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

Erasmus+

CREW

**Creativity, Resilience,
Empowerment for Work**

IO1 TRAINING COURSE IN DIGITAL LITERACY

Austrian Association of Inclusive Society
M&M profuture training
TATICS HUMAN EVOLUTION
ENOROSCONSULTING Ltd
KOKKALIS FOUNDATION
VERSLI MAMA

Table of Contents

Erasmus+

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

Table of Contents

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

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

Objectives and purpose of IO1

The internet became a commodity in XXI century, almost the same as oil, grain or sugar. It's the main ingredient for services to exist in many sectors, such as finances, health, marketing, entertainment, education. The internet is a kind of a raw material or a framework itself, which is employed as a building material for a variety of other services and ecosystems, evolving around it.

As digital and online tools evolve rapidly, merge together and produce an even wider range of services and innovative products, while the devices used in everyday personal and public activities become faster, widely adopted and connected, the digital literacy skills become essential in career building and successful competition in a labour market. The constant development of skills, meaningful and purposeful engagement in the digital world, ability to consume, evaluate and create the information over the internet, at the same time staying secure and resilient against fake and low quality information - all of it is of no less importance.

Highly skilled and versatile people, able to quickly adapt to ever changing conditions, especially in a digitized world, are most valued by employees. Being able to use a keyboard and a mouse, possessing a certain degree and knowledge is no longer considered as an advantage, people are required to have a very wide range of basic and a set of specialised digital skills as well as ability to acquire new ones at a very fast pace.

Therefore, the aim of this course is to help extend the basic skills already possessed by individuals improving their overall digital literacy skills and empower them for further development, while helping people with lower technical skills to fight their anxiety in digital skills improvement. This course is targeted to less proficient adult learners, helping them to become more involved into the society and labour market, as well as educators, organisations and institutions organizing learning courses, involved in teaching and training of digital literacy and related subjects, that can benefit by using our courses for their educational purposes.

1 MODULE

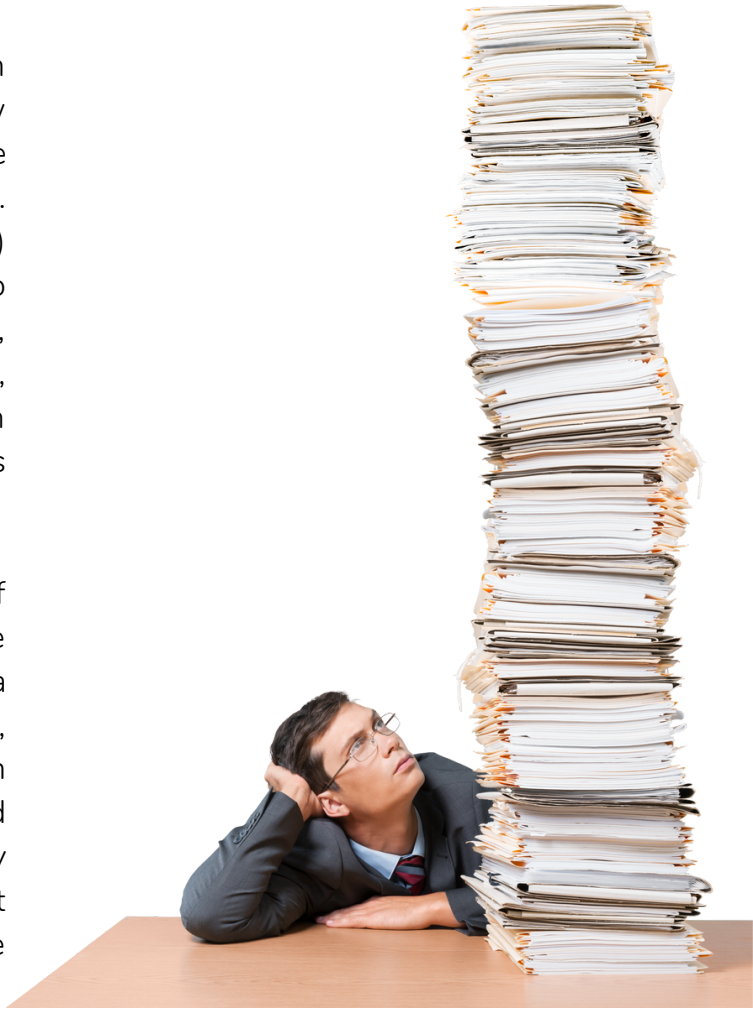
Co-funded by the Erasmus+ Programme of the European Union

CREW
Creativity, Resilience and Empowerment for Work

DIGITAL LITERACY THEORY AND METHODOLOGY

1.1 INFORMATION ACQUISITION

Even though the term of information acquisition is not something new, it creates new perceptions in so vastly connected world in the beginning of the 3rd decade in the XXI century. The American Library Association (ALA, 1989) defines information literacy as being able to ascertain what information is needed, understand how the information is prepared, find the best sources of information for a given need, identify those sources, assess the sources analytically, and share that information.

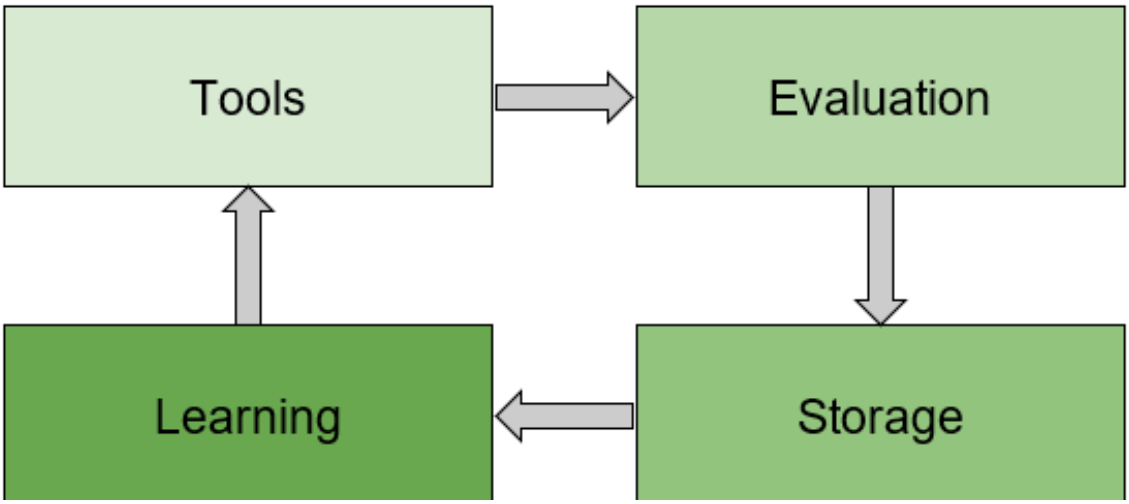


Over three decades old explanation of information literacy stands a test of time to quite well define what information acquisition from a digital literacy perspective may be. However, easily accessed, quickly changing and often unintentional flow of information in a digitized world makes the acquisition of information very much different because of the vastly different magnitude of information available over the internet.

We stick to the basics and emphasize on the following main pillars of what information acquisition in the scope of digital literacy is:

1. It's being able to properly use online tools to acquire information;
2. Critically evaluate the information and filter through irrelevant of low quality sources of information;
3. Being able to securely store and manage the acquired information;
4. Acquiring the new knowledge itself and being able to continuously develop new skills and keep learning non-stop to acquire more and better quality information.

Figure 1. An illustration of continuous cycle of information acquisition and quality improvement



Basic tools to acquire the digitised information are usually pretty well known and popular:

- Google and other search engines
- Wikipedia
- Youtube and other video services
- Social media - Facebook, Twitter, Linkedin
- News portals, forums, internet directories

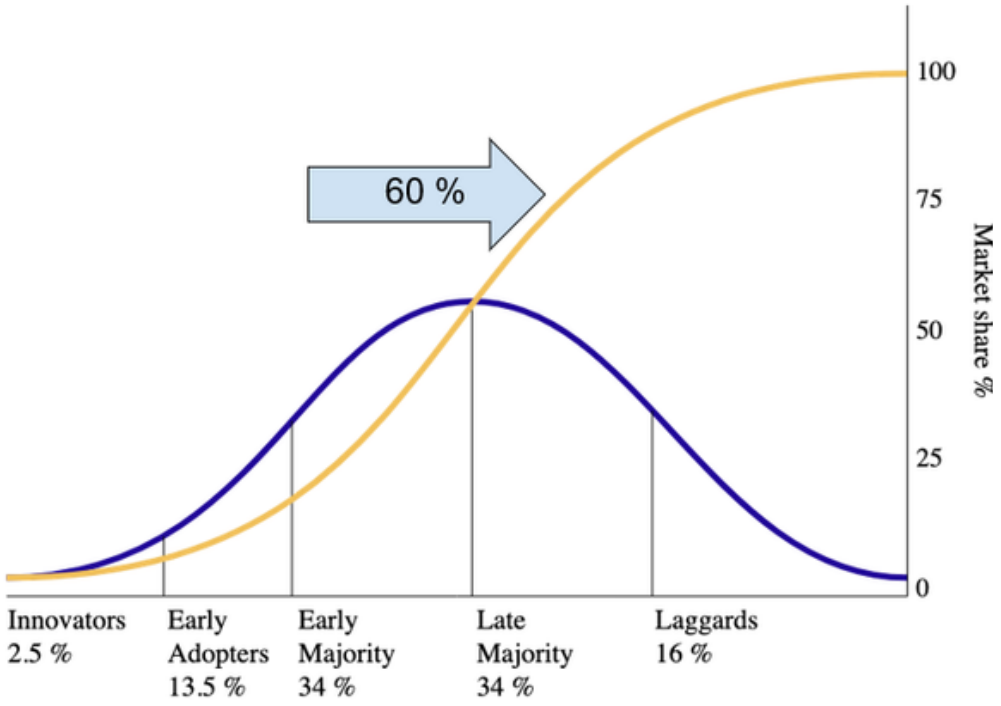
The storage of information is a rather technical topic, therefore we will cover the subjects, such as security, reliability and best practices or related topics for the information storage in further chapters.

The evaluation part is crucial to develop the necessary digital skills; therefore, we will dive deeper into this topic in the next chapter.

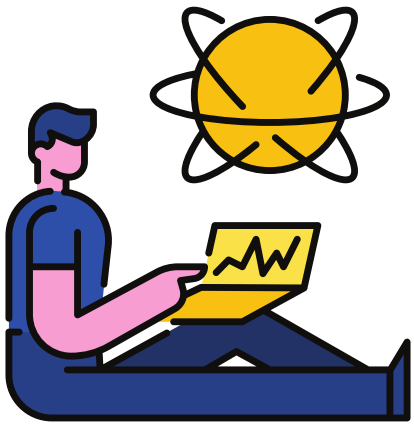
What is current adoption of how much is the internet is at the moment?

According to Everett Rogers' diffusion of innovations model, which can be used to well describe the evolution and adoption of any technology, we are still a long way to having internet adopted in the whole world.

Figure 2. Adoption of the internet based on internet penetration being 60% in 2021 [source: Statista.com][1]



Despite uneven adoption of the internet worldwide, we still may consider digital tools and internet connection being the major positive factor to spread the ideas, educate people, fight poverty and unemployment.



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

1.2 INFORMATION EVALUATION

Why do we need to evaluate the information?

Once you have found information that matches the topic and requirements of your research, you should analyse or evaluate these information sources. Evaluating information encourages you to think critically about the reliability, validity, accuracy, authority, timeliness, point of view or bias of information sources.

Just because a book, article, or website matches your search criteria and thus seems, at face value, to be relevant to your research, does not mean that it is necessarily a reliable source of information. It is important to remember that sources of information comprising the Library's print and electronic collections have already been evaluated for inclusion among the Library's resources. However, this does not necessarily mean that these sources are relevant to your research.

This does not necessarily apply to sources of information on the Web for the general public. Many of us with Internet/Web accounts are potential publishers of websites; most of this content is published without editorial review. Think about it. Many resources are available to help with evaluating web pages.

The easiest way to evaluate the information is to ask proper questions. What criteria should you use to judge information sources?

1. Initially, look at the author, title, publisher, and date of publication. This information can be found in the bibliographic citation and can be determined even before you have the physical item in hand.
2. Next, look at the content, e.g. intended audience, objectiveness of the writing, coverage, writing style, and, if available, evaluative reviews.

For example, following questions should be asked in order to step-by-step evaluate the quality of information:

Who is the author (may be individual or organization) and/or publisher?

1. What are the credentials and affiliation or sponsorship of any named individuals or organizations?
2. How objective, reliable, and authoritative are they?
3. Have they written other articles or books?
4. Is the author(s) listed with contact information (street address, e-mail)?
5. Has the publisher published other works?
6. Do they specialize in publishing certain topics or fields?
7. Is the publisher scholarly (university press, scholarly associations)? Commercial? Government agency? Self ("vanity") press?

What can be said about the content, context, style, structure, completeness and accuracy of the information provided by the source?

1. Are any conclusions offered? If so, based on what evidence and supported by what primary and secondary documentation?
2. What is implied by the content?
3. Are diverse perspectives represented?
4. Is the content relevant to your information needs?

When was the information published?

1. Publication date is generally located on the title page or on the reverse side of the title page (copyright date).
2. Is the information provided by the source in its original form or has it been revised to reflect changes in knowledge?
3. Is this information timely and is it updated regularly?

Where else can the information provided by the source be found?

1. Is this information authentic?
2. Is this information unique or has it been copied?
3. Why was the information provided by the source published?

What is the context around this information?

1. What are the perspectives, opinions, assumptions and biases of whoever is responsible for this information?
2. Who is the intended audience?
3. Is anything being sold?

A proper introduction to evaluation of information is crucial in order to achieve desirable results for digital literacy skills improvements especially while providing the learners the directions and guidelines for their self-improvement and self-learning by practice.

1.3. DIGITAL INFORMATION CREATION AS A LEARNING PROCESS

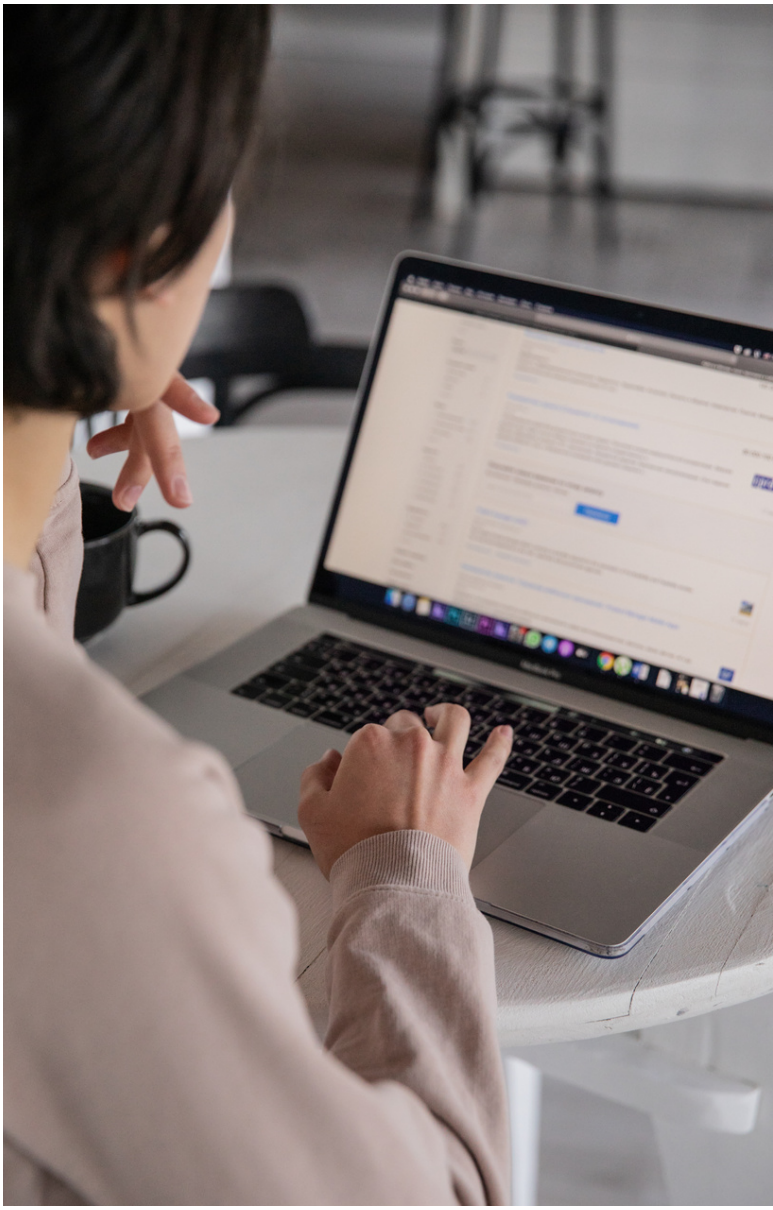
Information in any format is produced to convey a message and is shared via a selected delivery and distribution method. The iterative processes of researching, creating, revising, and sharing the information vary, therefore the whole process itself is a big part of the constant learning process while the information is being both created, consumed and distributed.

Learning-by-doing as an approach to education is very suitable for digital literacy skills improvement, because there is a very wide range of tools and software available, ready to be used by students of any skill level in order to achieve particular targets for the deliverables and learning purposes. Currently existing tools and instruments in the digital world are available in any country, support the majority of languages and are either very cheap or totally free to use. This makes digital skills acquisition available and relatively easy to anybody. To fine tune the education process, educators must choose the right medium to deliver their training.

Taking website building as a hands-on approach example. In order to be able to build a website, an individual need to have basic knowledge and computer usages skills, which would help him to find the necessary instructions and requirements for the website building. Those basic skills may be acquired earlier during formal education, however deeper knowledge will be acquired after practical tasks completion.

Website building is a complex task, which requires to improve the skills in information search and evaluation, storage, also creation and distribution, therefore we emphasize on this kind of exercise being a perfectly suitable way for digital skills improvement. If necessary, website building exercises may involve marketing and communication, writing of quality articles supplemented with interactive and rich media additions, research on internet users' behaviour and experience, security and privacy and how a website's design, structure or functionalities can help to achieve the best results.

Learners may choose either to work on personal blog creation or a simple e-commerce website creation, which forces them to acquire the necessary skills in areas such as finances, digital identity creation, precautions against cybercrimes, usage of e-signature and e-government services. They also should start to see themselves as being part of a never-ending process in both information creation as well as information consumption at the same time, which widens their perception in digital literacy as a whole.



Our methodological recommendation for digital literacy education is to use a practical approach of website building and adjust particular exercises based on actual skills, motivations and expectations of the learners.

2 MODULE

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

CREW
Creativity, Resilience and Empowerment for Work

MAJOR SKILLS DEVELOPMENT

2.1. DIGITAL LITERACY AS CULTURAL APPROACH

We are viewing a period of technological development that is both unprecedented and widely disruptive. In the short time since the Internet was created, much has changed, including the design of computer interfaces, the processing speed and portability of devices, the accessibility of information and knowledge, our methods of communication, the maintenance of our relationships, commerce, the protection of personal privacy, creative processes, publication of content, and the emergence of new digital tribes and virtual clans (Wheeler, 2009).

Several recently published articles have explored the notion of 'digital literacy', and as expected, there are numerous views. Anderson (2010) for example, describes digital literacies as the ability to exploit the potential of computer technologies. Literacies, in all their forms, are at once cultural, social and personal (Kress, 2009) and enable us to interact fully in specific cultures. Some warn that without an adequate level of literacy, digital media have the capacity to disadvantage some (van Dijk, 2005), whilst others warn of the nature of the web to undermine knowledge and competency (Carr, 2008; Keen, 2007). However, the overwhelming majority of commentators eulogise over the potential of the social web to liberate education, and democratise learning, with the caveat that digital literacies are practiced. The American Library Association's digital-literacy task force offers this definition: "Digital literacy is the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills."

The term “digital literacy” has become so popular and widespread over the last 10 years that it is almost taken for granted. With varying degrees of complexity, the phrase digital literacy is now used to describe our engagements with digital technologies as they mediate many (if not most) of our social interactions.

With this American Library Association digital literacy definition as a guiding light, it’s important to understand that even digital natives who know how to send a text and post to social media are not considered “digitally literate” by any means. It’s important to note that simply reading online or subscribing to an eBook service does not a digitally literate student make.

Digital literacy in education encompasses so much more. For example, you must have specific skills when reading online text that may contain embedded resources such as hyperlinks, audio clips, graphs, or charts that require you to make choices.

Digital literacy means having the skills you need to live, learn, and work in a society where communication and access to information is increasing through digital technologies like internet platform, social media, and mobile devices.

Developing your critical thinking is essential when you're confronted with so much information in different formats – searching, sifting, evaluating, applying and producing information all require you to think critically.

Communication is also a key aspect of digital literacy. When communicating in virtual environments, the ability to clearly express your ideas, ask relevant questions, maintain respect, and build trust is just as important as when communicating in person.

You also need practical skills in using technology to access, manage, manipulate and create information in an ethical and sustainable way. It's a continual learning process because of constant new apps and update and you need to keep your digital life in order!

Digital literacy is really important now and it will be really important in your professional future. In your workplace you are required to interact with people in digital environments, use information in appropriate ways, and create new ideas and products collaboratively. Above all, you need to maintain your digital identity and wellbeing as the digital landscape continues to change at a fast pace.

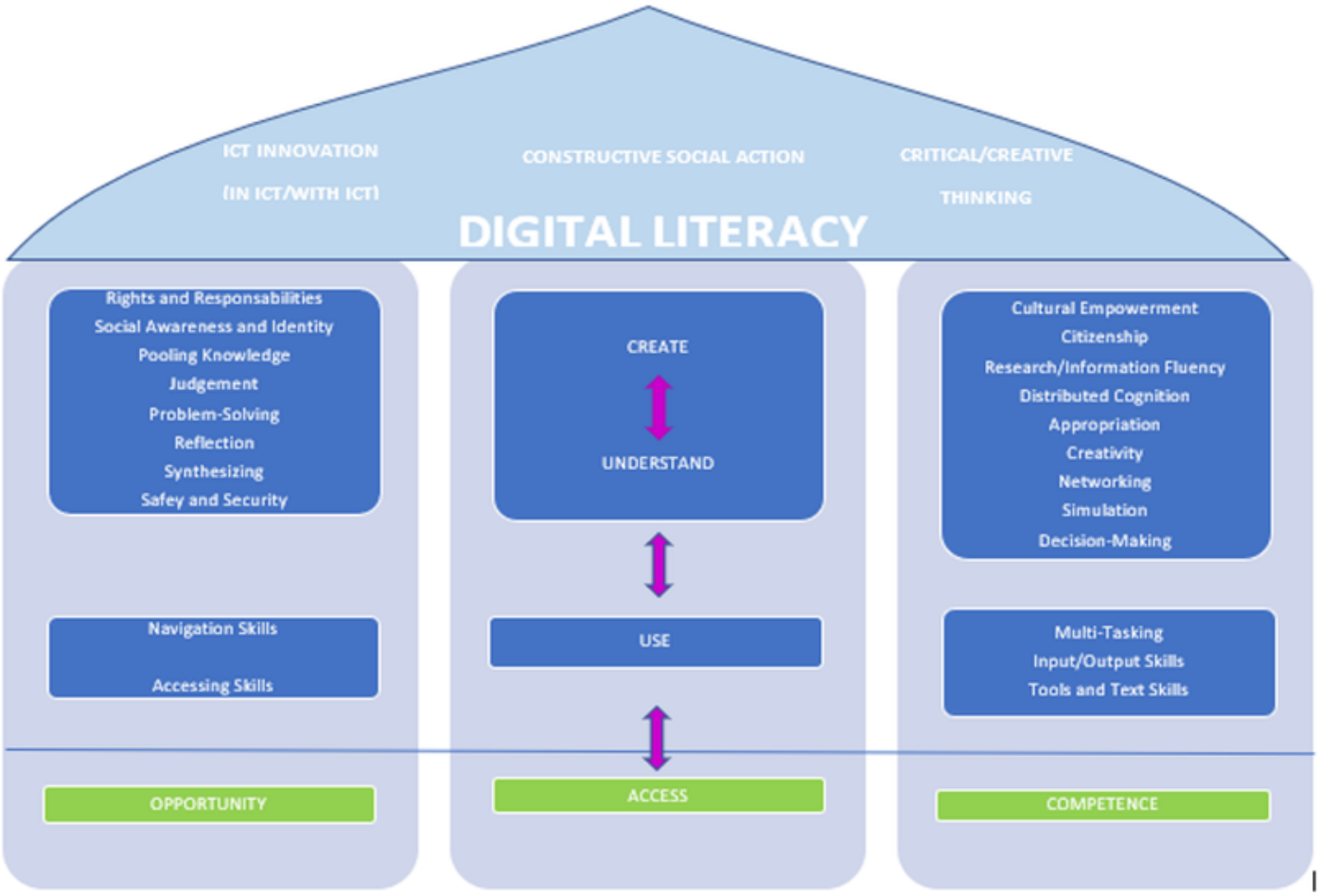
As mentioned, digital skills develop across a continuum, and they are constantly being updated in line with changes in technology. Digital skills frameworks serve a critical role in capturing the range of skills as well as these changes, thereby allowing policymakers and digital skills providers to ensure that their programmes and training curricula remain relevant and current. Many organizations and international agencies have developed digital skills frameworks. We highlight the work of the European Commission—the Digital Competence Framework for Citizens (or DigComp) that provides a common language on how to identify and describe the key areas of digital competence and thus offers a common reference at European level.

Globally, the International Society for Technology in Education (ISTE) frames its benchmarks for digital literacy around six standards: creativity and innovation; communication and collaboration; research and information fluency; critical thinking, problem solving and decision making; digital citizenship; and technology operations and concepts.

This model shows the many interconnected elements that fall under the digital literacy umbrella. There is a logical progression from the more fundamental skills towards the higher, more transformative levels, but doing so is not necessarily a sequential process: much depends on the needs of individual users, of your needs.

Figure 3. Digital Literacy Model

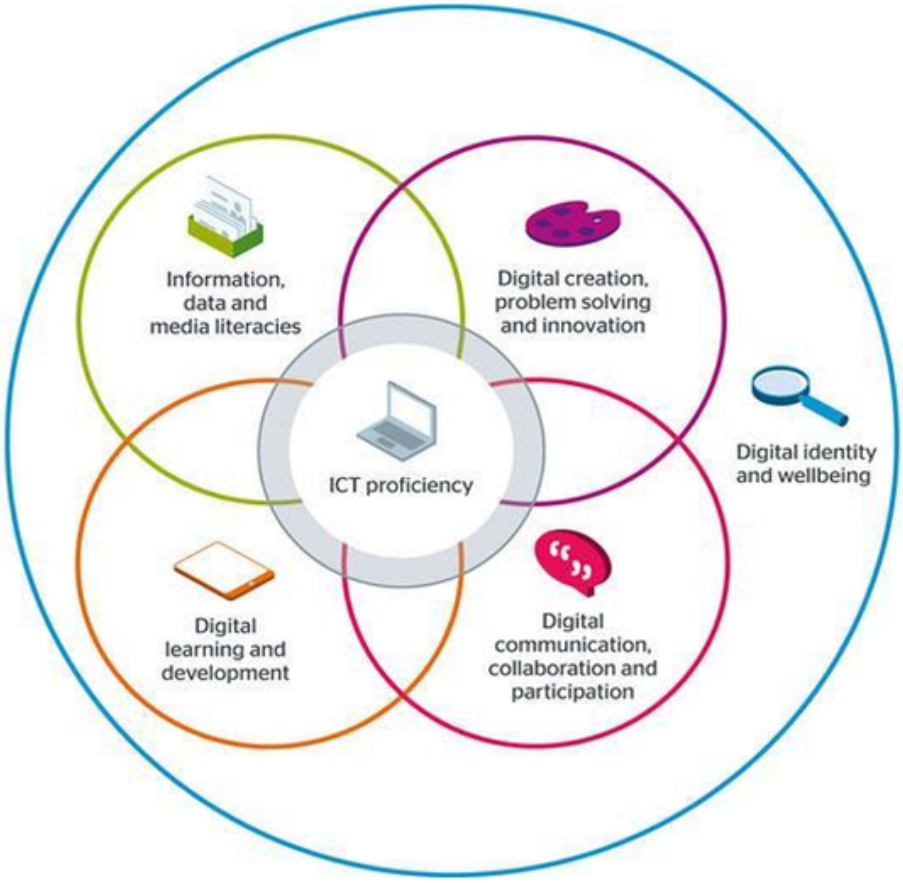
Illustration taken from Report of the Digital Britain Media Literacy Working Group (March 2009), DigEuLit – a European Framework for Digital Literacy (2005), and Jenkins et al., (2006) Confronting the Challenges of Participatory Culture: Media Education for the 21st Century.



What are the elements that make you digitally literate?

Digital literacy looks beyond functional IT skills to describe a richer set of digital behaviour, practices and identities.

Figure 4. The Jisc model



The Jisc model illustrates the idea that proficiency in ICT (Information and Communication Technology) is a core element in our digital literacy, whilst other skills overlap and build on this capability, and overarching it all is our digital identity and wellbeing.

Retrieved from https://www.jisc.ac.uk/rd/projects/building-digital-capability

2.2. REDUCING ANXIETY WHILE DEVELOPING DIGITAL SKILLS AND TEACHING

For some adults - including young adults - their incomplete use of the internet is linked with low literacy and numeracy, and to lacking the confidence and motivation to learn new skills and apply them in their lives. Digital skills are key to inclusion in society. Gaining these skills, along with the confidence and motivation to use them in real life, can help people to have better lives. People may feel embarrassed about not knowing how to use the internet and computer anxiety is a consequence. Computer anxiety is a widely occurring phenomenon since the introduction of computers into our life, showing that users who know little about computers are more likely to have anxiety about them but digital-anxiety can be reduced by increasing their ability to solve technological and digital problems. Anxiety itself is defined as a mental health disorder which encompasses “excessive” fears and worries. This often “silent” disability can manifest itself in numerous ways, and daily life is no exception.

Common signs that you may be experiencing digital stress when you aren’t skilled while starting to use digital tools include the following:

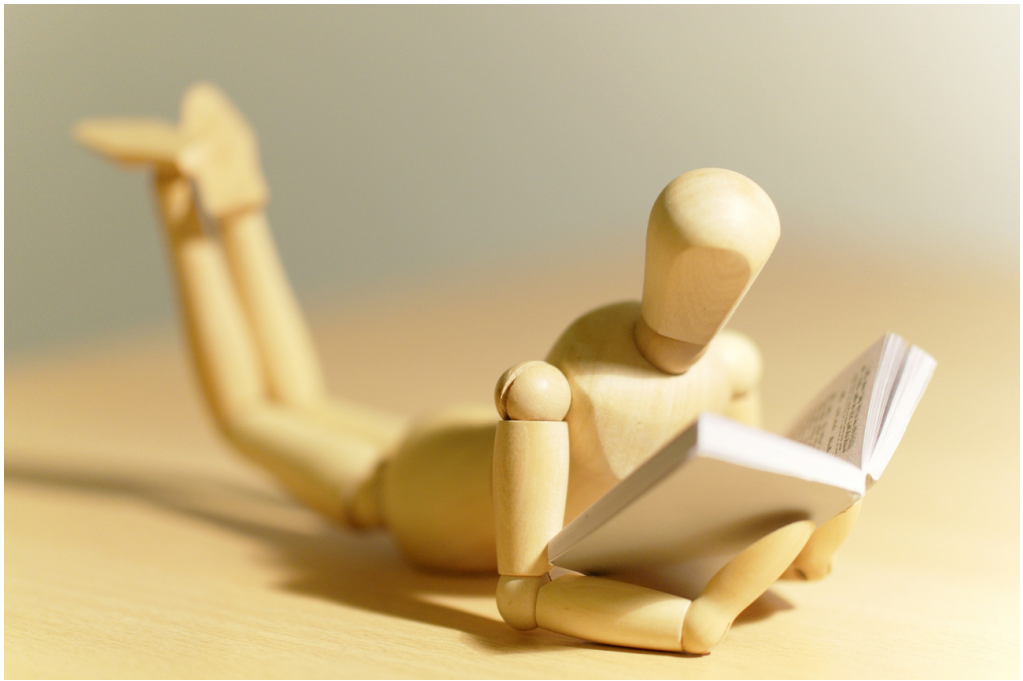
1. Anxiety or panic attacks
2. Isolation or withdrawal from social activities
3. Increased secrecy
4. Anger
5. Depression
6. Failing grades
7. Rebellion
8. Stomach-aches, headaches or other general body aches not explained by a medical condition

Access to technology and digital skills is critical in gaining access to key areas in school and social life, but is technology contributing to the apparent growth in anxiety problems seen in the modern world? What is it about digital and new technology that is making many of us anxious and stressed? IT anxiety is characterised by feelings of worry and apprehension along with physical tension relating to one's current or future use of computers, for instance, the fear of making mistakes or losing data. It can also lead to technostress. At its most extreme, IT anxiety can become 'technophobia' which involves resistance to using technology at all and can provoke a lack of information about technology and digital literacy.

How can you cope with this IT and digital anxiety?

Be Prepared

This is the Boy Scouts' motto for a reason: it's clever advice. When dealing with computers and the needed digital skills, many of us are a little intimidated, just wanting to learn the very basics and deal with the technical stuff as little as possible. While this is understandable, you can save yourself stress down the map by learning the nuts and bolts of how your systems work by reading the manuals and perhaps a book or two on computers, and practice, practice and practice.



Back up Often

If you don't already have this worked into your routine, it's vital that you start backing up your files regularly (we recommend once a week), so that if you run into main difficulties, you don't lose much of your precious time and work.

FOMO

But what happens if you aren't afraid of using computers but you need to constantly check email and be active in social media and you have the feeling that you have to be constantly connected and interacting and if you are not, you are lost and the consequences can be negative?

Figure 5. Fear Of Missing Out' explanation

F	Fear
O	Of
M	Missing
O	Out

We all have a love-hate relationship with email and social media and sometimes we complain that we get too much email but conversely, we check it far too often for the fear of missing out (FOMO). Email is often exacerbated by multiple email accounts to cover different areas of your lives, i.e., business, personal and interests such as sports clubs / church group, etc. Moreover, you have the necessity of checking social media again and again and again so you don't feel out of the loop: so, you know you're doing okay, so you don't feel left out.

How to manage your Fear of Missing Out? FOMO is self-invented psychological torture and it's a figment of our mind's worst imagination.

Here are 4 tips from keep your mental health during your FOMO feeling

1. Notifications

Be kind to yourself and turn off all email announcements on your desktop and mobile phone – you don't want the continuous intermission. This includes turning off the annoying email count number that often appears on the image of your email client. Seeing 100 unread emails is only going to peak your stress levels and entice you to take a peek at your emails.

You don't need to see every email, even from key stakeholders; email isn't a direct messaging and takes you away from doing in-depth work.

While you're there, turn off all non-essential notifications including Facebook, Twitter and WhatsApp – switching off notifications can be incredibly liberating. Also, move your email applications to the second page on your smartphone.

2. Healthy distance

Don't say "yes" to events for the fear of missing out, and keep a healthy distance from other peoples' screened versions of their lives. For one week, log the amount of time you spend checking emails, texts or social media on a daily basis. What else could you be doing with that time? The fear of missing out is real and FOMO can be dangerous, but if you know what to look for FOMO is reversible. Think JOMO. Joy of Missing Out.

3. Set priorities

Remember that the amount of information you are capable of handling is limited and focus on the people and data that really interest you or may be useful to you.

4. Take action

If you are permanently connected for fear of what you may miss, what you are really missing is life. Instead of looking at what others are doing, and spending your free time photographing, recording, and publishing your activities, enjoy good experiences and share them with those who matter to you.

2.3. SMART CONSUMER CONCEPT

The fast development of user-friendly tech and immediate access to information has made the clients of today smart and aware. With ever increasing possibilities available at a tap of the touchscreen, consumer behaviour and preferences are forever in flux.

When you hear the word consume – where does your mind go to? It probably starts thinking about food and what you eat. To be fair, it's not too far off. Consumption is about more than what you put into your mouth. It is what you do with your money and time. Your money buys food, shelter, clothing, games, car, knowledge, pensions, etc. Your time is spent learning a new skill or consuming the latest news event of the day. Getting this balance between creating and consuming can be tricky. If you get the balance right, it leads to improved financial capability.

New technologies are changing the ways in which consumers act. Thanks to technology, consumers are becoming more and more informed, empowered and demanding. Armed with knowledge collected from a multitude of sources, they are using their money on the goods and services they value. They want to interact in a way that is both relevant and timely: relevant to whatever they are shopping for, regardless of where, when and how they are shopping for it; and timely in fulfilling their needs. In short, today's consumers are getting smarter. But, how can you be a smarter consumer?

Consumers of all ages and in all parts of the world are swarming to social media.Understanding social media is no longer optional; it is an imperative for being a smart consumer. Media saturation needs to become more active as consumers, in part to manage the torrent of data pouring over us each day but also to make informed judgments about the significance of what we do see.

What are the best ways to combat “fake news” and develop information- digital skills? The proliferation of false news in recent years has been echoed by a proliferation of recommendations about how to deal with it. The skills involved in combating misinformation are in fact the skills that you need to develop. Your challenge is to think about how factors external to the source itself, such as the author’s identity, audience, and purpose, may produce subtle distortions. Combating “fake news” thus requires to exercise your brain in a more effortful way, read not just with comprehension, but also discernment—in short, applying critical thinking to what you’re reading and buying.

Here are some recommendations for how to be a smarter consumer in the Digital Age:

1. Start with the knowledge that anything can – and does – exist online.

That means real exists alongside fake, good alongside bad, legal alongside illegal, and everything in between. The internet can be a room full of dreams and it is also a place where you can see the most delicate part of the societal beast. It can be full of chances, conveniences, and enjoyment; it can also be a disloyal place waiting to trick, incite, be immoral and degrade. Buyer beware, times a million. The more you identify the internet’s duality, the more you will obviously see it for what it is, and also for everything that it isn’t.

2. Be your own researcher.

Anyone online can technically be a ‘thought leader,’ but it is up to us whether we decide to give these concrete individuals enough power to truly obtain that pedestal as the "led”. We’re all followers of social influencers, personalities or brands we want to imitate, or those we allow influence over our thoughts or buying choices. Just because they publish information online does not mean they are a source for valid information – this is not a 1:1 equation. What you consume online should always be questioned, researched and fact-checked.

3. Consider how your data is used.

The more data you facilitate online, the more targeted ads you will receive. But be aware that, beyond just what you offer, other private information is extracted from different sources. For example, think on deep before allowing online quizzes to access your profile information, which includes your birthdate, phone number, location, friends list, place of work, etc.

4. Protect yourself and your information.

Sharing, or oversharing, information can provoke to receive annoying ads for things that seem important, or worse, can be used to manipulate you into the creation of specific opinions, spending money or adding your name as an endorsement of things you may not fully understand or support.

5. It's your responsibility to pay attention and stay informed.

It's easy to want to ignore what is happening or to tell yourself that you can trust others to stay up-to-date on changes to internet usage, privacy laws and platform user agreements. However, if you continue to use the valuable parts of the internet, you need to accept there is a level of responsibility you own as a trade-off for those benefits.

Our modern society has become much more aware of products and services available to purchase, with highly intelligent advertising and marketing convincing us that we need that diamond ring, the latest phone or the toys for the shows that our kids watch on TV. Recognising this, there is an argument for practising good habits.

Figure 6. Smarter consumer (Source: Own elaboration).

2.4. CRITICAL THINKING AND EVALUATION TECHNIQUES

Using the Internet is probably a daily activity for many of you, but sometimes it's such second nature we don't stop to think about what underlies the information we use. We are now living in an era when information is widely available. Whenever people are faced with a question, their default response is 'Google it' rather than brainstorming for an answer. This contrasts sharply from what used to happen in the past whereby books were the main source of information. Nowadays, your critical thinking is a clue factor when analysing the digital information that surrounds us.

There are many definitions of critical thinking, in its most basic form, it is about being able to think for yourself. To be able to think critically, you need to be able to:

1. Examine and evaluate information and arguments
2. See patterns and connections,
3. Identify and build meaningful information

Someone with critical thinking skills can:

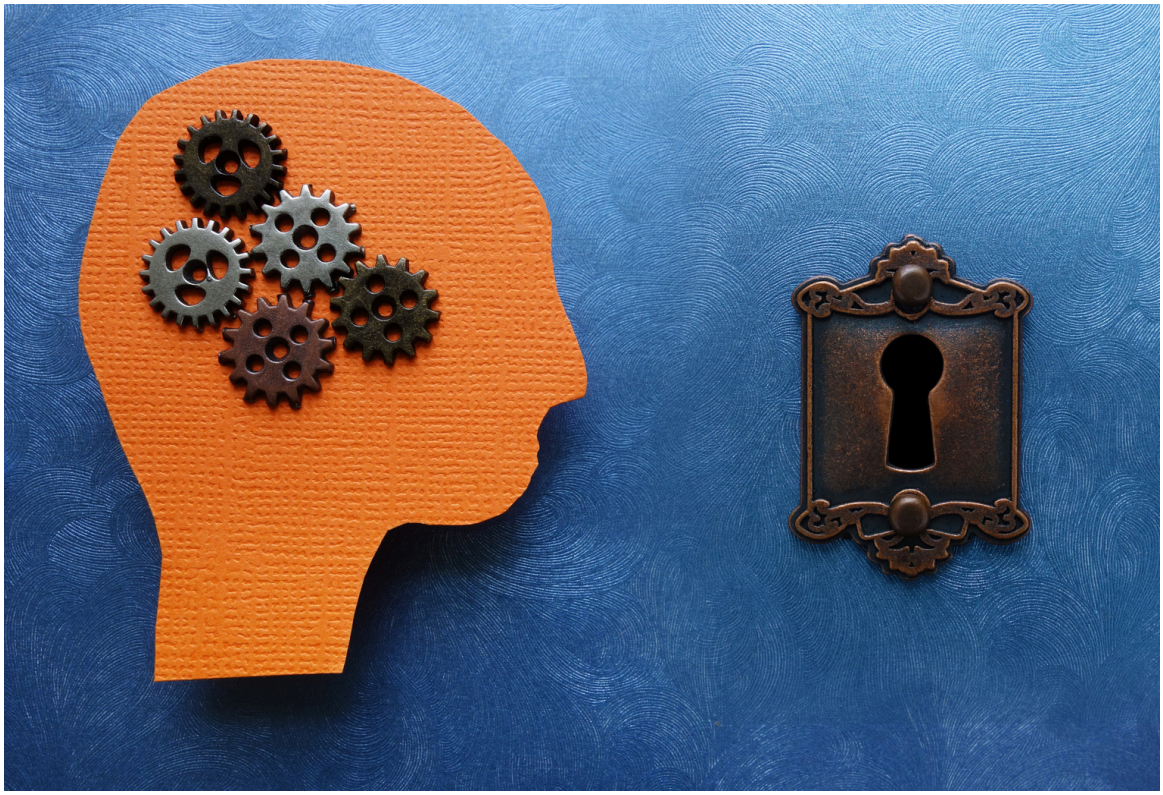
1. Understand the links between ideas.
2. Determine the importance and relevance of arguments and ideas.
3. Recognise, build and appraise arguments.
4. Identify inconsistencies and errors in reasoning.
5. Approach problems in a consistent and systematic way.
6. Reflect on the justification of their own assumptions, beliefs and values.

Figure 7. Critical thinking skills

You probably already have practice in critical thinking from other areas of life, such as deciding on which phone or computer or car to purchase, where to live, or even what to wear on a particular occasion. In each situation, you probably don't just do what someone else tells you to do, but you make a decision based on a range of factors. To apply critical ability in your digital skills means to use your capacity to find, evaluate, manage, curate, organise and share digital information. Moreover, this is the capacity to interpret digital information for academic and professional purposes, and to review, analyse and, re-present digital information in different settings. A critical approach to evaluating information in terms of its provenance, relevance, value and credibility. An understanding of the rules of copyright and open alternatives, e.g., creative commons; the ability to reference digital works appropriately in different contexts.

One of the most important elements of being online is the ability to be critically aware of where content comes from and who has authored it. You should be able to ask questions that will enable you to better understand context.

Related to your critical skill, it is important the capacity to collate, manage, access and use digital data in spreadsheets, databases and other formats, and to interpret data by running queries, data analyses and reports: your data literacy and the practices of personal data security.



An understanding of how data is used in professional and public life; of legal, ethical and security guidelines in data collection and use; of the nature of algorithms; and of how personal data may be collected and used. You don't need to be an expert or a professional of the data, but you have to be aware of its existence and the dangers that its misuse can cause you.

Another important factor is your capacity to critically receive and respond to messages in a range of digital media – text, graphical, video, animation, audio - and to curate, re-edit and repurpose media, giving due recognition to originators. A critical approach to evaluating media messages in terms of their provenance and purpose. An understanding of digital media as a social, political and educational tool, and of digital media production as a technical practice.

When it comes to evaluating digital content, you want to look for the best digital content available.For example, you want to avoid content that is simply an electronic version of the textbook without any added value. Digital literacy is about finding, evaluating, using, and creating digital content in meaningful and responsible ways. It requires thinking skills and technical abilities.

Taking into account that finding digital content about employing various search strategies to help source quality information, using multiple search engines to challenge personal filter bubbles using written, visual, and audio resources to navigate information in a variety of modes collecting a range of information that can then be evaluated to meet your requirements.

Other important point is that before you begin searching for relevant digital content, you must consider what is the inquiry question you are trying to answer or topic you are exploring the information you already have what information you need the type of information you need, for example, an overview, detailed analysis/research, or statistics how much information you need - what gaps are there in your knowledge.

In the present digital age, anyone can distribute any information on their websites, social media platforms, and other online forums. Unfortunately, those looking for parallel information do not really verify the authenticity of the information. As a result, propaganda and false information often gets construed as the truth thus causing decision-making problems. There is no standard for verifying the information.

How to make effective searching for digital content? You find better results using precise keywords and search strategies. Think of keywords from your inquiry question or topic, including synonyms, dictionaries and a thesaurus are useful for compiling a list of keywords. Look at the question or topic you want information on and choose the most relevant source for your search, for example, search engine(s) and/or online databases and try using different keywords and search techniques to broaden or narrow your search.

Common search techniques for the internet include:

Exclude words from your search	Put - in front of a word you want to leave out. For example, jaguar speed - car.
Search for an exact match	Put a word or phrase inside quotes. For example, "tallest building".
Search within a range of numbers	Put .. between two numbers. For example: camera €50.. €100.
Combine searches	Put "OR" between each search query. For example, marathon OR race.
Search for a specific site	Put "site:" in front of a site or domain. For example, site: youtube.com or site:.gov.
Search for related sites	Put "related:" in front of a web address you already know. For example, related: time.com.

Most information found on the Internet has a hidden reason behind it. The companies and writers who place the information on the Internet were probably trying to sell something to the readers. Others are propagandists looking to influence a reader's mode of thinking. Critical thinking helps us to think through problems and apply the right information when developing solutions. It is important that the digital age learns to differentiate factual and fake information. Moreover, it is good that information comes from various online and offline sources so that it is accurate and has enough facts.

Asking questions is always a good idea. It will make you a better learner and thinker. Critical questioning means going deeper into your questioning and not just asking Who, What, When, Where, Why, and How, but instead asking more descriptive questions like "Who benefits from this?" "What is getting in the way of action?" "Why has it been this way for so long?" or "How can we change this for our good?"

As says Jesse R. Sparks:
"We must develop the digital information literacy skills necessary to evaluate the veracity, relevance, credibility and argument quality of information to effectively learn, problem solve and make decisions in today's world."

2.5. CULTURAL PERCEPTION AND SOCIAL UNDERSTANDING

Digital technologies have transformed the cultural scene profoundly. That technology has infiltrated our lives, you can now shop, bank, communicate, socialise, browse and collaborate with people on your smartphone or device. In this sense, we must know that digital culture is not only connected with the digitization of analogue terms, but it also refers to a highly dynamic space in which multimedia modalities, cross media, transmedia, augmented reality and virtual reality all coexist. However, the digital scene is not without risks.

New technologies have modified space, time, relationships and types of communication that still continue to coexist with the other fields of knowledge inherent in a culture. It is clear that new technologies imply major advantages in terms of access to culture and it is also evident that in the digital age there are many more cultural offerings than users were formerly accustomed to.

Digital culture refers to the knowledge, beliefs, and practices of people interacting on digital networks that may recreate tangible-world cultures or create new strains of cultural thought and practice native to digital networks. Digital culture is the Internet, transhumanism, Artificial Intelligence, cyber ethics, security, privacy, and policy. It is hacking, social engineering, and modern psychology (Digital Culturist, 2015).

Mobile phones are extensively used by young people and adults alike. Websites such as YouTube and Wikipedia are the first port of call for many people looking for information about a selected area of interest. TV, films and music are stored and accessed on computers, MP3 players and online. Online shopping and banking have become more dominant and government services have become increasingly internet-based. Email allows instant communication between people across the world. Both online and offline gaming feature prominently in many people's lives and Web 2.0 technologies such as social networking sites allow people to collaborate by sharing and editing online content.

Today's society, often called "the information age", is marked by the rapid development of communication and information resources.

Cultural and social understanding equips you with a language and context for your digital literacy. Certainly, developing cultural and social understanding is crucial in enabling people to contribute not just socially and culturally but also politically, economically and intellectually. You need to recognize that there are certain social, cultural and historical influences that shape your understanding and learning.

How much might culture change when certain practices move online? How often can current cultural beliefs and expectations be transported to another reality? We frequently think of information and communication in a technical and instrumental way — as data and data transmission. However, information and communication are also social phenomena.

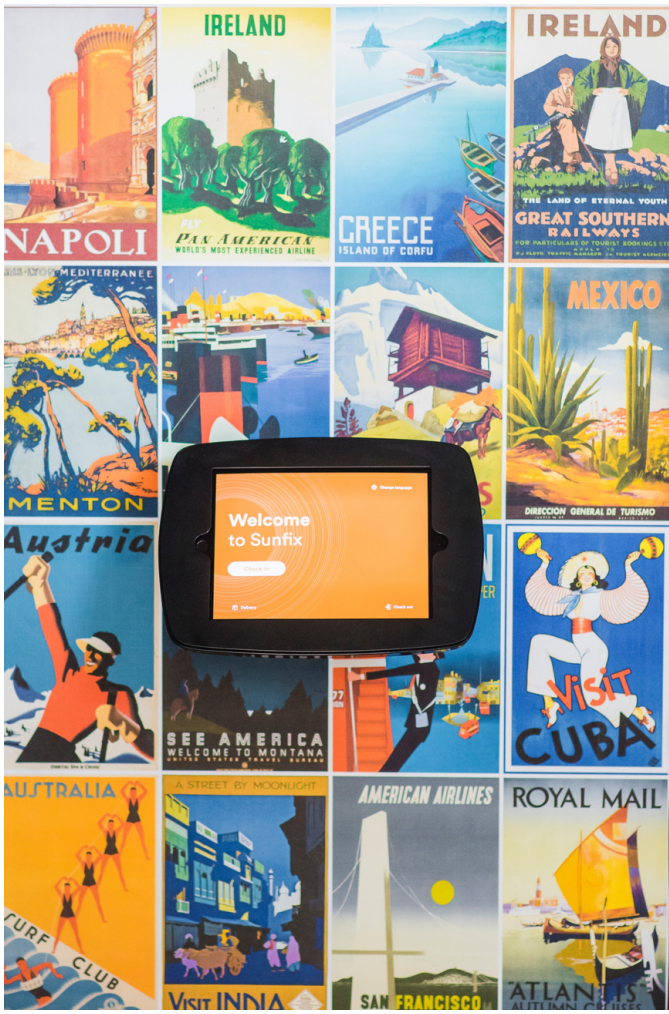
The propagation of technology not only affects social class status, but social class formation, division, and aspects that contribute to each group. Still, many persons understand less where they fall within social class as digital cultures muddle types of capital. This lack of clear identification or understanding does not diminish the significance of class hierarchy as the digital space categorizes content through aspects like class and worker issues aren't clearly addressed through such oversight or lack of digital social class cohesion.

Digital culture and technology have formed new ways of seeing social class theoretically including immaterial labour, digital labour, informational and cultural work, “concept of free labour under conditions of the New Economy, as well as the now-famous notions of social factory” (Qiu, 2018).

Building global online culture via new media should focus on how radical changes are adopted by democratic rules and principles. Digital technologies, principally online spaces, provide you with opportunities for many new forms of interaction. Increasingly these interactions are mediated by different modes of representation such as images and sounds. Being able to decode these multimodal texts requires an understanding of the social and cultural practices that surround your creation.

We differentiate cultural epochs according to the communication technology used. In oral culture, knowledge transfer could only happen in direct communication. In written culture certain types of knowledge or the memory of a particular person could be preserved and written messages could be sent through space and be recorded (and preserved) for the future. The press and broadcasting culture allowed the mass distribution of messages from centralized sources. Nowadays we can refer to concepts such as digital culture, internet and its participatory nature, convergence, ambient intelligence, etc.

The effect of the communication technologies on culture is important because the way we use them can effect changes in the very essence of our cultural and communication models but although digital tools intensify your possibilities, paradoxically, the exponential growth in content offerings from around the world sometimes has the opposite effect: it results in a glut that may detract your attention.



Based on these ideas presented, think about:

1. What extent do digital citizens' skills continue to improve their communication styles and abilities via new media?

2. What kind of online authentic experiences are associated with developing communication styles and abilities via new media?

3. What are digital citizens' patterns of participation in communication styles and abilities via new media?

4. What are the impacts of communication styles and abilities via new

Individuals can become active participants in their knowledge constructions rather than passive receptacles. In this constructivist milieu, digital citizens can work on complex global projects via new media.

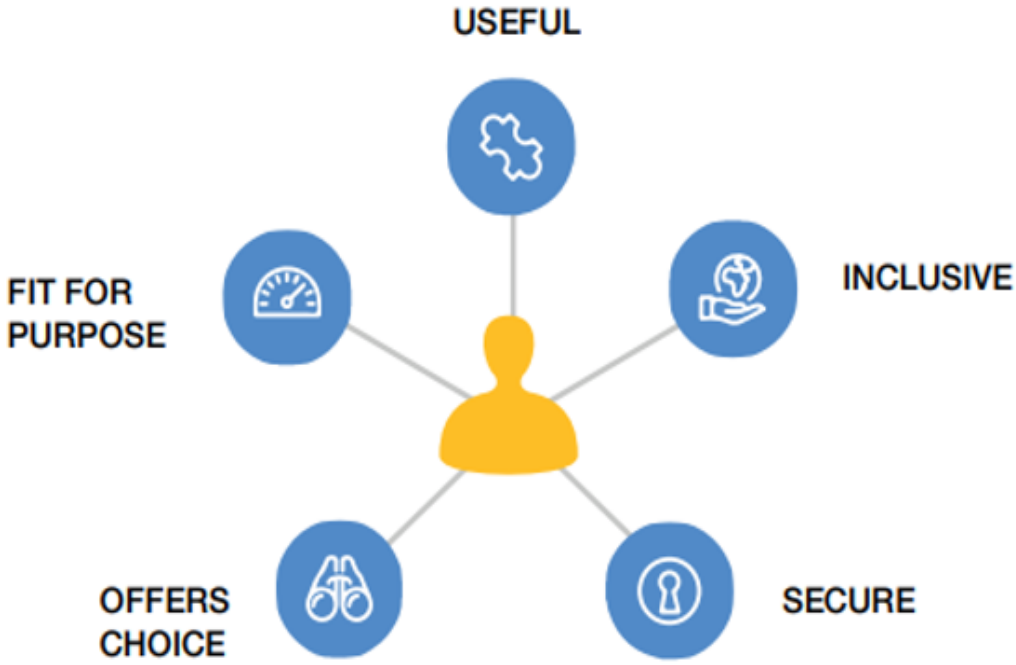
2.6. VIRTUAL IDENTITY CREATION, MANAGEMENT AND IMPLICATIONS

Our identity is, literally, who we are and presenting oneself online using a personal blog, webpage or social networking site needs a purposeful selection of text, pictures, graphics and audio to generate an impression. This is not done by chance. The online world requires people to write themselves into existence and so their profiles provide an opportunity to craft the intended impression through language, imagery and media.

At the World Economic Forum's Annual Meeting in Davos 2018 were identified an initial set of five elements that a good identity must satisfy:

1. Fit for purpose. Good digital identities offer a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms, and/or demonstrate their legibility to access services.
2. Inclusive. Inclusive identity enables anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity-related data, and without facing authentication processes that exclude them.
3. Useful. Useful digital identities offer access to a wide range of useful services and interactions and are easy to establish and use.
4. Offers choice. Individuals have choice when they can see how systems use their data and are able to choose what data they share for which interaction, with whom and for how long.
5. Secure. Security includes protecting individuals, organizations, devices and infrastructure from identity theft, unauthorized data sharing and human rights violations.

Figure 8. Five elements of good identity (Source: Own elaboration)



Resource: Insight Report - Identity in a Digital World A new chapter in the social contract. World Economic Forum (Sep 2018)
http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

If you Googled your name, what would you find? Having on mind that your online identity is not the same as your real-world identity because the characteristics you represent online differ from the characteristics you represent in the physical world; you may have heard of the idea of a digital footprint.

This refers to the traces of your personal and professional information that are left in online networks - both intentionally and unintentionally. Sometimes, you might hear advice about not posting anything that you don't want anyone to see. That makes sense, but also, think about what you would like future generations to see.

Posting material online effectively means you are letting go of control over it, so you want to be sure it will not damage your reputation or credibility. Even if you later choose to delete, there is no guarantee that someone hasn't already copied or shared it without your knowledge. Unfortunately, there are people who enjoy bullying others in digital spaces, or who will take advantage of you if given the opportunity.

What do you need to know during the procedure of Creating and Protecting Your Online Identity?

There are a variety of ways for you to use online social media when looking for work including:

1. Social networking sites like Facebook, Twitter, and LinkedIn
2. Participating in online forums and discussion lists
3. Creating a personal blog

When participating in social media it is always prudent to present yourself in a professional manner and it is also important to guard your personal information.

Some basic tips to remember when you are online:

1. The internet is a public space. When you post online, you waive your right to privacy
2. Online content can be permanent - it can be searched; it can reach many people, and it can reveal your location
3. When giving out information, be sure you know how it is being used
4. Provide sensitive or confidential information only through secure web sites
5. Use social networking wisely; adjust your privacy settings to your own comfort level
6. Despite all cautions, don’t be afraid to participate and connect!

What is about your professional identity?

These days' employers want to know who they have hired and many recruiters check the social media of potential employees. Social networking sites are good ways of broadcasting your interests, skills, and need for work. According to a 2017 survey, 70 percent of employers use social media to screen candidates before hiring. As well, 69 percent of employers are using online search engines such as Google, Yahoo and Bing to research candidates. Build and manage your public online profiles so that potential employers find positive and professional information about you, it is an important point when you are looking for a job.

Facebook, LinkedIn, Twitter, Pinterest (and every other online community) can be excellent tools for networking, finding resources, and promoting personal or professional interests – but only if used intelligently and intentionally. First impressions take shape before you even physically meet someone. Just like the saying "Your reputation precedes you", your online reputation today often precedes in-person meetings and interviews.

The thing to keep in mind is that online reputation management is one of those things that works better if you implement it before you actually need it.

Top 5 Tips & Tricks

1. Google yourself. It may sound vain but, in this case, you're excused - you need to know what people see when they look for you.

2. f you aren't using it – delete it. Find all of your old profiles and any unused accounts that you no longer use and delete them.

3. Remember, there's more than one page on Google. Make sure to look through as much of Google as you can in case you miss anything

4. Spring cleans your history. It will take time but go through your Twitter/Instagram/Facebook and check every post and delete any that paint you in a bad light.

5. Get rid of the evidence. Take down any pictures which make you look bad and ask friends to do the same.

Now what?

Think about what you are posting. You have spent all that time cleaning up your digital footprint. Don't undo all that good work by slipping into old habits and be careful with the content you share.

Go into lock-down

Make sure to tighten up your security settings on platforms like Facebook so that only friends can see you.

Be careful hitting the add button

We all love a new Facebook friend or Twitter follower but be careful. Sometimes it isn't wise to add colleagues or lecturers on social media. It's always a good idea to keep your private life, privacy.

Create great content

Do things that make you look good and make it a part of your digital footprint. If your boss goes on Facebook, let them find an album of pictures of you volunteering in the community. If you don't already use it – LinkedIn is a great way to showcase all the great stuff you do and can act like an online CV.

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

MOST IMPORTANT TOOLS IN MEDIA LITERACY IN GENERAL

3.1. BASIC SOFTWARE AND COMMUNICATION TOOLS

The basic software and computer programs allowing the execution of the majority of common tasks for computer users can be split into two groups: free software and paid one. We would like to emphasize free software, however paid and licensed products have their own advantages, for example support and a wider range of additional tools and possibilities. Most paid license software also provides limited, but free versions of it, unusually for personal use.
To make it simple, we prepared a list of most common tasks that can be solved by using either free or paid software. This list is also covering most of the tools that are usually required by the employers.

To make it simple, we prepared a list of most common tasks that can be solved by using either free or paid software. This list is also covering most of the tools that are usually required by the employers.

We also share the links to alternative tools online, as many of the tasks can be solved using cloud based solutions, especially as the digital evolution is rapidly moving towards cloud based computing. Personal devices are becoming more like terminals to access the remote and powerful machines and display the results. Note that the majority of the tools and programs have their own alternative versions in smartphone devices and are available to download in app stores.

A list of basic free and pad software

A task or purpose	Free (install)	Paid / alternative (install)	Access and use Online
Accessing the internet	Chrome, Firefox, Opera	Google News (app)	N/A
Searching for information	Google, Yahoo, Bing, Yandex	Duckduckgo	Quora, Wikipedia
Accessing and creating email accounts	Thunderbird	Microsoft Outlook	Gmail
Collaboration and communication	Skype, Telegram, Viber	Slack, Zoom	Trello, Asana
Editing documents, saving and viewing PDF	OpenOffice (Writer)	Microsoft Word	Google Docs
Making calculations, drawing tables and diagrams	OpenOffice (Calc)	Microsoft Excel	Google Sheets, Infogram.com
Protecting computer from viruses	GIMP	Photoshop	Snappa.com, Canva.com
Photo editing	VLC	Vimeo.com	Youtube.com
Media Player	Avast, Avira	ESET Antivirus	Eset online scanner
Securing and managing the passwords	LastPass (for individuals)	1password, Bitwarden	N/A
Secure browsing tools (VPN)	Opera built-in VPN	Nord VPN, Express VPN	N/A

We will dive deeper into certain basic tools and software in further chapters.

3.2. SEARCH ENGINES

A search engine is a website through which users can search internet content. Search engines allow users to search the internet for content using keywords. Each search engine works in a similar way.

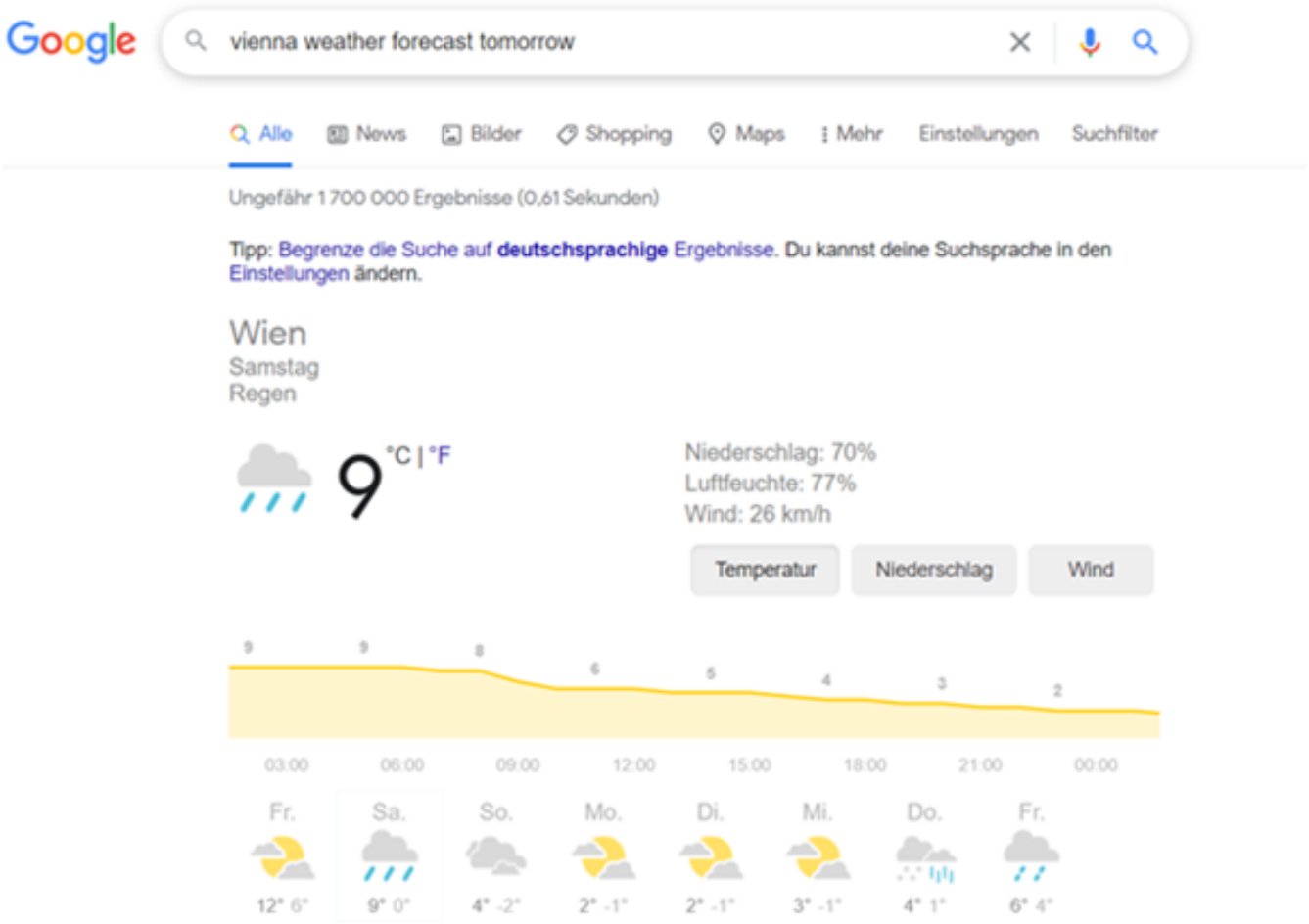
If you go to a search engine's homepage, you will find a single box. You simply type whatever you want to search for into that box. Search engines are a great way to find things on the web. If you search carefully you can find reliable and trustworthy information. With such a diversity of content and with the enormous volume of information on the Internet, retrieving the relevant information might be particularly challenging.

Keywords in your search criteria

You need to think carefully about the keywords you enter in your search. They need to be relevant. For example, to find out what the weather forecast is for tomorrow, you may type the keywords like: „Vienna weather forecast tomorrow" and the most relevant search results will appear.

You also need to think about the number of keywords that you use, too. If you use too few keywords you could get too many results and they will not all be relevant. However, if you use too many keywords, you might get no results at all. To help make your search more specific, you can use "quotation marks" around a set of words to find an exact phrase.

Figure 9. Search example: „Vienna weather forecast tomorrow" (Source: Google)



If you add a minus symbol (-) before a word it will exclude pages that contain that word. For example, 'Roman emperors -Caesar' will look for pages with 'Roman' and 'emperors' in it, but not 'Caesar'.

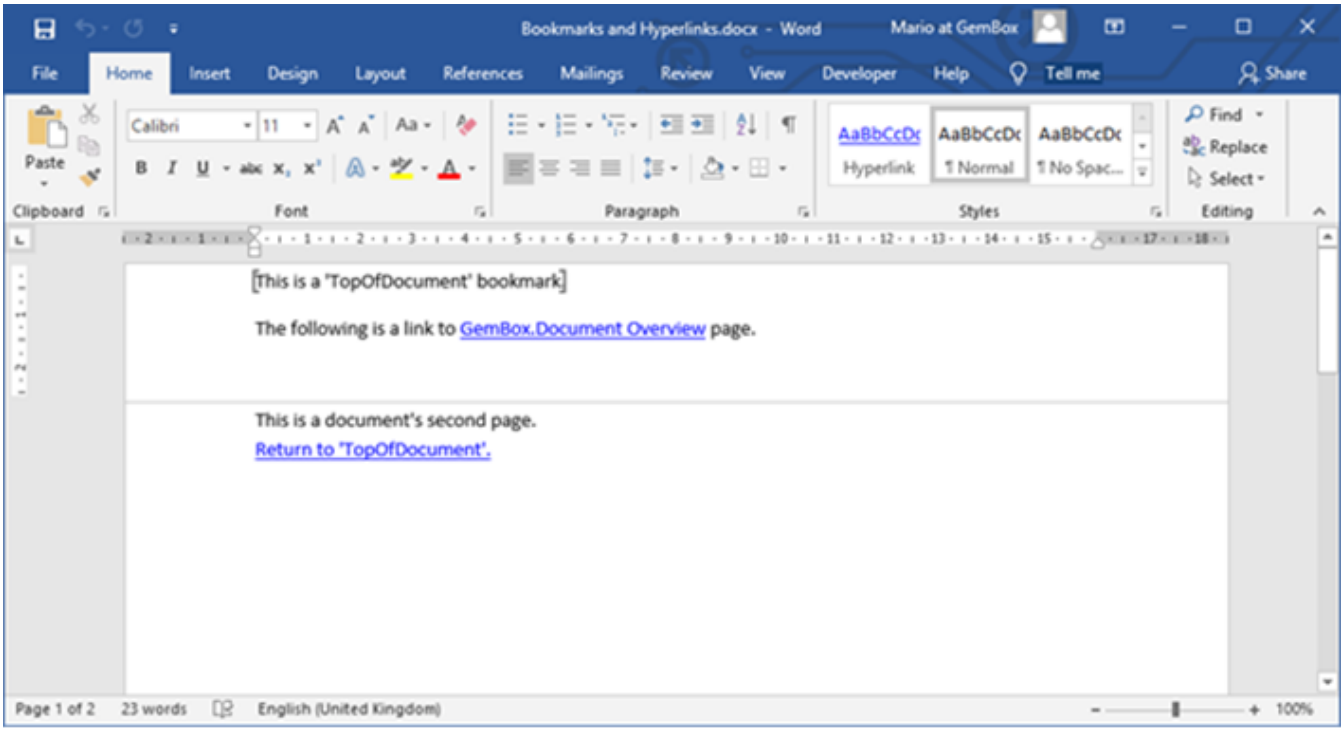
What is an URL?

Every website has its own online address, called a URL which stands for Uniform Resource Locator. When you are viewing a page on the World Wide Web, it is the long address that appears in the address bar at the top of your browser.

There are a few more different methods for locating the information on the Internet.

1. You may go directly to a Web page simply by knowing its location (for example you would like to visit the website of the company where you are applying for the job, and you are familiar with the exact address of their website).
2. The hypertext link emanating from a Web page provides built – in associations to the other pages that its author considers providing relevant information.

Figure 10. Bookmarks and hyperlinks. (Source: Own elaboration)



“Narrowcast” 'services can `push' pages at you that meet your user profile.

It is known that Google is the most famous online search engine in the world, but there are also many other options available. Furthermore, some of these alternative search engines are immensely popular in their own right – they just do not appear exceedingly popular when compared to Google. However, if you are not willing to trade privacy for convenience or have specific search needs, there are several alternatives to Google that offer more suitable search experience. Knowing the right search engine to make your query means you don’t spend your valuable time browsing through stuff you don’t need. One could easily get lost in the vast world of the internet without proper tools.

Here below we present you 15 search engines to try as alternatives to Google for better search results.

Most popular search engines

1. https://duckduckgo.com/	6. https://www.aol.com/	11. https://swisscows.com/
2. https://www.bing.com/	7. http://seznam.com/	12. https://startpage.com/
3. https://www.yahoo.com/	8. https://usearch.com/	13. https://www.ecosia.org/
4. https://yandex.com/	9. https://www.yippy.com/	14. https://www.naver.com/
5. https://www.ask.com/	10. https://www.searchencrypt.com/	15. https://www.baidu.com/

3.3. EMAIL

Electronic mail (email or e-mail) is a method of exchanging messages ("mail") between people using electronic devices. It is like traditional mail, but it also has some key differences.

For example: Traditional mail is addressed with the recipient ‘s name, street, address, city, state or province and zip code. E-mails are delivered electronically across the Internet. An e-mail includes a username, the @ (at) symbol, and the email provider’s domain. Usernames often include numbers and shortened versions of a name to create a unique email address, and will usually look like this: emarosa82@gmail.com

When you send an email to somebody, it arrives almost instantly and waits in the „inbox” until the recipient reads it. With email, there is a facility for adding pictures. However, before we go further with details, it is important to explain how to create an email account.

In order to start sending emails, you will need an email address which will be unique to you. To get this, you’ll need to sign up for an account with an email provider – you can choose among the various providers – Yahoo, Gmail, Hotmail, Outlook, GMX... It depends on your preferences and needs regarding the electronic mail. For example, if you need space and simplicity, Gmail is very suitable. If you just need a simple email program to send and receive mails, with few features, Yahoo can be a good choice. You may get information about each service provider by typing its name in the search box of the search engine and do the comparison.

Since Gmail was the most popular provider in 2020, I will now explain how to create a Gmail account (bear in mind that this methodology of creating an email may apply to almost all service providers).

Step 1. Type into your search engine www.gmail.com it'll take you to this page.
Click on „create account “, in the lower left corner and the following page will appear:

Figure 11. Google Sign in form

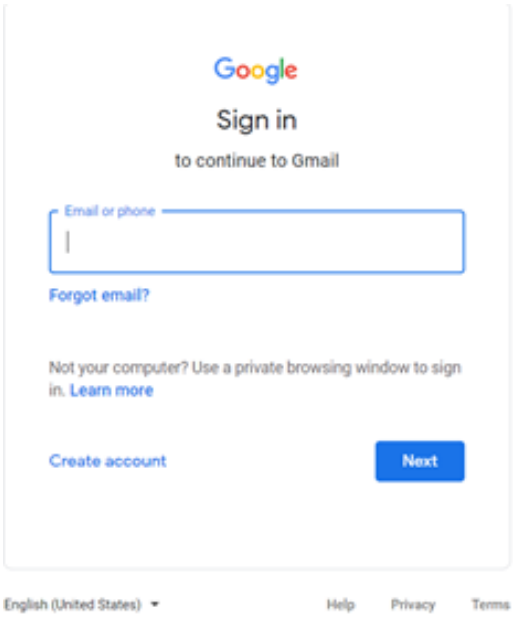
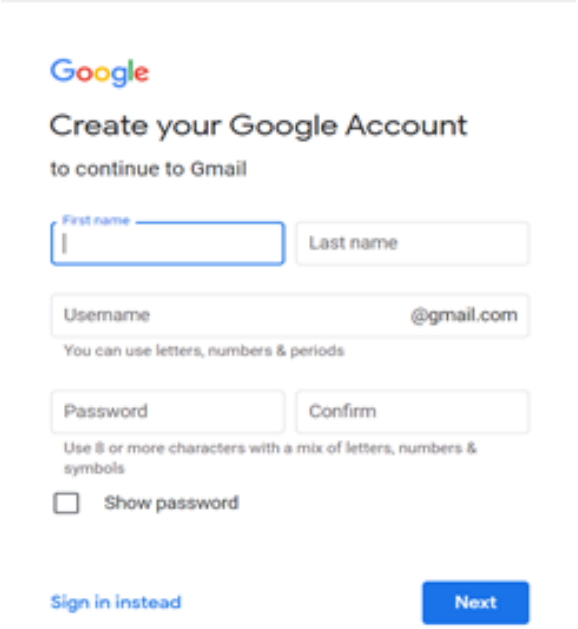
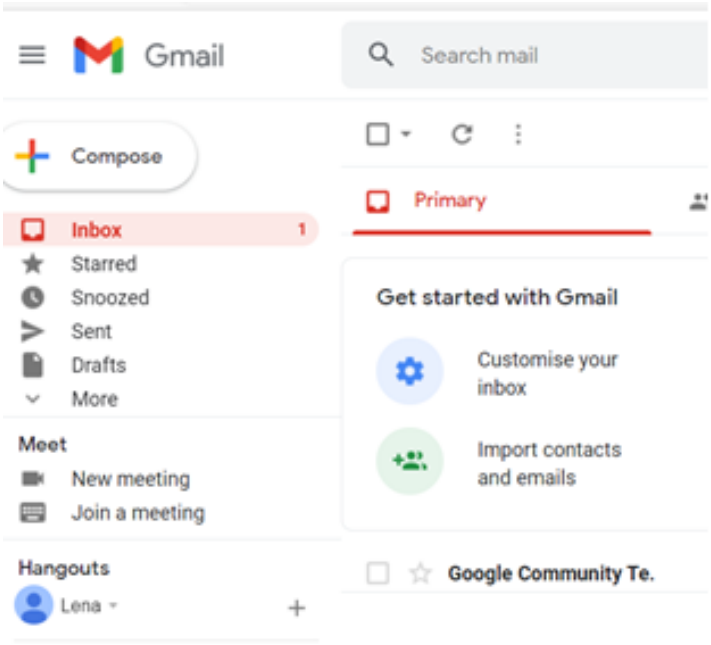


Figure 12. Form for account in Google creation



Type in your name, surname, username, and password. Be careful when choosing the right password, make sure that it is not going to be easy to guess it (avoid the date of your birthday for example because your family, friends and acquaintances might easily guess it and access your private mailing). You can make a combination of letters, numbers and signs in order to create a strong and reliable password for your account. After creating an account, you will be able to access the Gmail interface.

Figure 13. Gmail main page



As you can see, it is very user – friendly and intuitive. If you want to create an email, click on the „compose" button and one smaller window will appear on the lower right corner where you will need to type in the name (e-mail address) of the recipient and the subject of your email. The place for text is below the "subject" row.

On the bottom of the window, you will see a "send" button, as well as "paper clip" symbol if you would like to add some files to your e-mail or "insert emoji" if you would like to add smiling faces to your email. When you have composed your email, click on the "send" button and your email will be delivered to the desired email address and storage in the "sent" messages.

If you receive an email from someone, it will appear in your "inbox" as a bold, unread message. The most important messages might be marked with "star" and it will make it easier to find them by searching in the "starred" section.

3.4. SOCIAL NETWORKS

A social network is defined as a chain of individuals and their personal connections. Alternatively referred to as a virtual community or profile site, a social network is a website that brings people together to talk, share ideas and interests, or make new friends. This type of collaboration and sharing is known as social media.

Expanding one's connections with other people is a technique that can be used both for personal or business reasons. Social networking applications make use of the associations between individuals to further facilitate the creation of new connections with other people. This could be used to meet new friends and connect with old ones, as many people do on Facebook, or to expand one's professional connections through a business network like LinkedIn.

The process to create a new account for a social network differs for each social network. In general, visit the social network website of where you want an account and look for a "Sign Up," or "Create New Account," link. Follow the account creation steps to create your new account. You will likely need to provide your name, age range, and e-mail address at a minimum. Additional information may be required, depending on the requirements of the social network.
Be careful at the Privacy settings.

Also to be seen by companies and recruiters, you need to make sure you have a public profile. If you also use Facebook as a social network for leisure, you can change your privacy settings to restrict certain content to friends only and at the same time maintain a good public image, depending on the type of job you aspire to.

The top 10 social media platforms you need to care about in 2021

Pavadinimas	Nuoroda	Informacija
Facebook	www.facebook.com	The most popular social networking websites on the Internet. Facebook is a popular destination for users to set up personal space and connect with friends, share pictures, share movies, talk about what you're doing, etc.
Youtube	www.youtube.com/	An excellent network of users posting video blogs or vlogs and other fun and exciting videos.
Twitter	www.twitter.com	A very popular medium to communicate breaking news, digest bite-sized content. by using the hashtag you can filter the information to get the desired information.
Instagram	www.instagram.com	It is another widespread social network used by photography enthusiasts, as a leisure activity or for work. For those looking for work in creative fields, this social network is one of the most suitable.
Tik tok	www.tiktok.com	TikTok is a sort of visual karaoke, in which montages at the limit of science fiction become within everyone's reach, achievable directly with a few taps on their mobile phone. The Content that Works Best on TikTok: Entertaining, interesting, comedic and sometimes nonsensical short-form video content, usually set to the tune of popular songs. Think fun, catchy music-video style content.

Pavadinimas	Nuoroda	Informacija
Snapchat	https://www.snapchat.com	Snapchat still remains one of the most heavily used apps with the under 25 years of age demographic.Video-driven storytelling. If you have a knack for creating compelling (usually selfie-style) short videos that can entertain & educate a young audience, then Snapchat is a no brainer platform for you to form connections with your customers.
LinkedIn	www.linkedin.com/	It is the most famous professional social network. Professional "connections", look for work in the section dedicated to job offers and send your application direct, share public information on your personal page, videos, images or various documents as a way to get noticed by companies, many discussion groups and forums that you can join and have the opportunity to exchange opinions.
Pinterest	www.pinterest.com	Pinterest has become a very popular social bookmarking tool for saving ideas and finding creative inspiration when it comes to everything from cooking to DIY home projects, vacation ideas, interior design, business and everything in between.
Reddit	www.reddit.com	Community of registered users (redditors) submits content that is upvoted by the community. Reddit has a subreddit (board) for almost every category.
Google+	https://plus.google.com/collections/featured	It is a social network in which you can become part of "circles", that is to say, groups that talk about a certain topic and choose the one that interests you. In your profile you can add the addresses of other social networks in which you are registered.

3.5. BUSINESS SOFTWARE

Business software is in many cases either a fuel for the success of the business or a necessary tool for a wide range of business operations. Therefore, basically all positions of most businesses that exist, require at least basic knowledge and proficiency in most commonly used business tools.

We won't cover the basic software that any digitally literate person must know and operate, as it's already been covered in our previous chapter. The aim of this chapter is to better explain the generic set of tools and group them into most commonly used ones regardless of the industry.

It's worth mentioning that many software and tools that businesses use are both installed on a computer as a standalone program or it can be accessed via online tools, which is becoming an ever growing industry - SaaS. SaaS stands for "Service as a Software", which is usually a paid access to certain online.

The kind of software and set of tools businesses are using, mostly depends on the industry they operate in, the type of the customers they service - either other business or regular customers, as well as the size of the company. Small companies usually do not depend much on a wide range of tools that are essential to bigger corporations. Nevertheless, the success of any company depends much on skills and experience their employees possess, especially in using digital tools.

List of commonly used digital tools:

Remote conferences	„Zoom“, „Skype“, „Google Hangouts“
Marketing and advertising	Facebook Ads, Google Local Business and Maps, Google Ads, Linkedin Ads
Emailing, automated replies and follow-ups	„Mailchimp“, „MailerLite“, „Woodpecker“
Marketing automation and CRM	„Hubspot“, „Salesforce“
Project management, planning and efficiency	„Trello“, „TeamGantt“
Collaboration and communication	„Slack“, „Microsoft Teams“, „Asana“
Website performance monitoring and optimisation	„Google Analytics“, „Hotjar“, „Google Optimize“
Email accounts and many of the above	Google Workspace“
Cloud Storage	„Google“ diskas, „Dropbox“
Data flow, reporting automation and integration of tools	„Zappier“, „Supermetrics“, „Google Data Studio“
Electronic agreement and documents signing	„DocuSign“, „Docobit“
File sharing and transferring	„WeTransfer“
Writing assistant	„Grammarly“.

This list doesn't cover all the great tools businesses are using in their everyday activities, there are way more tools, dedicated for more niche and unique purposes to different kinds of business.

3.6. WEBSITES DEVELOPMENT, BLOGGING AND MARKETING

Websites are without doubt the most important element of the internet.

The central page of a website is called a home page. This is usually the first page you see when you call a website up and can also be called a 'start page' or 'index page'. From here onwards, the user delves into the site's subpages.

A digital web presence enables content such as texts, images, and videos to be displayed on the internet.

Depending on the size of the website, site visitors have the opportunity to access the website's subpages:

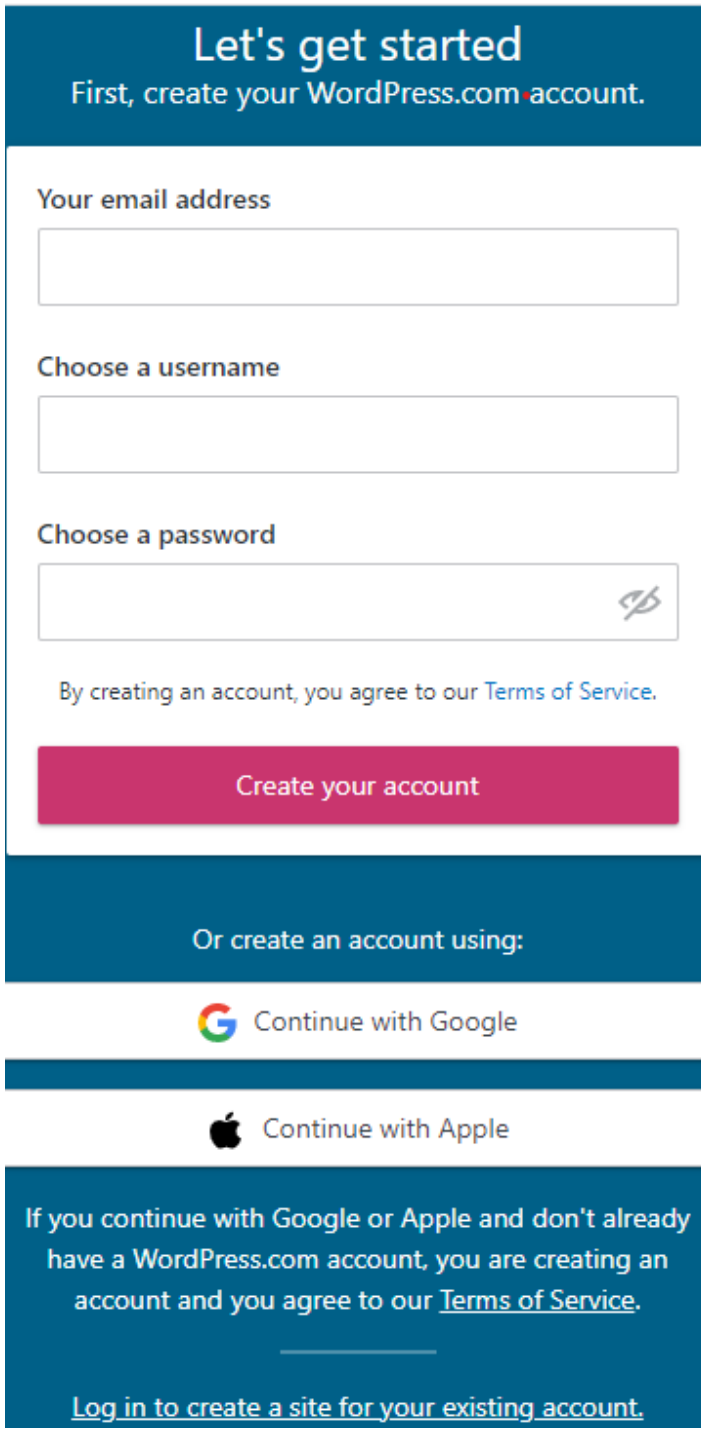
- Hyperlinks, or simply 'links' are used to connect single HTML documents of a website. Links to important subpages (e.g. departments, product categories, or representative information pages) are usually combined in the navigation and can be found in the header of the website.
- They are displayed on every subpage of the website and not just on the home page. The navigation helps the user to orientate and see an overview of the website's structure.
- Links to more subpages can also be placed in the text and image elements in the website's content.
- The footer at the bottom of a page often contains links to further information like the site owner and the legal framework.

Creating a free website using WORDPRESS

WordPress.com is the first solution to consider to create a free website using the famous CMS. This platform allows you to create your own website with a third-level domain (www.namewebsite.wordpress.com) by making a storage space of 3 GB available.

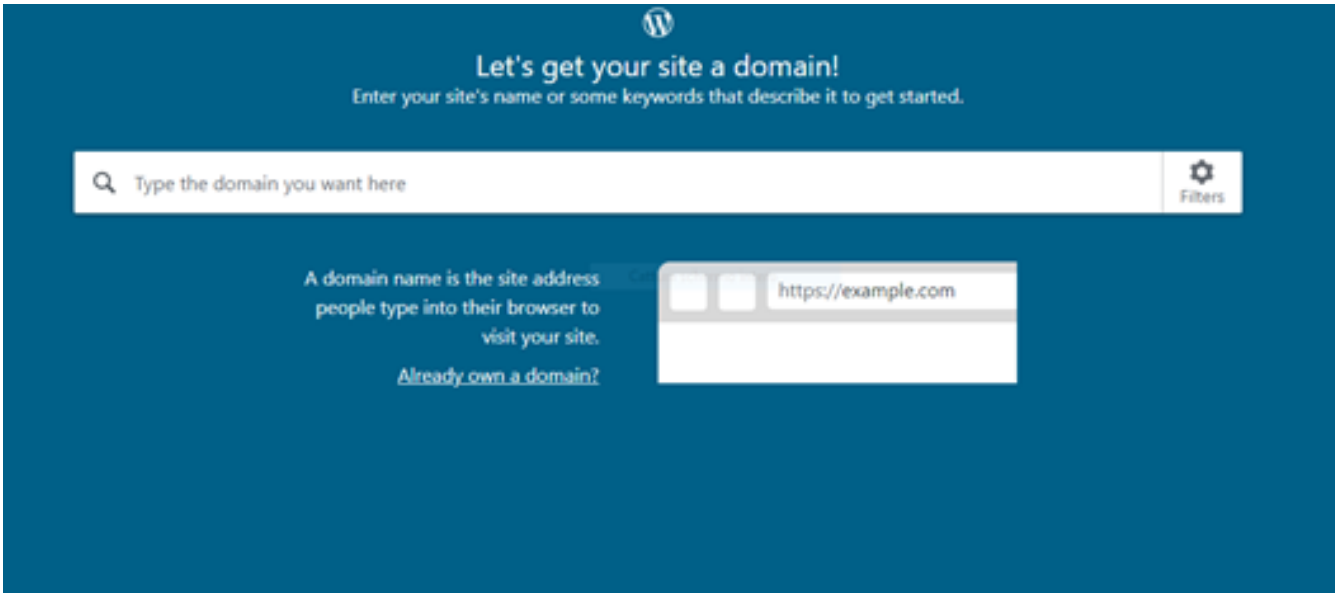
Go to the home page https://wordpress.com/, click on the Create your account. Subsequently, indicate in the appropriate text field the address free of charge.

Figure 14. Creating a wordpress account



Then, enter the name you want to show in your website's domain in the “Enter a name or keyword field” and click the Select button for the Free option. In the new open page, press the Start with free button, enter the required data in the fields Your e-mail address, Choose a username and Choose a password, click on the Continue button twice in a row and you're done.

Figure 15. Entering a domain name



Now, press the View site button to look at your website built with WordPress.com. To add new pages and articles, click on the Add button relating to the Site Pages and Blog Articles options, while selecting the Customize item in the left sidebar you can change the look and feel and choose another free theme available. Select one of the many templates available: to do so, click on the preview of the one you are interested in and click on the Apply button, to apply it directly to the site you have created; or click on the Customize button if you want to modify it a little.

To add new pages or new posts to the site, instead, click on the words Pages or Posts (on the left) and click on the (+) New page or (+) New post button located at the top left. In the screen that opens, you can create a new page or a new post by typing its title and body in the appropriate text fields. Using the buttons in the toolbar located at the top, you can also format the text, insert links, images, etc. By clicking on the Preview and Publish buttons, however, you can preview the content and publish it.

While running a website via Worpress.com hosting solution is easy and convenient, especially for the beginners, it is sometimes more suitable to choose a fully customisable approach for a website building and host it by yourself. You would need to purchase a hosting plan from one of many hosting service providers and install Wordpress CMS using a range of tools provided by the host.

As Wordpress is a platform, originally created for bloggers, it grew in popularity to being number one choice for all sorts of individual websites developers and also businesses. It supports a wide range of tools and plugins, which enable Wordpress to be adapted to e-commerce, forums, auctions or even social media platforms. Wordpress professionals see it rather as a very well optimised core for any kind of online project development on top of it, with original Wordpress components stripped off.

There are many alternative CMS platforms for Wordpress and among the most popular ones are Joomla, Drupal as CMS platforms, while Wix.com, Shopify.com are web platforms and packages of services, dedicated for particular needs, such as e-commerce and other.

Figure 16. Some of the most popular CMS platforms

To finalize, it's worth emphasizing that a truly successful website is usually the one which provides real value to website visitors - internet users. One way of providing value may be quality content creation by being able to write interesting and engaging articles and stories, therefore storytelling skills come in handy while creating any kind of content on the internet. We prepared a few tips for a successful storyteller in the following chapter by introducing what personal storytelling is and these skills may be useful.

3.7. PERSONAL STORYTELLING

Storytelling is the ability to captivate someone or a group of people with an engaging narrative that influences them and makes them feel like they were a part of the story. People remember stories much better than facts and figures. It is one of the most important skills you can learn to master.

Key points:

1. Storytelling influences change at individual practice as well as organisational level
2. Listening to stories facilitates better person-centred care and can lead to improved services
3. Hearing personal stories engenders greater understanding, empathy and reflection
4. Rapport, trust and care can be nurtured in practitioner-service user relationships through storytelling
5. Personal storytelling benefits the teller as it can empower, encourage personal growth and build resilience

Why is storytelling valuable to the storyteller?

Reframes self-identity and encourages personal development

Evidence suggests that the process of personal storytelling enables the concept of self and the life story to connect in a way that facilitates a reframing of identity and encourages personal growth. On imparting a story, an individual expresses the significant events in their own words and in their own time, and is empowered to reflect. The process enables new awareness and new meanings of the self to emerge.

Is a relationship that co-produces meaning

The storytelling relationship involves a listening and engagement that is different to that of a performer-audience or interviewer-participant. It is a relationship that bridges the divide between the person and those providing support, eg practitioner-service user.

Promotes resilience

Resilience involves a willingness to turn negative emotions involved in disruptive life events into something strengthening and empowering. Resilience is developed by a process of reflection on meanings, which enables emotional insights. The support of peer and other networks is key to forming bonds and feeling connected to other people. The combination of these factors results in a strength in people, which is based on the premise that life experiences (including negative experiences) offer opportunities for personal growth.

Is therapeutic

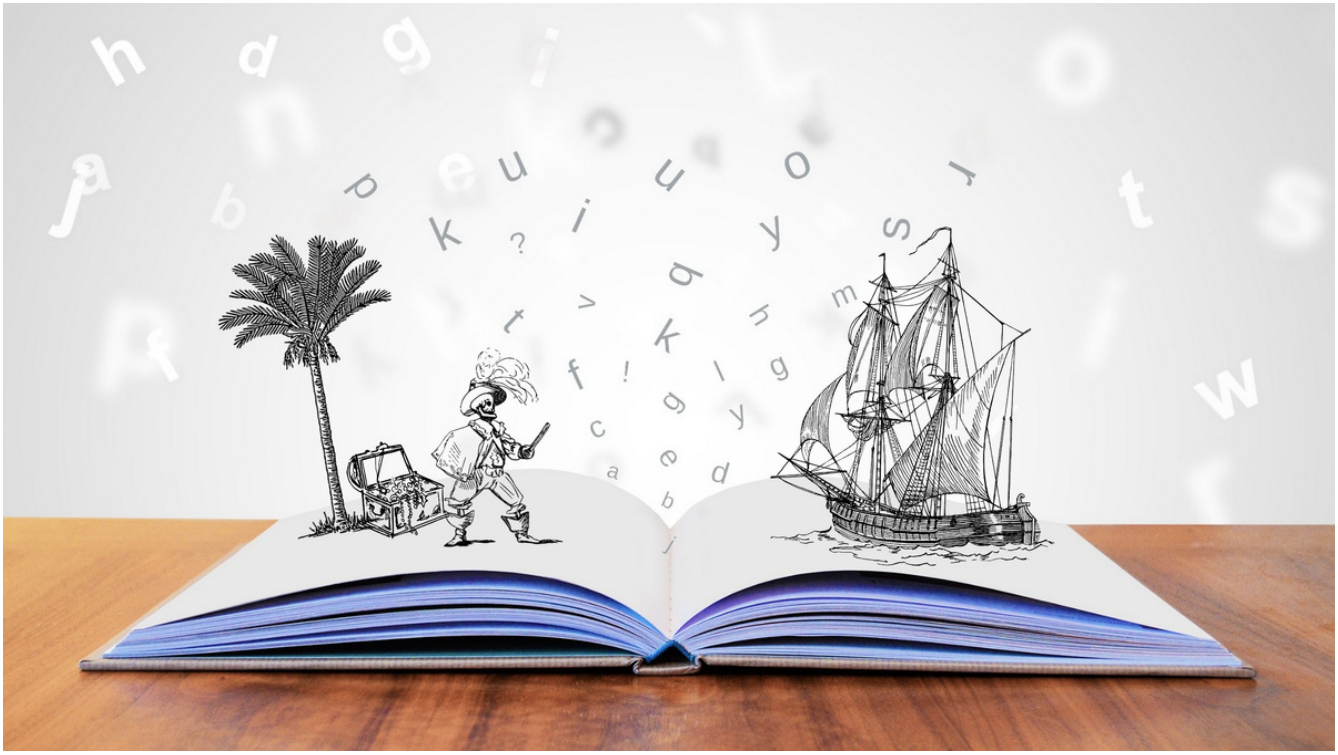
The therapeutic value of telling a story is often reported in storytelling work (Hardy, 2007; Scottish Recovery Network, 2012). While concern for individuals' well-being in storytelling is often expressed and some tellers have reported a degree of upset in relaying their story, it is recognised that, for the most part, the positives of telling their story far outweigh any emotional distress encountered. It is more often that the act of telling a story and reflecting on it has a cathartic effect and is a catalyst to recovery.

Storytelling techniques

The best storytellers are able to make narrative choices useful to move their stories forward, to involve the target audience through the dissemination of important information, to maintain attention, they know how to refer to their life experiences to give emotion to the text.

You should also be able to intimately get in touch with yourself, to the point that words and emotions become a single entity, capable of arousing awareness and reflections among the interlocutors.

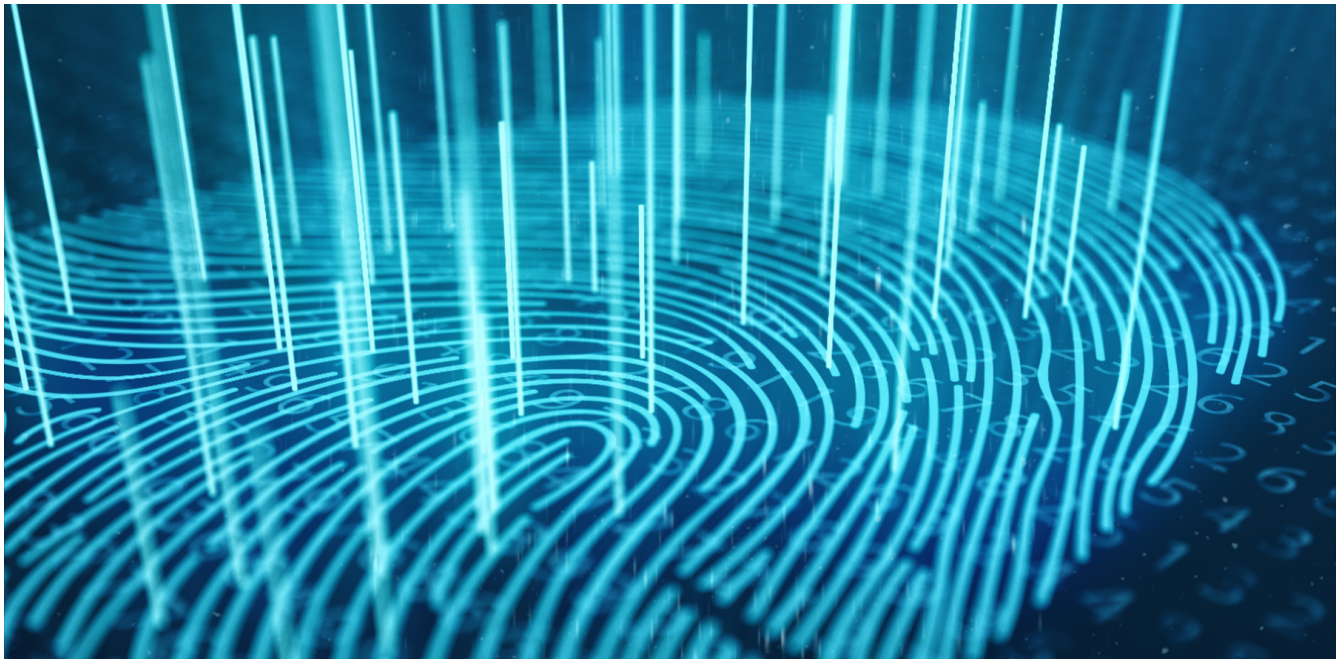
The latter represent the target, which is a group of potential customers to whom a company wants to sell its products or services, and will have to "fall in love" with the idea and the story being told. Storytelling can be adapted for any area that needs to be supported from a communicative point of view: a company, a product, a service, a brand, a person or an event.



3.8. E-SIGNATURE AND E-SERVICES

Electronic signatures

Electronic signatures deliver a way to sign documents in the online world, much like one signs a document with a pen in the real (offline) world. In the past, only hand-written signatures were legally valid. The Directive on a Community framework for electronic signatures (eSignatures directive), adopted in 1999, extended that recognition to electronic signatures. A reliable system of electronic signatures that work across the EU countries is vital for safe electronic commerce and efficient electronic delivery of public services to businesses and citizens. The eSignature Directive established the legal framework at European level for electronic signatures and certification services. The aim is to make electronic signatures easier to use and help them to become legally recognized within the EU Member States.



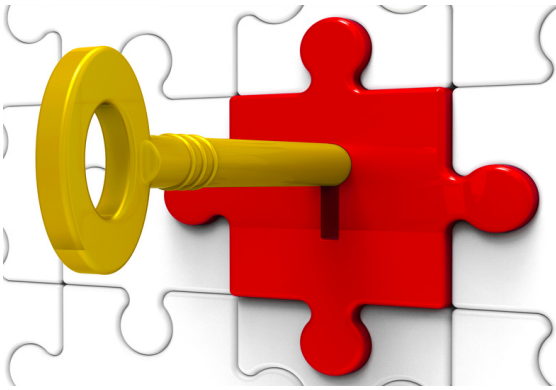
Definition of electronic signatures vary depending on the applicable jurisdiction. A common denominator in most countries is the level of an advanced electronic signature (an e-signature that meets the requirements set forth the EU regulation) requiring that:

1. Authenticity: The message originates from the given sender and the sender and the sender can be uniquely identified.
2. Integrity: Manipulation of the signature of the signed document can be detected immediately.

With the invention of the mobile phone signature, tools were designed to sign legally binding documents, invoices, and contracts electronically. It is possible to add an electronic signature to the PDF document quickly and securely, which is the legal equivalent of a handwritten signature. The authenticity of the signature and genuineness of the transmitted data can be verified at any time by sender or recipient.

Digital signature

Digital signatures present cryptographic implementations of electronic signatures used as a proof of authenticity, data integrity and non-repudiation of communications conducted over the internet. When implemented in compliance to digital signature standards, digital signing should provide end-to-end privacy with the signing process being user-friendly and secure. Digital signatures are generated and verified through standardized frameworks such as the Digital Signature Algorithm (DSA).



There are typically three algorithms involved with the digital signature process:

1. Key generation – this algorithm provides a private key along with its corresponding public key.
2. Signing – this algorithm produces a signature upon receiving a private key and the message that is being signed.
3. Verification – this algorithm checks for the authenticity of the message by verifying it along with the signature and public key.

The process of digital signing requires that the signature generated by both the fixed message and private key can then be authenticated by its accompanied public key. Using these cryptographic algorithms, the user's signature cannot be replicated without having access to their private key. A secure channel is not typically required. By applying asymmetric cryptography methods, the digital signature process prevents several common attacks where the attacker attempts to gain access through the following attack methods.

Biometric signature

Electronic signature may also refer to electronic forms of processing or verifying identity through use of biometric "signatures" or biologically identifying qualities of an individual. Such signatures use the approach of attaching some biometric measurement to a document as evidence. Biometric signatures include fingerprints, hand geometry (finger lengths and palm size), iris patterns, voice characteristics, or even retinal patterns. All of these are collected using electronic sensors of some kind. Because each of these physical characteristics has claims to uniqueness among humans, each is to some extent useful as a signature.

Figure 17. electronic signature application. (Source: https://bit.ly/2ZdPQmX)

Five most popular e-sign services:

1. „eSignly“

It is a leading e-signature solution for millions of users all around the world for the ease it provides in document signing and management. The app offers several features like in-person signing, scheduled signing, self-signing, team management, top-grade security, integration with popular work applications, audit trail etc.

2. „PandaDoc“

It is available for both Android and iOS mobile platforms. The online software is an award-winning electronic signature software that has an easy-to-use user interface.

3. „Adobe Sign“

It is available on both the iOS and Android mobile platforms. Adobe is a common name in the graphics world and as such, it said to be one of the pioneers in eSign services. The software is feature rich giving the user the power to manage continuous workflows from any location or device.The app has both the digital and electronic signatures.

4. „SignEasy“

It is another electronic signature software that is compatible with the Android and iOS platforms. SignEasy is not a heavy signature application because it offers a minimal user interface with the intention of making it easy to use. Signing using SignEasy accommodates self-signing, remote signing, as well as in-person signing.

5. „RightSignature“

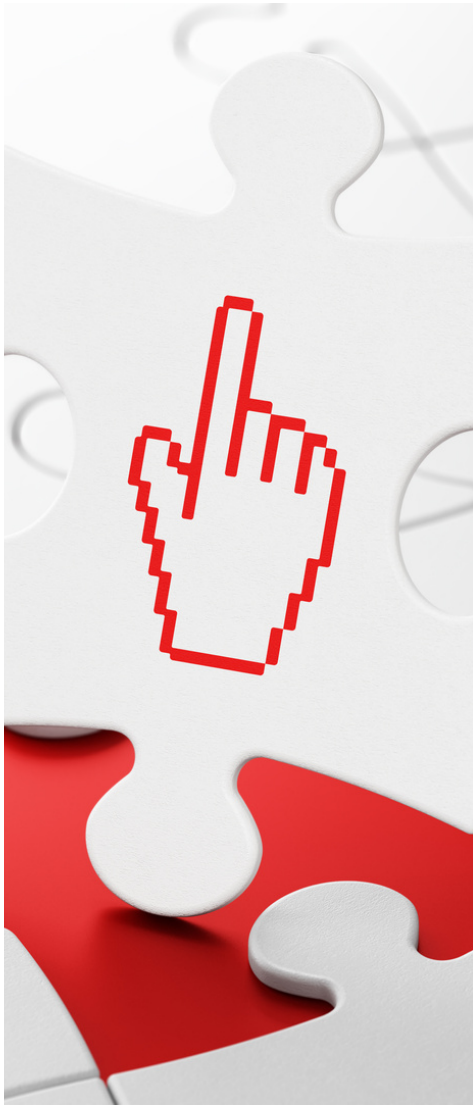
This mobile application uses the Android and iOS platforms. This e signature app uses speed to impress its users, as documents come in faster when sending and receiving for signatures. With it, you can upload, format, and send documents in the shortest time possible.

Adding or removing an electronic signature from a Microsoft Word or Adobe

Using an e-signature line in a Word document, you can request information about the signer and provide instructions. When an electronic copy goes to the signer, this person sees the signature line and a notification requesting their signature. The signer can:

1. Type a signature
2. Select a picture of an inked signature
3. Write a signature by using the inking feature on a touchscreen computer or other device

How to create a signature line in Word or Excel (Office 365 or 2019):



1. In the document, place your cursor where you want a signature line.

2. On the Insert tab in the Text group, click the Signature Line list. Then, click Microsoft Office Signature Line.

3. In the Signature Setup dialog box, type the information that will appear beneath the signature line:

- Suggested signer: the signer's full name
- Suggested signer's title: the signer's title, if any
- Suggested signer's email address: the signer's email address, if needed
- Instructions to the signer: instructions for the signer, such as "Before signing the document, verify that the content is correct"

4. Select one or both of the following checkboxes:

- Allow the signer to add comments in the Sign dialog box: The signer can type in the purpose for signing.
- Show sign date in signature line: The date the document was signed will appear with the signature.

In addition, you can remove a signature by clicking the arrow next to the signature in the Signature Pane and then clicking Remove Signature.

Alternatively, you might require an electronic signature in a PDF document. See the next section for how to use e-signatures in PDF files.

Electronically signing a PDF file

Adobe's Portable Document Format (PDF) is a common format for fixed-layout documents. Like Word, Adobe PDF has added a range of capabilities since it was introduced to the market in 1993. It's now possible to electronically sign a PDF file for authentication.

If you're a Windows user, you're probably familiar with PDF readers. They are computer programs that allow you to open PDF files, that is, files with the .pdf file extension. The most popular option these days is Adobe Acrobat Reader.

To add an electronic signature to a PDF, follow these steps:

1. Open the PDF file in Adobe Acrobat Reader.
2. Click on Fill & Sign in the Tools pane on the right.
3. Click Sign, and then select Add Signature.
4. A popup will open. Select an option — Type, Draw, or Image.
5. Click the Apply button.
6. Drag, resize, and position the signature inside your PDF file.

E-services

E-service (or eservice) is a highly generic term, usually referring to 'The provision of services via the Internet (the prefix 'e' standing for 'electronic', as it does in many other usages). E-services include all services and activities that are created by means of computers and offered and executed interactively via electronic media, such as the Internet.

E-services can be information and educational services such as e-education, e-learning, e-teaching, e-publishing, e-book, e-zine and e-catalog, procurement, trade and ordering services such as e-business, e-commerce, e-procurement, e-cash, e-shop, e-intermediary, e-auction, cultural and administrative services such as e-culture, e-government or e-vote, improvement of marketing, product or customer relationship services, electronic consulting services such as e-consultancy or e-advising, security-related services (e-security), production, scientific or logistic services.

E-services will be used in many other applications in the future.

How do you use e-services?

To use the services, you must first register as a new user on top of any page.

1. You will select the “Register” link and complete the required fields.
2. On registration you will receive a confirmation that you have been registered, which will enable application for any government service online.

3.9. SECURITY SOFTWARE

Any connected device may be a gateway for a security threat. The best way to secure a device, especially one connected to the internet, is to use proper and up to date security software, usually known as antivirus.

Extra layer of personal data security and both to the information transferred over the internet or the device itself may be provided by a special set of tools called VPNs, which stand for Virtual Private Network.

When browsing or especially making financial transactions while being connected to unsecure WiFi, people may expose themselves and their sensitive data to a security threat.

Antivirus tools and services usually provide a set of tools that are monitoring the internet traffic, scanning the files and trying to reveal potential security threats even of unknown viruses. Such tools would help to avoid malvertising, block potentially harmful websites and use other solutions to secure the user's device and information.

VPNs tools help to connect to the internet via a secured remote server, which hides the users' original IP address allowing the users to encrypt their traffic and disguise their online identity. This way anonymity and security is increased while browsing using public WiFi hot-spots or other unsecure network connections.

Some antivirus software may provide a VPN service as well.

Most commonly used antivirus software is the following:

- Avira
- Avats
- McAfee
- ESET
- Bitdefender
- AVG
- Kaspersky
- Microsoft security essentials
- Norton

Most commonly used VPN tools:

- Nord VPN
- Express VPN
- Surfshark
- Tunnelbear

3.10. PHYSICAL DEVICE SECURITY AND HARDWARE

We all know how annoying it is to lose a phone, get it stolen or simply drop it on the ground and get it's screen broken to a level the device becomes unusable. The issue is usually not considered as important until it happens. In order to avoid all sorts of damage to a device. Speaking about physical security, we assume that any device might suffer from physical damage of falling, hardware failure, water damage or might be lost or stolen.

We compiled a list of ways and solutions how losses might be avoided by using simple security of a physical device techniques:

Password or encryption

Avoid losing information due to theft attempts. Use a strong password, fingerprint or other biometric data to protect access to your device, both mobile phone and desktop. Avoid using the same password everywhere and password lock or encrypt important files. Enable built-in or installed tracking software that some vendors provide to be able to track your device using location services, even if it is locked when lost or stolen.

Backup

Always backup important files, store them in CDs or memory sticks or even in 3rd party cloud storage.

Common sense

Don't tempt thieves with unattended mobile devices, particularly in public places. Do not leave your laptop bag in the car, unattended in a cafe, airport or other public places.

Updates

Keep your software and devices up to date, install updates to the operating system when prompted.

Act quickly

Depending on the situation, if the device is lost, do not panic, start by changing your password to the most important systems, inform your supervisor or IT if the business device was lost and if necessary inform the police.

Selling

If you are selling an old device, a phone, tablet or a computer, make sure all your personal information is permanently deleted from the hard drive or memory of the device. You can use special software such as Eraser, File shredder or WipeFile or other similar tools.

3.11. INTERNET OF THINGS (IOT)

The idea of inter-connected devices where the devices are smart enough to share information with us, to cloud based applications and to each other (device to device).

Smart devices or “Connected devices” as they are commonly called, are designed in such a way that they capture and utilize every bit of data which you share or use in everyday life. And these devices will use this data to interact with you on a daily basis and complete tasks.

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

This new wave of connectivity is going beyond laptops and smartphones, it’s going towards connected cars, smart homes, connected wearables, smart cities and connected healthcare. Basically, a connected life.

These devices will bridge the gap between the physical and digital world to improve the quality and productivity of life, society and industries. With IoT catching up Smart homes is the most awaited feature, with brands already getting into the competition with smart appliances.

Wearables are another feature trending second on the internet. With the launch of Apple Watch and more devices to flow in, these connected devices are going to keep us hooked with the interconnected world.

10 Real World Applications of Internet of Things (IoT) – Explained in Videos

Application	Explanation	Video link
1. Smart Home	Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones. Smart Home products are promised to save time, energy and money	https://youtu.be/NjYTzvAVozo
2. Wearables	Wearable devices are installed with sensors and softwares which collect data and information about the users. This data is later pre-processed to extract essential insights about the user. These devices broadly cover fitness, health and entertainment requirements. The prerequisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized.	https://youtu.be/h8-TAqzYrno
3. Connected Cars	The automotive digital technology has focused on optimizing vehicles internal functions. But now, this attention is growing towards enhancing the in-car experience. A connected car is a vehicle which is able to optimize its own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity. Most large automakers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.	https://youtu.be/0HxZuQ0woLY

Application	Explanation	Video link
4. Industrial Internet	Industrial Internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines. According to Jeff Immelt, CEO, GE Electric, IIoT is a "beautiful, desirable and investable" asset. The driving philosophy behind IIoT is that smart machines are more accurate and consistent than humans in communicating through data. And, this data can help companies pick inefficiencies and problems sooner. IIoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency. According to GE, the improvement of industry productivity will generate $10 trillion to $15 trillion in GDP worldwide over next 15 years.	https://youtu.be/8NGzrtK7eV0
5. Smart Cities	Smart city is another powerful application of IoT generating curiosity among world's population. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities. IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied. By installing sensors and using web applications, citizens can find free available parking slots across the city. Also, the sensors can detect meter tampering issues, general malfunctions and any installation issues in the electricity system. To understand better the functioning of Smart Cities check out this video.	https://youtu.be/Br5aJa6MkBc

Application	Explanation	Video link
6. IoT in agriculture	With the continuous increase in the world's population, demand for food supply is extremely raised. Governments are helping farmers to use advanced techniques and research to increase food production. Smart farming is one of the fastest growing fields in IoT. Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT. If you are curious, the video below explains further about this concept. Read more to know the latest about IoT in agriculture.	https://youtu.be/q0FnMD2_0Fw
7. Smart Retail	The potential of IoT in the retail sector is enormous. IoT provides an opportunity to retailers to connect with the customers to enhance the in-store experience. Smartphones will be the way for retailers to remain connected with their consumers even out of store. Interacting through Smartphones and using Beacon technology can help retailers serve their consumers better. They can also track consumers' paths through a store and improve store layout and place premium products in high traffic areas. Watch this video to find out how connected retail will make your life easier. Read more to know the latest technology changing the face of retail.	https://youtu.be/gUcuqhduWao
8. Energy Engagement	Power grids of the future will not only be smart enough but also highly reliable. Smart grid concept is becoming very popular all over the world. The basic idea behind the smart grids is to collect data in an automated fashion and analyze the behavior of electricity consumers and suppliers for improving efficiency as well as economics of electricity use. Smart Grids will also be able to detect sources of power outages more quickly and at individual household levels like nearby solar panel, making possible distributed energy system. Here's a video to explain how a smart grid operates.	https://youtu.be/JwRTpWZReJk

Application	Explanation	Video link
9. IOT in Healthcare	Connected healthcare yet remains the sleeping giant of the Internet of Things applications. The concept of a connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness. The video below explains how IoT can revolutionize treatment and medical help.	https://youtu.be/8AkXW9EPFJg
10. IoT in Poultry and Farming	Livestock monitoring is about animal husbandry and cost saving. Using IoT applications to gather data about the health and wellbeing of the cattle, ranchers knowing early about the sick animal can pull out and help prevent a large number of sick cattle. With the help of the collected data and ranchers can increase the poultry production. Watch this interesting video.	https://youtu.be/eZ2sVriiluU

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

EXAMPLES, CASE STUDIES AND PRECAUTIONS TO DEVELOP RESILIENCE AGAINST

4.1. PRIVACY BREACHES AND THEFT OF DATA

What is data privacy breach?

1. A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach.
2. A privacy breach occurs when someone accesses information without permission. It starts with a security breach — penetrating a protected computer network — and ends with the exposure or theft of data. That data may include personally identifiable information such as your name, address, Social Security number, and credit card details.

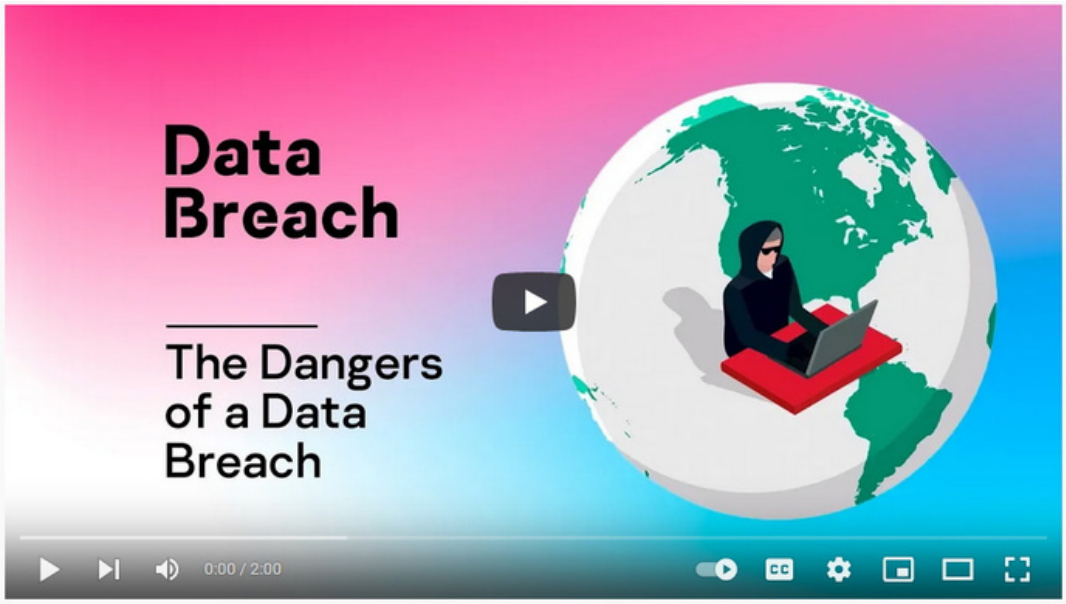
What are your privacy risks?

1. Privacy relates to any rights you have to control your personal information and how that information is used. Your information is in a lot of places. That includes government agencies, health care organizations, financial institutions, social network platforms, computer-app makers, and many other places.
2. Your information has value. That's why cybercriminals often target organizations where they can harvest personal data. They can use it to commit crimes like identity theft or sell it on the dark web.
3. Another similarity between privacy breaches and data breaches? There's not much you can do to prevent them. The security of your information is in someone else's hands. Even so, there are things you can do to help protect yourself.

How to prevent a data breach?

1. Create complex passwords. Use different ones for each account, and change your passwords if a company you've recently interacted with gets hacked.
2. Use multi-factor authentication when available. This allows access only after two or more pieces of evidence are presented—usually a password and a code that is sent to the user by phone, text or email during login.
3. Shop with a credit card. You may have less liability for fraudulent credit card charges.
4. Watch for fraud. If you receive a notice about the data breach, call the company to confirm that it's legitimate, using a number you know to be valid rather than a number that may be listed on the notice.
5. Guard against identity theft. Globally, 65% of data breaches result in identity theft, making it the most common outcome. If you become an identity theft victim, contact each credit card company to set up fraud alerts and freeze your accounts. Then get in touch with your local Social Security office for next steps.
6. Set up account alerts. You may be able to receive notifications of suspicious purchases or those that exceed a certain dollar amount. This may give you a heads-up that you've been hacked.

Video: The Dangers of a Data Breach https://www.youtube.com/watch?v=0kK902-ZvNM



4.2. HACKING AND CYBER EXTORTION

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.

Cyber extortion is an internet crime in which someone holds electronic files or your business data hostage until you pay a demanded ransom.

Video: Cyber Extortion https://www.youtube.com/watch?v=UNCBuFJRrYk

The negative financial impact of cyber attacks can be mitigated by cyber risk insurance. It is especially relevant for businesses that have a large IT farm and/or manage large personal databases. Many insurance companies provide these services in Lithuania. The main idea of such insurance is that as companies become more and more dependent on IT systems and data security, and as the number of crimes in the digital space grows, it is possible to get the company's property and civil liability for a certain premium insured.

Insurance companies usually offer to cover not only losses related to damage to the company's assets due to cyber attacks but also losses caused by the leakage of personal data of third parties stored by the company.

The best example of this is the case with the Lithuanian car-sharing company City Bee when 110,000 user data was kidnapped, find more at https://www.euronews.com/2021/02/17/thousands-of-citybee-users-have-their-personal-data-leaked-online.

More on cyber risk insurance: https://youtu.be/F7mYEm-kx-Q (available only in Lithuanian)

4.3. IDENTITY THEFTS

Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation.

Identity theft occurs when someone steals your personal information and credentials to commit fraud. There are various forms of identity theft, but the most common is financial. Identity theft protection is a growing industry that keeps track of people's credit reports, financial activity, and Social Security number use.

Video: What is Identity Theft? https://www.youtube.com/watch?v=kDFeSUUwRnA

Tapatybės vagystės tipai

Financial identity theft	Someone uses another person's identity or information to obtain credit, goods, services, or benefits.
Social Security identity theft	If identity thieves obtain your Social Security number, they can use it to apply for credit cards and loans.
Medical identity theft	Someone poses as another person to obtain free medical care.
Synthetic identity theft	A criminal combines real (usually stolen) and fake information to create a new identity, which is used to open fraudulent accounts and make fraudulent purchases.
Child identity theft	Someone uses a child's identity for various forms of personal gain.
Tax identity theft	Someone uses your personal information, including your Social Security number, to file a bogus state or federal tax return in your name and collect a refund.
Criminal identity theft	A criminal poses as another person during an arrest to try to avoid a summons, prevent the discovery of a warrant issued in their real name, or avoid an arrest or conviction record.

Video: Watch Out These 8 Types of Identity Theft -
https://www.youtube.com/watch?v=EZa2um76rFY

Identity Theft Protection

One way is to continually check the accuracy of personal documents and promptly deal with any discrepancies. There are several identity theft protection services that help people avoid and mitigate the effects of identity theft. Typically, such services provide information helping people to safeguard their personal information; monitor public records and private records, such as credit reports, to alert their clients of certain transactions and status changes; and provide assistance to victims to help them resolve problems associated with identity theft. Some government agencies and nonprofit organizations provide similar assistance, typically with websites that have information and tools to help people avoid, remedy, and report incidents of identity theft. Many of the best credit monitoring services also provide identity protection tools and services.

To prevent personal data theft, you need to:

- Secure all documents with personal information, such as driver's license, passport, bank statements, utility bills, etc.;
- Destroy old or unnecessary documents that show a person's name, address, or other personal information;
- Monitor your credit history report and regularly check your credit card and bank account statements for completed transactions;
- When changing the place of residence, inform your bank, credit card, mobile communication, TV/internet service provider, and other service providers about the change of address so that messages and letters with personal information do not reach other persons;
- Remember that the less information a person provides about himself, the lower the risk of the information falling into the wrong hands;
- When buying goods online, choose a secure website that displays the company's contact information, a clear privacy policy, guarantee of goods and services, and returns;
- When choosing an e-mail trading website, make sure that it applies encryption of the data sent (proper and valid SSL certificate), and check that the website address starts with HTTPS.

4.4. CYBERBULLYING

Cyberbullying can be defined as an aggressive, intentional and repeated act carried out by a group or individually, performed via electronic means such as mobile phones or the internet, against a victim who cannot easily defend himself or herself (Slonje, Smith and Frisén, 2013).

Bullying, in general, is separated from other aggressive behaviors based on two aspects. The first one is repetition, as mentioned in the definition above, and the second is power imbalance. Usually, the perpetrator's intention is not to repeat the abusive act but due to excessive use of technology, this may slip his/her control. For example, a picture with offensive content may be posted on the Internet once, but consequently may be shared multiple times by other people, not by the initial perpetrator. This way repetition is inevitable and embarrassment is experienced many times by the victim.

Concerning power imbalance in terms of cyberbullying, it is not necessarily referred to physical or psychological "weakness", but also to the lack of knowledge in ICTs and/or the anonymity cyberspace offers (Slonje, Smith and Frisén, 2013). Studies conducted so far, indicate that there is a correlation between students with advanced ICT knowledge and carried out, delinquent, online activities. Regarding anonymity usually the victim is not aware of the perpetrator's identity and, therefore, it is difficult to face him efficiently (Slonje, Smith and Frisén, 2013).

Motives

Motives of cyberbullying could be divided in two categories: internal and external. Internal motives include anger, jealousy, willing to revenge or even boredom (Slonje, Smith and Frisén, 2013). These may also indicate troubled family affairs. Furthermore, cyberbullying behavior may meet the need for imposition of power (Nika, Gioldasi and Vitta, 2017).

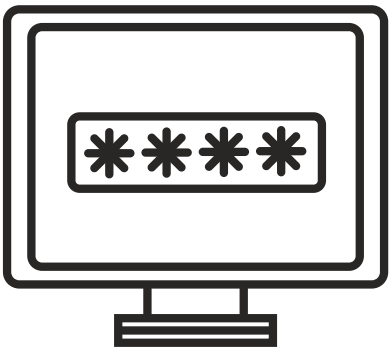
Concerning external motives these may be either the possible absence of serious consequences against the perpetrator or the fact that the perpetrator may be reluctant or afraid to proceed in a face – to – face encounter with the possible victim (Slonje, Smith and Frisén, 2013).

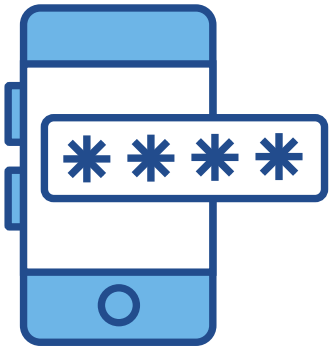
Consequences

1. The victim and the perpetrator at times experience negative emotions such as anger, sadness, anxiety, embarrassment, fear, self-blame and lack of self – esteem.
2. Regarding school context, negatively affected concentration, poor academic performance but also absence from school have been noticed (Šléglová and Cerna, 2011).
3. Victims can feel so helpless, lonely, embarrassed and desperate that may decide to commit suicide.
4. Both victims and perpetrators may be socially marginalized and therefore the aforementioned emotions are intensified.
5. The victims may not try to defend themselves because they think that this abusive behavior is “normal” or expected or that they deserve it, when feeling inferior (Šléglová and Cerna, 2011).

Ways to counteract

1. It is really important both adolescents and adults be informed and be aware of internet safety and the functional differences among several means of technology (Olweus, 2012).
2. Other practical solutions are blocking unknown people on social media and changing often passwords and usernames.
3. Ask for help from a familiar person or an expert (Slonje, Smith and Frisén, 2013). Open up about a bad experience you are going through or you went through in the past and share your feelings. This will help you to feel more relieved and will help you to easier come up with a solution.
4. Parents need to be open-minded and essentially close to their children, so that the latter will feel free to discuss such issues as cyberbullying and cybervictimization.
5. It is of vital importance when surfing on the internet to be aware of people rights and how to respect them.
6. Organize training courses or seminars concerning cyberbullying and ways to counteract.





Case studies

Brandy Vela (1998–2016), age 18, was a high school senior who killed herself in November 2016 after years of bullying in person and online by her peers about her weight. According to her sister, the bullies created dating websites, where they lied about her age, put up her picture, and used her phone number to tell people she's giving herself up for sex for free to call her. Brandy shot herself in the chest with a gun and died in the hospital the day after. After her death, a couple of teenagers were arrested for bullying her (Wikipedia contributors, 2020).

Megan Meier (1992–2006), age 13, was an American teenager from Missouri, who killed herself by hanging a few weeks before her fourteenth birthday. One year later, her parents, after having carried out an investigation into the matter of her suicide, found out that was attributed to cyber-bullying through the social networking website Myspace. Individuals intended to use Meier's messages to learn more about her and later humiliate her (Wikipedia contributors, 2020).

4.5. PHISHING TECHNIQUES

The theft of data is called the English term phishing which comes from password fishing. It is a form of fraud against organizations or private individuals when using unsolicited e-mail messages or falsified web pages, with the aim to obtain passwords for accessing information systems and other confidential information. data.

Most of the time, attacks of this type are directed against bank customers in order to find out their passwords for connecting to electronic banking systems or credit card data. Later, the information obtained in this way can be used in the commission of criminal acts: illegal connections to information systems, theft of money from accounts, or when paying for goods with foreign cards in the electronic space.

Data theft is carried out in two main ways:

1. Contacting directly individuals and tricking them to reveal such information willingly;
2. Using dedicated technologies that copy data from various websites or devices that are used to browse the internet and / or use remote services.

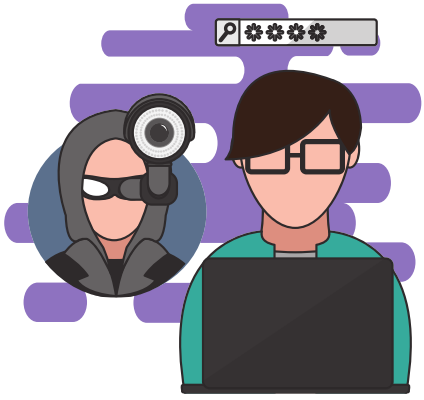
Most common type of phishing is so-called deceptive phishing. In this case a fraudster impersonates a legitimate institution or company (e. g. governing agency, law enforcement agency, financial service provider, large well-known brand company, etc.) and addresses individuals directly with a request to fill in personal details. The same email or other type of message is sent to thousands of individuals hoping that some of them will respond to it.

Such messages usually request to be reacted very quickly, noting that there might be undesirable negative consequences if an individual does not respond in time (e.g. the institution will take legal actions, funds from the individual's bank might be stolen, the prize will be awarded to another person and etc.).

Most often such messages might contain malicious links and / or other references to special sites asking individuals to enter the requested information there. As soon as an individual provides this information on such sites it becomes available to the fraudster.

More advanced fraudsters might exploit the session control mechanism and hijack the session of a legitimate site. When an individual logs into a web application, the server sets a temporary session cookie in his / her browser. Fraudsters might steal such session cookies or provide an individual with a link containing a prepared session ID prior he/ she enters into such an authentication session. These actions allow fraudsters later hijack the session by using the same session ID for their own browser session.

Phishing methods might also be used by creating fake e-shops or other sites. To make such sites more noticeable, fraudsters allure individuals with low prices, fast delivery of goods or other benefits. Various search engines are used in order to reach targeted audiences and direct it to such sites. Data is stolen while a targeted individual tries to register or buy the goods at such sites.



Fraudsters might take advantage of existing legitimate sites by altering an IP address so that it redirects to a fake site rather than the site an individual intended to go to.

Sending links or other references to files that are infected by certain viruses is also a very popular technique. Such files infect computers or other devices and might be programmed to ask to re-type passwords or other credentials while connecting to online banking or other remote services just for the purpose to transfer such information to fraudsters.

First of all it is important to understand and be aware that phishing and data thefts might take place anywhere, in any form and at any time, so you need to be constantly attentive and alert.

Secondly, take precautions to keep the devices you use safe:

1. Use tools and software that help keep your computer or other device secure (antivirus programs, etc.). Download such tools or software only from official and trusted sources. Update these tools and software on time.

2. Avoid visiting obscure and unreliable sites, register on or download files from such sites. Such sites may contain links or files that may infect your computer or other device with viruses that collect your personal data.

3. After using your personal account log out of it and close the browser window.

4. Choose secure and strong passwords which consist of numbers, letters and other symbols. Do not use easy-to-guess passwords (e.g. 12345, just your first or last name or date of birth). In case you have several different accounts, always use different passwords.

5. When creating accounts or emails choose service providers that use two-factor authentication systems (e.g. a password and phone number).

6. Beware of common online fakes that mimic:
a) e-mail websites providing mail service (gmail.com, yahoo.com, hotmail.com, etc.);
b) social websites (facebook.com, vk.com);
c) e-mail, which is extremely popular abroad. payment system Paypal (paypal.com);
d) other popular websites.

7. Do not click on suspicious or unclear links received in e-mails or found on web pages with suspicious content.

8. Before entering your personal details on online websites, always make sure that the website is not fake. It is necessary to pay attention to the domain name and the addresses of the links on the page. E-banking systems always use a secure SSL connection protocol, the address must have HTTPS at the beginning, and the site's certificate can be checked. The address of fake websites almost always starts with HTTP (without s).

Thirdly, note that legitimate institutions and service companies (e.g. banks or other financial services providers) do not request their clients to disclose their login passwords or other credentials. Such information is personal and only you are allowed to know it. If such information becomes known to third parties, you must immediately inform these service providers about these circumstances and change your passwords or other credentials.

Fourthly, if you receive a request for sensitive information, pay attention to these circumstances:

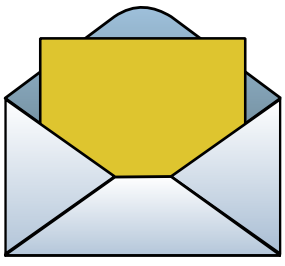
1. The address of the sender. Check whether the details of the institution / company in email or other messages match the data published on their official websites or other public sources. Institutions / companies usually use their dedicated mailboxes instead of publicly available general mailboxes (e.g. @gmail.com, @yahoo.com, etc.).

2. Text quality and content. Deceptive emails or messages often contain clerical or stylistic errors. The text might be translated literally without following the rules of that language (by using publicly available translation programs). The text may also use the household language, inaccurate names or legal forms of institutions or companies (e.g. a public authority may be referred to as a company). Reasons or other circumstances for contacting you may be described in a way that they could be adapted to any situation (e.g. allegedly the police department informs you that your login details to the banking services have been stolen and you need to change such login details immediately, but does not even name the bank).

3. Links that are provided. Fraudulent links often contain a series of numbers or unfamiliar web addresses. If you aren't sure a link is legitimate, don't click it.

4. Likelihood of getting the request or offer. You should assess whether you could have expected such a letter and whether it lines with the real facts or normal practice (e.g. you receive an email that you have won the lottery even though you have not participated in any lottery; you receive a message supposedly from your bank, even though it never sends messages that way).

If you have any doubts about an email or a message you received, contact the institution / company (that allegedly reached you) by its contact details publicly available on its official website or other reliable source.



4.6. FINANCIAL CRIMES AND INVESTMENTS FRAUDS

Financial crimes are crimes in which criminal organizations benefit financially. In financial crimes, usually, one party provides a financial benefit, and the other party suffers a financial loss. These are frequently committed for the personal benefit of the criminal and involve the illegal conversion of ownership of the property involved.

When we talk about 'consumer fraud' when someone suffers from a financial loss involving the use of deceptive, unfair, or false business practices. In the past two years, for instance, 60% of European consumers having purchased online in a timeframe of 12 months, have experienced fraud. Despite strong cybersecurity measures adopted by financial institutions (banks, payment companies etc.), fraudsters keep getting their way by exploiting the weakest link in the chain: humans and their predilection to trust their peers.

Most common types of fraud:

Phishing	Emails and phone calls, in which the fraudsters pretend to be a legitimate institution to get personal data from their victims.
Pharming	is an automatic redirection of the user to fake pages operated by fraudsters with the aim of stealing confidential personal information such as passwords or bank account numbers. Unlike other types of fraud, pharming does not require special actions from the user (victim). In the attack, the fraudsters simply change DNS or other queries automatically, inserting their own websites instead of the ones the user (victim) wants.
Device manipulation	Hacking of POS (point-of-sale) systems, ATMs. Smartphones or PCs to access data and/or money.
Identity fraud	Use of consumers personal data to cancel credit cards, change passwords, open accounts etc.
Social engineering	Manipulation of victims to obtain confidential information.
Money mules	Tricking innocent people into laundering stolen or illegal money through their bank account.

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

How to avoid becoming a financial fraud victim:

1. Check your bank account regularly and report any suspicious activity to your bank.
2. Keep in mind that your bank will never ask you for sensitive information (e.g. online account credentials) over the phone or email.
3. If you think you've provided your account details to a scammer, contact your bank immediately.
4. Perform online payments only on secure websites: check the URL bar for the padlock and https and use only secure connections (mobile network instead of public Wi-Fi).
5. If an offer sounds too good to be true, it's almost always a scam.
6. Keep your personal information safe and secure.
7. Be very careful about how much personal information you share on social network sites. Fraudsters can use your information and pictures to create a fake identity or to target you with a scam.
8. Always report any suspected fraud attempt to the police, even if you didn't fall victim to the scam.

Investment Fraud involves the illegal sale or purported sale of financial instruments. The typical investment fraud schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities.

Types of investment frauds:

Pyramid Schemes

This is when fraudsters claim that they can turn a small investment into large profits within a short period of time. But in reality, participants make money by getting new participants into the program. The fraudsters behind these schemes typically go to great lengths to make their programs appear to be legitimate multi-level marketing schemes.

Ponzi Schemes

This is when a fraudster or "hub" collects money from new investors and uses it to pay purported returns to earlier-stage investors, rather than investing or managing the money as promised. The Like pyramid schemes, Ponzi schemes require a steady stream of incoming cash to stay afloat. But unlike pyramid schemes, investors in a Ponzi scheme typically do not have to recruit new investors to earn a share of "profits."

„Pump-and-Dump“

A scheme in which a fraudster deliberately buys shares of a very low-priced stock of a small, thinly traded company and then spreads false information to drum up interest in the stock and increase its stock price. Believing they're getting a good deal on a promising stock; investors create buying demand at increasingly higher prices. The fraudster then dumps his shares at the high price and vanishes, leaving many people caught with worthless shares of stock.

Advance Free Fraud

This type of fraud plays on an investor's hope that he or she will be able to reverse a previous investment mistake involving the purchase of a low-priced stock. The scam generally begins with an offer to pay you an enticingly high price for worthless stock. To take the deal, you must send a fee in advance to pay for the service. But if you do so, you never see that money—or any of the money from the deal—again.

How to avoid becoming an investment fraud victim:

1. Verify the license of the person selling the investment
2. Verify the investment is registered
3. Beware of promises of high rates of return and/or quick profits
4. Be suspicious of high-pressure sales
5. Beware of unsolicited offers
6. Ask for prospectus or offering circular
7. Talk to a third-party person
8. Watch out for online scams

4.7. FAKE NEWS AND PROPAGANDA

Propaganda is defined as deliberate and consistent dissemination of theories and ideas in philosophy, science, religion, etc., in order to educate people using them, influence people's views, moods, manipulate with, promote certain actions that would contribute to the goals pursued by the propagandist. Propaganda aims to affect the emotions and opinions of the target group.

The effectiveness of propaganda is enhanced by partially telling the truth but not providing all the information and concealing the facts. Therefore, recognizing propaganda can sometimes be difficult. Propaganda presents certain correct facts, but changes or distorts the whole context. The accuracy of the facts presented can be verified, so the message sent by the propaganda seems to be true. However, this is intended to be misleading.

Propaganda is often defined in a negative context as an unacceptable, disinformation-based means of shaping public opinion. Synonyms used to describe propaganda are including but not limited to, lie, deception, distortion, manipulation, brainwashing, thought control, and psychological warfare.

However, propaganda is also used for marketing, social and educational purposes, i. e. propaganda can work in a positive context, and the most important thing is what it is used for. For example, the representations of harm of smoking on cigarette boxes. It is also propaganda because it has an attempt to influence people with emotions and change their behavior, i. e. to force them quit smoking. However, propaganda is most often used for negative purposes to incite hatred and hostility.

Propaganda is constantly affected by social, technological, cultural, and economic changes. It must therefore adapt and act in a way that is in line with the personality of the modern man. Propaganda is often associated with posters of World War II, but it has now taken on a variety of more subtle forms. The way it works can be as obvious as a swastika or as subtle as a comment on a news portal.

According to objectivity, propaganda can be divided into white, gray, and black.

White propaganda

White propaganda is the most transparent and open representation of facts. It is used for various social programs and initiatives. White propaganda seeks to present the findings of independent experts that reflect key views.
However, with skyrocketing competition among different public and business organizations, it is becoming increasingly difficult to determine the fairness of the approach, and the views of experts on the same issues are becoming very different. We, therefore, call white propaganda an intention to provide reasoned explanations without any efforts of distorting the facts.
Most often, white propaganda talks about the achievements of country, company, or organization and is positive. For example, the Republic of Lithuania promotes and demonstrates itself as a bridge between the West and the East, where an investment-friendly climate exists and financial security is guaranteed. This is propaganda, although it is based on correct information provided by official sources.

Gray propaganda

Gray propaganda. Its representatives deliberately associate the confirmed facts with the unconfirmed ones, presenting only an interpretation in their favor, and deliberately distort the context of the event. Gray propaganda is intensively used in guided informational, political or economic conflicts.
Gray propaganda forms a one-sided approach to the subject, avoiding criticism. Such propaganda, for example, states that one's own army is always right. Representatives of this propaganda avoid the open dialogue which may end in a disclosure, but still do not stick to a one-sided lie, leaving their attitude the opportunity of changing.
Gray propaganda is widespread on Russian television channels ORT and RTV during the presidency of Vladimir Putin, when any information about Putin and Russia is presented positively, even though the international forum strongly criticizes Russia for certain decisions.

Black propaganda

Black propaganda is based on the deliberate falsification of events and facts, i. e. lies. It was particularly prevalent in Nazi Germany, where methods of event staging were used. The Nazis, for example, disguised in uniforms of Soviet soldiers, ravaged the Polish villages, intimidating locals with the impending communist rule and its consequences.
Black propaganda is also based on black technology. For example, during an election, information is disseminated on behalf of an opponent, or events are staged so that later greatly complicate the opponent's chances of being elected. Black propaganda and black technology are being persecuted in many democracies.

Thus, propaganda communication is usually not entirely objective and presents facts selectively in order to influence attitudes. Overcrowded language is often used to elicit an emotional response to the information presented rather than the mind.

In the digital age we live in now, this conscious attempt to spread biased information is also taking place on digital platforms. Its purpose is to mislead and deceive. So we can speak boldly about “digital propaganda” (Bjola, 2018, p. 307).

As the propaganda process moved into the online space, new forms of propaganda known as trolls and bots emerged. Their purpose is to influence election results, demoralize, discredit or isolate political opponents, participate in public opinion polls, and spread propaganda and false news.

Trolls are tens of thousands of people hired by propagandists to work all day (or night) on the target group's news portals, social networks to comment on the latest news and posts and to raise a stallion among Internet users, spread misinformation, despise prevailing values and attitudes (Grigaliūnas, 2016).

How to recognize a troll?

- Records or messages of pro-Russian content;
- Spelling mistakes;
- Often a female user account;
- Small number of followers;
- Share messages @ the name of a specific person, such as @putin_leader;
- Claims to refer to alternative sources but does not indicate them;
- Comments or shares posts, posts only on a specific topic.

A bot is a computer program that automatically performs certain actions that a person working on a computer can perform. In propaganda, bots are used to write propaganda comments on news portals and posts on social networks. These programs generate different comments: a template is created and a new comment is regenerated from that template. Proxy servers provide different IP addresses, so it seems that many different people write comments. For example, about 15 percent of social network Twitter users are bots.

How to recognize a bot?

- Pay attention to the profile photo. These are usually drawings, images of nature, photos of politicians or celebrities, or no profile photos at all. You can find the origin of a profile photo using Google Images Search.
- Long user name. The username of many bots is unusual, with numbers or no meaning at all.
- Generic content or duplicate posts or messages. Bots are designed to dominate a particular topic or tag # on social networks. To achieve this, a message or post is shared many times.
- The user account is empty. Man-created user accounts contain a lot of personal information, created by bots – no or only basic information.
- Bots follow far more people on social networks than they have followers themselves.
- Bots share many posts and messages. If a user is constantly sharing a lot of records, even at night, there is a good chance that it is a bot.
- Bots share radical political content posts or messages. These are usually ideological clichés, patriotic, militaristic texts against prevailing values and attitudes.
- Many stereotypical recordings, such as sentiments, videos with animals, and so on, in the user news feed. Such content is used by bots during breaks between elections or other relevant events.

You can check if you are not following bots on the Twitter social network here: https://botcheck.me

By the way, there are not only trolls but also elves. These are usually active and civic people who reveal various misinformation and manipulations, fighting the disseminators of false news and propaganda in the online space.

Means of influencing that can be used as propaganda

Generalization

Generalization is an attempt to influence emotions by using abstractions; it is one of the simplest forms of propaganda. This method is often used during the election campaigns of politicians. This method is particularly effective in difficult times, such as an economic crisis. Emotional summative statements are often used, such as We deserve to live better, For the future, Order will be, Every man is of utmost importance, etc.

Symbols

Symbols help in enhancing the one's image. For example, a person in a photograph is surrounded by certain symbolic objects that form an image that that person is promoting the values symbolized.

Labeling

Labeling is when a negative idea, action, term is associated with a specific person, organization, and so on. Sarcasm or ridicule is often used. This is an effective way of propaganda, because sticky labels - liars, terrorists, corrupt - are hard to get rid of.

The herd's feeling

The herd's feeling creates an image that the idea has widespread acceptance, so rejecting it risks being isolated and out of place.

Emotional arousal

Emotional arousal seeks to evoke such strong emotions as fear, anger, sadness, and resentment. The most common attempt is to show that one or another phenomenon will have negative consequences, using a variety of human fears.

Card stacking

Card stacking is when only positive facts are told and negative facts are silenced. Although the arguments used in using this technique are usually valid, statistics are often presented that can distort the situation because information is taken out of context or important facts are omitted. In political campaigns, a candidate is presented only on the positive side, omitting the negative.

C.R.A.P. test

A quick check of the accuracy of the information on the website can be done using C.R.A.P. test (Currency, Reliability, Authority, and Purpose / Point of View). This test makes it possible to find out when and under what circumstances the published text was written, how reliable its author is, and finally, the purpose and attitude of this information (CyberWise, 2019).

Reliability • What kind of information is included in the resource? • Is content of the resource primarily opinion? Is it balanced? • Does the creator provide references or sources for data or quotations?	**Currency** • How recent is the information? • How recently has the website been updated? • Is it current enough for your topic?
Authority • Who is the creator or author? • What are the credentials? Can you find any information about the author's background? • Who is the published or sponsor? • Are they reputable? • What is the publisher's interest (if any) in this information? • Are there advertisements on the website? If so, are they cleared marked?	**Purpose/Point of View** • Is this fact or opinion? Does the author list sources or cite references? • Is it biased? Does the author seem to be trying to push an agenda or particular side? • Is the creator/author trying to sell you something? If so, is it clearly stated?

Ways to counteract

With so much information available in all digital platforms, it is easy to get duped. Studies show that approximately 75% of people, who see fake news, are not able to recognize they are actually fake.

Therefore, a quick way to check, whether a piece of information is real or not, is by using the C.R.A.P. Test. Find out if the article is Current, Reputable, if the Author is credible and finally the Purpose and Point of view of the article (CyberWise, 2019).

Definitely common sense is always needed. Some ways to spot fake news are briefly shown below (How to Spot Fake News, n.d.).

- Consider the source: Try to learn more about the source and consider whether it is credible.
- Read beyond: Headlines may be scandalous, in order to obtain more clicks. Search further information about the narrated story and try to find out the truth.
- Check the author: Has the author made other posts, except from the current one? Has he received any comments or judgment concerning his credibility?
- Supporting sources: Usually a website lists other links relating to the subject of the article provided. Check whether those links are really related to the initial article or they are just misleading.
- Check the date: Is the information up-to-date or is it reposted?
- Is it a joke? In case the information is really bizarre, it might be satire. You have to check again the author and the source, in order to be sure.
- Check your biases: Think about whether the news you are reading, how it influences your own biases. You might probably reject them, because you do not agree. But this does not make the news fake.
- Ask the experts: There are some fact-checking sites you can visit, in order to be sure about the information provided.

Case studies

An example of a propaganda campaign is the one between Russia and the United States of America, concerning the presidential elections of 2016. The main reason behind shaping the election results was the appearance of a variety of fake news in order to direct American citizens to vote for Trump.

Cambridge Analytica, a company that specializes in analyzing data and building psychological profiles for political purposes using data collected from American Facebook users, compiled the electoral profiles of thousands of people in the run-up to the presidential election to support Donald Trump's election campaign.

Facebook users who were analyzed were divided in two categories. The first included voters who intended to vote for Trump's opponent, while the second included those who intended to abstain. This was followed by a targeted fake news campaign about Hillary Clinton.

The "news" presented to the first-class voters was intended to persuade them not to vote, while those seen on the second-class cell phone were intended to urge them to vote for Trump. According to a Stanford University survey, 41% of fake news in the last month before the election went viral. Facebook has officially admitted that 126 million Americans, about 40% of the total US population, saw news and posts on social networks, which were "planted" by the now infamous Internet Research Agency, based in St. Petersburg (Tsompanidis, 2018).

An example of the ease fake news are nowadays spread, is the discovery of new homemade recipes, which are supposed to kill Covid-19, the new coronavirus. We heard things like “drinking alcohol kills the virus”, “drinking chlorine dioxide boosts the immune system”. These views are, at least, dangerous. But a recipe that was quickly circulated on social media was the one supporting that boiled garlic kills Covid-19 “Good news, Wuhan’s coronavirus can be cured by one bowl of freshly boiled garlic water. Old Chinese doctor has proven its efficacy. Many patients have also proven this to be effective. Eight (8) cloves of chopped garlic add seven (7) cups of water and bring to boil. Eat and drink the boiled garlic water, overnight improvement and healing. Glad to share this" (Spencer, 2020). This rumor was so disseminated that the World Health Organization (WHO) knocked it down reporting “Garlic is a healthy food that may have some antimicrobial properties. However, there is no evidence from the current outbreak that eating garlic has protected people from the new coronavirus” (Spencer, 2020).

The best ways to repel propaganda:

- Responsible, independent media;
- Deconstruction of myths and strategic communication;
- Free, educated society;
- Continuously developing the ability to critically evaluate information;
- Formation and strengthening of national narrative and historical memory.

EXAMPLE: Lithuanian Bayraktar story


Lithuania Posts English › الارشيف › Breaking News

Russian propaganda lie: Bayraktar, for whom Lithuanians raised money, has already been shot down

BREAKING NEWS Glenn Breaking News 3 months ago 190

‚Hundreds of Lithuanians collected 4.7 million in three and a half days. dollars to buy the unmanned Bayraktar in Ukraine. He was shot down 3.5 minutes after his first rise'.

It is presented as an ‚anonymous Twitter channel that publishes fictional news'. Commenters did not seem to pay attention to this detail and took the message seriously. In May 2022, hundreds of Lithuanians have chipped in together to buy an advanced military drone for Ukraine in its war against Russia in a show of solidarity with a fellow former Soviet Union country.

The target of €5 million was raised in just three and a half days — largely in small amounts between €5 and €100 — to fund the purchase of a Byraktar TB2 military drone, according to Laisves TV, the Lithuanian internet broadcaster that launched the drive.

The drone has proven effective in recent years against Russian forces and their allies in conflicts in Syria and Libya, and its purchase is being orchestrated by Lithuania's Ministry of Defence.

Find full story at https://lithuania.postsen.com/news/7172/Russian-propaganda-lie-Bayraktar-for-whom-Lithuanians-raised-money-has-already-been-shot-down.html

For more information regarding propaganda in the digital age and fake news you can visit:
https://www.youtube.com/watch?v=5__dZBZuzZc&ab_channel=OsloFreedomForum
https://www.youtube.com/watch?v=V4o0B6lDo50&ab_channel=CyberWise
https://www.cyberwise.org/fake-news
https://www.cybercivics.com/

PRACTICAL TASK. Wag the dog

Encourage training participants to watch the Wag the Dog, a 1997 American political satire black comedy film produced and directed by Barry Levinson and starring Dustin Hoffman and Robert De Niro.

The aim of the activity:
practicing and analyzing personal observation / critical thinking skills.
Skills that the activity develops: critical observation.

How many people the activity is suited for:
individual work with group discussion afterward.

Time requirement of the activity:
97 minutes for movie watching, and up to 15 minutes for a moderated discussion.

How many instructors are needed?
One for moderating discussion.

Other requirements for the activity (space, equipment...):
at home/auditorium / online session.

Description of the activity:
While watching the movie, ask participants to observe how things are going on.
Invite group members to reflect on several aspects of the political phrase 'wag the dog'.

Firstly, it can be used to indicate that attention is purposely being diverted from something of greater importance to something of lesser importance.

Secondly, if you say that the tail is wagging the dog, you mean that a small or unimportant part of something is becoming too important and is controlling the whole thing.

4.8. FRAUD ADVERTISING (FAKE PRODUCTS, SUPPLEMENTS)

Whenever money is involved, there is always an opportunity for a fraud. From a technical perspective, online advertising fraud has been relatively easy (and yes – lucrative) business for fraudsters and a financial disaster for advertisers, publishers and online ad platforms themselves.

Online ad business was built on a number of Internet Open Standard technologies which never meant to be fraud / scam / steal proof. As a consequence, ad fraudsters got a huge head start. According to Juniper, in 2019 online advertising industry was facing a stunning $42 billion loss due to ad fraud and unfortunately there isn't any reason to believe the figure will be less this year.

To clarify, digital ad fraud is an intentional activity that prevents advertisements from being delivered to the right audience or location. The malicious risks that marketers face today are getting increasingly sophisticated, and therefore greater, than previously anticipated.

The digital advertising environment now involves thousands of intermediaries, presenting a plethora of dark corners in which fraudsters can conceal criminal activity. Fraudsters know when they're being watched and have become even more dangerous, making it all the more challenging to prevent ad fraud.

As a result, 96 pc of consumers say they have little trust in digital advertising – making it harder for marketers to demonstrate that their ads are legitimate. So what steps should organisations take to prevent losing much of their budget to fraud and, with it, consumer trust?

Even if a small percentage of consumers still click the fraudulent ads and buy fake products or services, it's still a huge business and monetary intention to develop the techniques and marketing efforts.

Smart consumer needs to partial undertake the responsibility to mitigate the fraud in advertising by reporting fake and discouraging the less skillful people around them to.

How to recognise fake advertisements?

It's relatively easy once you understand and know the pattern:

1. Online ads quality usually stands out to be poor and content repetitive.
2. Huge and unrealistic claims and promises to deliver rather impossible results either to get rich quick or grow back the lost hair.
3. Landing pages will be hosted under weird domain names, unknown brands, photos of either celebrities or unexisting professionals will be used.
4. The font used in landing pages stand out to be colourful, very incentivising to take action and big discounts are offered.
5. The landing page and product description page might contain big quantity of fake and mostly very positive reviews

4.9. PC/ONLINE GAMING, CASINO, ADDICTION

Play is an innate human drive, which appears in early childhood (Kuss & Griffiths, 2012, p. 5). After the millennium internet gaming has increased significantly because of the huge technological development. PC gaming and, in general, online gaming gives players the opportunity to experience different gaming environments simultaneously, to design and develop virtual characters they could identify with and also to play with other players all around the world at any time (Kuss & Griffiths, 2012, p. 5).

Moreover, online gaming allows players to communicate with others via chatting and, thus, form new relationships (Kuss, 2013, p. 125). One more reason internet gaming looks so appealing to some people is that it gives the chance to escape from real life problems and in this way online gaming turns into a coping strategy. (Kuss, 2013, p. 125).

One of the most famous categories of online games is the Massively Multiplayer Online Role-Playing Games (MMORPGs), such as “World of Warcraft”. This kind of games allows players to set goals and reach them, like level advancing, thus gaining a higher virtual status and power in the gaming environment. Players can also motivate because of the admiration they might receive from the gaming community (Kuss, 2013, p. 125).

On the other hand, the aspects of socializing and escaping may be predictive of an addiction to online gaming (Kuss, 2013, p. 125). Other negative consequences are the ignorance of real-life relationships, rejection of sleep, work and studies, obsession with gaming, lack of attention resulting in aggression and stress increase as a consequence, difficulties with verbal memory and high levels of loneliness (Kuss, 2013, p. 125).

In some countries, such as South-East Asian countries, the negative consequences of online gaming have been so severe, that the governments took action and measures to reduce these negative impacts. For example, in Japan, the government has recognized the severity of the consequences leading to the development of “fasting camps”, where individuals addicted to online gaming are helped by being cut off from technology totally Kuss, 2013, p. 125).

Casino addiction

Casino gambling is a very popular activity worldwide. The last fifteen years gambling environment has changed significantly through the increased availability of online gambling (Gainsbury, 2015, p. 190). Nowadays an Internet – enabled device and a click of a button is all you need to have access to a gambling environment. In addition to that, access is also enabled due to how easily money can be spent through credit cards, electronic bank transfers and e-wallets.

Online casino and gambling have raised controversy regarding the possible consequent addiction (Gainsbury, 2015, p. 190). The fifth edition of the Diagnostic and Statistical Manual of Mental Disorders (DSM-5) added a new category of Non – Substance Behavioural Addiction within the context of Substance Addiction category. In order to diagnose a gambling addiction, the individual has to mention four or more of the following (DSM-5):

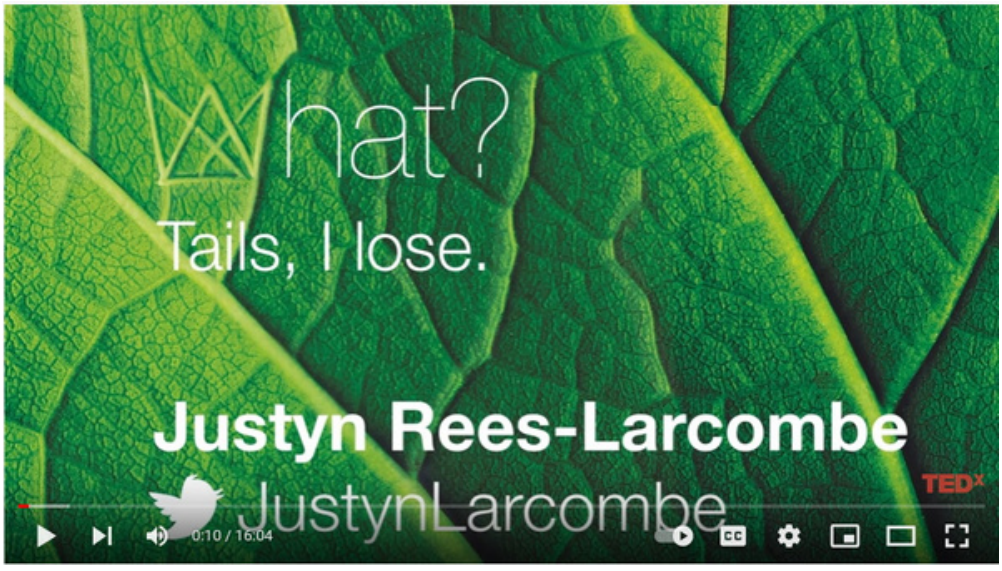
1. Needs to gamble with increasing amounts of money in order to achieve the desired excitement.
2. Is restless or irritable when attempting to cut down or stop gambling.
3. Has made repeated unsuccessful efforts to control, cut back, or stop gambling.
4. Is often preoccupied with gambling (e.g., having persistent thoughts of reliving past gambling experiences, handicapping or planning the next venture, thinking of ways to get money with which to gamble).
5. Often gambles when feeling distressed (e.g., helpless, guilty, anxious, depressed).
6. Lies to conceal the extent of involvement with gambling.
7. Has jeopardized or lost a significant relationship, job, or educational and/or career opportunity because of gambling.
8. Relies on others for money to relieve desperate financial situations caused by gambling.

Risk factors for Internet gambling (Gainsbury, 2015, p. 190)

- Younger adults and older adolescents
- Male
- Alcohol or drug abuse
- Irrational cognitions
- Willpower to make money fast and easily

Nevertheless, studies conducted so far do not define a specific personal and behavioural pattern to distinguish between Internet and non – Internet problem gamblers.

In the following link you can find the story of a man, named Justyn Rees Larcombe, who gambled away £ 750.000 and lost his family, too.
https://www.youtube.com/watch?v=7AN3VLLIkdI&ab_channel=TEDxTalks



5 MODULE

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

CREW
Creativity, Resilience and Empowerment for Work

GOVERNMENT ROLE AND INSTITUTIONS WHERE TO APPLY

5.1. E-PRIVACY REGULATION IN EU

The ePrivacy Regulation (ePR) is a proposal for the regulation of various privacy-related topics, mostly in relation to electronic communications within the European Union. Its full name is "Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)." It would repeal the Privacy and Electronic Communications Directive 2002 (ePrivacy Directive) and would be lex specialis to the General Data Protection Regulation. It would particularise and complement the latter in respect of privacy-related topics. Key fields of the proposed regulation are the confidentiality of communications, privacy controls through electronic consent and Browsers, and cookies.

The scope of the ePrivacy Regulation is still under discussion. According to some proposals, it would apply to any business that processes data in relation to any form of online communication service, uses online tracking technologies, or engages in electronic direct marketing.

Some of the most important e.provisions of the privacy regulation that are still under discussion:

New market participants	92% of Europeans say that it is important for them that e-mail and online messages would be kept confidential. However, the current E-Privacy Directive only applies to traditional telecommunications operators. The privacy rules will now also apply to new providers of electronic communication services such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber.
Stricter rules	The fact that the current directive is proposed to be updated with a directly applicable regulation means that all EU citizens and businesses will be guaranteed the same protection for their electronic communications, and one common set of rules will apply across the EU.
Content and Metadata of Communications	It is proposed to ensure the privacy of the content and metadata (such as the time and location of the call) of electronic communications. Both the content and metadata of electronic communications are highly private, and the proposed rules would require them to be anonymized or destroyed (unless such data is needed for billing purposes) if users do not consent to their processing.
New business opportunities	By obtaining permission to process communications data (content and/or metadata), traditional telecom operators will have more opportunities to use the data and provide additional services. For example, they will be able to produce color maps showing where people are; such maps could be useful for public authorities and transport companies when preparing new infrastructure projects.
Simpler cookie rules	The so-called cookie policy, which requires Internet users to constantly respond to requests to allow the use of cookies, would be simplified. The new rules would give users more control over their browsing settings by providing a simple way to accept or decline persistent cookies and other identifiers if privacy is at risk. The proposal clarifies that consent will no longer be required for non-invasive cookies (such as cookies to remember what has been added to the shopping cart) used to ensure the convenience of online browsing. Consent would also no longer be required for cookies used to count website visitors.
Spam protection	Among the proposed proposals is an effort to establish a ban on sending unsolicited messages by all means of electronic communication, such as e-mail or SMS message, and in principle also by phone, if the user's permission has not been obtained. Member States may decide to use the option to give consumers the right to opt-out of telemarketing calls, for example by putting their number on a do-not-call list. Marketing callers will need to display their phone number or use a special code to identify it as a marketing call.
More effective enforcement	National data protection authorities would be tasked with ensuring compliance with the confidentiality rules set out in the regulation.

The proposed penalties for noncompliance would be up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover, whichever is higher. The ePrivacy Regulation originally was intended to come in effect on 25 May 2018, together with the GDPR, but has still not been adopted.

Video: The impact of the European ePrivacy regulation
https://www.youtube.com/watch?v=Q8YFLkvEcLE

Difference between Regulation and Directive

1. The (new) ePrivacy Regulation will repeal the (current) ePrivacy Directive.

2. Contrary to an EU Directive, an EU Regulation is a legal act of the European Union that becomes immediately effective as law in all member states simultaneously.

3. The current ePrivacy Directive is a legal act of the European Union that requires member states to achieve a particular result without dictating the means of achieving that result. It has therefore been implemented into national laws and regulations.

4. If the proposed ePrivacy Regulation became effective, these laws would be superseded and will (for reasons of clarity) likely be repealed. The ePrivacy Regulation would be self-executing and not require many implementing measures.

5.2. GDPR AND CCPA

General Data Protection Regulation (GDPR) is a privacy and security law concerning the protection of personal data. Personal data are considered to be any information that can, directly or indirectly, lead to the identification of an individual (Goddard, 2017, p. 703). Personal data include information regarding the location, ethnicity, gender, biometric data, religious beliefs or web cookies. Pseudonymous data can also be included in personal data's context, if it is easy to reveal an individual's identity. GDPR was carried out and passed by the European Union (EU), however it imposes obligations onto organizations worldwide as long as they interact and collect data related to citizens in the EU (Wolford, 2019). In this way all EU residents are protected from the location of data processing.

Brief historical look

1950 European Convention of Human Rights stated that "everyone has the right to protect his private and family life"	**1995** European Data Protection Directive implemented least data privacy and security standards	**2000** Many financial organizations offered online transactions
2006 Facebook made its first appearance	**2011** A Google user arraigned the company on checking her emails	**2016** European Parliament put into force GDPR

Penalties

In case GDPR is violated, then fines are really high. There are two kinds of penalties. The first one is a fine of about 20 million euros or 4% of the global revenue, and the second is that people, whose data weren't protected, have the right to ask for compensation (Wolford, 2019).

Principles of data protection (Wolford, 2019).

Processing of personal data should be carried out according to seven core principles:

1. Transparency – Lawfulness – Fairness.
2. Purpose limitation: Data should only be used for the purposes the subject has been informed about.
3. Data minimization: You should collect only the data that is totally necessary for your purpose.
4. Accuracy: Data must be kept accurate and up to date.
5. Storage limitation: You can save the data for as long as your purpose requires.
6. Integrity and confidentiality: Processing of data must be conducted in such a way, to ensure protection and confidentiality.
7. Accountability: The person processing the data is in charge of demonstrating GDPR compliance with all the aforementioned principles.

Consent

It is mandatory that the data subjects give their consent, in order to allow the process of their data. But what does consent constitute?

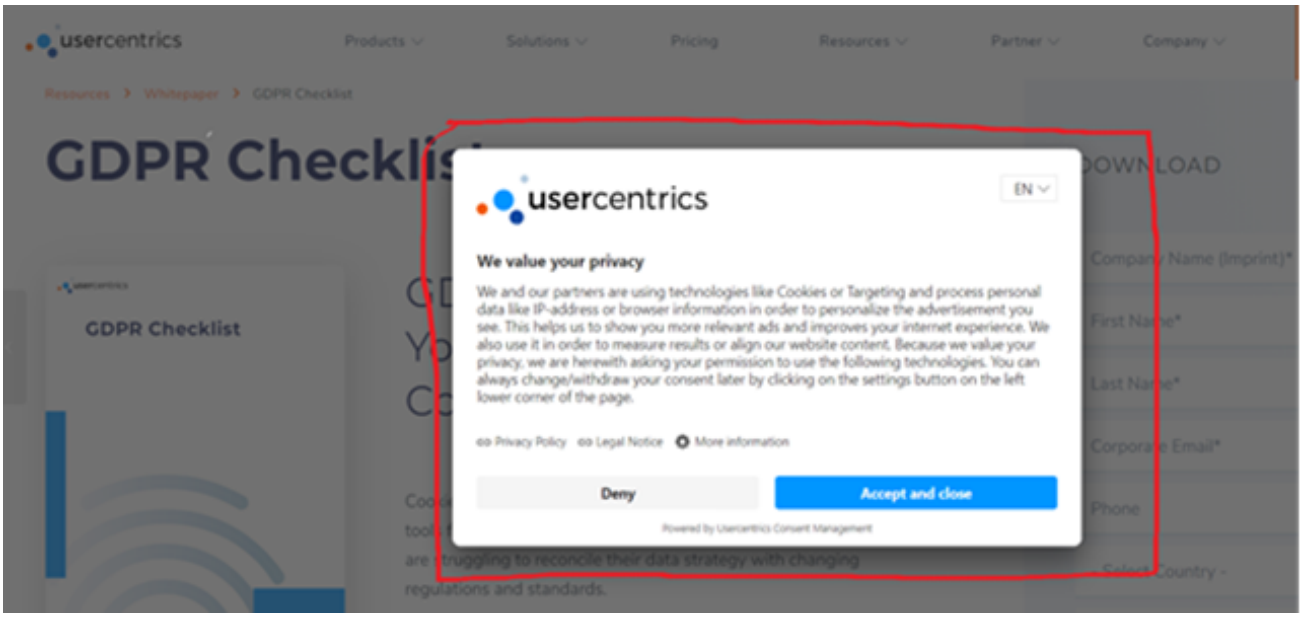
- Consent should be freely given, be specific and unequivocal.
- Requests for consent should be clear, distinguishable and presented in simple words.
- Data subjects have the right to retract their consent any time they feel like.
- When it comes to children under age 13, parents' permission is compulsory.
- Documentary evidence of consent needs to be saved.

Privacy rights

The individual, who agrees to reveal personal data, also has privacy rights. They are listed below (Wolford, 2019):

- The right to be informed
- The right of access
- The right to correction
- The right to deletion
- The right to limit processing
- The right to data portability
- The right to express objections
- Rights in relation to automated decision making and profiling.

Figure 18. An example of how access to personal data is asked through the internet



The California Consumer Privacy Act (CCPA) reinforces privacy rights and consumer protections for California residents. It's a California state law that was actually voted in June 2018 but didn't go into effect until January 1st, 2020 (Cooman, 2020).

According to CCPA personal data are considered to be any information that may lead to an individual's identification (such as name, address, email, passport number, social security number etc), commercial information (such as products purchased), electronic network activities, audio or visual data and conclusions drawn from any of the aforementioned information to create a profile about a consumer reflecting his preferences.

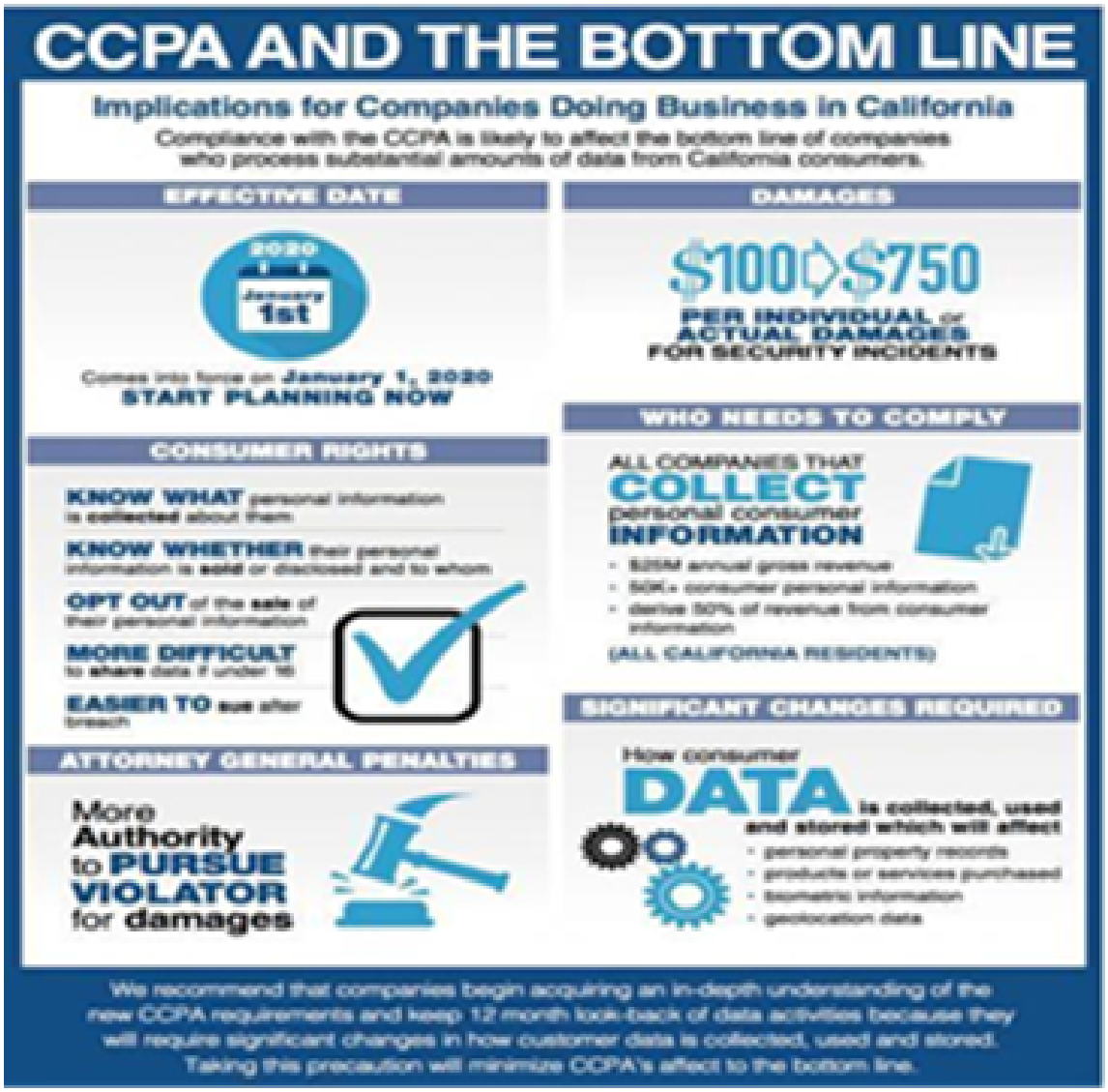
Similar to the GDPR, California's new CCPA law enshrines the rights of individuals to obtain information from technology companies about what data they have collected about a particular user and to demand that the companies delete all of the user's personal data.

One of the key aspects of the CCPA deals with the sale of consumers' personal data: the CCPA provides that consumers not only have the right to demand that companies disclose what data about a particular consumer is being collected for sales and business purposes, but also that consumers can demand that their personal data would not be sold.

Objectives of CCPA

1. Own your personal data
2. Control your personal data
3. Protect your personal data
4. Hold big companies liable

Figure 19. CCPA's basic elements



Main differences between GDPR and CCPA

Although GDPR and CCPA share common points, they are not interchangeable. Their key differences relate to the territorial scope and application of the law, to penalties – in case of violation – to nature and collection limitations and to the fact that GDPR requires lawful basis for all processing of personal data (A., 2021). The aforementioned are indicated in the following picture (A., 2021).

5.3. STATE DATA PROTECTION AUTHORITIES

State Data Protection Authorities (DPAs) are independent public authorities in charge of superintending the implementation of data protection laws, via investigative and corrective powers (What Are Data Protection Authorities (DPAs)? 2018).

DPAs offer expert advice concerning data protection matters and they are responsible for dealing with denunciations made due to violations of the General Data Protection Regulation (GDPR) and the respective national laws. In the context of GDPR all EU Member States should have a data protection authority, which is acting as the mediator among stakeholders within that Member State (Clerck, 2019).

State data protection authorities in the project partner countries:

- Lithuania: State Data Protection Inspectorate (https://vdai.lrv.lt/lt/)
- Austria: Austrian Data Protection Authority (https://www.dsb.gv.at/)
- Spain: Spanish Data Protection Agency (https://www.aepd.es/es)
- Greece: Hellenic Data Protection Authority (https://www.dpa.gr/en)
- Cyprus: Office of the Commissioner for Personal Data Protection http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
- Italy: Italian Data Protection Authority (https://www.garanteprivacy.it)

6 MODULE

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

CREW
Creativity, Resilience and Empowerment for Work

FINAL WORD

6.1. EVADE MID-CAREER "CRISIS" - STAY UP-TO DATE TO TECHNOLOGY

Technology is becoming more integrated with every aspect of our lives each day. Many people share their concerns regarding the fact that the world is changing so quickly and that they might find themselves out of the loop. This is a very legitimate thought currently, more common than one would assume.

No matter which field you are in, it is particularly important to stay up to date with technology to influence your personal and professional life. Technology has been rapidly increasing over the last decades and things that were previously thought to be impossible are being made possible at a very fast pace.

To know about the advancements in technology is by itself a fascinating treat to the mind. It is also important to get familiar with the new technology, because the old technology that you are used to work with will become obsolete quickly. You will gain the advantage in every field if your knowledge in technology is up to date. In the following section, the importance of keeping up with the new trends in technology development, needed for everyday life, will be presented.

Technology keeps us connected (especially with our family and friends)

As families continue to grow, members often move away from home for school, work, or to pursue their own families. Luckily, with the help of technology, communication has never been easier. Whether it be through text messaging, FaceTime or Skype, or any of the various social media sites, it's easy to stay connected with family and friends from afar. Modern tablets, computers and mobile phones almost all have the ability to use any of the above forms of communication to keep family and friends connected no matter where in the world they are.

Technology helps you to stay informed

The fastest and the most affordable way to learn about what is happening across the country or all over the world, is by "clicking" and "scrolling" on the news portals on the Internet. You may also subscribe for the news provider of your choice or to download the mobile phone application (in most of the cases for free) and it will enable notification on the current events that will keep you informed.

Technology enhances your productivity

There are many productivity apps that can help with staying productive and organized. For example, "Evernote" is a productivity app that works as an amazing file cabinet. It helps keep mental clutter at bay since it organizes everything for you.

Utilization of job portals as the most efficient technique for job seeking

We have come a long way from scooting for the next career option in every newspaper's career editorials and spreading the word about our joblessness in closed circuits of family and friends only hoping to get a reference sooner. However, the latest digital sensation is our saving grace and time, here careers are made on clicks. The job portals are the latest go-to for all you job seekers who are looking to just get started, interested in a change in career paths or just want to work outside of their old walls or to find a job in general.

E-services that make your life easier (online banking for example)

There's no doubt that digitalization has led to a revolution in financial matters. Online banking is done either through a laptop, tablet, or phone app is now the norm. Bank users can now check their incoming and outgoing payments remotely, as well as arrange money transfers and bill payments. Outside of banking, other financial matters, such as buying and selling currency and shares can be dealt with online. Transferring money between accounts both nationally and internationally has also seen a great deal of innovation in recent years.

6.2. INTERACTIVE GAMES AND APPS

DUOLINGO (https://www.duolingo.com/) helps you learn a foreign language.

STUDYBLUE (https://www.studyblue.com/) is a mobile study buddy designed to help you "conquer your course" using flashcards, notes, study guides, and more.

TYPINGCLUB (https://www.typingclub.com/) data-driven activities help mastery of keyboarding skills.

TED (https://www.ted.com/) – spread of intriguing or inspirational thoughts, usually in videos of 18 minutes or less.

YOUTUBE (https://www.youtube.com/) type the words "how to" into the app's search bar and you'll find everything.

QUIZLET

(https://quizlet.com/) – study aid supports learning at home, at school, and on the go.

LEARN CRYPTIC CROSSWORDS

(https://www.learncrypticcrosswords.com/) – cryptic crosswords aren't so cryptic once you start to learn some of the methods for solving them. This app does a really good job of explaining how to tackle puzzles, testing you with exercises.

ELEVATE: BRAIN TRAINING

(https://elevateapp.com/) – Self-isolation doesn't have to mean stagnation. Brain training apps such as Elevate are designed to keep your wits sharp with short daily exercises that test your memory, maths and other skills.

SKILLSHARE

(https://www.skillshare.com/) drawing, photography, graphic design and other creative disciplines.

COURSERA

(https://www.coursera.org/) offers programming, art and design, sciences and business and other subjects across 3,500 online-learning courses, complete with video lectures and instructors, with fellows to chat to.

GOOGLE ARTS AND CULTURE

(https://artsandculture.google.com/) – virtual tours of more than 2,000 "cultural institutions" around the world, using photos, videos and virtual reality.

Find out more about games and apps on:

https://bit.ly/2KOFFiK
https://bit.ly/2NA3Br9
https://bit.ly/39b33

Bibliography

1. Wheeler, S. (2009, Ed) Connected Minds, Emerging Cultures: Cybercultures in Online Learning. Charlotte, NC: Information Age.
2. Anderson, J. (2010) ICT Transforming Education: A Regional Guide. Bangkok: UNESCO Publication
3. Kress, G. (2009) Literacy in the New Media Age. Abingdon: Routledge.
4. Van Dijk, J. (2005). The Deepening Divide. Inequality in the Information Society. London: Sage Publications
5. Carr, N. (2008) Is Google Making us Stupid? The Atlantic, July/August Issue Retrieved May 21, 2012, from
6. http://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/6868/#
7. Keen, A. (2007) The Cult of the Amateur: How Today's Internet is Killing our Culture and Assaulting our Economy. London: Nicholas Brealey.
8. International Society for Technology in Education (2007). iste.nets.s: Advancing Digital Age Learning. Iste.org/nets.
9. http://www.newmedialiteracies.org/files/working/NMLWhitePaper.pdf
10. Qiu, Jack Linchuan. 2018. "China's Digital Working Class and Circuits of Labor." Communication and the Public 3 (1): 5–18. https://doi.org/10.1177/2057047318755529.
11. Refine web searches: https://support.google.com/websearch/answer/2466433?hl=en
12. https://ec.europa.eu/digital-single-market/en/trust-services
13. Nika, D., Gioldasi, P., & Vitta, F. (2017). Cyber bullying) vs cyber stalking.
14. Olweus, D. (2012). Cyberbullying: An overrated phenomenon?. European journal of developmental psychology, 9(5), 520-538.
15. Šléglová, V., & Cerna, A. (2011). Cyberbullying in adolescent victims: Perception and coping.
16. Cyberpsychology: journal of psychosocial research on cyberspace, 5(2).
17. Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for
18. prevention. Computers in human behavior, 29(1), 26-32.
19. Savižudybių, priskirtų patyčioms, sąrašas. Vikipedija.
20. https://en.wikipedia.org/wiki/List_of_suicides_that_have_been_attributed_to_bullying
21. Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election.
22. Journal of Economic Perspectives, 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211
23. Bjola, C. (2018). The Ethics of Countering Digital Propaganda. Ethics & International Affairs,
24. 32(3), 305–315. https://doi.org/10.1017/s0892679418000436
25. CyberWise. (2019, August 10). What Is Fake News? YouTube.
26. https://www.youtube.com080/21670811.2017.1360143

Erasmus+

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

Bibliography

27. How to spot fake news. n.d. [Illustration].
28. https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps
29. Spencer, S. H. (2020, February 11). Fake Coronavirus Cures, Part 2: Garlic Isn't a "Cure." FactCheck.Org.
30. https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/
31. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). Defining "Fake News." Digital Journalism, 6(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143
32. Tsompanidis, G. (2018) "Translated bibliography". Propaganda from the point of view of modern international law.
33. Gainsbury, S. M. (2015). Online Gambling Addiction: The Relationship Between Internet Gambling and Disordered Gambling. Current Addiction Reports, 2(2), 185–193.
34. https://doi.org/10.1007/s40429-015-0057-8
35. Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework.
36. Journal of Substance Use, 10(4), 191–197.
37. Kuss, D. J. (2013). Internet gaming addiction: current perspectives. Psychology research and
38. behavior management, 6, 125.
39. Kuss, D. J., & Griffiths, M. D. (2012). Online gaming addiction in children and adolescents: A
40. review of empirical research. Journal of behavioral addictions, 1(1), 3-22.
41. 2019 is the Year of . . . CCPA? [Infographic]. (2019). The National Law Review. https://www.natlawreview.com/article/2019-year-ccpa-infographic
42. A. (2021, January 7). CCPA vs. GDPR – differences and similarities. Data Privacy Manager.
43. https://dataprivacymanager.net/ccpa-vs-gdpr/
44. Cooman, G. (2020, January 28). What is CCPA and why should it matter to you? Proxyclick.
45. https://www.proxyclick.com/blog/what-is-ccpa-and-why-does-it-matter-to-you#DDP
46. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 59(6), 703–705. https://doi.org/10.2501/ijmr-2017-050
47. Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? GDPR.Eu.
48. https://gdpr.eu/what-is-gdpr/
49. What are Data Protection Authorities (DPAs)? (2018, August 1). European Commission - European Commission.
50. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

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

Bibliography

51. Clerck, J. (2019, November 25). Supervisory authorities: consistency and Data Protection Authorities (DPAs) under GDPR. I-SCOOP.
52. https://www.i-scoop.eu/supervisory-authorities-consistency-and-data-protection-authorities-dpas/
53. Allcott, H., & Gentzkow, M. (2017). Socialinė žiniasklaida ir netikros naujienos 2016 m. rinkimuose. Journal of Economic Perspectives, 31 (2), 211–236.
54. https://doi.org/10.1257/jep.31.2.211
55. Bjola, C. (2018).
56. Kovos su skaitmenine propaganda etika. Etika ir tarptautiniai reikalai, 32 (3), 305–315. https://doi.org/10.1017/s0892679418000436
57. „CyberWise“. (2019 m., rugpjūčio 10 d.). Kas yra netikros naujienos? „YouTube“. https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise
58. Kaip aptikti netikras naujienas.
59. https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps
60. Spenceris, S. H. (2020 m., Vasario 11 d.). Netikri koronaviruso vaistai, 2 dalis: česnakai nėra „gydymas“. „FactCheck.Org“.
61. https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/
62. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). „Netikrų naujienų“ apibrėžimas. Skaitmeninė žurnalistika, 6 (2), 137–153. https://doi.org/10.1080/21670811.2017.1360143
63. http://esaugumas.lt/lt/duomenu-vagystes.html
64. Gintautas Mažeikis. Metodinis leidinys „Propaganda“. Šiauliai, 2006.
65. https://atviri.emokymai.vu.lt/mod/book/tool/print/index.php?id=12
66. https://www.stuff.co.nz/technology/digital-living/68293880/japans-first-internet-fasting-camp-for-teens-a-success
67. Julius Zaleskis. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė (GDPR). Registrų centras, 2019.
68. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en
69. https://www.europarl.europa.eu/factsheets/en/home
70. https://researchguides.ben.edu/source-evaluation

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