts and help them if they suspect suspicious activities or have security issues. Stay up to date with the latest online threats and provide ongoing guidance and support. For example, show them how to review their recent account activity and logins on various platforms.

Personal Information: Teach them to be careful when sharing personal information online and to limit the amount of information they post. Limit the amount of information they post, such as addresses, phone numbers, or school information. It fosters privacy and the importance of protecting your online identity.

Backup Important Data: Regularly backup important data to prevent loss in case of a security breach or device failure.

4.2 Best Practices around the World

4.2.1 Cyber Europe

ENISA has been organizing Cyber Europe [4] since 2010, a series of cyber incident and crisis management exercises featuring exciting scenarios inspired by real-life events and developed by European cybersecurity experts. Every two years, public and private sectors from EU and EEA countries, as well as European Institutions, Bodies, and Agencies, collaborate to strengthen their existing technical and operational capabilities.

The Cyber Europe exercise takes place over two days and simulates large-scale cybersecurity incidents that escalate to cyber crises affecting the entire EU. Participants in this exercise will be able to analyze advanced technical cybersecurity incidents, deal with complex business continuity and crisis management situations requiring coordination and cooperation ranging from the local to the EU level.

The Cyber Europe exercise series aims to improve Europe's preparedness to deal with large-scale cybersecurity incidents and crises by allowing participants to test and improve their preparedness across the EU, build trust within the EU cybersecurity ecosystem, and provide training opportunities.

Participating in Cyber Europe provides an excellent opportunity to:

- Raising cyber awareness.
- Create and/or put cyber crisis management procedures to the test.
- Improve communication within the cyber response chain.
- Create a common language and improve the understanding of one another.
- Develop a variety of individual and collective resilience abilities and skills.
- Analyze complex technical cybersecurity incidents; handle complex business continuity and crisis management situations.

4.2.2 Adaptation of Interface and Technology

Japan has been a pioneer in adapting technology and devices to make them more accessible to older people. For example, some Japanese smartphones and tablets have simpler user interfaces and improved accessibility features, making them easier to use for people with limited digital skills. Other countries and technology manufacturers may adopt such policies to ensure that older adults can use digital devices safely and effectively. Adoption of these practices by other countries and technology manufacturers can ensure that older adults have access to more user-friendly digital devices, helping to improve their online safety and participation.

There are several courses in the European territory aimed at raising awareness of the use of these tools by older people. For example, the ACDA association in Paris offers low-cost courses to introduce older

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

people to the world of technology. This association's courses offer the opportunity to learn from the basics how to operate a computer. The discovery of computer units, applications, file formats. After that the participants can acquire more advanced skills such as managing and organizing one's mailbox and learning the use of word on how to process a written document[5].

4.2.3 Helplines and Specialized Support

Singapore has established its own helpline for seniors facing digital security issues. This helpline offers advice and technical assistance to resolve cybersecurity issues. Other countries may consider introducing similar services to provide a direct and secure communication channel for seniors in need of online help. These services provide older people with a direct and secure communication channel to get help with cybersecurity issues, such as online fraud or malware. The introduction of similar services in other countries can be an important support network to protect older people in the digital world.

For example, in the European territory the association AGE UK[6] prioritizes supporting older people most vulnerable to digital exclusion.

In addition to providing services to the elderly population, the courses will focus specifically on assisting a high-risk group to access the digital world. Although the core components of the program will remain largely unchanged while working with these high-risk groups, some adjustments will likely be necessary to ensure that the program remains accessible and effective for those who need it most.

High-risk services in the Digital Champion Program will target older people who:

- Have dementia and/or memory loss.
- Have a low income.
- Live alone.
- Have mobility problems.
- Are housebound.

4.2.4 Awareness Campaigns and Education

Countries such as Australia and Canada have implemented cybersecurity campaigns and digital security education programs for older adults. These campaigns provide information on common cyber threats, tips on how to protect yourself from online fraud, and the importance of keeping your devices up to date. Governments can partner with local organizations, community centers and volunteer groups to reach out to the older population and provide training on digital skills. These information and education campaigns aim to empower the elderly through digital safety education. They are taught how to identify and avoid online fraud, protect their personal information, and use security tools such as antivirus and strong passwords. They are also informed about the risks associated with using social media and the importance of proper online privacy settings. The association listed above ACDA in Paris also offers courses in Digital Security.

[5] http://www.aucoursdesages.fr/cours.php

[6] https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

Another association that focuses on digital awareness is the Orange Foundation which informs fragile groups about the latest in technology and directs them to safer digital use[7].

Furthermore, Orange foundation have been organizing a range of free digital training courses throughout France for young people and women who are often unemployed, lack qualifications and sometimes in precarious situations. By training these people in digital skills, they help them to re-socialize, look for a job, adopt the professional uses of digital technology, develop a business, or even make digital their profession.

4.2.5 Financial Protection Programs

Countries such as the UK and US[8] have introduced policies to protect retirees from online financial scams. These policies include liability limits for victims of fraud and remedies to recover stolen funds. Other countries can explore these initiatives and adapt them to their financial systems to protect seniors against potential financial losses. Financial protection for older adults is an important part of digital security. Programs specifically designed to prevent and mitigate online financial fraud can provide this population with a greater level of security. Setting limits on the liability of fraud victims and creating mechanisms to recover stolen money are steps that can be taken. These policies not only protect the financial well-being of older adults, but also send a clear message that their well-being and financial security are taken seriously.

In Europe Setting limits on the liability of fraud victims is a vital aspect of safeguarding the financial well-being of older adults. When victims of fraud are held liable for the financial losses they suffer, it can lead to severe consequences, including financial ruin and emotional distress. By implementing policies that establish reasonable limits on liability, society recognizes the unique vulnerabilities faced by older adults and seeks to alleviate the burden placed upon them. This measure provides a safety net, ensuring that older adults are not unjustly burdened with the repercussions of fraudulent activities. Establishing limits to the liability of fraud victims is a key aspect of safeguarding the financial well-being of the elderly. On European soil, many associations are dedicated to protecting the elderly who are often victims of online fraud, who lack awareness and may suffer financial losses. One such association is Marketing Management IO (MMIO) a certified agency in Spain and France.[9]

When victims of fraud are held accountable for their financial losses, this can lead to serious consequences. Hence the importance of awareness. By implementing policies that set reasonable limits to liability, society recognizes the unique vulnerabilities of the elderly and seeks to ease the burden on them. This measure provides a safety net, ensuring that the elderly is not unfairly burdened by the repercussions of fraudulent activities.

Marketing Management IO (MMIO) includes subjects such as Internet opportunities, natural referencing, online visibility, content marketing and increasing sales. The concepts are simplified, and the actions are free. Bonus resources are also available.

[7] https://fondationorange.com/en/digital-solidarity

[8] https://www.bankofamerica.com/signature-services/elder-financial-services/

[9] https://www.marketing-management.io/blog/formation-digital-marketing

The course includes 5 lessons with videos. Facebook offers a platform with free access to over 70 online courses. These courses focus specifically on using Facebook to improve your online presence and business sales, the security, and the awareness.

4.2.6 Collaboration with the Technology Industry

Some countries, such as the United States, have partnered with technology companies to address the digital security challenges associated with an aging population. This collaboration can include enhancing security software, improving fraud detection, and implementing security features in digital products and services. Collaboration with the technology industry can be an effective way to keep abreast of the latest security threats and solutions, such as implementing advanced security technologies, improving fraud detection, and promoting security practices for digital products and services aimed at the elderly. Collaboration with the technology industry ensures a faster and more up-to-date response to digital threats.

Other countries such as France, and England have digital security courses to help older people understand defense technologies; the courses offered enable them to build a foundation in digitization and understand how to safely navigate the Internet.

For example, Konexio[10] offers training in digital skills - from the most basic to the most advanced - to promote social and professional integration. Innovative, based on practical case studies and with a strong emphasis on transversal and relational skills or soft skills, our training courses aim to enable everyone to be included in the digitalization of society. They offer various formations: digital skills, web designer, systems and networks technician, digital helpers. The program focuses on learning the soft skills and social codes of the professional world through workshops. It also offers opportunities for direct connection with the professional world through our network. It offers regular follow-up and personalized support to help our learners make progress and resolve any difficulties they may encounter.

4.2.7 International Resources, Reports, and Initiatives

These resources provide valuable guidance and best practices for improving digital security in adult education in the EU.

An Open, Safe and Secure Cyberspace: This report provides an overview of the EU's cybersecurity strategy, which aims to promote an open, safe, and secure cyberspace in Europe. The report includes best practices for improving cybersecurity, including risk management, incident response, and public-private partnerships.

ENISA Threat Landscape Report: This report by the European Union Agency for Cybersecurity (ENISA) provides an overview of the current cybersecurity threat landscape in Europe, including the most common types of cyber-attacks and the sectors most at risk. The report includes best practices for preventing and mitigating cyber-attacks, including security awareness training, vulnerability management, and incident response planning.

NIS Directive and EU Cybersecurity Act: This report provides an overview of the EU's legal framework for cybersecurity, including the Network and Information Systems (NIS) Directive and the EU Cybersecurity

[10] https://www.konexio.eu/formations.html

Act. The report includes best practices for complying with the legal requirements, such as incident reporting and risk management.

EU Cybersecurity Certification Framework: This report provides an overview of the EU's cybersecurity certification framework, which aims to improve the security and trustworthiness of digital products and services. The report includes best practices for obtaining and maintaining cybersecurity certifications, including security by design, testing and evaluation, and ongoing monitoring and assessment.

Cybersecurity for SMEs: This report provides guidance and best practices for small and medium-sized enterprises (SMEs) on how to improve their cybersecurity posture. The report includes advice on risk management, security awareness training, secure software development, and incident response planning.

Digital Skills in the Adult Population: This report by the European Commission provides an overview of the digital skills of the adult population in the EU. It includes a section on digital security, which highlights the need for adults to have basic knowledge and skills to protect themselves from cyber threats.

Digital Skills for Lifelong Learning: This report by the European Commission provides guidance and best practices for developing digital skills among adults. It includes a section on digital security, which provides advice on risk management, safe browsing, password management, and data protection.

The Cybersecurity for Digital Education Project: This project by the European Schoolnet provides resources and training on cybersecurity for teachers and learners in Europe. The project includes a range of materials, including online courses, lesson plans, and assessment tools, all focused on improving digital security in education.

The Digital Security for Senior Citizens Project: This project by the European Union Agency for Cybersecurity (ENISA) provides resources and training on cybersecurity for senior citizens. The project includes a range of materials, including online courses, guides, and videos, all focused on improving digital security among older adults.

Digital Skills and Jobs Coalition: This initiative by the European Commission aims to improve the digital skills of Europeans to enable them to fully participate in the digital economy. It includes a range of resources and training opportunities, including on digital security.

4.3 Best Practices of Adult Education on Digital Security

ENISA Train the Trainer Program

All the online training materials and training courses in the 'Training Courses for Cyber Security Specialists' section are based on the 'Train the Trainer' philosophy. The 'Train the Trainer' program and philosophy aim to expand the network of trainers and promote better information exchange. This will serve several purposes, including:

- Sharing training materials to save time and money on training,
- Creating regional training efforts,
- Fostering cooperation among different training providers,
- Promoting good training practices,
- Cutting down on competition and duplication.

ENISA's online training materials will include a Trainers Handbook, a Students Toolset, and Virtual Machines for download. This allows potential trainers to prepare the course, and the Handbook will assist

them in guiding the students through the course. It will contain cheat sheets, potential small tests to see if the students have grasped the important lessons from the courses, and extra information or exercises that the trainer can use to make the course more interesting or challenging.

Learning from each other's successes and failures allows both novice and experienced trainers to better design and deliver trainings, making them more successful, more "fun," and with better and longer lasting results.

TiK – Technology in Brief

The high-tech project follows an intergenerational approach through the training offered by young volunteers (age 16 to 30) as so-called “Tablet-Trainers”, who are educated along a special tablet-education-curriculum. The courses have the distinction of a multitude of methods and flexible leading questions and a special commitment of the young trainers. They offer low-threshold courses voluntarily for only a small expense allowance. The further development of the courses is ensured by the feedback of the participants and the trainers who also elaborated them own special materials and barrier-free hand-outs for the elderly. The courses are within easy reach for those interested and much attention is paid to a wide geographical distribution of the “TiKmodules” and of information on www.digitaleseniorinnen.at. Participants of the courses are persons and especially poor women on a low educational level. Until the end of 2018 more than 2000 persons learned with the modules and another 1000 persons participated in the course-program. The oldest participant who just takes part in a course is 97 years old, he gets his education by a young man in a nursery home. The project was awarded several times on the federal and provincial level.

5 Training Adults: How to Build Digital Resilience

Andragogy as a study of adult learning originated in Europe in the 1950s, but it was not until the 1970s that it was pioneered as a theory and model of adult learning by Malcolm Knowles, an American practitioner and theorist of adult education, who defined andragogy as "the art and science of helping adults to learn" (Fidishun 2000). Fidishun (2000) suggested that andragogical principles be used in the design of online classes to facilitate "flexibility and the ability of the learners to move through lessons whenever, wherever, and at their own pace."

5.1 Four Principles of Andragogy

Considering that adults have their own, unique way of learning, there are 4 central principles that explain how to best develop training for them.

- When it comes to learning, adults want or need to be involved in how their training is planned, delivered, and executed. They want to control what, when, and how they learn.
- Adults gain more when they can pull past experiences into the learning process. They can draw on what they previously known to add greater context to their learning.
- Memorizing facts and information isn’t the right way for adults to learn. They need to solve problems and use reasoning to best take in the information they are being presented with.
- Adults want to know “How can I use this information now?”. What they are learning needs to be applicable to their lives and be implemented immediately.

5.2 How Adult Trainers Will Implement Andragogy

Enabling Self-Directed Learning

In the past, learning has often been a mandatory activity done at a certain time. Now with technologies like a learning management system, we can create a much more self-directed, independent learning environment for adult learners. We can allow them to train when and where they want, offer them a selection of courses that they can choose to enroll in and enable them to have their own distinct learning goals.

Using Real-World Learning Examples

As the theory states, adults like to know how the training will have an immediate application and benefit for them. So, when creating course content, we should inject it with as many real-world examples as possible.

When training adult learners on digital wellbeing and/or digital security, walk them step-by-step through a workflow they will actually be using and explicitly state how and why they would use it. State how the training will help, and then use genuine examples to train.

Letting Adult Learners Figure it Out Themselves

Since adults prefer problem-solving over just the facts, when creating content, it's a good idea to not just lay out all the answers straight away. Why not get creative instead and build courses that get your learners' brains going?

We can do this in a few simple ways, including adding assessments and simulations that outline specific problems a learner might encounter, and then getting adult learners to use their skills to overcome it.

6 Conclusion

The digital security of older people is a key issue that requires attention and action by governments and society at large. By implementing the above-mentioned good practices, countries can improve the digital protection and well-being of their ageing population. Awareness raising, education, dedicated support, technological adaptation, and industry collaboration are key pillars to ensure a safe and positive online experience for older adults.

The DigiWELL project aims to incorporate digital well-being principles into adult education. Its initiatives are towards contributing to overall practices of adult education organizations, networks, and initiatives. The project understands how crucial it is to address how technology is affecting adults' mental health, productivity, and general well-being in the digital age. DigiWELL's main goal is to provide adult learners with the information, abilities, and resources necessary to navigate the digital world ethically and conscientiously. The DigiWELL project also involves the creation and execution of additional adult learners' empowerment initiatives. The goal of these activities is to provide a supportive environment where adults can share their experiences, difficulties, and triumphs in promoting digital well-being. DigiWELL project presents many opportunities for individuals and adult organizations to become aware and enlightened on the importance of digital wellbeing and on how to promote digital wellbeing of adult individuals and adult educators and trainers. Enabling digital wellbeing with a holistic approach is much more possible if all relevant parties take actions to support digital wellbeing needs of individuals. Consequently, the information, tips and good practices presented in this manual invite people and interested organizations to take initiatives so that more of us have better digital wellbeing and stronger digital lives.

7 References

Free available online resources were used in the preparation of the dictionary: online dictionaries, scientific articles, and literature in the field of information security, digital technologies and services, digital well-being and digital resilience, as well as terms and definitions from the subject Information security. All sources are listed in the text database of the working version of the dictionary.

1 BAI. Committee on National Security Systems (CNSS) Glossary (2015). In *BAI Information Security Consulting & Training [online]*. Retrieved from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Capterra Glossary*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Cybersecurity glossary of terms*. Global Knowledge. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Glossary*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Glossary*. The Digital Wellness Lab. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Online browsing platform (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Fifth edition.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, July 16). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Glossary of key information security terms*. NIST. Retrieved from: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Computer security: Principles and practice*. *Third edition.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *TVETipedia Glossary*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Teaching adult students to use computerized resources: Utilizing Lawler's keys to adult learning to make instruction more effective. *Information technology and libraries*, *19*(3), 157-157.

15 European Commission, Directorate-General for Education, Youth, Sport and Culture, Key competences for lifelong learning, Publications Office, 2019, https://data.europa.eu/doi/10.2766/569540