MILEAGE

RISK ANALISIS AND BARRIERS

MILEAGE

INTRODUCTION

The main objective of the MILEAGE project is to create a new and more engaging way to foster seniors' digital skills and media and information literacy (MIL) to empower them in the use of ICT tools in everyday life raising awareness on digital dangers and how to face them.

How?

- With a report on risks and barriers faced by seniors in the digital environment
- With the development of virtual risks scenarios (role playing)
- With the creation of micro lessons with explanations on the defined risks
- With the drafting of a handbook for adult educators with guidance supporting training activities (multiplier effect).

This report on risks and barriers presents the main social media, communication tools and other platforms largely used nowadays. We describe the risks and dangers associated with them specifically : each issue or risk is analyzed and a solution to overcome it is offered, listing also the competences needed and activated in doing so.

This document is created to give trainers , seniors and the general public some information related to the digital environment that the senior individuals face in their daily life, offering some tips and advice to enhance seniors' digital competences and trust in the digital world. This document will guide the development of our training content and of the risk scenarios created through the project to support media and information literacy for seniors.

MILEAGE

CONTENT

Name of the social media / tool	**WHATSAPP**
General information	WhatsApp is a free smartphone communication program to download. WhatsApp sends messages, photos, audio, and video over the internet. The service is quite similar to text messaging services; but, because WhatsApp sends messages over the internet, it is substantially less expensive than texting. You may also use Whatsapp on your computer by visiting the Whatsapp website and downloading the program for Mac or Windows. Because of features like group chatting, audio messages, and location sharing, it is very popular among youngsters.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Privacy Profile theft Recording of the calls (cybercrimes)
Barriers/difficulties for adults	Privacy settings.
Danger of the social media/tool in adults	Hackers Unencrypted Backups
Solutions that we can have	Never give out your registration code or PIN for two-step verification to anybody else. Create a code for your device. Keep track of who has access to your phone on a physical level. Knowledge of the applications and its settings.

Name of the social media / tool	**VIBER**
General information	Viber is a free app that allows users to make free calls, send text messages, photos, and videos to other Viber users. It may be used to connect with individuals all around the world and works on both mobile and desktop computers. The messaging app had 236 million monthly active users as of February 2015. Picture sharing, video, and group chat are all popular features for youthful consumers, similar to WhatsApp.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Cyberbullying Privacy Spam calls
Barriers/difficulties for adults	Privacy settings
Danger of the social media/tool in adults	Hackers
Solutions that we can have	Keep track of who has access to your phone on a physical level. Knowledge of the applications and its settings. Blocking another user on Viber (When receiving a message from an unknown contact.)

Name of the social media / tool	**ACCOMODATION COMPANIES**
General information	An accommodation provider is understood to be anyone who provides accommodation for remuneration or who accommodates more than 5 foreign nationals, except in cases where the foreign national and the provider can be considered as being in a close relationship. Examples: Hotels, B&Bs, Airbnb, Booking
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Scams Misinformation / misleading Card frauds
Barriers/difficulties for adults	Use of technology to book the accommodation Terms and conditions that are not visible
Danger of the social media/tool in adults	Use of technology to book the accommodation Terms and conditions that are not visible Not accessible to elders Isolation
Solutions that we can have	These difficulties do not imply that aging in place is an unattainable or undesirable aim, but rather that extensive planning is required at both the individual and community levels. The first stage is to educate accommodation companies about the financial and physical issues they may face if they stay in their existing home, as well as the solutions available to solve them. As is ensuring that local governments are aware of and prepared for the issues that their senior citizens will confront.

Name of the social media / tool	**FLYING COMPANIES**
General information	An organization that provides air transportation for passengers and freight.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Scams Misinformation Card frauds
Barriers/difficulties for adults	Use of technology to book the flight
Danger of the social media/tool in adults	Use of technology to book the flight Terms and conditions that are not visible Not accessible to elders
Solutions that we can have	Plan ahead Research senior air travel and assistance Manage your parking to accommodate mobility concerns Prepare for airport security Check for discounted airfare for senior citizens Choose the right flight time

Name of the social media / tool	**DATING PLATFORMS**
General information	Dating platforms are websites or apps that allow individuals to contact and communicate in order to develop a relationship. Accessing these sites often requires users to provide personal information such as age, gender and geographic location. There are hundreds of different dating platforms. It can be generalist or specialized for a type of relationship (love, erotic, friendship) or a type of members (religious or ethnic belonging, sexual orientation, and age group). Some of the most well known platforms are: Meetic, Tinder, Bumble, eDarling, Badoo, OkCupid, etc. Although most dating platforms are free, some require a monthly subscription fee or to pay for additional paid features.
Risk associated to the social media/ tool:	Privacy Catfish
Barriers/difficulties for adults	The main difficulty for seniors with dating platforms is the practical use of these tools. To be able to use such platforms, seniors need quite an advanced knowledge of ICTs. For example, they need to use an email address to log in, which implies they need to know how to create an email address and use it. The platform also requires uploading pictures, but seniors do not necessarily know how to do it.
Danger of the social media/tool in adults	**Privacy** Users share personal information on dating platforms, hoping to find the best matches. The information they share includes photos of themselves, sexual orientation, age, religion, gender, their hobbies, if they have children, height, etc. Moreover, dating platforms often offer the option to link their profiles to their social media accounts such as Facebook or Instagram, allowing the dating app to be synced with social media and displaying personal information like images to automatically load in on their dating profile. Several dating platforms experienced a security breach, which can be particularly harmful to users as sensitive data are shared on those platforms. **Catfish** Seniors that register on dating platforms are often lonely (divorced, widowed) and therefore place high hopes on meeting a potential partner. However, a lot of fake profiles and scams happen on these platforms. People pretend to be something they're not and invest themselves in a sentimental relationship to establish a bond, and use it to extract money.
Solutions that we can have	Before creating an account, users should review the platform's privacy policy and terms of service. It is important to pause to read and understand those terms as much as possible to be able to give informed consent.

	Catfishing can cause real damage. To prevent it, users can ask for a video call with the person they're talking to in order to verify that they match the pictures on the website. Users can also use tools such as Google Reverse Photo Search to verify if the photo is an original or if it comes from somebody else. Most importantly, it's important that users trust their gut if they feel they are being catfished and therefore stay guarded on sharing a lot of details.

Name of the social media / tool	**ONLINE BANKING**
General information	Online banking is also known as Internet Banking, net banking or e-banking. It is an electronic payment system that enables the customer of a bank or a financial institution to make financial or non-financial transactions online via the internet. This service gives online access to almost every banking service, traditionally available through a local branch including fund transfers, deposits, and online bill payments to the customers. It can be accessed by any individual who has registered for online banking at the bank, having an active bank account or any financial institution. Online Banking offers 24-hour access to the users' accounts every day. It is quick and convenient allowing to perform transactions anywhere, anytime, on any device (computer, smartphone, tablet) with access to the Internet Some online banks are traditional banks which also offer online banking, while others are online only and have no physical presence. According to Eurostat, in 2020, the mean average of the population using online banking in the EU was 60%. In the Czech Republic it reached 70% but in Poland it was only 49%. In Italy, 86.8 percent of individuals that use the internet also used a banking-related website or app. In the latest World Retail Banking Report, 57% of consumers say they now prefer internet (online) banking to traditional branch banking. And 55% of consumers now prefer using mobile banking apps to stay on top of their finances, up from 47% in the pre-pandemic era.
Risk associated to the social media/ tool:	Privacy Cyber-crimes: data theft and fraud.

Privacy, accuracy, property, accessibility, Violation of laws, Copyright	
Barriers/difficulties for adults	The difficulties for senior adults relate to the issue of fear and trust as well as lack of knowledge and guidance on how to use the online banking system of their bank.
Danger of the social media/tool in adults	**Lack of trust** The data collected by Casalo et al (2007) showed that web site security and privacy, usability and reputation have a direct and significant effect on consumer trust in financial services web site. It is observed that trust is a key mediating factor in the development of online banking. **Fraud & Data theft** This risk is more a common fear than a frequent problem. Indeed, according to a survey conducted in 2020 by the European Agency for Fundamental Rights, a quarter of Europeans (24%) is very worried that their online bank account or payment card details will be misused. But overall, fewer than 1 in 10 (8%) experienced online banking or card fraud in the five years before the survey. People in the UK (24%), France (19%) and Denmark (15%) are more likely to have such an experience. **Security** The security risk is connected with the increasing number of fraudulent bank websites, with fake emails purporting to be sent from banks, with the use of Trojan horse programs to capture user IDs and passwords. Hacking risks (a hacker entering in a bank account and stealing the funds) also exist although they are very rare. **Privacy** According to a 2020 study published by KPMG, 87% of consumers say data privacy is a basic human right. Yet 68% say they don't trust companies to ethically sell their personal data. **Data breach and phishing** In 2020, specialists discovered a security issue with a bank, the 5th largest bank in Europe and the 16th largest in the world. The bank's Belgian Branch had a misconfiguration in its website domain, allowing its files to be downloaded. These files contained sensitive information (name, email, phone) that could be used by hackers to potentially the bank's customers. Phishing is a type of attack often used to steal a user's data, including login credentials and credit card numbers. It occurs when an attacker, pretending to be a trusted entity, dupes a victim into opening an email, instant message, or text message and steals its information.

Solutions that we can have	**Learning how to use online banking – tutorial** In order to guide you in practice in the usage of your online banking tool, please ask your banker for the bank's tutorial. Each bank has produced one. **Security & Online Banking** Online banking portals are secured by unique User/Customer IDs and passwords. Some of them need a secure key (device) that generates a unique code at each connection). **Fraud Prediction** In the context of online banking, fraud prediction constitutes in creating a customer profiles based on historical information collected during online banking activities (terminals used, usual time and place of connection, connection and activity journeys, etc.) then predict the degree of fraudulence of the current operation, by comparing the current behavior of the customer with their profile. If the degree of fraudulence is considered high, the operation is blocked. **Reaction to Fraud** Banks also offer a direct line (phone or online) to denounce fraud as well as guidance to prevent fraud. **Practical tips** ● Use secure passwords and update them regularly ● Choose unique passwords for each digital banking account, don't use the same password for multiple accounts ● Use a secure password keeper to store your passwords ● Avoid using unsecured public Wi-Fi when accessing financial accounts online ● Know how to recognize email or text phishing scams ● Only visit secure websites ● Install anti spyware and malware protections on your devices ● Set up alerts to track your accounts and monitor transaction activity ● Enable multi-factor authentication

Name of the social media / tool	**ONLINE PAYMENTS**
General information	Payments online are done on e-commerce websites through credit cards but also through e-wallets. Bank transfers, virtual cards and vouchers are also other methods of digital payment. According to Statista, in 2019, one out of five Europeans preferred to use Fintech payment applications for their online purchases in 2019. Debit cards ranked as the most popular online payment method, with Apple Pay and Google Pay being used by roughly three percent of respondents. Regarding e-wallets, data is still unavailable but it is a market that constantly grows. Online payment platforms & e-wallets: • PayPal • Google Pay • Apple Pay • Ali Pay • Samsung Pay • Mobikwik • Paytm • Amazon Pay • Microsoft wallet • Stipe • Klarna
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Privacy Cyber-crimes: data theft and online fraud.
Barriers/difficulties for adults	The difficulties presented for senior adults relate to the issue of fear and trust as cases of payment fraud are very mediatized. The other difficulty relates to the practical use of this tool. The different types of online payment can be hard to understand and the numerous steps necessary to conclude it might be technically challenging.
Danger of the social media/tool in adults	**Privacy** While today, cash allows for anonymous payments - and therefore no tracking of purchases made and no risk to privacy - it is not the case for online payments that are highly traceable (IP address, name, surname, address, card number etc).

	Data theft The amount of data shared during online payment transactions raises the question of data theft. According to the Norton Global Cyber Safety Report 2019 more than half respondents had experienced a cybercrime, whereas 1 in 3 had fallen victim in the past 12 months. 4,1 billion records were exposed internationally and there was an increase by 54% in the number of breaches reported. **Online fraud** According to the European Central Bank, the total value of fraudulent transactions using cards issued worldwide amounted to €1.80 billion in 2018. When it comes to cards issued in the euro area only, the total value of fraudulent card transactions amounted to €0.94 billion in 2018.
Solutions that we can have	**Multi Factor Authentication (MFA) or Two Factor Authentication (2FA)** It is an electronic authentication method in which a user is granted access to a service only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: **Knowledge**: something only the user knows, normally presented as an answer to a question such as the name of a pet **Possession**: something only the user has such as a smartphone or token. In the case of the smartphone, a sms will be sent to your phone with a code to type. **Inherence**: something only the user is encompassing the use of eye and face recognition or fingerprints. **Request the CVV** It is the three numbers behind the credit card and asked to you during an online payment transaction to insure you are in possession of your credit card. **Secure payment processing** It occurs through online payment portals which are PCI, SSAE-16, and HIPAA certified. Customers and providers do not have to worry about their sensitive data being leaked and stolen by hackers.

Name of the social media / tool	INSTAGRAM
General information	Instagram is an American photo and video sharing social networking service. The app allows users to upload media that can be edited with filters and organized by hashtags and geographical tagging. Posts can be shared publicly or with pre-approved followers. Users can browse other users' content by tags and locations and view trending content. Users can like photos and follow other users to add their content to a personal feed. The service also added messaging features, the ability to include multiple images or videos in a single post, and a 'stories' feature which allows users to post photos and videos to a sequential feed, with each post accessible by others for 24 hours each. At the end of 2021, there were 2.9 million users in the Czech Republic. This is the fastest growing network. It is most popular among users aged 15 to 29.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Privacy Profile theft Impact on mental health (depressing symptoms, anxiety, stress, addiction, satisfaction with appearance, false self-presentation, body image, loneliness, social exclusion, life satisfaction etc.)
Barriers/difficulties for adults	Difficulty finding peers (71% of Instagram users are under 35 years old). Request for personal data (as the date of birth). Privacy settings.
Danger of the social media/tool in adults	Privacy - the network user should pay attention to who he/she follows and by whom he/she is being followed, or who can see the personal information and photos/videos. Profile theft – the account could be “stolen”, the user´s photos could be used somewhere else or the hackers could act in his/her name.
Solutions that we can have	Knowledge of the applications and its settings, rules how to behave on Instagram. Using a strong password and its regular change. Two factor authentication (in a computer and on the phone). Private account for personal profile. Using authorized applications only.

Name of the social media / tool	**SKYPE**
General information	Skype is a proprietary telecommunications application operated by Skype Technologies, a division of Microsoft, best known for VoIP-based video telephony, videoconferencing and voice calls. It also has instant messaging, file transfer, debit-based calls to landline and mobile telephones (over traditional telephone networks), and other features. Skype is available on various desktop, mobile, and video game console platforms. The popularity of skype increased significantly during the pandemic.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Privacy Profile theft Recording of the calls (cybercrimes)
Barriers/difficulties for adults	Privacy settings.
Danger of the social media/tool in adults	Unsolicited calls. Distrust of other users.
Solutions that we can have	Knowledge of the applications and its settings. Well-chosen background - where the camera is pointing (not to show the equipment of the apartment etc.). Turn off the camera when not needed. Silence during a call (do not turn on the TV, for example), mute the microphone when it is not necessary. Use of headphones. Not to tolerate the entry of unwanted participants, not to click on suspicious links.

Name of the social media / tool	**FAKE NEWS**
General information	Fake news, or commonly understood as disinformation, is defined as "news articles that are intentionally and verifiably false and could mislead readers" (Allcott and Gentzkow, 2017, p.213) The term „fake news" is not new. Wardle and Derakhshan (2017) broke the term fake news into three different types. They defined misinformation as "false information shared without harmful intent", disinformation as "false information shared with harmful intent" and finally, malinformation is defined as "genuine information shared to cause harm" (p.5). Where else, researchers Lazer et al. (2018, p.2) defined fake news as "fabricated information that mimics news media content in form but not in organizational process or intent". Therefore, Fake-News often refers to news stories that are false, but which appear to be legitimate news stories. The internet is a common source for fake news, with fake news frequently promoted and disseminated on social media. Fake news can be about any topic. For example, a considerable amount of fake news has been produced about the coronavirus and about vaccines.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	People across the world are witnessing a dramatic increase in access to information and communication. While some people are starved for information, others are flooded with print, broadcast and digital content. Recent studies conducted globally among people have shown that they have trouble critically thinking about media and judging its credibility, especially online. Among many issues, the study suggested that most people - don't have a good understanding of what constitutes "fake news" vs. real news. couldn't tell the difference between sponsored articles and real news stories. didn't bother to verify where photos online came from and blindly accepted the photos' stated contexts. couldn't tell the difference between a real news article and a real-looking fake news article on social media. couldn't identify biased content from independent news sources supported by groups like lobbying firms as being less reliable than a mainstream news source In the face of multiple problems of hate speech, or cyberbullying, or hacked YouTube content, or fake news etc., we are witnessing urgent calls to manage the media environment better – especially, to regulate the internet. But in the face of clashes of positive and negative rights, regulatory difficulties, powerful global companies and short-termist political expediency, this call in turn quickly morphs into a call for the supposedly 'softer' solution of educating the internet-using public.

Barriers/difficulties for adults	What worries scholars is the effect of false news on public perception causing them to make reasonable decisions based on misinformation (Tandoc et al., 2018). This is even more so when users are most likely to share negative news, and with the recent pandemic, there are many news related to Covid-19 that are negative (Nyilasy, n.d.). 374 Consequently, Chen et al. (2011) stressed the need for individuals to be new media literate to engage competently in this new environment. The most salient danger associated with "fake news" is the fact that it devalues and delegitimizes voices of expertise, authoritative institutions, and the concept of objective data—all of which undermines society's ability to engage in rational discourse based upon shared facts. Three corollary harms were noted: first, the problem of increasing fragmentation and politicization; second, the promotion of "safe news" at the expense of difficult or challenging news stories; third, the need for credible sources to allocate ever-diminishing resources to debunking inaccurate information (which poses both financial and reputation costs).
Danger of the social media/tool in adults	The growing numbers of senior citizens who are rapidly adopting social media and becoming vulnerable to disinformation is a matter of special concern. Older users may be particularly vulnerable to the issues of absorbing false information, but there are factors that universally impact all age-brackets and people's ability to distinguish facts from fiction. A person's age and the source of a piece of content are important when analyzing the spread of misinformation, but these factors do not explain why some people still believe false information long after being presented with the evidence correcting it. A fact-checking organization said there are three factors that shape everyone's ability to fall for false information. The first is repetition – if an incorrect statement is repeated over and over, it becomes more believable. The second is how the information appears. The report found that font sizes, word complexity, contrast, and grammar all impact how much someone is likely to believe a false statement made online. Pictures tend to be more easily believed as being real because they create an illusion of factual evidence of an event, and are easily processed. The report also highlights the bias people already have before consuming information. The views of people will influence the way in which new information is accepted, even when the person knows otherwise. Political or social beliefs can stop people from accepting information, despite their levels of education or media literacy.

	Most seniors have heard the term fake news and are aware that the spread of misinformation online is a problem. While people of all ages fall victim to fake news, studies have shown that older adults are more vulnerable to fake news and digital misinformation. One study showed that Facebook users age 65 and older posted seven times as many articles from fake news websites than adults age 29 and younger.1 Older adults are also less likely to be able to spot the difference between advertisements that are designed to look like real news stories and articles that are actual news stories. Profile theft – the account could be "stolen", the user´s photos could be used somewhere else or the hackers could act in his/her name.
Solutions that we can have	Because of the above cited problems, an extensive research among senior citizens that was conducted between 2009-2019 by Päivi Rasi, Hanna Vuojärvi, and Susanna Rivinen revealed that interventions should be offered seniors with health problems (Xie, 2011b), seniors over 76 years of age, older people with less experience with technology, and minority populations with low health literacy skills who live in different countries (Bertera, 2014; Lee & Kim, 2018; Vaportzis et al., 2017). Also, interventions and services should also be provided for homebound seniors who are at great risk of social isolation (Lee & Kim, 2018). Besides offering training for older people in the use of digital technologies and media (e.g., González et al., 2015; Taha et al., 2016; Xie & Bugg, 2009), there is also a great need to develop more strategies to improve older people's confidence and self efficacy in mastering Internet activities (Chu & Chu, 2010). Pertaining to the media literacy dimension of "understand," media-literacy interventions should target older people's health media literacy and ehealth literacy (Manafò & Wong, 2013; Xie, 2012; Young et al., 2012). The practical implications of dealing with older people's abilities to create media content, in particular the need to pay attention to older people's ability to tell personal and public stories about their lives to challenge the mainstream representation of their demographic (Manchester & Facer, 2015). The European Commission's Digital Services Act intends to address and make providers surface safer. However, every citizen must do their best to develop appropriate skills to protect himself/herself from harm. Thierry Breton, Commissioner for Internal Market, said: "We need to rein in the infodemic and the diffusion of false information putting people's lives in danger. Disinformation cannot remain a source of revenue. We need to see stronger commitments by online platforms, the entire advertising ecosystem and networks of fact-checkers. The Digital Services Act will provide us with additional, powerful tools to tackle disinformation." "Digital literacy is something that can be taught and it's a skill that can be developed. It has become more important for seniors to learn how to distinguish between misinformation and real news. If you believe the argument that seniors have more trouble spotting fake news than younger groups because of digital illiteracy, then it follows that this is a problem that can be addressed through

	digital education. Digital literacy is something that can be learned and improved. One way to improve your digital literacy is to take a course or attend a webinar on digital literacy. These courses teach seniors how to check facts and provide tools and techniques for evaluating online content. **What steps can seniors take to avoid falling prey to fake-news?** A senior citizen claimed that "I now realize that fake news is much more complicated and insidious than I thought it to be." Fake news is not new, though; as long as words could be spoken or pen put to paper, misinformation has been around either intentionally or mistakenly. As one Guardian article put it: "The age of post-truth, indeed, stretches as far back as you care to look, there has never been a golden age of transparency." Whether or not the concept of fake news is new, consuming information especially now requires having a toolbox of skills. It can be especially helpful to use a series of questions that can assist in evaluating new information. When working to determine whether something is real, ask yourself: Who wrote the information? What credentials does the article's author have? Is the information up-to-date? Is the website reputable? Are they trying to sell you a product? Is a company or organization sponsoring the website? Does the website support alternate or differing views of the topic being discussed? **Other Practical Strategies** **Check the source and context** Are websites reliable or trusted sources? "Misinformation can come from multiple places — it's not enough to avoid where you think it will be. It's best to have a filter that all information passes through," Check website suffixes, for example, to see whether they end with .gov or .edu and are thus official government websites or educational institutions, respectively. Senior Planet also emphasizes understanding context, such as recognizing satire. It's easy to mistake a funny image or a joke article as real. **Be observant about image too** Look for disjointed angles and/or odd lighting to detect if images have been doctored. Again, note the source and context.

	Opinions versus facts Understand the distinction between opinion and facts, especially because anyone can post content online. 'Lateral reading' – or checking other reliable sources to verify information as you read – is a term first used by the Stanford History Education Group. Key questions to ask yourself as you do so: "Who is behind the information? What is the evidence? What do other sources say?" Libraries can also provide helpful resources. Libraries might offer events to learn about media literacy — and librarians are trained to "parse out information and all the noise every day," Pause before sharing or reacting online "Pause, consider, and have more click restraint." Getting someone to engage more with click-bait content through likes or comments may be a way for websites to generate revenue. If friends or family share misinformation online, offer fact-checking resources. Beware bots and trolls Bots are fake automated accounts. Identify them by spotting new accounts with few followers, no photo, odd usernames with lots of numbers, and non-sensical or inflammatory comments. Bots and trolls are often online troublemakers. Whether bots or not, think twice about engaging online with someone you don't know. Is it necessary or constructive to do so?

Name of the social media / tool	**EMAIL SCAMS**
General information	Email is one of the most beneficial ways to communicate with anyone. But it is also a primary tool used by attackers to steal money, account credentials, and sensitive information. If users interact with the email scammer and provide sensitive information, it can cause long-term issues, including identity theft, financial loss and data corruption. Email fraud (or email scam) is intentional deception for either personal gain or to damage another individual by means of email. Almost as soon as email became widely used, it began to be used to defraud people. Email fraud can take the form of a "con game", or scam. Confidence tricks tend to exploit the inherent greed and dishonesty of its victims. The prospect of a 'bargain' or 'something for nothing' can be very tempting. Email fraud, as with other 'bunco schemes,' usually targets naive individuals who put their confidence in schemes to get rich quickly. These include 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices. Many people have lost their life savings due to fraud.

Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	Many email scams have existed for a long time. In fact, a number of them are merely "recycled" scams that predate the use of email. **LOTTERY Scams** You receive an email claiming you've won a little-known lottery, and always with a huge payout. You may also be asked to pay a small sum to "release" your winnings. You're asked to send personal details as verification, and suddenly you're the victim of identity fraud and the money you sent is gone. **Job offers and Bogus Business Opportunities** These scams promise the opportunity to make a great deal of money with very little effort. They're normally full of enticements such as "Work only hours a week," "Be your own boss," "Set your own hours," and "Work from home." The email messages offering these "opportunities" often have subject lines that look like the following:Make a Regular Income with Online; Put your computer to work for you!: Auctions; Use the Internet to make money; eBay Insider Secrets Revealed 6228; Get Rich Click You receive an unsolicited email offering a job, typically not in your area of expertise, often for a mystery shopper or similar position. When you accept, you're paid by check or money order, for an amount greater than your "employer" offered. You're then asked to send back the difference, only to discover the original check or money order was fake, and you're out of the money you sent to your fake employer. In most cases, the email gives very little detail about the nature of the business opportunity. Most provide an address or web site from which you can, for a fee, obtain an "information kit" about the opportunity. These opportunities, however, usually amount to nothing more than pyramid schemes in which the "opportunity" involves your ability to recruit more unsuspecting people to buy into the scam. Eventually, the scam is uncovered or the pool of new recruits runs dry and it fails. **Charity Fraud Scams** After large-scale natural disasters or high-profile public tragedies, scammers try to capitalize on the public sentiment. They set up fake donation sites and accounts, and then craft an emotional pitch email to solicit funds that never reach the victims. These scams can be successful because they play on the sympathy and goodwill of people! **Beneficiary Scams** You get an email from someone who is looking to move some money around quickly. These emails sometimes come from people claiming to be an important

	businessman or functionary who says he has millions to move out of the country and wants your help in exchange for a cut of the profits. **The Imitator** Many scams imitate legitimate companies in an effort to fool consumers. The simplest way to avoid these fakes is to never click on a link sent in an unsolicited e-mail. Find the company link on your own using a search engine, or, if you know the company address, type it in yourself. **PC Repair Scams** A scam that starts in the real world and quickly moves into the online one, you receive a phone call from someone who claims to work for "Microsoft" or another large software company claiming they can fix PC issues like slow Internet speeds. It sounds helpful, and so when the email arrives in your inbox, you download a remote access program, which allows scammers to take control of your computer. **The 'Official Notice'** These scams attempt to fool consumers into believing they've received an email that requires them to take some action. Often purporting to be from government agencies, these emails notify you of a problem. This example was sent in May, a time when people are more likely to believe an announcement is from the IRS. Here you're supposed to be relieved that the IRS is acknowledging they received your payment, and then be anxious that there is a problem, and click without thinking. **The Survey** These scams rely on people's desire to weigh in on issues and be heard on the issues of the day. In an election year one flavor is the voting survey, but any hot topic will do: global warming, attitudes towards war, the handling of the latest natural disaster, and so on. **Health and Diet Scams** Health and diet scams prey on the insecurities some people have about the state of their well- being. These insecurities make some people particularly susceptible to the scams because they may be reluctant or embarrassed to discuss their problems with a doctor, or they can't afford to buy legitimate drugs or treatment. The scams attempt to lure consumers with promises of quick fixes and amazing results, discount pricing, fast delivery, waived prescription requirements, privacy, and discreet packaging. The email offering these items will have subject lines that look like the following:Increase Your Sexual Performance Drastically; CONTROL YOUR WEIGHT!!; Need to lose weight for summer?; Natural Health Remedy That Works!; Reduce body fat and build lean

	muscle without exercise; Young at any age; Takes years off your appearance; Gives energy and burns fat; **Trojan Horse Email** Trojan horse email offers the promise of something you might be interested in—an attachment containing a joke, a photograph, or a patch for a software vulnerability. When opened, however, the attachment may do any or all of the following: create a security vulnerability on your computer; open a secret "backdoor" to allow an attacker future illicit access to your computer; install software that logs your keystrokes and sends the logs to an attacker, allowing the attacker to ferret out your passwords and other important information; install software that monitors your online transactions and activities; provide an attacker access to your files; turn your computer into a "bot" an attacker can use to send spam, launch denial-of- service attacks, or spread the virus to other computers. Trojan horse emails have come in a variety of packages over the years. One of the most notorious was the "Love Bug" virus, attached to an email with the subject line "I Love You" and which asked the recipient to view the attached "love letter." Other Trojan horse emails have included the following:email posing as virtual postcard; ema; il masquerading as security bulletin from a software vendor requesting the recipient apply an attached "patch"; email with the subject line "funny" encouraging the recipient to view the attached "joke"; email claiming to be from an antivirus vendor encouraging the recipient to install the attached "virus sweeper" free of charge. **Virus-Generated Email** Note that, in some cases, a familiar "from" address does not ensure safety: Many viruses spread by first searching for all email addresses on an infected computer and then sending themselves to these addresses. So, if your friend's computer has become infected with such a virus, you could receive an email that may, in fact, come from your friend's computer but which was not actually authored by your friend. If you have any doubts, verify the message with the person you believe to be the sender before opening any email attachment. Please find an extensive list of different types of email scams at his link - https://en.wikipedia.org/wiki/Email_fraud
Barriers/difficulties for adults	Much like any other kind of fraud, the perpetrator can cause a significant amount of damage, especially when the threat persists for an extended period. Email fraud has a list of negative effects , including loss of money, loss of intellectual property, damage to reputation, sometimes with irreparable repercussions.

	Although older people rarely report being victims of financial cybercrime, there is evidence that older online users are at increased risk. An in-depth research investigated how, why and in what circumstances older adults become cybercrime victims and extrapolated this to consider rational intervention strategies. According to the research, social isolation, cognitive, physical and mental health problems; wealth status, limited cyber security skills or awareness, societal attitudes and content of scams led to victimization. It found that most interventions to enhance older internet users' awareness and skills have been tried to date. Other theoretically plausible interventions include: offender management programmes, tailored security measures, society-wide stigma reduction and awareness-raising with groups who support older people.
Danger of the social media/tool in adults	The act of scamming senior people is a massive problem all over the world. Scams that start on the Internet are becoming more and more frequent among this population, too, especially as Internet-savvy folks start to age. Scammers do not discriminate when it comes to who they try and get money out of: rich, poor, black, white, 65 and healthy, 85 and ailing. They'll try and take money from anyone. The research estimates that about 5 percent of the senior population (which equates to around two to three million people) suffer from some sort of scam every year. "What's worse, it's very likely an underestimate," This is most likely because it's expected that a large percentage of Internet scams go unreported. Scamming older persons is a giant business that drains the seniors of their retirement funds and government benefits. It points out that older persons lose out on about $3 billion to scammers every year. Less conservative estimates project that seniors lose up to $36 billion every year. It is also reported that the median amount that someone over 80 lost was over $1,000 and the median amount someone between 70 and 79 lost was over $600. **Why do seniors fall victim to email scams? The main issues** Far too many seniors fall victim to scams, but it's not their fault. This population is largely trustworthy and made up of financially fruitful people whose cognition may have decreased due to varying ailments. Let's dig into the characteristics and reasons why elderly people become vulnerable to scammers. Aside from why seniors may be targeted, these scams come in various forms that take advantage of their vulnerabilities. **Isolation** Loneliness can eat away at many facets of a senior's life, including making them become extremely susceptible to scams. First off, when they are isolated, there

	isn't anyone to provide a check-in on their finances. It may be far too late to do anything if a loved one finds out about it years later. Isolated elderly people also may be more vulnerable to social interaction, which can set them up for an eager scammer who uses a "relationship" to start their scheme. **Money Situation** An older person's financial situation is a major reason why they become targets for scams. On one side, an elderly person could have millions of dollars at hand after saving for retirement and getting monthly pension checks and government benefits. This may make the person a little less strict with their money, which in turn makes an email or message from a "grandson" requesting money a no-brainer. On the other hand, a senior could be financially insecure and in need of a get-rich-quick source of income, making a pyramid scheme appealing without knowing that they'll never get their money back. **Trusting** According to research people who grew up in the 1920s, '30s, and '40s—a.k.a. Those frequently targeted for scams—are generally more trusting than other generations, which makes them susceptible to con artists who want to find the most vulnerable personalities. **Insecurity** Sometimes, the elderly simply get bullied into handing over money to scammers. Whether in-person or over the phone, a scammer could relentlessly press an elderly person for money until they break. Additionally, a scammer may target an elderly person's own insecurities like their health or social status, saying that they need to pay a certain medical bill or else they will no longer be able to receive government-funded health insurance. **Lowered Cognition with Age** As we age, we are more likely to have some sort of cognitive brain condition like dementia, which affects memory and overall cognitive function. These cognitive conditions can affect your memory in myriad ways, including who your family is and how much money you have—and what's real or fake. Scammers will attack these weaknesses. For instance, a scammer can call someone in their 80s pretending to be their grandchild. The elderly person may remember they have a grandchild, but they may not remember their actual names or what they sound like, so they'll go along with whatever the scammer is saying. **Embarrassment** The elderly can simply get embarrassed by getting scammed, leading them to not report it to the authorities. This makes them attractive targets because scammers know there's a high possibility they won't get caught for trying to (or

	succeeding in) dupe someone. On top of that, many elderly people have no idea where to report scams to, which is sadly all the better for scammers. Less conservative estimates project that seniors lose up to $36 billion every year. It is also reported that the median amount that someone over 80 lost was over $1,000 and the median amount someone between 70 and 79 lost was over $600.
Solutions that we can have	Email provides us with a convenient and powerful communications tool. Unfortunately, it also provides scammers and other malicious individuals an easy means for luring potential victims. The scams they attempt run from old-fashioned bait-and-switch operations to phishing schemes using a combination of email and bogus web sites to trick victims into divulging sensitive information. To protect yourself from these scams, you should understand what they are, what they look like, how they work, and what you can do to avoid them. The following basic recommendations can minimize your chances of falling victim to an email scam: Filter spam. Don't trust unsolicited email. Treat email attachments with caution. Don't click links in email messages. Install antivirus software and keep it up to date. Install a personal firewall and keep it up to date. Configure your email client for security. **What You Can Do to Avoid Becoming a Victim** **Filter Spam** Because most email scams begin with unsolicited commercial email, you should take measures to prevent spam from getting into your mailbox. Most email applications and web mail services include spam-filtering features, or ways in which you can configure your email applications to filter spam. Consult the help file for your email application or service to find out what you must do to filter spam. You may not be able to eliminate all spam, but filtering will keep a great deal of it from reaching your mailbox. You should be aware that spammers monitor spam filtering tools and software and take measures to elude them. For instance, spammers may use subtle spelling mistakes to subvert spam filters, changing "Potency Pills" to "Potençy Pills." **Regard Unsolicited Email with Suspicion**

	Don't automatically trust any email sent to you by an unknown individual or organization. Never open an attachment to unsolicited email. Most importantly, never click on a link sent to you in an email. Cleverly crafted links can take you to forged web sites set up to trick you into divulging private information or downloading viruses, spyware, and other malicious software. Spammers may also use a technique in which they send unique links in each individual spam email. Victim 1 may receive an email with the link <http://dfnasdunf.example.org/>, and victim 2 may receive the same spam email with the link <http://vnbnnasd.exaple.org/>. By watching which links are requested on their web servers, spammers can figure out which email addresses are valid and more precisely target victims for repeat spam attempts. Remember that even email sent from a familiar address may create problems: Many viruses spread themselves by scanning the victim computer for email addresses and sending themselves to these addresses in the guise of an email from the owner of the infected computer. **Treat Email Attachments with Caution** Email attachments are commonly used by online scammers to sneak a virus onto your computer. These viruses can help the scammer steal important information from your computer, compromise your computer so that it is open to further attack and abuse, and convert your computer into a 'bot' for use in denial-of-service attacks and other online crimes. As noted above, a familiar "from" address is no guarantee of safety because some viruses spread by first searching for all email addresses on an infected computer and then sending itself to these addresses. It could be that your friend's computer is infected with just such a virus. **Use Common Sense** When email arrives in your mailbox promising you big money for little effort, accusing you of violating the Patriot Act, or inviting you to join a plot to grab unclaimed funds involving persons you don't know in a country on the other side of the world, take a moment to consider the likelihood that the email is legitimate. **Install Antivirus Software and Keep it Up to Date** If you haven't done so by now, you should install antivirus software on your computer. If possible, you should install an antivirus program that has an automatic update feature. This will help ensure you always have the most up-to-date protection possible against viruses. In addition, you should make sure

	the antivirus software you choose includes an email scanning feature. This will help keep your computer free of email-borne viruses. **Install a Personal Firewall and Keep it Up to Date** A firewall will not prevent scam email from making its way into your mailbox. However, it may help protect you should you inadvertently open a virus-bearing attachment or otherwise introduce malware to your computer by following the instructions in the email. The firewall, among other things, will help prevent outbound traffic from your computer to the attacker. When your personal firewall detects suspicious outbound communications from your computer, it could be a sign you have inadvertently installed malicious programs on your computer. **Learn the Email Policies of the Organizations You Do Business With** Most organizations doing business online now have clear policies about how they communicate with their customers in email. Many, for instance, will not ask you to provide account or personal information via email. Understanding the policies of the organizations you do business with can help you spot and avoid phishing and other scams. Do note, however, that it's never a good idea to send sensitive information via unencrypted email. **Configure Your Email Client for Security** There are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as "text only" will help protect you from scams that misuse HTML in email. **Other ways to protect yourself from email scams** Prevention, through awareness, is a vital tool in combating scammers. There are some handy tips to help you avoid getting scammed on the phone, online, by mail or on your doorstep. There are a few general tips to protect yourself from becoming a victim of a scam. Never give out personal information. This can be used to steal your identity and access accounts. Always check the credentials of any company or legal professional you're unsure about. You can look them up on Companies House(external link opens in a new window / tab) to find out their background or search for reviews online. Don't make any advanced payments until you are sure the company you're dealing with is legitimate.

	Avoid being added to mailing lists which scammers sometimes get hold of. **Clues to spot scam emails** Scammer are becoming more and more shrewd at forging emails and fake messages, in several languages. It is always important to look for signs of a forgery, such as : Generic Greetings Poor quality of grammar, vocabulary Possible spelling mistakes Imperfect design of graphic elements **Ask these Questions** Why am I being approached? Is this thing too good or too bad to be true? Do I really know who my online love is? Have I ever met my online love? Have I ever been on a phone or video connection with him? Does he repeatedly ask me for money, citing possible travel expenses, passport purchases, or various dramatic things and other stories? **SCAM TEST - Use these for steps to scan your emails** Seems too good to be true Contacted out of the blue Asked for personal details Money is requested REMEMBER: financial institutions, utility companies, law enforcement, government bodies, internet & telecoms providers or other public bodies: Will NEVER ask for payment in vouchers. Will NEVER ask you to transfer money because your account is compromised. Will NEVER threaten you over the phone, by letter or email for not paying a fee. Will NEVER threaten arrest if payment isn't made immediately. Will NEVER ask for money for a 'free gift', 'admin fee' or as part of a promotion. Will NEVER ask to reveal your account security codes or online passwords in full. Will NEVER call out of the blue and ask for remote access to your computer or devices or to download software. Will NEVER inform you about tax returns by email, text or voicemail.

Name of the social media / tool	**PHISHING**
General information	Scams targeting seniors are a very big business that robs seniors of their hard-earned savings, retirement funds, and even government benefits. The damages can be devastating. While there are many methods cyber criminals use to defraud older adults, phishing is one of the internet's oldest and most well-known scams. Phishing is a type of internet hoax in which scammers use email and other methods to steal personal information, such as financial details or account passwords. This approach earned its unusual name because it uses attractive "bait" to lure people to websites and solicit their data under false pretenses. Phishing is not the same as spam. While spam is just another term for junk mail and unwanted ads, phishing attacks are deliberate attempts to steal your information and use it in harmful ways. Email Phishing scams are carried out online by tech-savvy con artists and identity theft criminals. They use spam, fake websites constructed to look identical to real sites, email and instant messages to trick you into divulging sensitive information, like bank account passwords and credit card numbers. Once you take the phisher's bait, they can use the information to create fake accounts in your name, ruin your credit, and steal your money or even your identity.
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	There are three main components to a phishing scam: (1) The attack is conducted via electronic communications. Although email is common, phishing can also be carried out via text messages, social media accounts, voicemail, and even phone calls. (2) All forms of phishing aim to convince you that a fake communication is real and credible. The attacker claims to be an individual or organization that's familiar and trustworthy to you. (3) The goal of a phishing attack is to obtain sensitive personal information, such as login credentials, bank details, or credit card numbers. With all phishing attacks, the scammer delivers a carefully crafted pitch aimed at getting you to click a link, download an attachment, or provide specific personal information. Some common phishing attack examples include: **A plea for help:** With a goal of tugging at your heartstrings, the attacker sends you an email pretending to be a good friend or relative (e.g., your grandchild). They claim to be in financial dire straits and request your assistance immediately. How are cyber criminals able to impersonate people you know? With social media, scammers have access to more of our personal information than ever before. This allows them to make their messages highly targeted—and often very believable. **You're the grand prize winner:** You receive a text message congratulating you on being the winner of a very big prize, whether it's an irresistible travel package deal

	or free tickets to the event of the year. You're asked to provide your personal details in order to claim your award. **Your bank account has been compromised:** You get an "urgent" notice that appears to be from your bank, alerting you of suspicious activity on your account. You're then asked to click a link that takes you to a website, where you'll be prompted to confirm your bank account information. **The government is after you**: Few things in life are as jarring as an authoritatively worded notice from a government organization. Scammers know this, which is why many phishing emails appear to be from the government. An email like this typically has a threatening tone and mentions big, scary penalties—unless you provide the payment or personal data they demand. These types of phishing attacks have a flip side, too. In some cases, they're sent during tax season, offering you a generous refund after you confirm your financial details. **Why does phishing work so well?** Emails, text messages, voicemail messages, and even voice calls are not authenticated. This means that, just like a postcard sent through the mail, there's no real way to validate where they came from. That gives scammers plenty of freedom to mimic trusted brands in their communications. Phishing is one of the most common and pervasive threats. Sophisticated phishers are very skilled at creating spoof email templates and websites that are almost indistinguishable from the real thing, right down to the URL (website address) and security certificates. You may think you're receiving a credible message from a bank, online store, or credit card company. And if you're not paying close attention, you might not notice the trickery until it's too late. **Types of Phishing You Need to Know to Stay Safe** Phishing is typically carried out by email spoofing, instant messaging, and text messaging. It is a deceptive way of making individuals reveal personal information. It is also a form of trickery to download malware or ransomware onto a system. Either way, the perpetrator gets privileged access to sensitive information. This is an increasingly frustrating threat because there are numerous ways through which perpetrators attack. Phishing has evolved to become whatever cybercriminals need it to be to steal your credentials. Their methods now take many forms, and if you're unfamiliar with terms like smishing, vishing, pharming, and BEC, here is a guide:

	STANDARD PHISHING Casting a Wide Net - At its most basic, standard phishing is the attempt to steal confidential information by pretending to be an authorized person or organization. It is not a targeted attack and can be conducted en masse. **EMAIL PHISHING** The most common phishing scenario takes the shape of malicious emails sent to individuals mimicking an authentic organization. Also known as spam phishing, this kind of attack lets the cybercriminal get access to a large number of customers registered on a site. So phishing emails are often sent en masse. There is a high possibility of success since some individuals out of the lot will often fall prey. 9 **MALWARE PHISHING** Beware the Macros Using the same techniques, this type of phishing introduces nasty bugs by convincing a user to click a link or download an attachment so malware can be installed on a machine. It is currently the most widely used form of phishing attack. **SPEAR PHISHING** Catching the Big One - Where most phishing attacks cast a wide net, hoping to entice as many users as possible to take the bait, spear phishing involves heavy research of a predefined, high-dollar target often relying on publicly available information for a more convincing ruse. This also implies a technique where the phisher targets a specific individual or group of individuals rather than a generic user base.These attacks succeed precisely because they are more personalized. The perpetrator customizes emails with the recipient's name, company, phone number, and similar information, making the target believe that they share some form of connection to the sender. Achieving convincing spear-phishing emails takes a great deal of time since the phisher has to acquire multiple data from various sources. It is no wonder then that this kind of malicious attack is prevalent on social media platforms like LinkedIn, where the phisher can utilize social engineering tactics. **SMS + PHISHING = SMISHING** Just Don’t Click - SMS-enabled phishing uses text messaging as a method for delivering malicious links, often in the form of short codes, to ensnare smartphone users in their scams. The advent of mobile technology brought about a myriad of advantages in communication and online banking. At the same time, it opened up

	a new point of contact for unscrupulous individuals to commit more crimes. One of such is smishing, where cybercriminals lure victims through text messaging to: Visit rogue websites Download malicious apps Contact tech support Whether in the guise of a coupon code or an offer to win free tickets or free money, a smishing attempt will more often than not require you to click on a link that redirects you to a website. Quite common also are links that trigger the automatic download of dangerous apps. Although they appear to be from legitimate sources with URLs that are familiar to you, they are merely aimed at stealing personal information or installing malware on your mobile device. **SEARCH ENGINE PHISHING** Careful What You Choose - In this type of attack, cyber criminals wait for you to come to them. Search engine phishing injects fraudulent sites, often in the form of paid ads, into results for popular search terms. **VISHING** Keeping You On the Line - Vishing involves a fraudulent actor calling a victim pretending to be from a reputable organization and trying to extract personal information, such as banking or credit card information. Most often, the “caller” on the other line obviously sounds like a robot, but as technology advances, this tactic has become more difficult to identify. **PHARMING - Poisoning the Waterhole** Also known as DNS poisoning, pharming is a technically sophisticated form of phishing involving the internet’s domain name system (DNS). Pharming reroutes legitimate web traffic to a spoofed page without the user’s knowledge, often to steal valuable information. On opening the malicious website, link, or attachment, your computer is automatically loaded with malware that spreads to other systems within the company. To perpetuate successful watering hole attacks, the hacker will often identify websites that you visit regularly and monitor email patterns. With pharming, the perpetrator doesn't attack individuals. Rather the attack is directed at the DNS (Domain Name System), where the fraudster causes DNS cache poisoning. This changes the IP address associated with a website name, so even when individuals input the correct site name, the scammer can still redirect users to the malicious website. Although less widespread, targeting the DNS server could compromise millions of URL requests by web users.

	CLONE PHISHING In this type of attack, a shady actor makes changes to an existing email, resulting in a nearly identical (cloned) email but with a legitimate link, attachment, or other element swapped for a malicious one. These attacks can't get off the ground without an attacker first compromising an email account, so a good defense is using strong, unique passwords paired with two-factor authentication. **MAN-IN-THE-MIDDLE** The Public WiFi Phisherman - A man-in-the-middle attack involves an eavesdropper monitoring correspondence between two unsuspecting parties. When this is done to steal credentials or other sensitive information, it becomes a man-in-the-middle phishing attack. These attacks are often carried out by creating phony public WiFi networks at coffee shops, shopping malls, and other public locations. Once joined, the man in the middle can phish for info or push malware onto devices **MALVERTISING** That Ad Isn't What You Think It Is - This type of phishing takes advantage of exploits within advertising or animation software to steal information from targeted users. Malvertising is usually embedded in otherwise normal-looking ads—and placed on legitimate websites like Yahoo.com—but with malicious code implanted within. **DOMAIN SPOOFING** The second kind of email phishing comes in the form of domain spoofing, where the perpetrator spoofs a notable organization's domain name. This technique makes it appear as if you are receiving an email from a legitimate company. Email addresses are unique, so the phisher can only mimic the organization's address. They do so by using character substitution like 'r' and 'n' together for 'rn' instead of 'm.' Otherwise, they use the organization's name with a different domain, in the hopes that only the local part of the email address will appear in the inbox of the recipient. A domain spoof could also create a fraudulent website that looks like the real deal. They would replicate the real site's design. Once again, the emphasis is on the phrase "looks like." While the fake domain may be similar, it is not identical to the original website. **EVIL TWIN** WI-FI access points are frequented by hordes of individuals looking for fast wireless connections to surf the web and carry out other internet-based activities. The hacker in this scenario replicates the WI-FI hotspot with a fake. When users connect, they are then able to eavesdrop on their network traffic. The attacker steals account names and passwords. The phisher is also able to view any attachments that the user accesses while on the compromised network.

Vulnerable WI-FI access points include those at coffee shops, airports, shopping malls, hospitals, and other public hotspot locations.

Real-Life Examples of Phishing Attacks

According to recent research by Google, there was a 3505 increase in phishing websites from January to March 2020. Another survey by Check Point Research revealed that 64% of businesses in the past year had been victims of phishing attacks. More findings by Verizon have confirmed that phishing is involved in 78% of cyber-espionage incidents. These are five of the most notable examples:

Whaling Attack Leads to Firing of FACC Boss

In 2016, Austrian Aerospace company FACC had been subject to one of the most prominent Whaling attacks ever, dubbed the Fake President Incident, where the attacker made away with $56 million. In a classic whaling attack, the perpetrator impersonated the CEO and sending an email to an employee of the finance department requested an immediate funds transfer.

The attack didn't only cost the firm financial losses, but it also cost the CEO at the time, Walter Stephan, his position. Although the details were not revealed, the sack was on the grounds of violation of duties.

Spear Phishing Targeted at Ubiquiti Networks Inc.

In June of 2015, the American network technology company Ubiquiti Networks became the target of a spear-fishing email campaign. The attacker impersonated higher-ranking executives from an overseas branch with spoofed email addresses and domain look-alikes. The employees were fooled into believing that they were getting legitimate requests from company officials to transfer funds to a secure account. Ubiquiti Networks was unaware that it was being scammed until it was notified of the activity by the FBI.Didn't suffer any compromise to its systems, it lost $46.7 million in transferred funds.

Facebook and Google Invoice Scam

Between 2013 and 2015, US behemoth companies Facebook and Google were reportedly scammed out of $100m in an elaborate wire fraud scheme. The perpetrator set up a fake business impersonating the Taiwanese Quanta Computer company. The latter regularly conducted multi-million dollar transactions with the social media companies, and over the two years, the attacker would send phishing emails with forged invoices to be paid to fake bank accounts. The scheme avoided suspicion for so long by creating phony supporting documents for transactions and forged corporate seals. The attacker was later identified as Lithuanian Evaldas Rimasauskas, who was given a five-year prison sentence following his arrest in 2017.

Apple Smishing

In 2020, one of the biggest smartphone companies in the world, Apple, was reported to have been the target of a smishing campaign. With a fake Apple

	chatbox, the messages informed users that they had won the chance to be part of Apple's 2020 testing program for the new iPhone 12. The recipients were requested to pay a delivery charge. Redirecting to a malicious website, the attackers hijacked the victims' payment card credentials. People nowadays keep lots of sensitive information on their smartphones, and the widespread usage of iPhones and iPads has made them recurring targets for SMS phishing schemes. Attackers regularly send out messages to users. These messages will contain a link to follow to unlock a frozen Apple ID account or to prevent it from expiring from future messages of the sort. Others will bait users with the idea that a lost iPhone has been found. Victims are duped out of their login credentials, and the hackers gain access to their media, documents, and other information stored on the device. As an ongoing threat, the amount lost during successful attempts adds to the statistics for annual cybercrime losses. Even though not everyone falls victim, the attacker earns significant rewards for the small percentage of people that wasn't any wiser. **RSA Security Breach** All it took for an attacker to gain access to the popular cybersecurity company's network system was an email with the subject line "2011 Recruitment Plan." In the email was a virus-infected Excel file, and once opened by an unknowing employee gave the attacker access to private passwords. Making this a perfect example of a watering hole phishing attack. Ironically, the RSA provides cybersecurity services to several branches of the US government and other business enterprises. This breach gave the hackers access to the networks of US government departments, becoming an Advanced Persistent Threat. Watch this video https://www.youtube.com/watch?v=4AcROYO8BLA
Barriers/difficulties for adults	Emails, text messages, voicemail messages, and even voice calls are not authenticated. This means that, just like a postcard sent through the mail, there's no real way to validate where they came from. That gives scammers plenty of freedom to mimic trusted brands in their communications. Phishing is one of the most common and pervasive threats. Sophisticated phishers are very skilled at creating spoof email templates and websites that are almost indistinguishable from the real thing, right down to the URL (website address) and security certificates. You may think you're receiving a credible message from a bank, online store, or credit card company. And if you're not paying close attention, you might not notice the trickery until it's too late.

Danger of the social media/tool in adults	According to Wikipedia, phishing is a fraudulent attempt to obtain sensitive data by impersonating oneself as a trustworthy entity. Much like any other kind of fraud, the perpetrator can cause a significant amount of damage, especially when the threat persists for an extended period. 11 Much like any other kind of fraud, the perpetrator can cause a significant amount of damage, especially when the threat persists for an extended period. Email fraud has a list of negative effects, including loss of money, loss of intellectual property, damage to reputation, sometimes with irreparable repercussions. Although older people rarely report being victims of financial cybercrime, there is evidence that older online users are at increased risk. According to the research, social isolation, cognitive, physical and mental health problems; wealth status, limited cyber security skills or awareness, societal attitudes and content of scams led to victimization. The financial loss for older victims was nearly twice as much per scam as for younger victims However, it is important to note that the financial loss for older victims (those aged 55 and over) was likely to be nearly twice as much per scam as that for younger age groups. Also, it may be surmised that, for many older people on a fixed income (and no easy means of building new savings for example), it is likely to be more difficult for them to replace money that is lost as a result of fraud than for people of working age. Nearly half (49 per cent) of all people aged 75 and over live alone; and 17 percent of older people have less than weekly contact with family, friends and neighbors. People who are more socially isolated may well be more vulnerable to fraud, for instance, if they have little chance to discuss matters with others. **How do senior citizens fall prey to phishing?** The act of scamming senior people is a massive problem all over the world. Scams that start on the Internet are becoming more and more frequent among this population, too, especially as Internet-savvy folks start to age. **If you've responded to a phishing scam, the attacker can possibly:** Hijack your usernames and passwords Steal your money and open credit card and bank accounts in your name Request new account Personal Identification Numbers (PINs) or additional credit cards Make purchases Add themselves or an alias that they control as an authorized user so it's easier to use your credit Obtain cash advances

	Use and abuse your Social Security number Sell your information to other parties who will use it for illicit or illegal purposes How did a phishing scam find me? This style of identity theft is extremely widespread because of the ease with which unsuspecting people share personal information. Phishing scams often lure you with spam email and instant messages requesting you to "verify your account" or "confirm your billing address" through what is actually a malicious Web site. Be very cautious. Phishers can only find you if you respond. **How will I know if I've been phished?** Phishers often pretend to be legitimate companies. Their messages may sound genuine and their sites can look remarkably like the real thing. It can be hard to tell the difference, but you may be dealing with a phishing scam if you see the following: Requests for confidential information via email or instant message Emotional language using scare tactics or urgent requests to respond Misspelled URLs, spelling mistakes or the use of sub-domains Links within the body of a message Lack of a personal greeting or customized information within a message. Legitimate emails from banks and credit card companies will often include partial account numbers, username or password. **Impacts** **Loss of money** From every phishing incident that has ever taken place in history, one constant effect is financial loss. The financial losses experienced by individual consumers is estimated to be over £9 billion per annum. However, while these figures are useful indicators, they are likely to significantly under-estimate the scale of financial loss experienced by individuals as it does not appear that they included all types of fraud and, as indicated, many fraud offences go unreported. Confusingly, the figure of £3.5 billion is also frequently referred to as an estimate of total financial losses experienced by people as a result of fraud or scams. **Other impacts** In general, the other effects of fraud for victims may vary depending on people's individual circumstances and their existing resources and capabilities, but the severity of the potential impact should never be under-estimated. The psychological effects can be severe and debilitating, including stress, anger, loss of self-esteem, shame and upset.

	The negative impact of financial abuse, regardless of the source, can result in someone becoming in need of support from social services, having not previously required such help. A study into doorstep crime showed that victims' health declines faster than non victims of a similar age Analysis of the effects of doorstep crime found that: 40 percent of victims said it had resulted in them having reduced confidence generally. 28 per cent said it had left them feeling down or depressed. 46 per cent said it had caused them financial detriment. 16 per cent had not told anyone about the crime, and 40 percent of these said the reason was embarrassment Victims are often vulnerable people who may be in financial distress or are older or socially-isolated. The personal impact on them and on their families is often devastating in terms of future peace of mind and health. Victims can be left with damaged self-esteem and a reduced sense of self-worth. Victims suffer stress, anxiety and depression. Lives can be ruined.' Nearly half (49 per cent) of all people aged 75 and over live alone; and 17 percent of older people have less than weekly contact with family, friends and neighbors. People who are more socially isolated may well be more vulnerable to fraud, for instance, if they have little chance to discuss matters with others. How do senior citizens fall prey to phishing?
Solutions that we can have	The best defense against a phishing scam is to verify with the person or organizations who sent the email or message before clicking on anything. **How can you protect yourself from phishing?** When you arm yourself with information and resources, you're wiser about computer security threats and less vulnerable to phishing scam tactics. Take these steps to fortify your computer security and get better phishing protection right away: Do not provide personal information to any unsolicited requests for information Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser If you suspect you've received phishing bait, contact the company that is the subject of the email by phone to check that the message is legitimate Type in a trusted URL for a company's site into the address bar of your browser to bypass the link in a suspected phishing message Use varied and complex passwords for all your accounts Continually check the accuracy of personal accounts and deal with any discrepancies right away Avoid questionable websites

	Practice safe email protocol: Don't open messages from unknown senders Immediately delete messages you suspect to be spam **Make sure that you have the best security software products installed on your PC for better phishing protection:** Use antivirus software protection and a firewall Get antispyware software protection An unprotected computer is like an open door for email phishing scams. For a more potent form of protection, use a spam filter or gateway to scan inbound messages. These products thwart dangerous malware before it can enter your PC, stand guard at every possible entrance of your computer and fend off any spyware or viruses that try to enter, even the most damaging and devious strains. While free anti-spyware and antivirus downloads are available, they just can't keep up with the continuous onslaught of new spyware strains. Previously undetected forms of spyware can often do the most damage, so it's critical to have up-to-the-minute, guaranteed protection. **Compare & Find The Best Phishing Protection Software** Online scammers will try to trick you into relinquishing your passwords or other personal information by posing as legitimate websites. Often, they'll even act the same as the websites you regularly log into. These threats are easily avoided with an antivirus program in place. It's our pleasure to show you which ones provide the best protection against phishing attacks without affecting your computer's performance or getting in the way of your work. **What's The Best Antivirus Solution?** Bitdefender, the antivirus brand trusted by 500 million-plus users across 150 countries, is one of the world's leading providers of consumer cybersecurity products and a pioneer in antivirus protection. This brand has won multiple antivirus awards from leading online test laboratories, including AV-Comparatives, AV-Test, PCMag, and The Anti-Malware Testing Standard Organization. Netcraft's countermeasures service helps organizations to combat these techniques. Once a phishing site has been detected, Netcraft immediately responds with a set of actions which will significantly limit access to the site, and will ultimately cause the fraudulent content to be eliminated. Netcraft's approach to removing phishing sites is distinguished from other providers of takedown services through its ability to immediately block access to the site for users of a wide range of technologies. **The Best Anti-Phishing Softwares**

	Online scammers will try to trick you into relinquishing your passwords or other personal information by posing as legitimate websites. Often, they'll even act the same as the websites you regularly log into. These threats are easily avoided with an antivirus program in place. It's our pleasure to show you which ones provide the best protection against phishing attacks without affecting your computer's performance or getting in the way of your work. **Verified Mark Certificates?** Verified Mark Certificates (VMCs) allow you to render your logo next to the "sender" field in email clients so that users see your mark—and that your organization has been authenticated—before they even open your message. It's the email equivalent of a checkmark on social media, with added validation and security requirements to help protect your customers and your brand against phishing and spoofing attacks. Logo-verified email is part of a groundbreaking initiative—in cooperation with Brand Indicators for Message Identification (BIMI) and email client providers— to promote a consistent, trusted and visually authenticatable email experience for both businesses and consumers. Here's how it works: (watch the video) https://www.digicert.com/content/dam/digicert/videos/digicert-vmc-product-reveal.mp4 **HOW TO PROTECT YOURSELF FROM PHISHING ATTACKS** Protecting yourself from phishing attacks starts with knowing what's out there. Never click on links from unknown senders or if any detail about the exchange has aroused suspicion. henever possible, hover over a link to ensure the destination matches your expectations. Note this will not work on mobile or if short codes are used, so be extra wary on mobile devices. If you suspect an email is a phishing attempt, double check the sender name, specificity of the salutation, and a footer for a physical address and unsubscribe button. When in doubt, delete. If you're unsure if a communication is legitimate, try contacting the brand or service via another channel (their website or by calling a customer service line, for instance). Avoid entering personally identifiable information unless you are extremely confident in the identity of the party you are of the party you are communicating with. Closing All Your Security Gaps While staying vigilant will keep most attackers at bay, no one can be 100% secure on their own. After all, phishing only exists today because it works. This is why it's important to combine security awareness training with quality business endpoint protection—with AI-enhanced threat intelligence, cloud-based updates, and real-time anti-phishing—DNS protection, and reliable data backup.

	To Prevent Senior Citizen Scams If you're worried about fraud, there's plenty you can do to prevent it from happening to you : Set up credit monitoring and identity theft protection - Criminals almost always commit elder fraud with the goal of pulling off financial scams. The easiest way to protect yourself or your loved one's finances is to sign up for credit monitoring. **Further Steps to Take:** STOP: Take a breath and think about the situation. Does anything feel suspicious? LEAVE: Hang up, shut the door, or close the email. If someone is pressing you to act now, they could be a con artist. ASK: Call a family member for advice, search online for more details, and find out if organizations are real. You can also ask a visitor for identification. WAIT: Take the time to absorb what you've learned and make a plan of action. Don't rush any decisions. ACT: Only visit legitimate websites and call verified, safe phone numbers. You can use independent review websites and email address lookup services to check someone's identity. Share your stories of attempted fraud. Ask your more tech-savvy family members to share examples of scam emails or messages they've received. Have a plan and a password - Sharing bank account details early can ensure that your family's money stays safe. Be suspicious of any unsolicited call or message - A little suspicion can save you a lot of heartache. Know that these scams exist, and always ask yourself, "what if?" when confronted with an unusual request for money either online or in person.

Name of the social media / tool	**FACEBOOK**
General information	Facebook is an American online social media and social networking service owned by Meta Platforms. Founded in 2004, its name comes from the face book (https://en.wikipedia.org/wiki/Face_book) directories often given to American university students. At the beginning the membership was limited only to Harvard students. Since 2006, it was available for anyone over 13 years old. In it was the most downloaded mobile application. Right now Facebook can be accessed from different types of devices equipped with Internet connectivity. You can easily use it on personal

	computers, tablets and smartphones. To use the application, you must be a registered user, which means to create a profile revealing information about yourself. After that process you can create text posts, including photos and multimedia, you can share it with any other users who have agreed to be your "friend". Facebook allows to adjust different privacy settings, either your profile is available publicly or is available only for now to you users. Facebook application allows also to communicate among users with Facebook Messenger. You can run private conversations, but also you can join create groups or join common-interest groups.
Risk associated to the social media/ tool: **Privacy,** **accuracy,** **property,** **accessibility,** **Violation of laws,** **Copyright**	Facebook has often been criticized over issues such as user privacy, mass surveillance, psychological effects political manipulation, such as addiction and low self-esteem, and content such as fake news, conspiracy theories, copyright infringement, and hate speech. ***Privacy:*** On the FB page you can find the direct link to the privacy rules: https://www.facebook.com/privacy/policy ***Accuracy:*** https://www.facebook.com/policies_center/ads ***Property:*** Facebook considers it its duty to help individuals and organisations protect their intellectual property rights. Facebook's Terms and Conditions prohibit users from posting content that infringes the intellectual property rights of others, including copyright and trademark rights. ***Copyright*** Copyrights are statutory rights that protect original works of authorship, such as books, musical works, films and works of art. In general, copyrights protect original expressions, such as statements or images. They do not protect facts or ideas, but may protect original statements or images that describe an idea. Copyright also does not protect names, titles or slogans. Their protection is provided by trade mark laws. ***Trade marks*** A trade mark is a word, slogan, symbol or design (e.g. a brand name or logo) that distinguishes the products and services offered by an entity, group or company from those offered by other entities, groups or companies. The general function of trade mark law is to help consumers recognise what entity is responsible for a particular product or service. https://www.facebook.com/help/399224883474207/?helpref=uf_share ***Accesibility:***

	Facebook provides a comfortable experience for all users. Features and technologies are available to help people with disabilities, such as visual and hearing impairments, use Facebook as much as possible. ***Violation of laws:*** State institutions may consider that the content published by a user on Facebook violates local laws, they may ask for a restriction on this content. If you publish content that does not comply with local laws, a court may order a restriction on the publication of the content or report allegations that the content is unlawful, from non-governmental institutions and members of the public. Submissions are reviewed in accordance with Global Network Initiative commitments and the Corporate Principles for the Protection of Human Rights. https://transparency.fb.com/data/content-restrictions/content-violating-local-law/ ***Copyright:*** Laws may vary from country to country. Copyright information is available from the US Copyright Office or the World Intellectual Property Organisation (WIPO). Facebook does not provide legal advice, so it is advisable to consult a lawyer if you have questions about copyright. In most countries, copyright is a statutory right that protects original works of authorship. Usually, the creator of an original work obtains copyright in that work at the time of creation. Many different types of content are protected by copyright, including: • *Visual or audiovisual material*: video content, films, television programmes and broadcasts, video games, paintings, photographs • *Audio content*: songs, musical compositions, sound recordings, recordings of oral statements • *Written content*: books, plays, manuscripts, articles, musical notations The copyright protects only original works. To be considered sufficiently original for copyright protection, the content must be the work of the author and must have been created by a specific amount of creative effort.
Barriers/difficulties for adults	• high level of identity disclosure on Facebook similarly to other social network sites. The information included can be, name, email address, physical address, phone number, gender, hometown, birth date, photo, friend network, sexual orientation, relationship status, interests, job/occupation, favourite books, favourite films, favourite music, school, information, post code (or ZIP code) and political affiliation. Above mentioned information are particularly sensitive as people identify themselves authentically. • the use of real names to represent a profile may be encouraged through technical specifications, registration requirements, or social norms (connecting participants profiles with their public identities).

	• stalking, re-identification, demographic re-identification, face re-identification, and identity theft. Users can be manipulated through social engineering, harassment, stalking and spamming due to the element of "creepiness" • of the site • Facebook can also be addictive. • online communication is more appealing than face to face interaction, this in turn can increase internet socializing. This can create compulsive and excessive use of online social networks that can have adverse effects to outcomes at work and home (counteracting other deficiencies such as, relationships, lack of friends, physical appearance and disabilities. • no possibility of reporting sex offenders to police, • police have raised concern with Facebook not agreeing to provide a panic button to each users profile page, Facebook failing to tackle the threat of paedophiles • the rise in crimes such as harassment and actual bodily harm as a result of Facebook use •
Danger of the social media/tool in adults	• Losing control of the time you spend online. The layout of pages, every button, every colour is carefully chosen by experts to attract attention. • The number of fake Facebook accounts is huge - so-called internet trolls • Hackers know very well how to crack a password on FB. • It is very common to fake social network login pages and send false messages • Facebook is often used as a tool for spreading false information • Information that we publish ourselves on social media can be used by third parties • The Koobface worm was active on Facebook for over a year • Sharing your location with applications and other users can result in you being tracked (e.g. observation of your whereabouts, burglary) • Biometric authentication for access to e.g. your mobile phone or online profiles (using a face scan or fingerprint) has also emerged as a threat.
Solutions that we can have	On line training on how to : • Safely use the Facebook; • What not to publish on social networks (how to limit sharing private information about yourself) • Privacy settings on FB. • Creating a secure password for your account • Setting up two-factor authentication. • Accepting invitations (identifying an invitation from a person). • Keeping antivirus and other security software up to date. • Using the Private Conversations module. • Sharing content, photos and posts from other social media. • How to report content that appears suspicious.

Name of the social media / tool	**GOOGLE+**
General information	**Google+** was launched on June 28, 2011, in an attempt to challenge other social networks, linking other Google products like Google Drive, Blogger and YouTube. It is usually known as Google Plus, sometimes called G+ was a social network owned and operated by Google. Substantial changes led to a redesign this social network in November 2015. On March 7, 2019 it was decided to shut down the social network for business and a month later on April 2, it was also shut down for personal users. The reason of this decision were both low user engagement and disclosed software design flaws that potentially allowed outside developers access to personal information of its users. Google+ continued to be available as "Google+ for G Suite"; all users transitioned to "Google Currents". The next step will be eventually the transition from Google Currents to "Google Chat" in 2023. On Google+, people may share ideas and personal news, post photos and videos, stay in touch, play games, plan get-togethers, send birthday wishes, do homework and business together, find and contact long-lost friends and relatives, review books, recommend restaurants and support causes. The list goes on – you can see how individual its use is. Social networking also includes getting and giving validation and emotional support, lots of informal learning, as well as exploring personal, academic and future professional interests. You need to be a registered user to have a full access to Google + options. While making the sign in/registration you will be asked to answer a few simple questions such as your real name, a username, a password and your birthday. In U.S to get an account, you must be at least 13 years old, the same in other countries. You will also be given an opportunity to add a profile picture and then you'll be whisked directly into Google+. During the registration process you will be asked to "find people you know on Google+" by entering an email address from Yahoo or Hotmail. This is optional. Google+ won't contact the people in your contact list but will import contacts from those services and give you the option of adding your contacts from those services to your circles. Once you have an account, the first time you visit Google+ you'll be asked several questions, which are optional (school or work name and where you live to make it easier for friends, family and others to find you).
Risk associated to the social media/ tool: **Privacy, accuracy, property, accessibility, Violation of laws, Copyright**	***Privacy:*** The privacy setting allowed users to disclose certain information to the circles of their choice. Users could also see their profile visitors. There were privacy settings that you could get to by clicking on your name in the upper right of your screen and then Privacy. This included links to managing circles, network visibility (who was in your circles and who could see who had

	added you to their circles) and other settings. There was also a link to the Google+ privacy help section. ***Accuracy:*** No data. ***Property:*** Some property management companies used Google+ to share their own blog posts, third party articles, news about their business or the industry in general, etc. Google My Business has now become the central hub where web visitors can find and learn more about your company. ***Accessibility:*** Most of the things you can do on Google+ on the Web can also be done via the Google+ Smart phone app for Android and iPhone, and there is a Web app that works with other Internet-connected phones. Google Messenger is a feature for smart phones (but not the desktop version of Google+) that allows groups of people to have a conversation. ***Violation of laws:*** Google works hard to enforce these rules, but with millions of users and zillions of posts they can't do it all by themselves. That's where the community comes in. It's up to all of us to make sure Google+ remains a safe and comfortable place. If you see content that appears in violation of the standards, you have the option to click the down-arrow to the right of the post or content and select Report abuse. You're then asked to specify why it's abusive by checking the appropriate box. There is also an option to "Report this profile" in the left column of each person's profile if the profile itself contains content that is likely to violate Google's community standards. ***Copyright:*** The standard reference for the question of copyright infringement is Google's Terms of Service. The Google service "We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act. We provide information to help copyright holders manage their intellectual property online. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center."
Barriers/difficulties for adults	• The most common risk is social aggression (cyberbullying)

	• Posting embarrassing or damaging info about ourselves – text, photos, or videos that could embarrass us now or later, whether posted by ourselves or others. This is the reputation issue. • The screen-time challenge – too much time on any one thing can be detrimental to other activities in our lives. • Risk of inappropriate contact with strangers/hackers • Be careful who you invite to a hangout, and realize that anyone who is invited can invite additional people you may not know.
Danger of the social media/tool in adults	For the moment Google + will not be a danger for adults, as the social network is shut down since 2019.
Solutions that we can have	Manuals or guides that will support in downloading the data put on the Google + account created before 2019.

MILEAGE

Partners

E-Seniors (France) • www.eseniors.eu

CARDET (Cyprus) • www.cardet.org

EDUCATOR (Czech Republic) • www.educatorspolek.com

Framework (Italy) • www.aframework.it

WSBINOZ (Poland) • www.wsbinoz.edu.pl

Join us!

mileageproject info@mileageproject.eu www.mileageproject.eu

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 2021-1-FR01-KA220-ADU-000033422