Erasmus+Project Cybersecurity literacy to empower seniors towards safe Digitalisation

2023-1-CY01-KA210-ADU-000150806

Guide to Safe and Responsible Use of the Internet for Adult Education Trainers

TABLE OF CONTENTS

1. Introduction of the Erasmus+ project CYBERUP **3**
1.1 Participant Profile and Research 4
1.2 . Data collection and results 5
2. Internet Safety **8**
2.1. Digital Literacy 9
2.2. Online Communication 12
2.3. Digital identity and footprints 13
2.4. Privacy and Security 15
2.5 Recommendations for responsible habits 16
3 Practical Activities: **17**
A: Digital Literacy 18
1: Activity: “Evaluating Online Sources” 18
2: Activity: “Advanced Search Techniques” 21
3: Activity: Virtual Collaboration Project 22
4: Activity: Multimedia Presentation 23
B: Digital Communication 26
1: Activity: “Request a Place” 26
2: Activity: “Shall we have a meeting?” 28
3. Activity: “Sharing my trip” 32
C: Digital identity 34
1. Activity: "Map Your Digital Footprint" 34
2. Activity: “Profile Creation” 37
3. Activity 3: Analysis Case Study 39
D: Privacy and Security 42
1. Activity: Password Challenge 42
2. Activity: "Spot the Phish" 44
3. Activity: "Safe or Unsafe” 46
4. Activity: Privacy Check-Up 48
5. Activity: "Fact or Fiction” 51
References and resources **53**

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1. Introduction of the Erasmus+ project CYBERUP

The Erasmus+ project CYBERUP (2023-1-CY01-KA210-ADU-000150806) main objective is to develop knowledge, attitudes and digital skills applied to cybersecurity in seniors for a more efficient and inclusive use of the most common digital technologies in people over 60 years old with low digital skills.

Today's widespread use of technology, accelerated by the COVID-19 pandemic, increases the importance of access to digital devices and the Internet, and of acquiring the digital skills needed to participate in society but above all, to make safe and equitable use of new technologies and avoid becoming a victim of cybercrime. The widespread use of technology in all areas of life has also led to significant risks, including misinformation and disinformation, misuse of personal data and the possible translation of the digital divide into a learning divide, leading to further inequalities.

These developments reinforce the need to pay more attention to digital skills especially for seniors, and to foster citizenship skills. Cyberattacks and cybercrime are on the rise across Europe, and are becoming increasingly sophisticated. This trend will continue to worsen in the future.

This project aims to respond to the needs of digital transformation in terms of cybersecurity literacy to ensure a safe digital transition in both education and society. The main objective of this project is to develop knowledge, attitudes and digital skills applied to cybersecurity in seniors for a more efficient and inclusive use of the most common digital technologies in people over 60 years old with low digital skills.

Specific objectives:

- To provide trainers with a tool that assists them in promoting lifelong learning in digital skills and cybersecurity in the field of adult education.
- To promote digital literacy in terms of cybersecurity for seniors to avoid digital threats and reduce cybersecurity skills gap.
- To raise awareness on the need and importance for empowering seniors towards a more safe and fair digital transformation.

The project objectives are linked to the priorities established as follows:

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Digital Erasmus+. This project aims to respond to the needs of digital transformation in terms of cybersecurity literacy to ensure a safe digital transition in education and society as well.

- The setup or enlarging of an access to upskilling pathways for adults with a low level of skills. The project aims to address the needs of the main target group (adult people over 60 years old with low digital skills) in terms of digital safety and empower them towards a more inclusive digital transformation through a tailored training on cybersecurity literacy.

- Extending and developing the competences of educators and teachers. The project aims to support the promotion and implementation of cybersecurity in adult education (through the methodological guide for trainers) as a fundamental aspect to help achieve a fairer and safer transition in the current digital education.

1.1 Participant Profile and Research

First step of the project is the creation of the “Guide to safe and responsible use of the Internet for Adult Education Trainers”. This guidecontain, on the one hand, relevant information on the current situation of seniors in terms of their digital and cybersecurity skills in the partner countries, as well as the new challenges they face, as well as the new challenges they face. On the other hand, it contains information, resources and methods to help trainers apply and promote cybersecurity as part of lifelong learning in the field of adult education.

The needs analysis report on attitudes and needs related to digital skills applied to cybersecurity in seniors for a more efficient and inclusive use of the most common digital technologies in people over 60 years old with low digital skills. Participants' profiles are based on seniors over 60 years old, from both countries involved in the project, Cyprus and Spain. This population group has gone digital to a considerable degree in the last two years, precisely because of their increasingly constant use of technological tools in the wake of the covid-19 pandemic years, increasing the risk of becoming an easy target for cybercriminals who take advantage of their vulnerability. The methodology followed in this study report is based on a questionnaire with a focus group based on the target group with 10 questions to collect the necessary information for the creation of this methodological guide for each country involved in the Erasmus+ project, Cyprus and Spain.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The report comes from having first done an individual one for each country and through this report we bring together a research phase of literature needs and the practical phase, having used the two focus groups. Each focus 54.5% seniors from Spain and 45.5% seniors from Cyprus with 15 participants. men and women, ages in between 60 to 95. 70% were aged between 60-67 years old in Spain and in Cyprus. But we were also seniors in their 70´s, 80,s and also 90,s.

1.2 . Data collection and results

The selected group of seniors selected from both countries involved, Cyprus and Spain, with the focus group based in 15 people per country, has gone digital to a considerable degree in the last two years, precisely because of their increasingly constant use of technological tools in the wake of the covid-19 pandemic years, increasing the risk of becoming an easy target for cybercriminals who take advantage of their vulnerability. This population group grew up in a generation in which these technologies did not exist and they are afraid to use them, which makes them even more vulnerable in terms of digital security.

First, Participants' profiles are based on seniors over 60 years old from both countries involved. 54.5% seniors from Spain answered the report and 45.5% seniors from Cyprus. Age can intersect with other socioeconomic factors, such as income, education, and geographical location, influencing disparities in digital literacy and access to technology. Identifying age-specific barriers to digital inclusion can inform policies and initiatives aimed at reducing the digital divide and promoting equitable access to digital resources and opportunities for individuals of all ages.

Overall, considering was focused about digital literacy valuable insights into how digital skills, attitudes, and behaviors is a necessity to the target group of

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

this project, to face the cognitive challenge of acquiring new skills and abilities; and secondly, it favors their autonomy and emotional well-being since technology breaks down the barriers of loneliness and isolation, but also to be integrated into the new digital era, to promote digital inclusion, enhance digital literacy education, and address the diverse needs and preferences of individuals across the lifespan. Regarding the age, most of the respondents were between 60-67 years old in Spain and in Cyprus. But there are seniors in their 70´s, 80,s and also 90,s. too.

The project partners, in this project, Connecting Dots from Cyprus and Inercia Digital from Spain delivered a questionnaire, with 10 questions implemented in a google form which was distributed to 15 stakeholders in Cyprus and 15 stakeholders in Spain. Below we show the explanation of the results for each of the questions in the questionnaire. With it we intend to have a better vision and understanding of the real use that people over 60 years of age make of technologies, and digital use in their daily lives, and thus find and better design a future digital security and usage guide.

It has been the facilitators and staff of our organizations who have been able to recapitulate the answers to the questions that they were mentioning. Their accessibility when distributing them since they can be easily shared through a link and can be completed from any device connected to the Internet, be it a computer, mobile phone or tablet; and the automatic collection of responses that Google stores directly in a spreadsheet, thus facilitating the analysis of the data collected during the investigation.

Target group of the research phase expressed the use of digital devices such as smartphones, computers, tablets every day.

- **Necessity one:** use of digital devices: that shows a significant proportion of participants who use digital devices daily, indicating a high level of engagement with technology in their daily lives. With nearly half of the participants using digital devices every day, it underscores the integral role that technology plays in modern society.
- **Necessity two:** Basic usage implies that the target group may primarily use social media platforms for fundamental functions such as browsing, viewing content, or occasional posting, without extensively utilizing advanced features or engaging in interactive or participatory activities like creating content, networking, or joining online communities. This suggests varying levels of social media literacy among users, with some

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

potentially needing support or guidance to leverage social media platforms more effectively.

- **Necessity three:** digital communication. The Target group of the Research when it comes to most of them are aware of the very basics.The results are about the skills in using social networks such as Facebook, Twitter or Instagram stated regularly, and very basic.
- **Necessity four:** confident. Tailored workshops, tutorials, and educational materials can help seniors to improve their skills and confidence in organizing and managing digital files more effectively.
- **Necessity five:** Daily use for modern life. With nearly a third of participants accessing the internet daily, it underscores the pervasive role of the internet in modern life. Daily internet access has become essential for various activities, including education, and online transactions, but of course communication, information retrieval and entertainment, which is a strong use for most of the respondents as they wanted to make it clear.
- **Necessity six:** Interest in learning and participation of it. Understanding the reasons behind the reluctance to participate in digital literacy programs can inform the development of more effective and inclusive initiatives aimed at promoting digital inclusion and empowering older individuals to leverage technology for personal enrichment, social connectivity, and lifelong learning. Strategies to increase participation may be offered concerning the practical benefits of digital literacy skills for elderly groups, and addressing misconceptions or concerns about technology.
- **Necessity seven:** Use of social media. The participants on the research would like to know better how to use social media and a variety of applications that are available on smartphones for watching live football, online paying, etc. The interest in improving social media skills highlights the importance of online socialization and connectivity for seniors. Participants are interested in staying connected with friends and family, engaging with communities of interest, and access information and entertainment.
- **Necessity eight:** lack of access. When it comes to having access to support resources to improve their digital skills highlights several important considerations such a lack of access to resources specifically designed to help them improve their digital skills and cybersecurity to feel comfortable using it. This could include the actual development of the present Guide.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2. Internet Safety

Through this guide, the opportunity to know more about the needs and challenges that seniors are currently facing in the partner countries, gain deeper knowledge on cybersecurity and know how to apply it among the seniors community to help them become part of the digital transition in a more participative, but above all, in a safe and responsible manner. To achieve so, it is important to place trainers as transmitters of all knowledge, skills and behaviors that promote cybersecurity literacy and ensure the digital safety of the seniors population.

Internet safety and technology use are increasingly relevant issues, especially for seniors. As technology becomes an integral part of our daily lives, it is important that all people, including seniors, are informed and protected.

Digital skills for work and life are one of the top priorities on the European policy agenda. The EU digital skills strategy and related policy initiatives aim to improve digital skills and competencies for digital transformation.

The Digital Competence Framework for Citizenship, also known as DigComp, provides a common language to identify and describe key areas of digital competencies. It is an EU-wide tool to improve the digital competence of citizens, help policy makers to formulate policies that support the development of digital competence and plan education and training initiatives to improve the digital competences of specific groups. This frame of reference will help us make this methodology for seniors. as this is a framework that defines the key components of digital competence in differents areas such as articulating of information needs, locating and retrieve digital data, information, and content, judge the relevance of the source and its content and Identify needs and problems, and resolving conceptual problems and problem situations in digital environments for seniors, including digital tools to innovate processes and products to Keep up-to-date with the digital evolution.

It is crucial to provide education and awareness about internet safety and technology use to seniors. This includes teaching them about the importance of strong passwords, how to recognize and avoid online scams, how to protect their personal information, and how to safely use social media and other online platforms. Seniors should be aware of the importance of protecting their personal information online, such as social security numbers, credit card numbers, and passwords.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2.1. Digital Literacy

Digital literacy refers to the ability to use digital technologies effectively and critically. It involves not only technical knowledge of how to use devices and software, but also the ability to evaluate, analyze and create digital information responsibly. According to Jones (2020) it is an essential competence in contemporary society, and in this specific case for the seniors groups that are digital immigrants, where digital technologies are omnipresent in almost all aspects of daily life, work and education. But for the Seniors it is crucial to facilitate active participation in the digital society, allowing them to engage in public debates, access government services and participate in the digital economy but also to promote social Inclusion that reduces the digital divide, ensuring that everyone, regardless of age, has the same opportunities to access and benefit from digital technologies.

There are several aspects about Digital Literacy that must be considered such us:

Technical Skills, basic knowledge of how to operate devices such as computers, tablets and smartphones, as well as the use of software and applications.

In the context of the digital age, these often relate to the use of technology and software. Common technical skills:

- Programming and Coding: Understanding languages such as Java, HTML, JavaScript.
- System Administration: Managing operating systems (Windows, Linux),
- Technical Writing: Documenting processes, creating user manuals, writing technical reports.
- Basic Computer Skills: Operating a computer, using operating systems, managing files and folders.
- Internet Proficiency: Effective use of search engines, understanding URLs, and navigating websites.
- Communication Tools: Using email, instant messaging, video conferencing tools (Zoom, Skype).

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Social Media Literacy**: Understanding social media platforms, managing privacy settings, creating content.

Integrating Technical Skills and Digital Literacy

Both technical skills and digital literacy are crucial in today's workforce and everyday life. That is why we must Incorporate both technical training and digital literacy programs in the educational curriculum, and encourage continuous learning and professional development through online courses, workshops, and certifications. Establish organizational policies that promote responsible use of technology and continuous upskilling and develop community-based programs to improve digital literacy among various age groups and socio-economic backgrounds. But ensuring access to necessary technology and resources for learning and application of both technical skills and digital literacy.

By combining technical skills with digital literacy, individuals can not only perform specific tasks more effectively but also navigate the digital world responsibly and critically.

Information Comprehension, ability to search, evaluate and manage online information effectively and critically. This includes recognizing reliable sources and detecting false or biased information. Digital information comprehension involves understanding, interpreting, and critically analyzing information from digital sources. As digital media becomes the primary source of information for many, developing these skills is essential for navigating the digital world effectively and responsibly. We must follow the following step for a complete comprehension:

- First step: assessing the credibility and reliability of digital sources, including websites, blogs, and social media. Identifying the authorship, publication date, and intent behind digital content.
- Second step: Evaluating the accuracy and validity of information found online.
- Third step: Recognizing biases, propaganda, and misinformation in digital media.
- Fourth step: Contextual Understanding, which means interpreting digital information within its broader context, including cultural, social, and historical perspectives, understanding how digital content can be influenced by its platform and audience.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

By developing digital information comprehension skills, individuals can navigate the complexities of the digital world, make informed decisions, and fully participate in modern society.

Ethically and responsibly in the digital environment, respecting the rules of conduct and laws related to the use of digital technologies.

In summary, digital literacy is a fundamental competency in the modern world, which not only improves people's ability to use technologies, but also enhances their ability to participate fully and effectively in the digital society. Promoting and improving digital literacy is essential to create a more equitable society.

One of the most serious problems is potential violations of data ethics, (Knight, 2015)[1] Data ethics refers to the use of data in accordance with the wishes of the people whose data is being collected.

Organizations are facing growing pressure to handle consumer data responsibly and transparently. As such, they need to attend to questions of data usage, digital ethics, and privacy technology. Indeed, organizations should not only understand the ethical issues behind data collection and the current regulatory environment. they should proactively implement a plan and practice of data ethics.

The second factor is the increasingly normalized collection of data from online activity. Users generate data when they shop, use search engines, or interact on social media. Data can be collected ethically, as when consumers willingly submit their information to retailers. However, most of the time, third parties without a direct relation to users collect online data through cookies or other sources. This is an ethically questionable practice.

Some laws are on the side of protecting the citizen/consumer. For instance, under the European Union's General Data Protection Regulation (GDPR[2]), companies must gain an individual's explicit consent to collect their data for each purpose data is used for. Data subjects may also withdraw their consent at any time.

Elsewhere in the world, the data privacy regulatory landscape is in a similar state of upheaval. Given disparate privacy laws and historical and cultural differences between countries, a unified approach is unlikely. However, most

[1] Knight, Alison. "Data Analytics and the GDPR: Friends or Foes?" *Data Privacy Review* 8, no. 2 (2015): 123-145.
[2] https://gdpr-info.eu/

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

countries do share some key data protection elements. These include restrictions on cross-border transfers for personal data, notification in the event of a data breach, and individual access and correction rights.

2.2. Online Communication

Effective online communication is essential in today's digital age, whether for personal interactions, professional collaborations, or educational purposes. To understand the processes we must talk about different aspects of digital communication. Online communication refers to the exchange of information and ideas through digital platforms, including emails, instant messaging, video conferencing, social media, and other online channels.

There are different types of Digital Communication:

- Synchronous Communication Real-time interaction, such as video calls, live chats, and webinars.
- Asynchronous Communication Delayed responses, such as emails, forum posts, and recorded videos.

According to the type of communication we focus on criteria Selection:

- The purpose, which determines the purpose of communication that could be casual chat, formal meeting, collaborative project, etc.
- Audience: Consider the preferences and technical capabilities of the audience.
- Evaluate features such as file sharing, video conferencing, screen sharing, and integration with other tools.
- Ensure the platform offers robust security measures to protect sensitive information.

Popular Platforms involving Digital communication:

- Emails: gmail, hotmail
- Instant Messaging: Slack, Microsoft Teams
- Video Conferencing: Zoom, Google Meet
- Collaboration Tools: Trello, Asana
- Social Media: Instagram, Facebook, Whatsapp, Twitter

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

All these platforms are using digital communication, for different purposes, and involve text and images that communicate in different ways to the audience.

Ethics in online communication are crucial as digital platforms become increasingly integral to our personal, professional, and educational interactions.

Online Communication must be based on treating others with respect, regardless of differences in opinions, backgrounds, or beliefs and avoid inflammatory language, personal attacks, or discriminatory remarks, being transparent about your identity and intentions when communicating online. Avoid misleading or deceptive practices, such as using fake identities or spreading misinformation, but also respect the privacy of others and avoid sharing sensitive information without consent.

In conclusion, understanding the different types of online communication, choosing the right platforms, adhering to best practices, and continuously improving your skills, you can communicate more effectively and achieve your personal and professional goals.

2.3. Digital identity and footprints

A. **Digital identity** and footprints refer to the online presence and activities that individuals create as they interact and engage in digital environments. Digital identity is the representation of an individual's identity online. It includes personal information, online behavior, interactions, and activities across various digital platforms.

Components of Digital Identity:

- Personal Information: Name, age, gender, location, and other identifiable details shared online.
- Online Profiles: Social media profiles, professional networking profiles (LinkedIn), and accounts on various websites.
- Online Behavior: Interactions, posts, comments, likes, shares, and contributions across digital platforms.
- Digital Assets: Content created and shared online, such as photos, videos, blogs, and articles.

Digital identity shapes how individuals are perceived online and can influence opportunities in education, employment, and social interactions.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

It is crucial for managing privacy, security, and reputation in the digital realm.

B. **Digital footprint** refers to the trail of data left behind by an individual's online activities. It encompasses all digital interactions and contributions made across the internet.

Types of Digital Footprints:

- Active Footprint: Intentional actions such as social media posts, comments, uploads, and interactions.
- Passive Footprint: Data collected about an individual through online activities, such as browsing history, cookies, and digital transactions.

Characteristics of Footprint:

- Permanence: Information shared online may remain accessible and searchable indefinitely.
- Visibility: Digital footprints can be visible to others, influencing how individuals are perceived online.
- Impact: Footprints can affect reputation, privacy, and opportunities in education, employment, and personal relationships.

In order to manage your footprint you must follow the steps:

- Privacy Settings: Adjust privacy settings on social media and other platforms to control who can view your information.
- Think Before You Share: Consider the potential impact of your posts and contributions before sharing online.
- Monitor and Clean Up: Regularly review your digital footprint, delete outdated or irrelevant content, and manage online profiles.
- Transparency: Be transparent about how personal information is used and shared online
- Respect: Respect others' privacy, intellectual property rights, and digital boundaries.
- Take responsibility for your online actions and digital footprint.

Understanding digital identity and footprints is essential for navigating the digital landscape effectively. You can enhance your online presence, protect your privacy, and build a positive digital reputation understanding first the use and ways to communicate online.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2.4. Privacy and Security

Privacy in digital communication refers to the right of individuals to control the collection, use, and dissemination of their personal information transmitted over digital channels.

Key Concerns in Digital Communication Privacy

- Data Collection: Avoiding unauthorized collection of personal data by third parties.
- Data Sharing: Controlling who has access to personal information and how it is shared.
- Consent: Ensuring individuals give informed consent before their data is collected or used.

Smith (2021) emphasizes the importance of cybersecurity in protecting sensitive data. **Security** in digital communication refers to measures taken to protect the integrity, confidentiality, and availability of data transmitted and stored online.

Key Concerns:

- **Cyberattacks:** Protecting against unauthorized access, malware, phishing, and other cyber threats.malicious activities conducted through digital channels with the intent to compromise computer systems, networks, or devices, and to steal, alter, or destroy data. These attacks can have serious consequences for individuals, businesses, and organizations. Most common are **Malware** which is malicious software designed to infiltrate or damage a computer system without the user's consent. Some examples would be viruses, worms, ransomware, spyware. The impact of the cyber attackers disrupt operations, steal sensitive information, or demand ransom payments. A very popular one nowadays is **Fishing,** a fraudulent attract that attempts to obtain sensitive information (such as usernames, passwords, credit card details) by posing as a trustworthy entity. Examples of fishing very important nowadays are fake emails, websites, or messages that appear legitimate but are designed to deceive users. The impact of it is of course, identity theft, financial loss, unauthorized access to accounts. **Denial-of-Service (DoS)** is another example of cyber attack concerning overwhelming a network, server, or website with a flood of traffic to disrupt normal operations. The consequences are flooding a server with

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

excessive requests or coordinating attacks from multiple sources, producing the direct impact of service disruption, loss of revenue, and reputational damage.

How can we mitigate cyberattacks

- Implement firewalls, antivirus software, and intrusion detection systems to protect against malware and unauthorized access.
- Conduct cybersecurity awareness training to teach employees and individuals how to recognize phishing attempts and other social engineering tactics.
- Regularly update software, operating systems, and applications to patch vulnerabilities and protect against known security threats.
- Use strong, unique and enable multi-factor authentication to add an extra layer of security for accessing accounts and systems.

Data Protection Laws:

Familiarize yourself with data protection regulations such as GDPR[3] (General Data Protection Regulation) in Europe. Ensure compliance with legal requirements regarding data collection, processing, and storage:

In conclusion, privacy and security in digital communication are essential for protecting personal information, maintaining trust, and mitigating risks associated with cyber threats. Staying informed about emerging threats, and prioritizing ethical considerations, individuals and organizations can enhance their digital resilience and safeguard sensitive information effectively.

2.5 Recommendations for responsible habits

Responsible cybersecurity habits are essential to protect personal information and maintain digital safety. Implementing the following recomendation practices the user could significantly enhance the cybersecurity posture and help protect against various cyber threats.

- Use strong, unique Passwords: create complex passwords using a combination of letters (both uppercase and lowercase), numbers, and symbols.
- Avoid using the same password across multiple accounts. Consider using a password manager to keep track of and generate strong passwords.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Keep software updated: regularly update operating systems, applications, and antivirus software to protect against the latest threats. Enable automatic updates when possible.
- Be wary of phishing Scams: do not click on links or open attachments in unsolicited emails or messages. Verify the authenticity of requests for personal information.
- Secure your devices: use antivirus and anti-malware programs. Lock your devices with a password, PIN, or biometric method.
- Use secure connections: avoid using public Wi-Fi for sensitive transactions; if necessary, use a virtual private network (VPN). Ensure websites are secure (look for "https://" in the URL) before entering personal information.
- Limit sharing of personal information: be cautious about the amount and type of personal information shared online. Review privacy settings on social media platforms and adjust them for maximum security.

3 Practical Activities:

This section contains 15 practical activities divided into the 4 main topics of the guide: Digital Literacy, Digital Communication, Digital identity, Privacy and security.

Each activity is following the structure below: Name, Objective, Needs, Material needed and Instructions to perform ir, if needed, we add infographics or pictures to help the user to perform it or examples in case it is required.

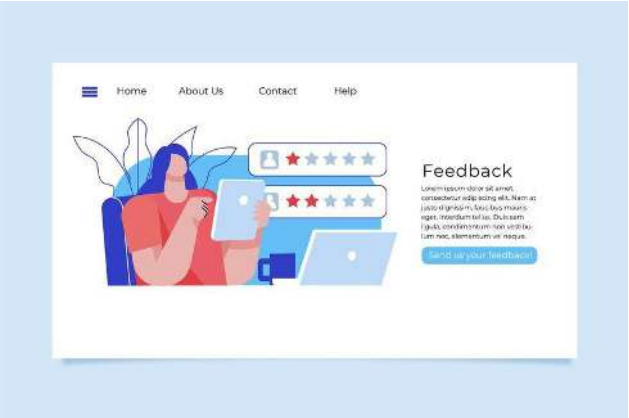
The images used in this section come from screenshots of the page cited for the activity, (Facebook, Google, etc) and images created with AI through freepik.es used legally as free images.

The order of activities can be altered according to your convenience.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

A: Digital Literacy

1: Activity: “Evaluating Online Sources”

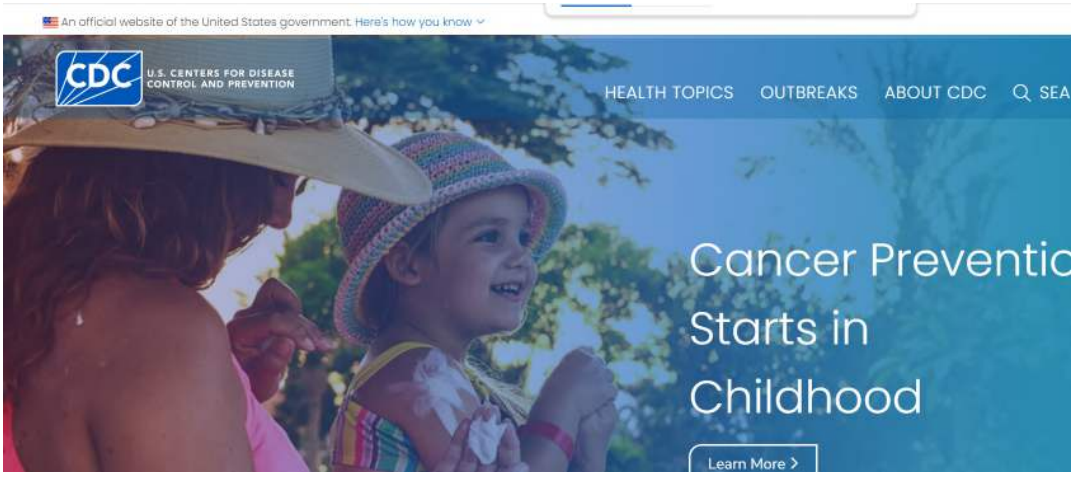


The objective of this activity is to learn to assess the credibility of online sources. Based on it, the Needs are related to the Knowledge of researching online with veracity. To perform this activity the Material needed will be a Computer or tablet with Internet access. This activity takes 40 minutes and it should be performed in pairs.

The activity consists of a list of websites provided for you to evaluate each site's reliability, accuracy, and bias. Criteria may include checking the author’s credentials, the website’s domain, and cross-referencing information with trusted sources**.** First you will see an example.

Example: www.cdc.gov

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



The following are examples of the information you should search for the activity websites:

- Author's Credentials: Articles and information are typically written by experts in public health, epidemiology, and medical research.
- Website's Domain: .gov (official government website, highly reliable).
- Cross-Referencing Information: The CDC is a primary source for public health information and widely referenced by other reputable sources.
- Bias and Objectivity: Generally objective, focused on evidence-based information, though some political influence may exist as it is a government agency.

Now, Please check the webpages to evaluate in pairs:

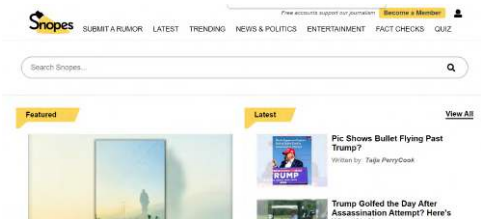
www.naturalnews.com

www.nytimes.com

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.theonion.com

www.snopes.com



www.infowars.com

The next step is the evaluation criteria: the following list of quality criteria has beencreated for you as a guidelines to be able to evaluate as much aspects as you can from the different web pages suggested:

- Check the author's background: Look for information about the author's qualifications, expertise, and other articles they have written.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Authors with relevant degrees, professional experience, and a history of accurate reporting are more credible.
- Government and educational domains: Sites ending in .gov, .edu, and reputable organizations' .org are generally reliable.
- Commercial domains: Sites with .com and .net require more scrutiny as they can be owned by anyone.
- Check if other reputable sites report the same information.
- Fact-checking sites: Use sites like Snopes, FactCheck.org, or PolitiFact to verify claims.
- Identify bias: Analyze the language used (is it neutral or emotional?), the range of perspectives presented, and the site's funding sources.
- Evaluate whether the site provides balanced viewpoints or pushes a specific agenda.

After discussing and checking all the websites, make your decisions according to the criteria, take notes because in activity 2, 4 and 5 you will need that first research on the websites mentioned before.

2: Activity: "Advanced Search Techniques"

The objective of this activity is to improve search engine skills. According to that, the needs are advanced search operators (e.g., quotes for exact phrases, minus signs to exclude terms) and specific search tools like Google Scholar for academic articles. To perform this activity the material needed is a computer or tablet with internet connection.

Instructions: Use advanced search operators and Google Scholar to find academic articles on the impacts of climate change on biodiversity or in other topics you may be interested in. This Activity takes 40 minutes.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The First step will be Formulate a specific research question or topic related to climate change and biodiversity. Example: "How does climate change affect biodiversity in tropical rainforests?"

Be aware of the following tips:

- Use Advanced Search Operators: Quotes (" "): Search for exact phrases.

  Example: "climate change impacts on biodiversity"

- Minus Sign (-): Exclude terms to narrow down results.

  Example: climate change impacts on biodiversity -marine

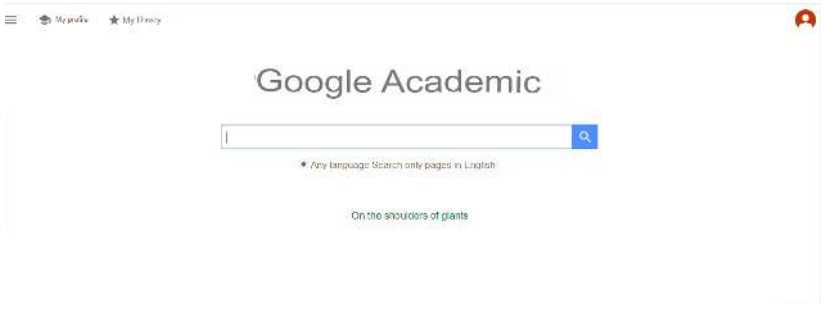
- Site: Limit your search to specific domains or sites.

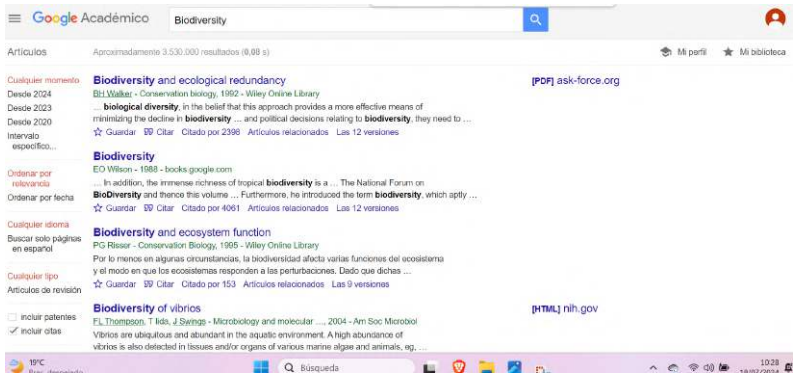
  Example: site:scholar.google.com climate change impacts on biodiversity

- Filetype: If needed, specify the file type for documents.

  Example: climate change impacts on biodiversity filetype:pdf

Now is time to perform the Search, by using Google Scholar (scholar.google.com) to conduct your research.





Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Please, enter your refined search query using the advanced operators mentioned before. Then review the search results and evaluate the relevance of each article based on titles, abstracts, and keywords. Check the citations and number of times the article has been referenced (if available) to gauge its impact and relevance. Click on the links to access full-text articles directly from Google Scholar or through your institution's library access. Read the selected articles carefully, focusing on the methodology, findings, and conclusions related to climate change impacts on biodiversity. After finishing the steps, summarize key points and insights gained from each article. Please, keep this info available as you will need it for the next activity 3.

Here you can find a table with the evaluation aspects and one example:

Link	Title	Abstract	Keywords
EXAMPLE https://www.science.org/doi/abs/10.1126/science.1131758	How Does Climate Change Affect Biodiversity?	Climate change is a critical driver of biodiversity loss, affecting ecosystems and species worldwide. This article reviews the multifaceted impacts of climate change on biodiversity, with a focus on tropical rainforests.	Climate Change Biodiversity Tropical Rainforests Temperature Increase Precipitation Patterns Species Distribution Habitat Degradation Extinction Risk Conservation Efforts Ecosystem Disruption Diseases and Pests Climate Adaptation

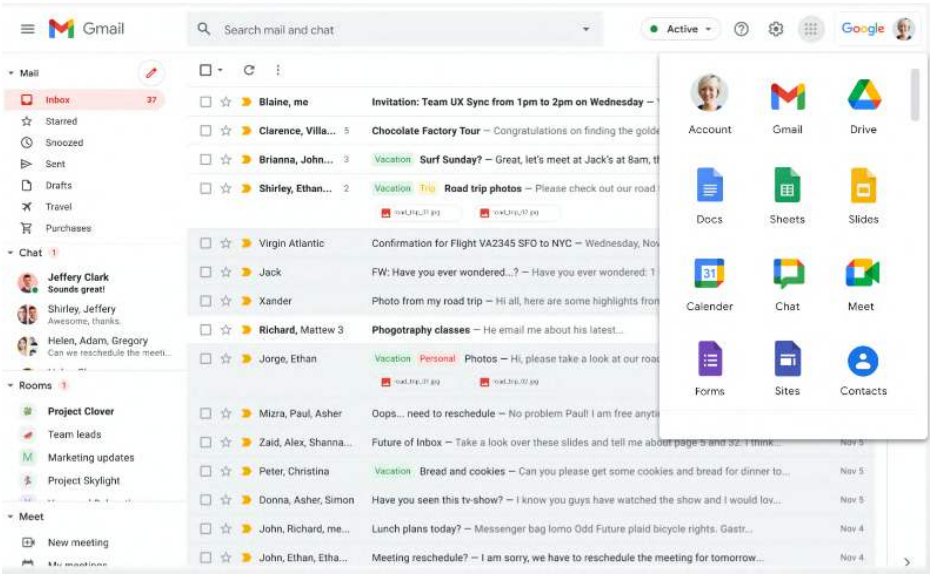
3: Activity: Virtual Collaboration Project

The Objective of this activity is to make use of digital tools for collaboration, and the Needs covered are tools for collaboration such as Google docs. The

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

purpose for the activity is to evaluate and practice your ability to communicate, share resources, and manage tasks effectively.To perform this activity the material needed are activities 1, and 2 in this section completed and, computer, and internet connection.

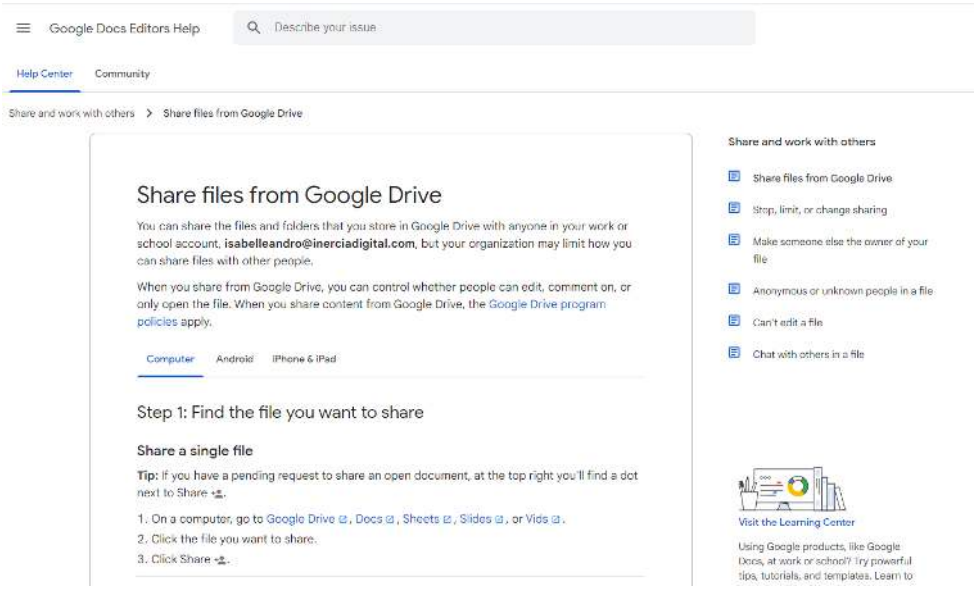
Now, it is time to perform the activity, it will take 40 minutes. Use Google Docs to collaborate with other peers or colleagues. Open your gmail account, and click right up corner to find google docs. There are many ways to open it but let's use this simple way:



The following step would be that you create a new doc. All individually in separate computers can add info at the same time, please use the research and notes from Activity 1 and 2.

You will see how you create the same document without the necessity of being together in the same room with the same computer. You can share the doc so that different people can add information at the same time. The following pictures shows the instructions to perform it properly.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



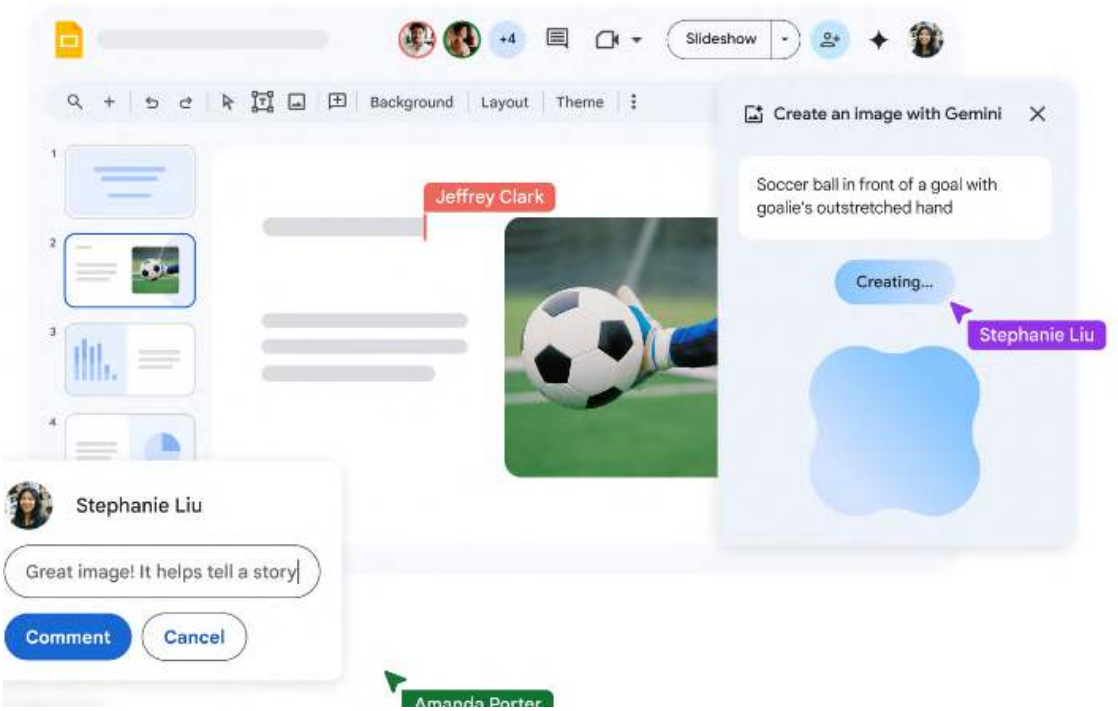
4: Activity: Multimedia Presentation

The objective of this activity is to develop skills in creating digital presentations. It covers *Digital Literacy and Digital Communication. The* needs covered is a topic to present using Google Slides, and the material needed will be a computer with internet connection.This activity takes more than 1 hour to perform it correctly.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Digital presentation can also be performed with the use of an AI plugin like Slide AI that can enhance your presentation by automating design elements, generating content, and providing smart recommendations. Artificial Intelligence used can help to generate bullet points or key facts about your presentation.

Now is time to practice. Use the previous topic activity 1, 2 and 3 to present using Google slides. You should incorporate text, images, videos, and interactive elements to create a compelling presentation. The following picture will help to start. When you can open google options, look for slides, click and it will be open to start the creation:

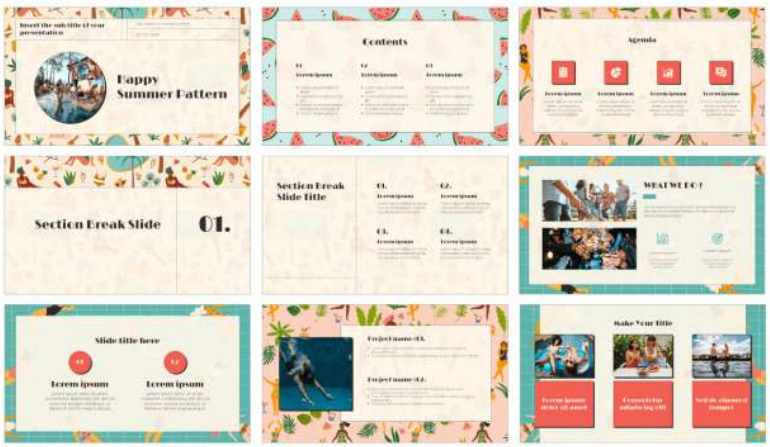


Compile your findings into a report or presentation summarizing the current understanding of climate change impacts on biodiversity based on the academic literature. You can change the image, include, delete, duplicate, etc.

Please you must include references to the articles you used and discuss any conflicting viewpoints or gaps in research.

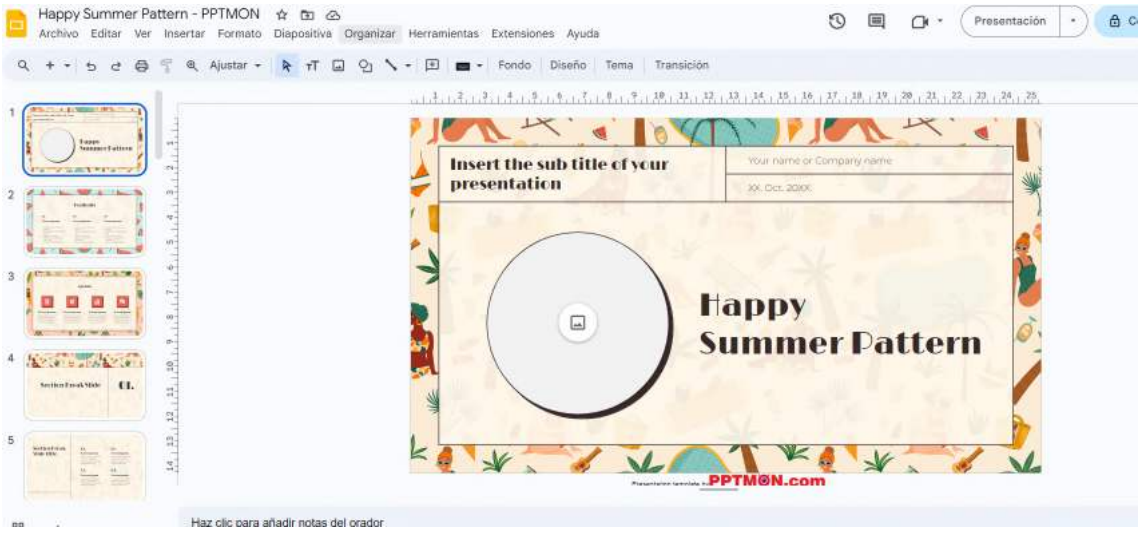
Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The Maximum is 9 slides including front, index at the beginning and References, greetings and contact details at the end. The following picture is and example, some templates are free, find here the topic ”Happy summer”



Use the example, find here the emplate:

https://docs.google.com/presentation/d/1_7IeG7vQNruGATabXvQm-4WqIAIlV8SX1KKWId8DTDY/template/preview

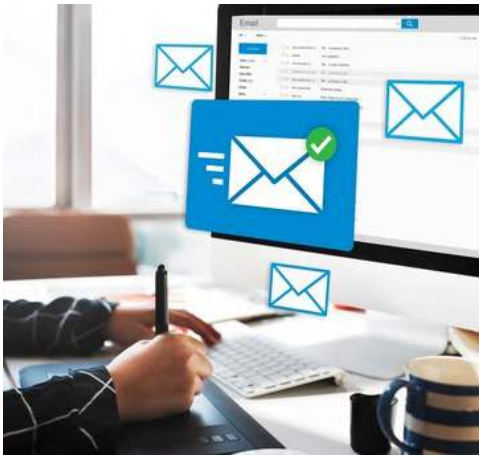


Now is the time to prepare yourselves in groups of two and Present it! Good luck!

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

B: Digital Communication

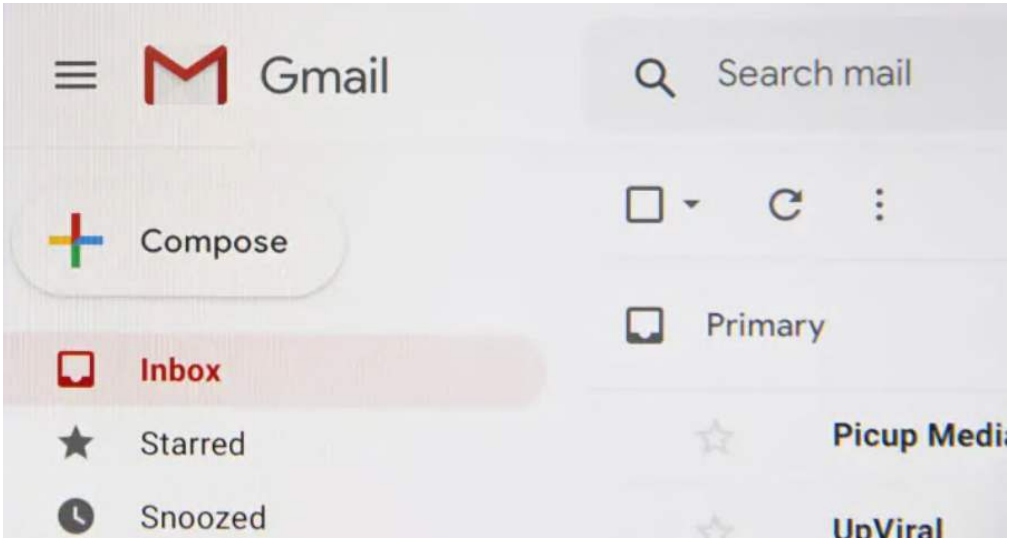
1: Activity: "Request a Place"



The objective of the following activity is to learn how to write a formal email. The needs covered are, formal/informal digital communication to request a place for one activity. According to the needs, the material needed to perform the activity will be computers or tablets and mobile devices, with Internet access. Active email account for each participant. This activity will take 20 minutes to perform.

Now is time to practice, first you have a suggestion with some details. The basic structure of a formal email would be to include greetings, body of the message and farewells. Then add the Subject with a brief and clear line text indicating the purpose of the email. Greeting Formal, such as "Dear [Name]." After it you can write the body, clear and direct information about the request. To end the email farewell, be courteous, such as "Sincerely" or "Best regards." Finally your signature with full name and contact information.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Now your turn. Here is an example:

Subject: Request for Place in Dance Class

Dear [Name of Instructor or Person Responsible],

I am writing to you to request a place in the dance class that will be taught on [days of the week] at [time] in [location].

I am passionate about dance and would love the opportunity to join your class to improve my skills and enjoy the atmosphere.

I would appreciate it if you could inform me about availability and the steps to follow to register.

I await your response.

Sincerely,

[Full name]

[Telephone contact]

[Email]

Individual Writing, please write their own email using the guide provided.

After finishing the group will review and Feedback.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

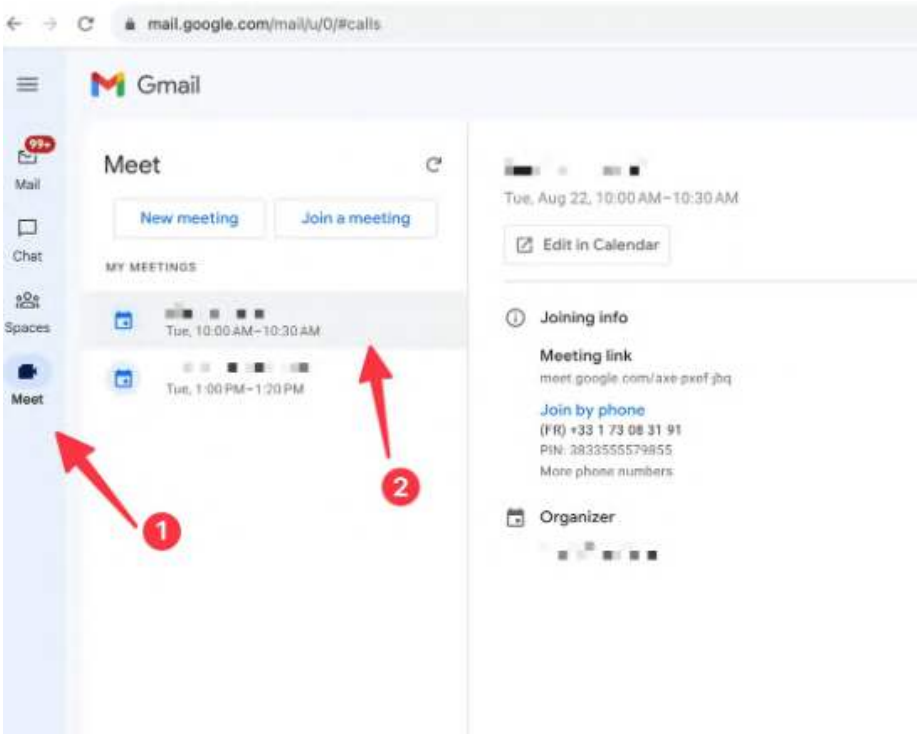
Participants exchange emails to review them and give constructive feedback. Discuss as a group the strengths and areas for improvement. Send the Mail to the participants and send the real email to the person in charge of the dance class, or a test email to an instructor.

2: Activity: "Shall we have a meeting?"

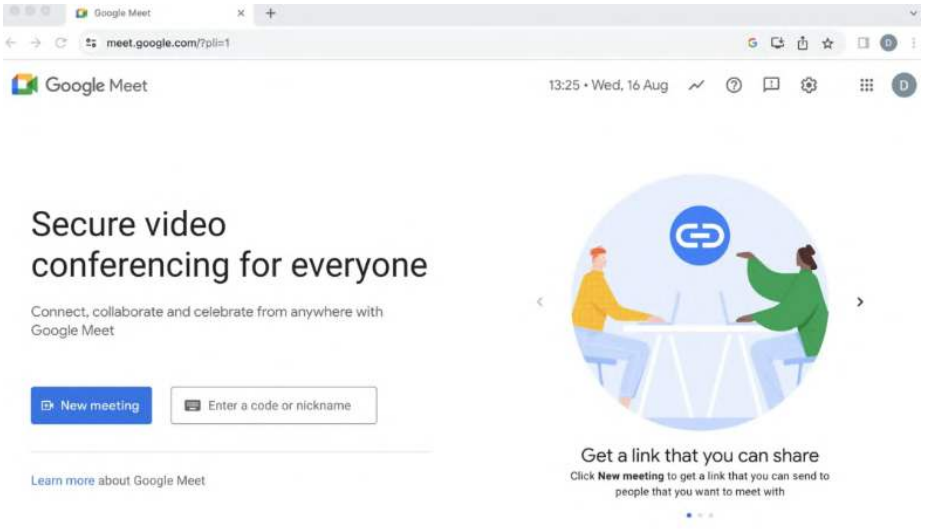
The objective of the activity is how to create, schedule, and join an online session and familiarize them with its basic features. We will use the most popular one although there are many options: Google meet. The needs covered are becoming comfortable with creating and managing Google Meet sessions, enabling them to stay connected and engaged in the digital world to communicate online. The material needed is Computers or tablets with internet access and Google accounts for each participant.

Now is time to practice, this activity will take 30 minutes. Navigate to Gmail and click on the 'Meet' icon located on the left panel. Select the meeting you wish to join and click on 'Join now'.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

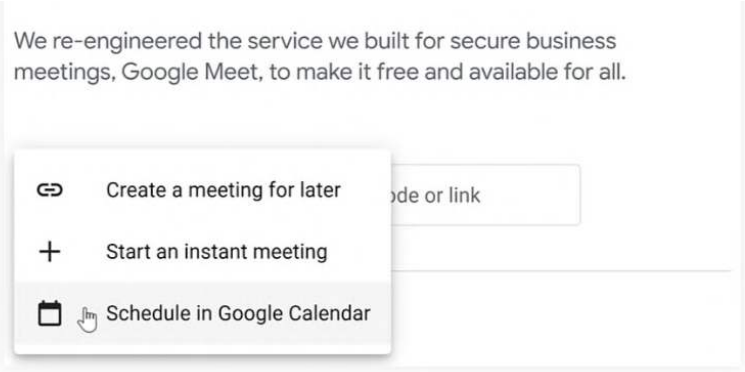


Another option is create it and be the host, open a web browser and go to Google Meet.

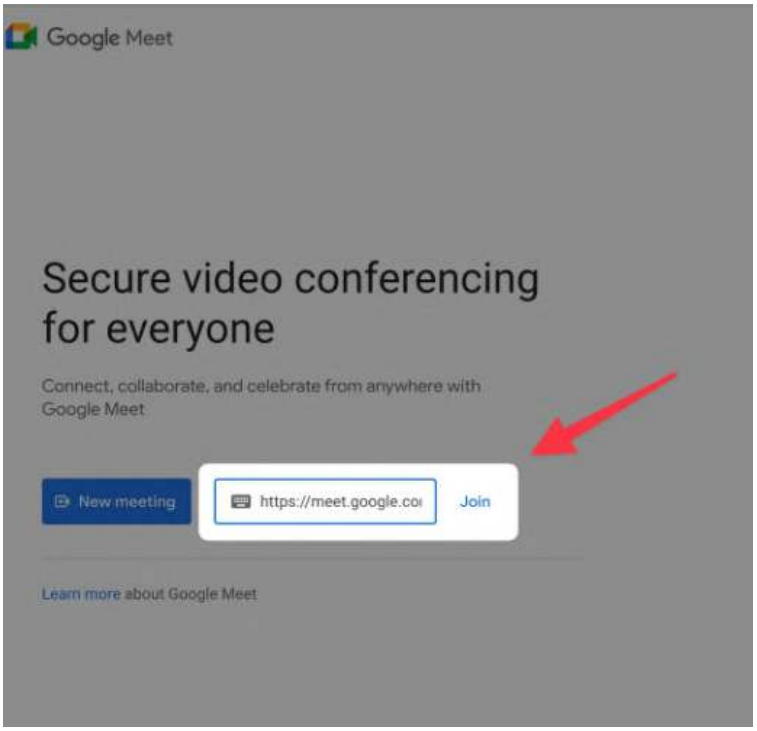


Click on "New meeting" and select "Create a meeting for later" or "Start an instant meeting" o the option of the Google calendar.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



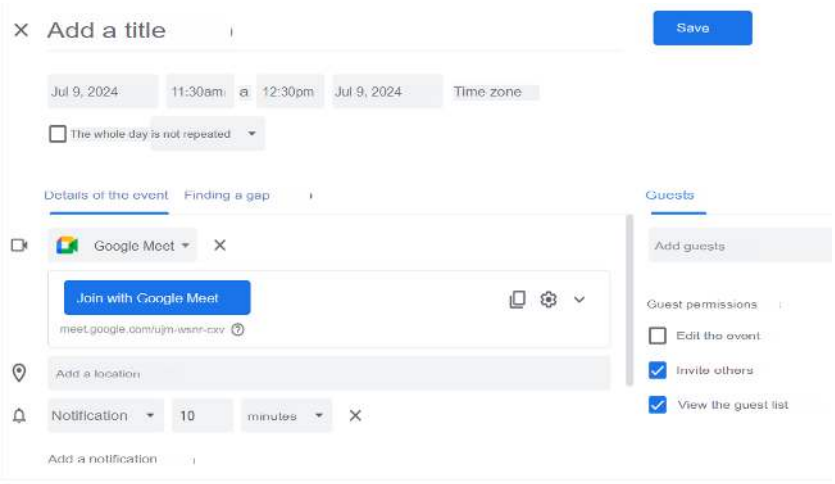
(If you have the link provided then copy the link directly. Copy the meeting link provided.)



To join a Google Meet without a Google Account, the participant must receive a conference link or code from the meeting host. It's important to note that these users cannot initiate a meeting themselves. Also, they can only join a meeting using the desktop version of Google Meet, as the mobile application is not accessible without a Google Account.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Now is time to create your own Google Meet sessions by following the steps demonstrated.



Scheduling a Google Meet: Open Google meet. Participants schedule a Google Meet session, and invite 2 more partners from the class. Joining a Google Meet Session . Check audio and video settings before joining. Ensure understanding how to mute/unmute their microphone and turn their camera on/off. The chat function, screen sharing, and changing the layout.

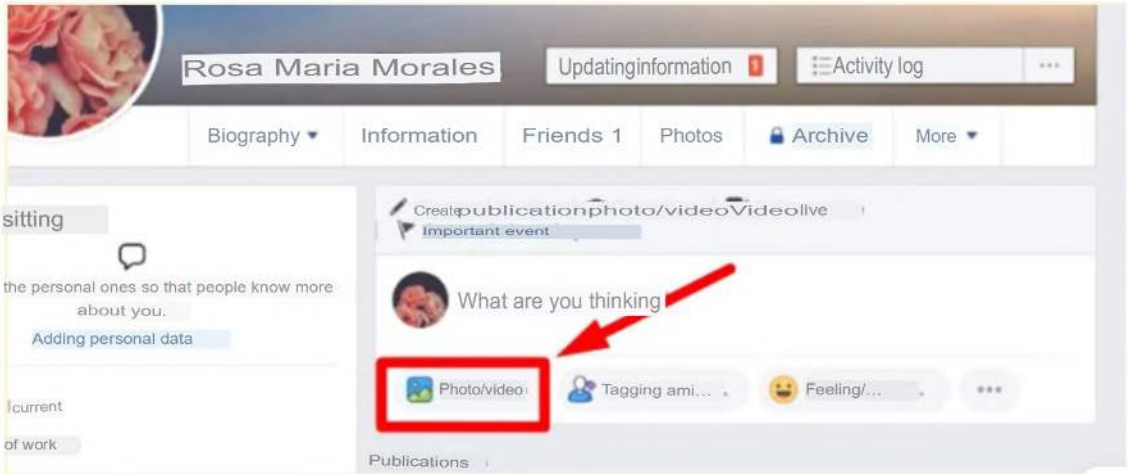
In groups of three practice online meetings together. Well Done!

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3. Activity: “Sharing my trip”

The order of activities can be altered according to your convenience. In that case, we recommend you to perform the “Profile Creation" Activity 2, from next section D: Digital Identity and after you create your profile (if you don't have any already) then you should come back to this activity.

The objective of this activity is to learn how we communicate on Social Media. To perform the activity the need covered is the ability to share information on social media with security, and to be able to perform if the material needed will be internet connection, laptop or tablet, and facebook profile. To make a post with a photo, it is possible to edit the image from Facebook before publishing it, as well as tag a person and add other elements.



Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

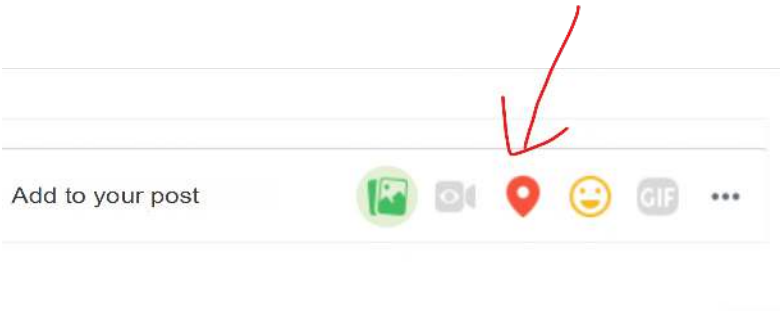
To create a photo post on Facebook, you will need to follow these steps, this activity will take 30 minutes.

First step is to Login Facebook. In the space that says “What are you thinking?” Click Photo/Video. Select the photo you want to upload to the publication. (be aware of pictures that show only people that already gave you consent to post it. And try not to post children's faces). In any case you can practice with a picture you took on your last trip with no people involved. If you want to edit the photo, click on the small icon with the brush that says: Edit photo. The following pictures will help you.

From the editing window it is possible to: add a filter, label, add text, crop the photo and add emojis. After editing it, click Save. To add an emotion or activity related to the photo, click Feeling/activity.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Choose the location related to the publication that is made. For example, if you put a photo about your trip you can choose the option location and add the place.



Click SHARE!!!!! your post is done! Congratulations!

C: Digital identity

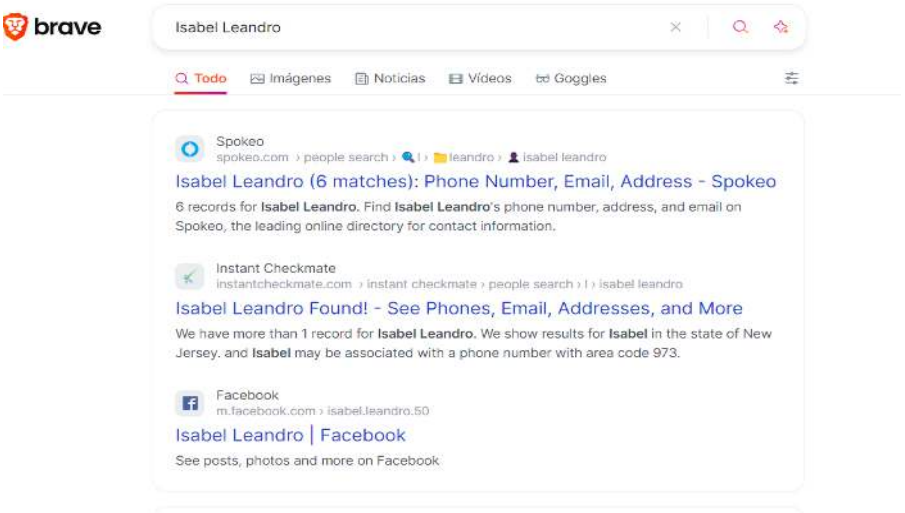
1. Activity: "Map Your Digital Footprint"

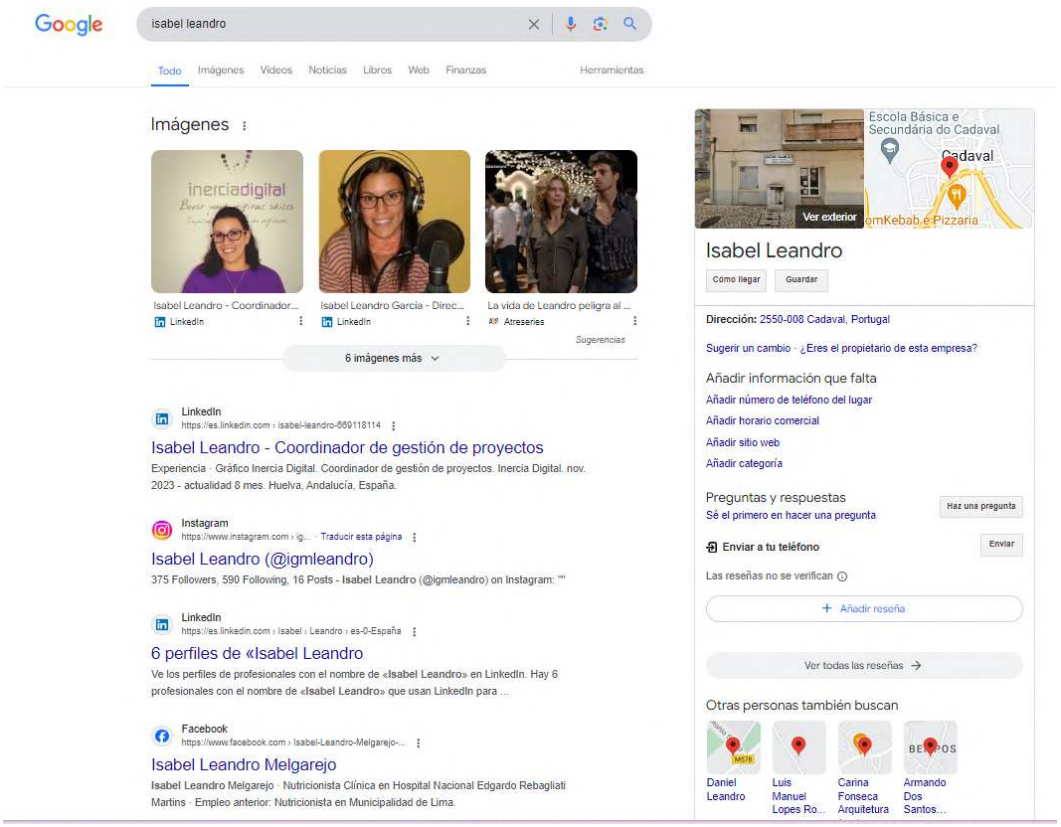
The objective of the following activity is to understand what information is publicly available about oneself online. The need covered is the awareness of one's digital footprint and the importance of protecting personal information.To perform it the materials needed will be computers/tablets with internet access, projector/screen, paper, and pens.

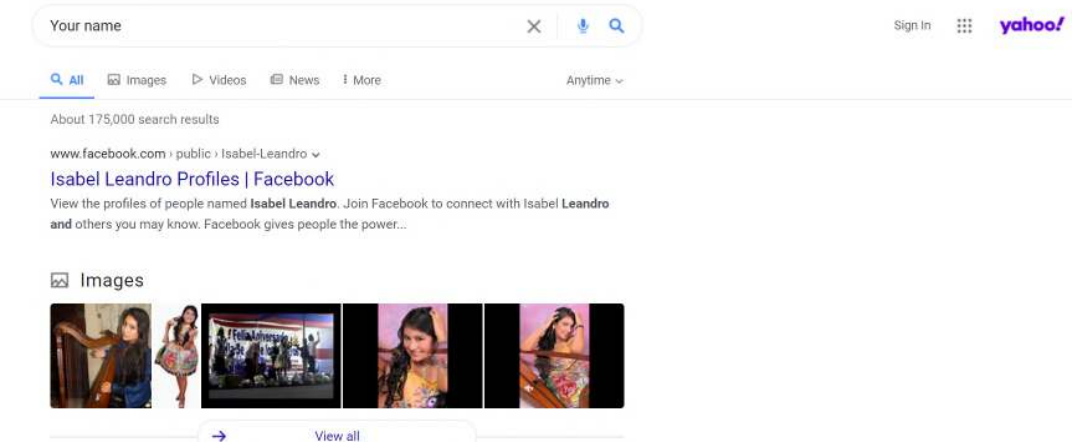
Now is time to practice, the activity will take 20 minutes. Whenever you use the Internet, you leave a trail of information known as your digital footprint. A digital footprint grows in many ways: for example, when you post on social media, subscribe to a newsletter, leave an online review, or shop online.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Have learners search for their names on various search engines. Use search engines to check your footprint. Enter your name in the search engines. Include your first and last name and any variations in spelling. If you changed your name, search for both your current and previous names. We can use: Brave, Google, Yahoo, The following figures are examples with the name: Isabel leandro.







Note what personal information you find. Reviewing search results will give you an idea of what information about you is publicly available. If any of the results show you in a negative light, you can contact the site administrator to see if they can remove it. Setting up Google Alerts (or any other engine you normally use) is one way to keep an eye on your name. Review your social media privacy settings and make sure they are at a level you are comfortable with. Delete inactive accounts, to minimize your exposure to potential data breaches. Use strong passwords and make sure you use different, strong passwords for each account. Be aware of your online actions. It is important to be aware of your online actions and how they can affect your digital footprint.

Discuss in small groups. How many times does your real name appear and is related to what? Are there any pages you are not related to?

Discuss how this information could be used by others and the importance of managing one's digital footprint. The digital footprint is the trail of data you leave when you use the Internet. It is important to be aware of the importance of your digital footprint and how it is used, and take steps to protect your privacy and security online.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2. Activity: "Profile Creation"

The Objective of this activity is to develop an online presence (profile) . The needs covered are to evaluate the completeness and coherence of the created profiles. The material needed will be a computer or tablet, with Internet Connection.

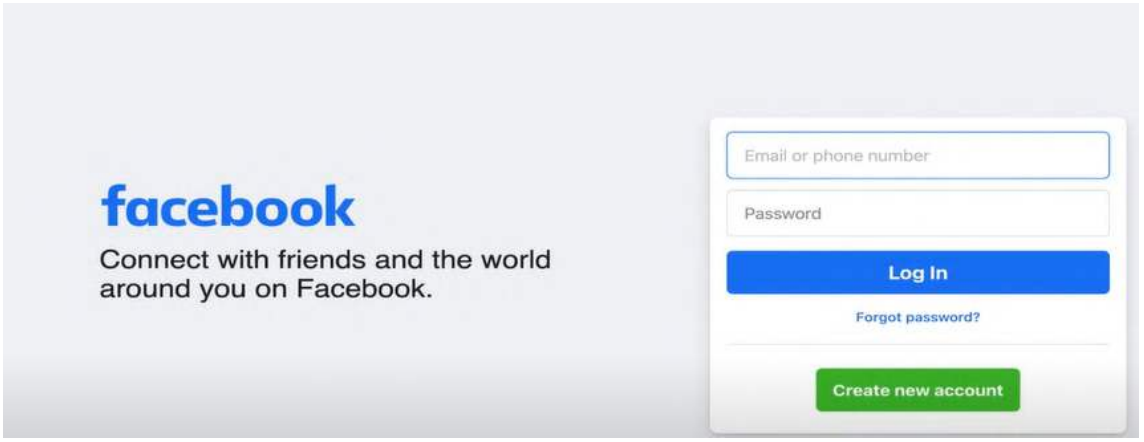
Now is time to practice, this activity will take 30 minutes. Create or update their Facebook profiles or equivalent profiles. This includes writing a compelling headline, summary, listing work experiences, education, background, skills, and obtaining recommendations. Then Follow few pages you are interested in. Complete as much as possible your profile, and prepare the pictures you want to upload. Here are some tips such as using a strong password. Don,t share. Be careful with the information you share. You can use "Facebook support" for any questions.

Find here a very useful link that could help to evaluate password security and it can be useful for you in that activity process:

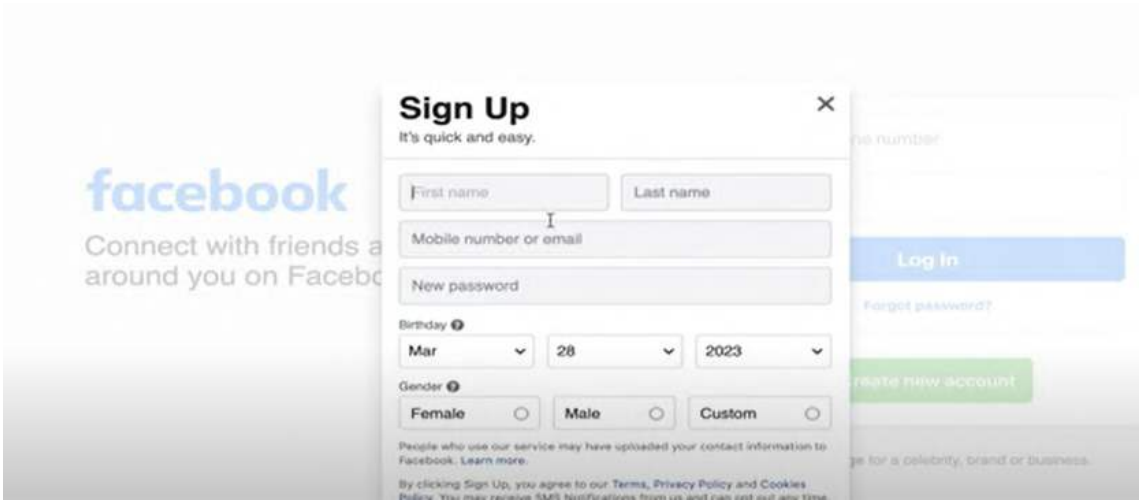
https://password.kaspersky.com/es/

The following pictures will help you to find the information to perform the activity. First Open facebook page and click on create an account.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

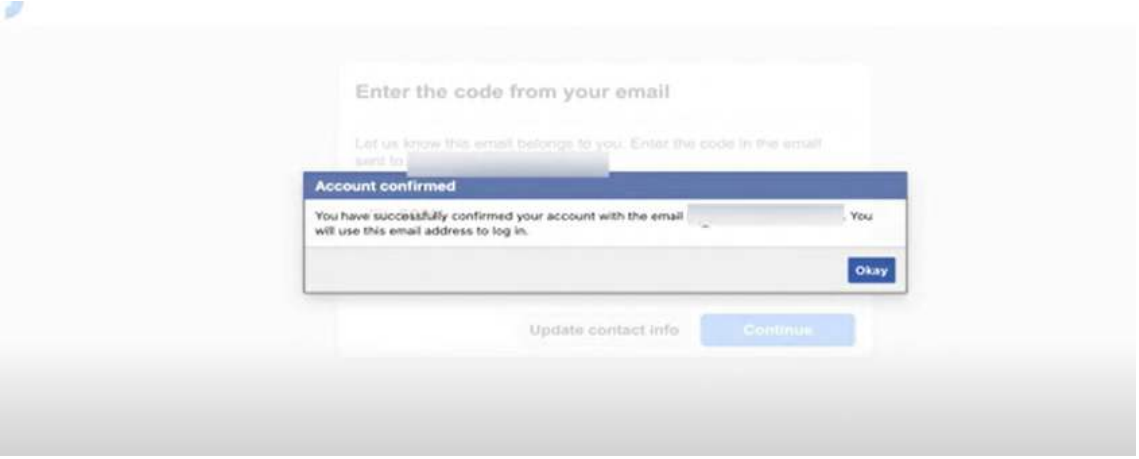


Then complete the information below:

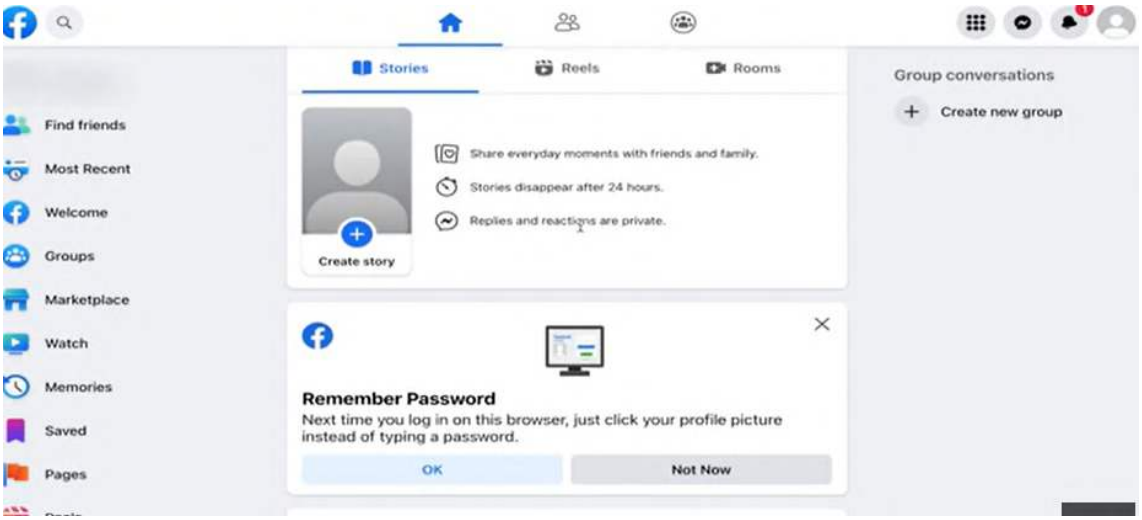


You will receive on your e-mail account a code that you need to introduce.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Once it is created and open, you can start uploading the profile pictures, and add your information on different sections, such as interests, background, etc.



Share it with partners and try to find new friends!

3. Activity 3: Analysis Case Study

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The objective of this activity is to learn from real-world examples of digital identity management to understand effective strategies and common pitfalls. The needs covered are for the Participants that will analyze case studies of public figures or companies that have successfully managed or damaged their digital identities. This analysis will help participants identify key strategies, understand the impact of digital identity on reputation, and apply these lessons to their own digital identity management. To perform the activity the material needed will be computer and Internet access. The activity will take 25 minutes to perform it.

Now is time to practice. A variety of case studies that highlight both successful and unsuccessful digital identity management. Here you can find a positive case that shows Taylor Swift's strategic use of social media, NASA's engagement on Twitter, or a company's successful crisis management like Tylenol's response to tampering in the 1980s.

https://press.farm/taylor-swifts-social-media-strategy-for-success/

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

On the other hand, a negative Case, Elon Musk's controversial tweets, United Airlines' response to passenger removal incidents, or a company's mishandling of a data breach.

https://www.nytimes.com/2017/04/14/business/united-airlines-passenger-doctor.html

After reading the articles and discussing it, it is time to Research and Analysis. Into small groups and assign each group a case study. Check with your group the background, overview of the individual or company and their digital presence before the incident. Check the incident and create a detailed

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

description of the event that impacted their digital identity. Analyze the steps taken to manage the situation, including social media posts, public statements, and other digital communications. After it you can make an evaluation of the results of these actions on their digital identity and reputation.

We all make a class discussion to compare different strategies and outcomes, and discuss how these lessons can be applied to their own digital identities.

D: Privacy and Security

1. Activity: Password Challenge

The objective of the following activity is to create strong, memorable passwords and understand the importance of password security. The needs covered are the ability to create and manage strong passwords to enhance online security. To perform the activity the materials Needed will be computers/tablets, projector/screen, paper, and pens.This activity will take 20 minutes.

What makes a password strong? Tips include numbers, capital letters, symbols and try to not use some details related to you. To generate a strong password it is important to balance security with ease of remembering it.

Now we show you two different methods, method 1, use an easy-to-remember phrase. Choose a meaningful phrase. It can be a phrase from a favorite song, a popular saying, or something personal that is easy to remember. Example: "In April there are a thousand flowers"Also shorten the sentence, such that we take the first letter of each word and combine them. Example: "Eafm"

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Add numbers and symbols: Add some numbers and symbols to increase security. Example: "Eafm2024#"

The second Method 2 is to use random words. Select random words and choose four words that are unrelated but easy to remember. Example: "cat moon river table" Or combine words, put the words together and add a number and a symbol. Example: "GatoLunaRioTable!9"

Now find additional tips, and be sure to use a mix of uppercase and lowercase letters. Avoid personal information. Do not use personal information such as dates of birth, family names or addresses. Use a password manager: If the elderly person has difficulty remembering multiple passwords, a password manager can be a good solution.

Examples of strong passwords: (remember that you can use again the link we to create the passwords with security checking:

https://password.kaspersky.com/es/

"C0nchaC4r4col!23"

"P3rro&Gat0_456"

"Happy*Birthday2024"

These passwords are relatively easy to remember but sufficiently secure.

Create your own strong passwords using a mix of letters, numbers, and symbols. Discuss best practices for password management.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2. Activity: "Spot the Phish"

The objective of the activity is to recognize phishing emails and understand how to respond to them. The Needs covered are to enhance the ability to recognize phishing scams and take appropriate action. To perform the activity, the materials needed are examples of phishing emails. This activity will take 30 minutes to complete.

In phishing emails, cyber criminals often ask for the following information, date of birth, social security number, phone number, home address, credit card details, login details, Password (or other information needed to reset your password), also clicking an attachment, enabling macros in a Word document, updating a password, responding to a social media friend or contact request, connecting to a new Wi-Fi hot spot.

Now is time to practice, please check the following examples:

Example 1: Bank Alert

Subject: Urgent: Account Verification Required

Dear Customer,

We have detected unusual activity in your account and need you to verify your identity to ensure the safety of your funds. Please click the link below to verify your account information:

[Verify Your Account] http://santanderbank.com/rstcnn

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Failure to verify within 24 hours will result in the suspension of your account.

Thank you for your prompt attention to this matter.

Sincerely,Bank Security Team

Example 2: Invoice from a Known Company

Subject: Invoice Payment Due

Dear [Your Name],

Your invoice for the month of July is attached. Please ensure payment is made by the due date to avoid any late fees.

[Download Invoice](http://PODIUM ENGINEERING LIMITED company.com/invoice)

Thank you-

Best regards,

PODIUM ENGINEERING LIMITED Billing Department

Example 2: Social Media Notification

Subject: New Login Attempt from Device

Hi [Your Name],

We detected a login attempt from an unfamiliar device. If this was not you, please secure your account by clicking the link below and updating your security settings:

[Secure Your Account](http://facenonbooksocialmedia.com/security)

Thank you for keeping your account safe.

Best,

Facenonbook Support Team

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Now please work in pairs to identify phishing indicators. Discuss and detect findings as a group. Find the following information in the previous emails:

- Sense of urgency
- Suspicious link
- Generic greeting "Dear Customer"
- Threats of account suspension
- Unsolicited attachment or link
- Generic or misspelled company name
- Unusual or unfamiliar invoice details
- Unsolicited security alert
- Suspicious link
- Generic greeting
- Poor grammar or spelling errors
- Reflection to share tips on how to handle suspicious emails.

3. Activity: "Safe or Unsafe"

The objective is to understand and practice safe browsing habits. The need covered is the Knowledge of safe browsing practices to protect personal information online. To perform the activity, the materials needed are computers/tablets, projector/screen, paper, and pens. This activity will take 25 minutes to complete.

Configure your browser safely: enable privacy and security on your browser, and avoid the installation of untrustworthy extensions.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Check and follow the following steps: We will divide the group into two groups. 1 CHROME and 2 MOZILLA.

Group 1 will use Google Chrome.

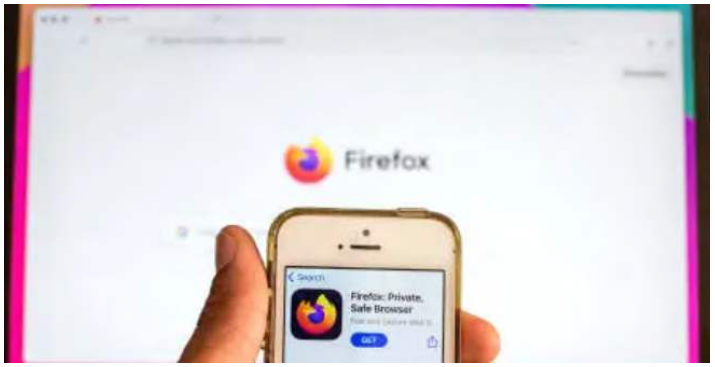
Update Chrome: Go to Menu (three dots) > Help > About Google Chrome and ensure you're using the latest version.

Enable Safe Browsing: Go to Settings > Privacy and security > Security. Choose Enhanced protection under Safe Browsing. Block Third-Party Cookies: Go to Settings > Privacy and security > Cookies and other site data. Select Block third-party cookies.

Enable Do Not Track: Go to Settings > Privacy and security > Cookies and other site data. Toggle on Send a "Do Not Track" request with your browsing traffic. Clear Browsing Data: Go to Settings > Privacy and security > Clear browsing data. Choose what to clear (e.g., browsing history, cookies, cached images) and select Clear data.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Group 2 we will use Mozilla Firefox



Update Firefox: Go to Menu (three lines) > Help > About Firefox to check for updates. Enable Enhanced Tracking Protection: Go to Menu (three lines) > Settings > Privacy & Security. Under Enhanced Tracking Protection, select Strict. Block Cookies: Go to Settings > Privacy & Security > Cookies and Site Data. Select Manage Exceptions to block specific cookies or Delete cookies and site data when Firefox is closed. Clear Browsing Data: Go to Settings > Privacy & Security > Cookies and Site Data.

4. Activity: Privacy Check-Up

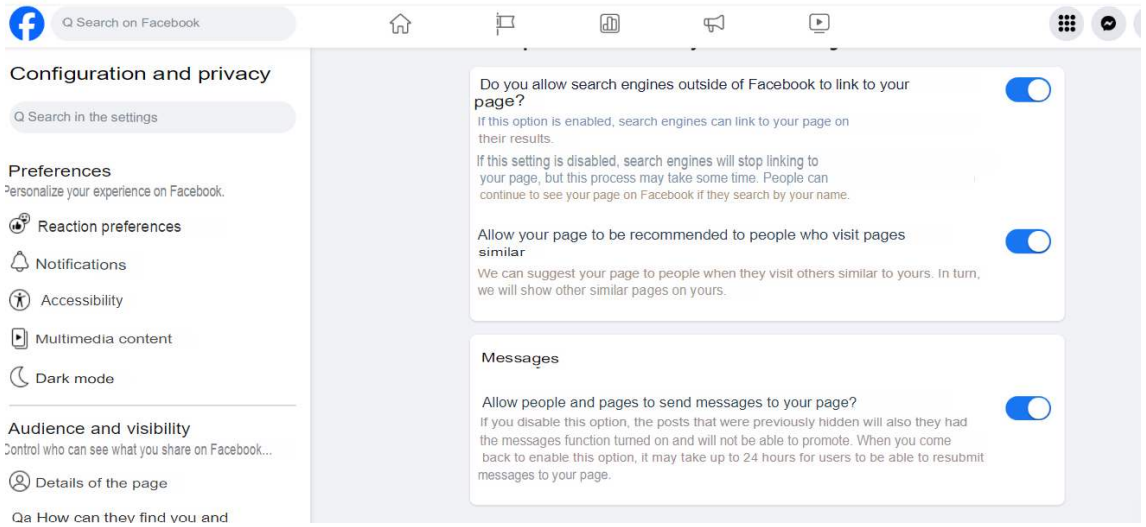
The objective is to understand and manage privacy settings on social media platforms. The need covered is the ability to effectively manage privacy settings on social media platforms. To perform it the materials needed areComputers/tablets with internet access. This activity will take approximately 25 minutes.

The importance of privacy settings on social media. Check preferences is always the first step using social media, nowadays with the introduction of AI

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

you must check and refuse or choose your security and privacy preferences. This step is crucial for the future use of your profiles on Social Media platforms.

The privacy settings of popular social media platforms, we will divide the group into two groups: 1 Facebook 2 Instagram). Adjust your settings to enhance privacy.



Before you start, be aware that Meta, the parent company of Facebook and Instagram, has announced its intention to use user data to train its artificial intelligence (AI) systems starting June 26, 2024. Below are the changes and Steps to prevent your data from being used for this purpose. Meta will use all posts, comments, audios and photos shared on Facebook and Instagram, except private messages, to train its AI systems.

Process to reject: you must: Enter from your computer and click on the profile photo. Go to “Settings and privacy” and select “Settings”. Select “Privacy Policy” and then “Right to Object”. Fill out a small form specifying that you do not want your data to be used to train Meta's AI.

Group 1: Facebook

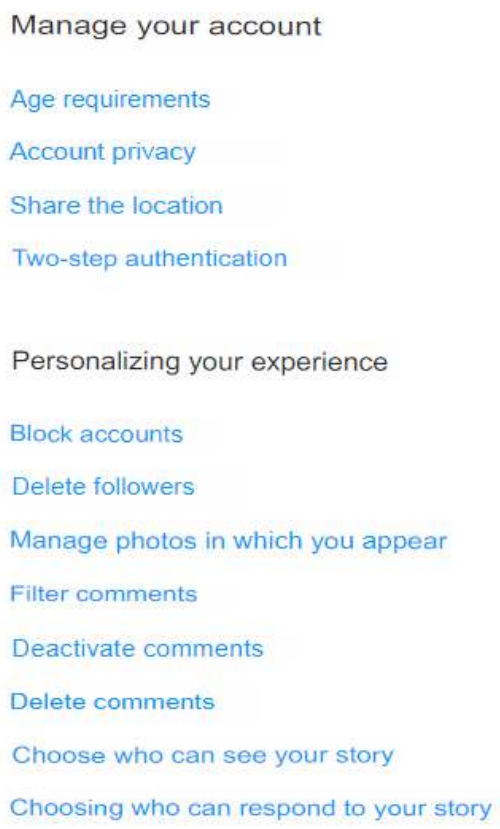
Access Privacy Settings: Click the downward arrow at the top-right corner and select Settings & Privacy > Settings. Privacy Checkup: Go to Settings & Privacy > Privacy Checkup.

Follow the steps to review and adjust your settings for posts, profile information, and more.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Who Can See Your Posts: Go to Settings > Privacy. Under Your Activity, choose who can see your future posts and limit the audience for past posts.

Group 2: Instagram



Access Privacy Settings: Go to your profile and tap the three horizontal lines at the top-right corner. Select Settings > Privacy.

Private Account: Toggle on Private Account to make your posts visible only to followers you approve.

Story Settings: Under Privacy > Story, choose who can see your stories, reply to them, and share them.

Activity Status: Under Privacy > Activity Status, toggle off Show Activity Status to hide your online status.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Photos and Videos: Under Privacy > Posts, control who can tag you in photos and videos and approve tags manually.

5. Activity: "Fact or Fiction”

The objective is to develop skills in critically evaluating the reliability of online information. The need covered is Improved ability to critically evaluate the reliability of online information. To perform the activity the Materials Needed are computers/tablets, projector/screen. This activity will take 30 minutes to complete.

The Society of Professional Journalists (SPJ) Code of Ethics is a guiding principle for journalists, emphasizing the importance of public enlightenment, accuracy, fairness, and transparency.

The code consists of four broad principles, which are supported by additional explanations and position papers: https://www.spj.org/pdf/spj-code-of-ethics.pdf

Watch this video: Ethics 101: The 5 Core Values of Journalism

Fake news can easily proliferate, particularly in times of political turbulence and instability. Take a look at the following examples of fake news:

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Putting a Viral Video Clip of Biden in Context: A 10-second clip of Joe Biden showed him delivering a quote devoid of the full context, which construed his meaning.
- Fake Coronavirus Cures: A recipe circulating on social media claimed that garlic cured coronavirus.
- False Claim That Wisconsin Counted More Votes Than Registered Voters: A social media rumor incorrectly compared the number of registered voters in 2018 to the number of votes cast in 2020.

After checking information and news, ask yourself and discuss in groups of 3 identifying fake news requires critical thinking and skepticism. Questions to ask yourself to determine whether a piece of news is fake or credible:

- What is the source of the news?
- Is it from a reputable and well-known media outlet, or an obscure website?
- Is the author identified and credible?
- Does the author have a track record of reliable reporting? Can you verify their credentials?
- Does the URL look suspicious?
- Does the headline seem exaggerated or intended to provoke an emotional response?
- Are there spelling or grammatical errors?
- Is the content logically consistent and coherent?
- Does the story make sense as a whole, or are there contradictions and logical fallacies?
- Does the article cite credible sources?
- Are the claims supported by quotes from experts, official statements, or links to primary sources?
- Can you find the same news reported by other reputable outlets?
- Cross-check the story with multiple reliable sources to see if it is being widely reported.
- Are there embedded links that lead to supporting evidence?
- What is the purpose of the article?
- Does it aim to inform with factual reporting, or does it seem designed to mislead, entertain, or push a specific agenda?
- Does the article include a date and time stamp?
- Does the news evoke a strong emotional reaction?
- Are you inclined to believe the news because it aligns with your existing beliefs?
- Are the images and videos in the article authentic?

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

References and resources

Arruda, W. (2019). *Digital you: Real personal branding in the virtual age*. Hoboken, NJ: Wiley.

Doorley, J., & Garcia, H. F. (2015). *Reputation management: The key to successful public relations and corporate communication* (3rd ed.). New York, NY: Routledge.

Van den Hurk, A. M. (2013). *Social media crisis communication: Preparing for, preventing, and surviving a public crisis*. Boston, MA: Pearson.

Smith, J. (2021). *Digital Literacy: Concepts, Strategies, and Practices*. Springer.

Jones, A. (2020). Teaching digital literacy in the classroom. En B. Brown & C. Davis (Eds.), *Advances in Digital Education* (pp. 45-67). Routledge.

Smith, J. (2020). *Cybersecurity Essentials*. Wiley.

Knight, Alison. "Data Analytics and the GDPR: Friends or Foes?" *Data Privacy Review* 8, no. 2 (2015): 123-145.

Garcia, M., & Lee, S. (2021). Current trends in cybersecurity. *Journal of Cybersecurity*, 5(2), 112-130. https://doi.org/10.1177/1234567890123456

Brown, C. (2023, Enero 15). Cyber threats on the rise. *New York Times*. https://www.nytimes.com/article/cyber-threats-rise.html

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://www.nist.gov/cyberframework

Avery, J. (2020). The power of social media in crisis management. *Harvard Business Review*. https://hbr.org/

Digital Marketing Institute. (2021). Understanding digital reputation management. https://digitalmarketinginstitute.com/

Llopis, G. (2013). The role of personal branding in professional success. *Forbes*. https://www.forbes.com/

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Funded by the European Union. Views and opinions expressed are however those of the Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.