DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

MANIFESTO

October 2018

www.digitproject.eu

Project number: 2017-1-PL01-KA204-038433

Editor in chief: Júlia Vilafranca Molero, Olena Korzhykova, Inma García (DomSpain)

Design: Elsa Prédour, Andrea Lapegna, Martina Gerli (LLLP)

With the contribution of all DIGIT partners:

We believe: Júlia Vilafranca, Inma García (DomSpain)
Tips for adult learners: Antonella Tozzi (DLearn); Martina Gerli, Ulla-Alexandra Mattl (LLLP)
Didactic and pedagogic guidelines for educators: Tina Baloh, Sabina Cokan (UPI); Júlia Vilafranca (DomSpain)

Topic 1: Tina Baloh, Sabina Cokan (UPI); Júlia Vilafranca, Olena Korzhykova (DomSpain)
Topic 2: Antonella Tozzi (Dlearn); Spyridon Blatsios (Platon)
Topic 3: Erika Conchis (Inova); Pauline Boivin (LLLP)
Topic 4: Katarzyna Pydzińska Azevedo, Gabriela Uberna (INnCREASE)

Glossary and resources: all partners

Thanks you also to the **educators** who reviewed the draft as well as the **proof-readers** and **translators**.

Project number: 2017-1-PL01-KA204-038433

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

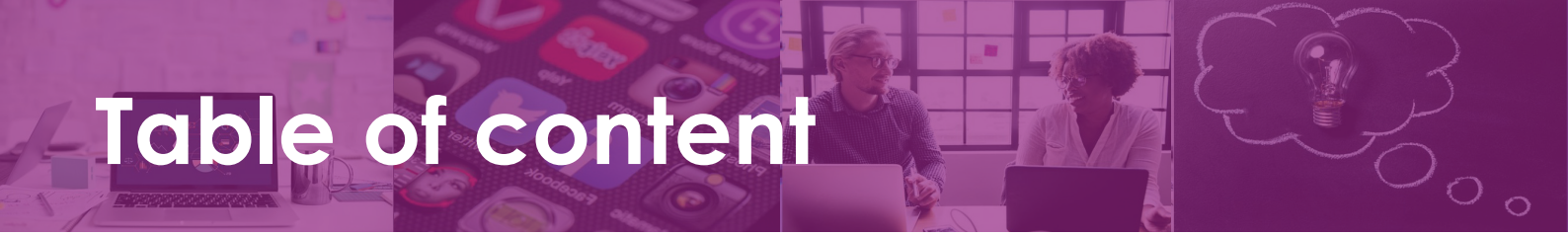
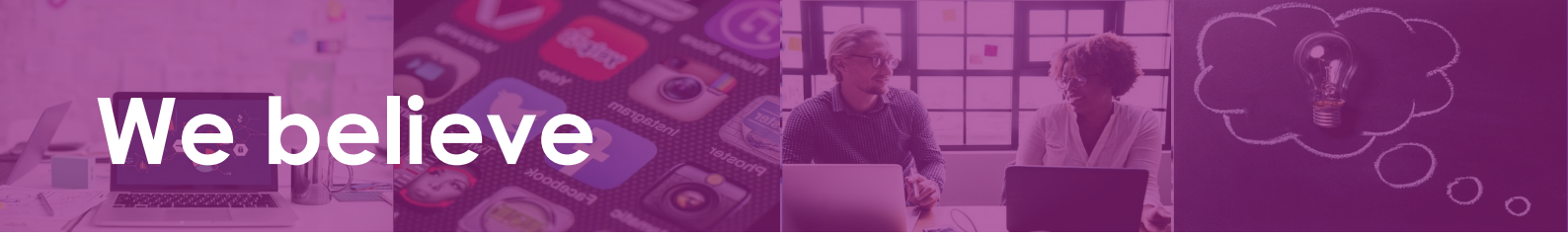


Table of content



We believe

DIGIT - 'Boost Competences for a responsible use of online identity' is a European project, funded under Erasmus+ KA2 'Strategic partnerships' and coordinated by Polish company INnCREASE. Partners stem from seven different countries: Belgium, Spain, UK, Poland, Greece, Italy and Slovenia. The project will last for two years (2017-2019) and seek to boost digital competences for a responsible use of online identity. Through this project the consortium aims to investigate digital identity implications for adults and provide the necessary educational instruments and supporting tools for adult educators.

This project is an initiative to raise awareness amongst European citizens about their responsibilities as digital users and improve their competences and skills in terms of digital identity, cyber threats to one's data and to one's public image and some aspects of cyber bullying and hate speech. 'DIGIT' was born from partners' concerns about the current digital challenges our society faces in terms of digital literacy. Research shows 44% of the EU population have low or no (19%) digital skills, despite the fact that the pace of technological and digital change is having a profound effect on our economies and societies. Similarly, studies show "Not having the necessary competences to successfully participate in society [...] increases the risk of unemployment, poverty and social exclusion".[1]

Due to the issues mentioned above, *this partnership believes*:

✓ **Digital skills** are now as vital as literacy and numeracy in Europe; therefore, there is a demand for digitally competent individuals to ensure they can fulfil their potential in society and feel socially included. The concepts of 'virtual citizenship and identity' pose a growing challenge for society and individuals to be informed about how their identity and digital footprint can be tracked on the Internet.

✓ There is an urgent need to raise awareness about the concept of 'a Digital Footprint.' This partnership defines **Digital Footprint** as a person's online trace or trail of data, which is created while using the Internet, which can be either a passive digital footprint (unintentional) or an active digital footprint (intentional). The general lack of awareness of the implications that a Digital Footprint has for individuals and the underestimation of its impact in our daily life, needs to be addressed as this concern continues to grow.

✓ **Digital Literacy** is understood to be an "individual's ability to find, evaluate, produce and communicate clear information through writing and other forms of communication on various digital platforms"[2] , we believe it should be one of the main educational goals for our society and that the existing lack of a public education system tackling such topics directly evidences that all EU governments educational agendas should include this issue if we are serious about raising awareness.

✓ Finally, given the **complexity** of the topic and the **numerous existing realities** around Europe, there is a need to create and run even more projects both internationally and transversally in this area.

[1] European Commission (2018), Council Recommendation on Key Competences for Lifelong Learning, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0604%2801%29.
[2] "Digital Literacy Definition | ALA Connect", connect.ala.org. Retrieved 2018-03-03.

Tips for adult learners

A digital footprint is the record or trail left by the activities you do online, such as social media interactions, information on your personal website, your browsing history, your online subscriptions, any photo galleries/videos you've uploaded — essentially, anything that can be traced back to you online.

In this section you can find some useful tips to help you understand the concept of DIGITAL FOOTPRINT and what actions you can take to become a responsible digital citizen.

DIGITAL FOOTPRINT: **do you think about it when you are online?**

✓ Digital footprint develops as you spend more time online!

✓ Reflect before posting something online and ask yourself: which kind of message am I sending to the public?

✓ Do you consider privacy options when opening a new account?

✓ Be sure to Google yourself, to check what others can see about you and see what information is out there about you.

MANAGEMENT OF PERSONAL ACCOUNTS AND IMAGE

With **your accounts online**, you can take many actions: from sending and receiving email, buying things, to staying in touch with your friends!

✓ Check and review your privacy settings every once in a while – do you know all your contacts personally? What do you want them to see?

✓ Read terms and conditions when you subscribe to something so you can see what third parties can register about your personal information.

✓ Limit the number of email accounts and delete those you don't use anymore... Are you still using MySpace for instance? Delete it!

✓ Always check the latest data regulation and privacy policies.

✓ Set control options for the financial operations you make online as purchases, or through your bank e.g. instant message when you transfer money or strong authentication settings.

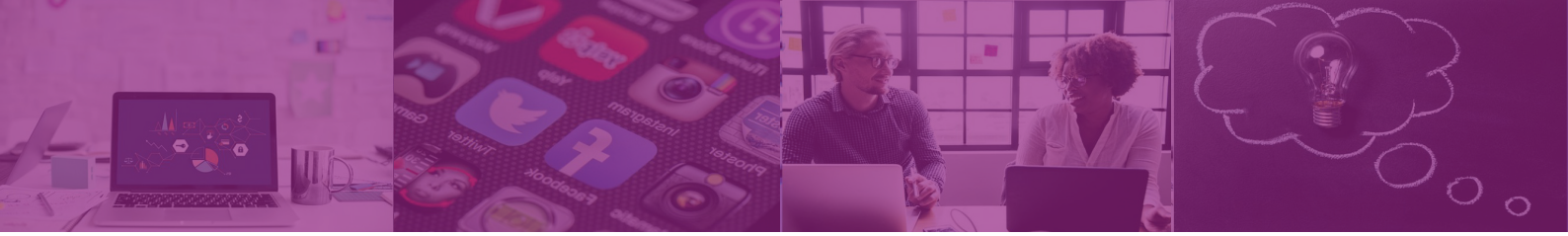
✓ Do not overshare personal information e.g. address, fiscal code, personal life details etc.

BE SAFE ONLINE AND SECURE YOUR PC

Be smart! There are some tricks you can apply to **navigate safely**.

✓ Use connections you can trust especially when you are in Wi-Fi mode.

✓ Change your passwords frequently and do not use the same for all your accounts. When you set a password, use long words, numbers and symbols and if you struggle to remember them consider using a password keeper!



✓ Consider antivirus and antispyware as an investment that can help protect your PC. There a lot of options, including free or very cheap ones.

✓ Try to stay informed on recent hacking cases, especially those involving big providers so you are aware of potential breaches of your data (such as recent Facebook and Twitter breaches!).

BE A RESPONSIBLE DIGITAL CITIZEN

Your **behaviour** online is equal to the one you have in public. Be a responsible citizen both online and offline!

✓ When you write something think about it: am I offending someone? Are there other ways to express my opinion? Apply etiquette the same as you would in person.

✓ When posting a picture, reflect on the subject! Is it appropriate? Is it damaging to me, my reputation or even someone else?

✓ When you share something, try to verify the source of the information and make sure you are not facing a case of fake news.

✓ Understand that when you send something online it can be traced forever.

BE AWARE OF THE SIDE EFFECTS OF EXCESSIVE INTERNET USE

The use and the overuse of the Internet involves **psychological and physical factors** which can lead to issues like addiction, isolation, nomophobia etc.

We should also pay attention to episodes of **cyberbullying** which may affect both us and the people around us.

✓ Balance the time you spend online, especially if you have children, so you can set a good example for them.

✓ Be informed of the symptoms of online addiction so that you can understand when you or a person around you is affected, and act upon this.

✓ Be aware of the fact that the information and advertisements you see online from social media are displayed according to your online habits, so they are not purely informative and can make you feel like you are living in a bubble.

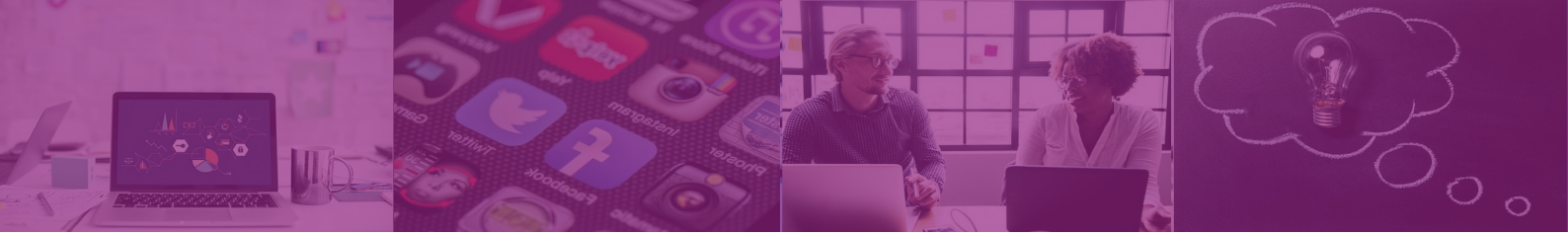
Didactic and pedagogic guidelines for educators

These **didactic and pedagogical guidelines** are dedicated for educators and other professionals who are already running, or would like to start running workshops, training courses and other learning activities for adult learners regarding digital footprint. It can also be used by those who have no experience in implementing teaching activities about digital footprint but are interested in the topic for personal or professional reasons or apply the recommendations included in this document in their ongoing classes (like language/IT, etc).

The guidelines refer to **four different topics/units** and include a set of suggested topics for discussion, learning goals and outcomes, examples of teaching activities and assessment activities. These guidelines are not prescriptive but aim to be a helpful tool when designing and running workshops about various aspects of digital footprint. The listed examples of activities and teaching methods within individual units could be adapted according to the focus of a particular teaching activity as well as to the needs of the target group. They should provide inspiration to create further activities or simply be an educator's timesaver.

These guidelines are to be used in a face-to-face **learning environment**; however, educators are encouraged to provide extra activities, tasks or homework to their learners if they consider it appropriate. Educators should also be aware that the time estimated for each suggested activity can vary depending on the group of learners.

Each unit stands for itself and is advised to start after a 10-15 min introductory activity to briefly present the project background, create a positive atmosphere and engage learners. It is highly recommended and important to discuss learners' expectations in the beginning of the workshop and elicit some of their existing knowledge. It can be helpful to motivate and engage them in the process of knowledge acquisition.



Introduction to DIGIT

TIME LOAD 10-15 minutes

ACTIVITY 1: about DIGIT

Explain how the course was developed and the main ideas of the DIGIT project. Show your learners how to access DIGIT website and all other materials already developed.

ACTIVITY 2: ice-breaking activity

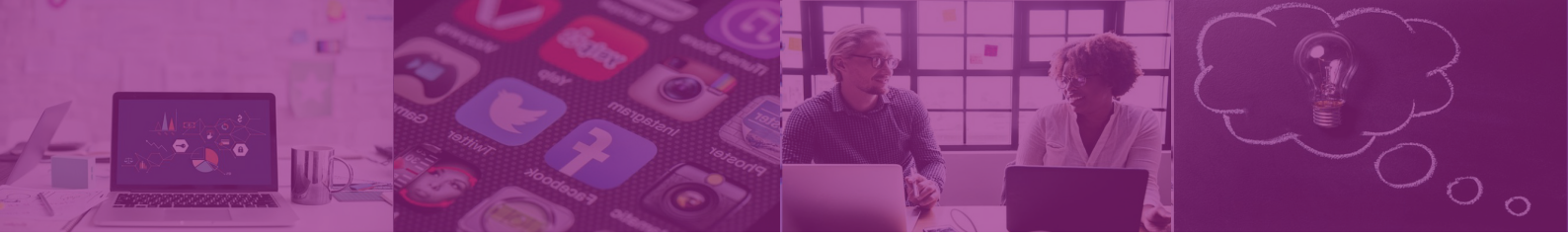
Start a discussion and brainstorming with your learners to check their previous knowledge on the topic. You can use these questions as prompts for discussion:

- Have you ever been surprised at how Gmail or Facebook knew certain things about you?
- Do mobiles or websites sometimes know your location even if you don't tell them?
- Do you see ads related to what you're interested in? Are they different from the ads your children/parents/friends see?

ACTIVITY 3: wrap-up

Ask learners to think about their expectations for the workshop and check them at the end of the workshop.

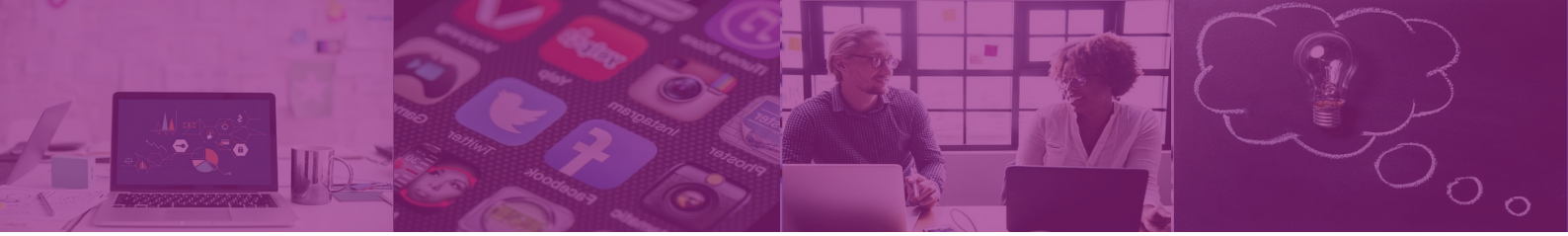
They can write them on post-it notes so they can be put on a visible spot in the venue.



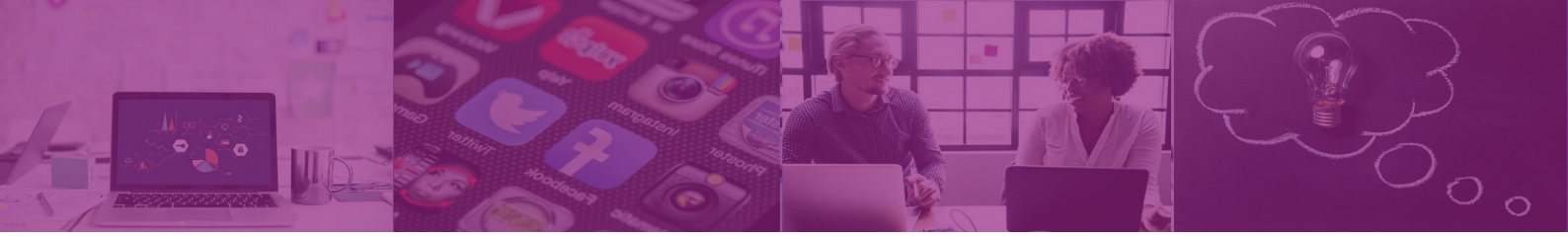
Topic 1:

Management of personal account and image

GENERAL INDICATIONS	
Time load	2-3 hours
Target group	Adult learners
Objectives of this unit	○ To make learners aware of different kinds of online accounts they are using; ○ To make learners aware of their online habits; ○ To teach learners how to check their privacy settings, especially in their social media accounts, and to show them how to change them; ○ To discuss an example of social media account abuse; ○ To show learners how to buy and make online reservations safely; ○ To learn about some of the most widely used shopping platforms and payment methods (e.g. eBay, Amazon, PayPal) and learn about the differences between them; ○ To teach learners about online banking and virtual banks and about digital certification and authentication systems and about the (dis)advantages; ○ To help learners understand the meaning of OIM.
Group size	5-15 people (recommended: 10)



Educator's competences required	Educators are able: ○ To create and manage one or multiple digital identities; ○ To protect one's own reputation; ○ To deal with the data that one produces through several digital tools, environments and services; ○ To share data, information and digital content with others through appropriate digital technologies. Educators are regular social media users.
Main topics and content	○ Personal accounts; ○ Social Networks; ○ Online shopping and banking; ○ User's rights; ○ GAFAM: Google, Apple, Facebook, Amazon, Microsoft; ○ Online Image Management (OIM).



Development of the didactic unit

LEARNING OUTCOMES

✓ Learners are aware of different kinds of online accounts they are using;

✓ learners are aware of their online habits;

✓ learners know how to find and how to change their privacy settings;

✓ learners are familiar with some very bad consequences of social media or e-mail account abuse;

✓ learners are informed about the advantages and disadvantages of online banking and shopping;

✓ learners are able to buy online and make online reservations;

✓ learners know some widely used shopping platforms;

✓ learners know how online banking and virtual banks work and know what digital certification and authentication systems are;

✓ learners understand the meaning of OIM (Online Image Management).

INTRODUCTION AND INITIAL EXPLORATION

This is an introductory phase. The estimated time is 10-30 minutes, depending on how much your students already know about the topic.

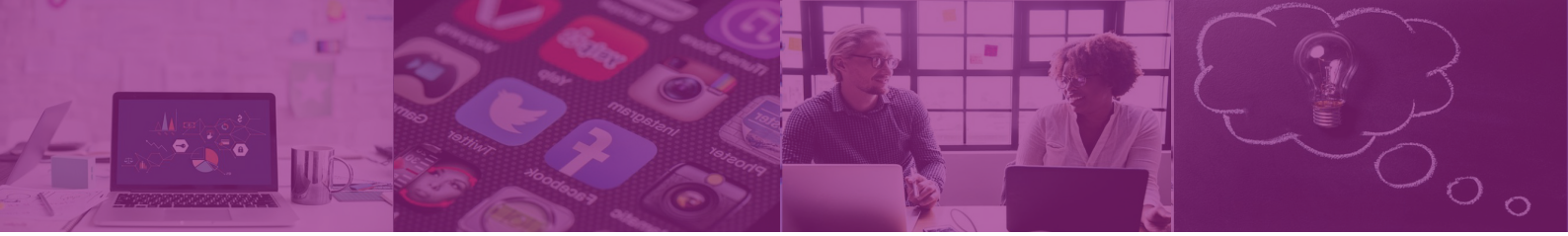
After making sure that both learners' expectations and the learning goals of the unit are on the same line, start introducing the topic. An important aspect at this point is to introduce the vocabulary you are going to use: collect all terms and concepts that might be new to anyone and go through them. It is also important to give them an overview of the topics you are going to present and about how relevant they are in their lives.

Start with a **pre-assessment test**: check what concepts and terms they know. Then, discuss the test as a group or by peer-reviewing it.

Suggested **practical activities**:

a. *Pair/group work* (≈10 minutes): organise the group into pairs, or groups of three and give them some vocabulary items. Ask each group to write down a definition for each term. Then, they will read only the definitions aloud and the others have to guess the term.

b. *Working on definitions* (≈10 minutes): provide incorrect or partly incorrect definitions of the vocabulary you consider more difficult. Discuss in small groups or as a class why they are incorrect and how they would change them.



Examples

» *Digital Certificate is a «password» that allows a person to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate.*

The above definition is not precise enough.

→ Correct: *Digital Certificate is an electronic «password» that allows a person and organisation to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate.*

» *Passive digital footprint is a data trail that other people post about you.*

→ Correct: *A passive digital footprint is created when data is collected without the owner knowing (also known as data exhaust), whereas active digital footprints are created when personal data is released deliberately by a user for the purpose of sharing information about oneself by means of websites or social media.*[1]

» *Online identity management (OIM) is a set of methods for creating a person's special profile on social networks such as Facebook, Instagram or Snapchat.*

→ Correct: *Online identity management (OIM) is a set of methods for creating a distinguished Web presence of a person on the Internet.*

c. *Brainstorming* (≈15 minutes): learners think about and write down all online personal accounts they use. Hold a more open discussion/brainstorm to start working on the topic. Some suggested questions are:

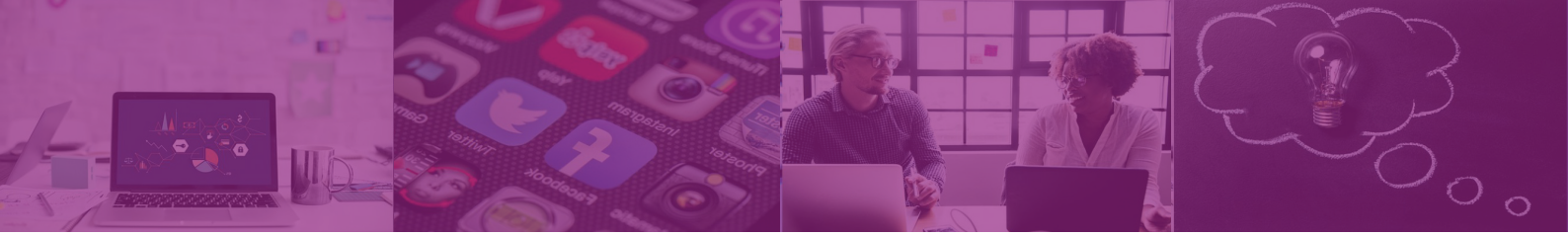
» How often do you check privacy settings of your various accounts? Do you ever adjust them?
» How many social media accounts do you have? What kind of information on your social media account do you share with public?
» Why do you think having a digital footprint is a necessity in our day and age?

d. *Introduction video* (≈15 minutes):

» learners watch a video about teenage social media use (TedX conversation with Simon Sinek);
» use a video or short clip to introduce the topic: choose an example of influential people or 'youtubers' to engage them in discussions about how our privacy is shared online and about its consequences (e.g. DG JUST | Take control of your personal data).

e. *Short lecture* (≈15 minutes): provide a short

[1] Source: https://en.wikipedia.org/wiki/Digital_footprint



intro lecture by giving the learners some interesting (statistical) facts to challenge their thinking (teaching source to be added later).

f. *Short Q&A session* (≈10 minutes): ask some introductory questions to make people start thinking about whatever topic you want to discuss further:

» Do you use online banking?
» Which one do you prefer: online or "regular/normal" shopping and why?
» Do you think online banking/shopping make our lives better?
» Do you know what OIM stands for?
» Do you ever read User's rights?

g. *Quiz* (≈15 minutes): present a short introductory quiz about online habits (adapt the quiz that was used for focus groups).

DEVELOPMENT AND APPLICATION

In this phase, students develop and build up their knowledge on the topic. The estimated time is 30-45 minutes.

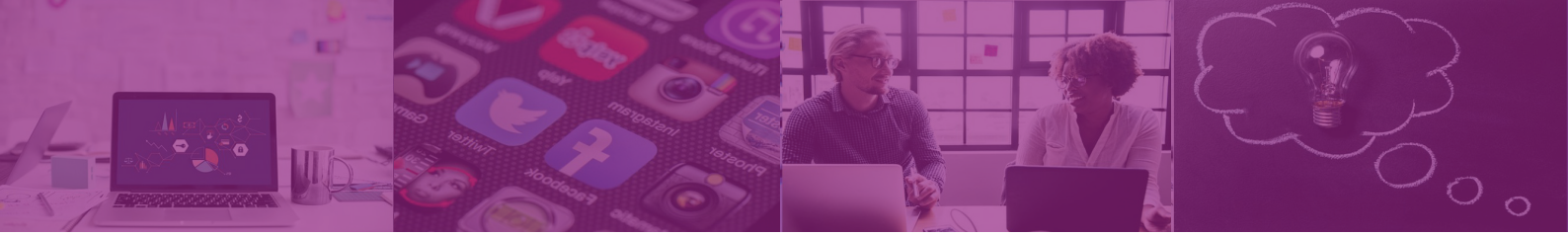
Now it is the learners' turn to use their previous experience and the information gathered in the exploration phase to build up new knowledge and to apply it. It is important to engage them in group discussions and make them share ideas. Educators should encourage peer-work to get the most out of every individual in order to show students how to identify problems about this topic in different contexts (at work, in their personal lives, in the educational community) and in different types of groups (teenagers and young people, adults, elder people...). In addition, they are acquainted with and/or suggest possible solutions to presented challenges.

Suggested **practical activities**:

a. *Group discussion* (≈15 minutes): talk about our real and online identity. Give students a set of questions:

» What is identity? Is it important for us?
» Are real identity and online identity the same thing?
» Do we lie when we are online?
» Do we behave differently in each type of our Social Media profiles?

b. *Group presentations* (≈20 minutes): divide your group in pairs or small groups and give each of them a research task: research online about a close friend or a family member of yours. Make them prepare a short presentation using PowerPoint, Prezi or similar visual aids showing how much they



have been able to find online about their personal/private life. After the presentation, encourage a debate/discussion about it and about how this issue could be prevented.

c. *Pro and contra debates* (≈20 minutes): split the group in two and give them a chart to fill in, with pros and cons of different statements (do the groceries online; always pay by credit card; pay with your phone, etc.) Afterwards, share the groups' ideas and encourage a debate/discussion about it.

d. Present your students different *case studies* (≈20 minutes) about identity theft by taking examples from the Internet (your country or abroad (e.g. NordVPN | Identity Theft - 8 Case Studies). Students discuss the possible reasons for identity theft, the consequences, and they think about possible solutions. They try to think of similar case in their environment or their country. Eventually, they share their opinion/experience with other groups.

e. Ask your students to list down all *daily activities* (≈15 minutes) they carry out *using the Internet*. Then, identify those they could do without the Internet and those, which would be impossible without it. Start a debate on whether it is a choice using the Internet for almost all our daily activities.

f. *Work in groups* (≈20 minutes): divide your class in pairs or small groups. Each pair chooses an online platform or Social Network (Facebook, Gmail, Drive, Instagram, Dropbox...), goes through (skimming) the *terms and conditions* and writes down all those sentences which are complex, ambiguous and difficult to understand. Let them share their findings. Start a debate about how users should be informed about the terms and conditions.

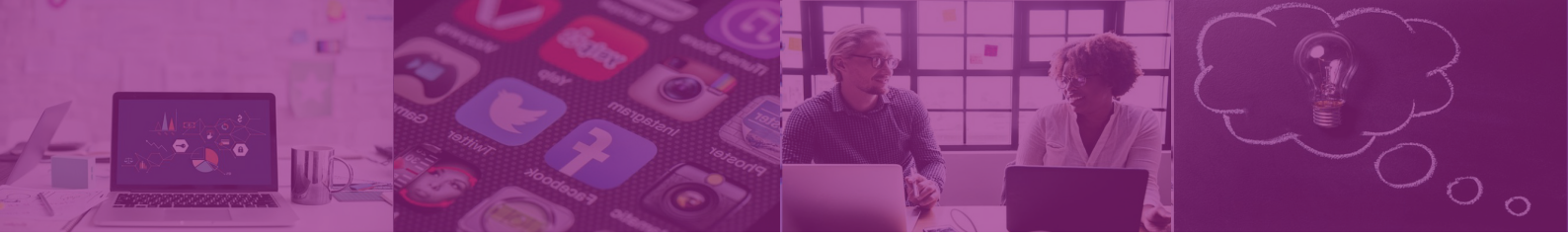
CONCLUSION

This is the final and concluding phase of the unit. The estimated time is 10-20 minutes.

For the last 10-20 minutes of the session, summarise the main points discussed and refer to further learning resources. It is also time for students to share their impressions and provide some feedback. Encourage them to ask questions or express their doubts about any issues that are still not clear to them.

Suggested **practical activities**:

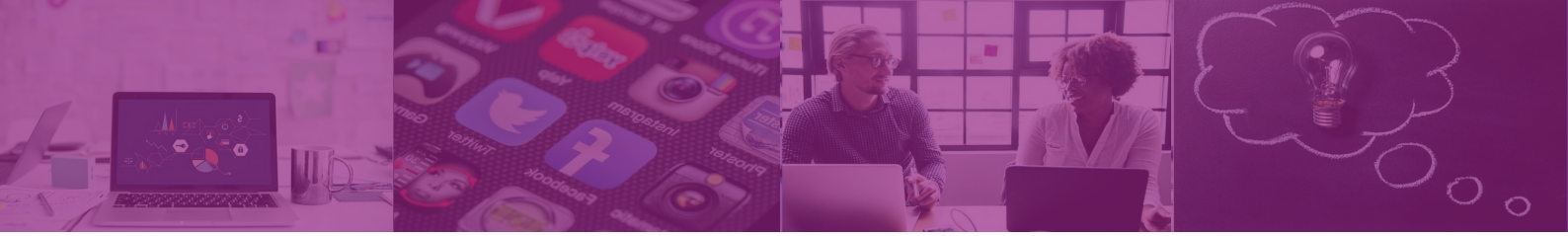
a. *Self-reflection activities* (≈15 minutes): ask the students if they would change their behaviours online after this session and encourage them to share their ideas.



b. *Quiz* (≈20 minutes): use an online tool (such as Kahoot) to revise and check students' understanding of the main concepts you have dealt with.

c. *Post-assessment test* (≈10 minutes): check if all concepts and terms discussed have been understood, give your students an assessment test with exercises such as defining vocabulary, yes/no questions or multiple choice. Correct the test as a group or by peer-reviewing it.

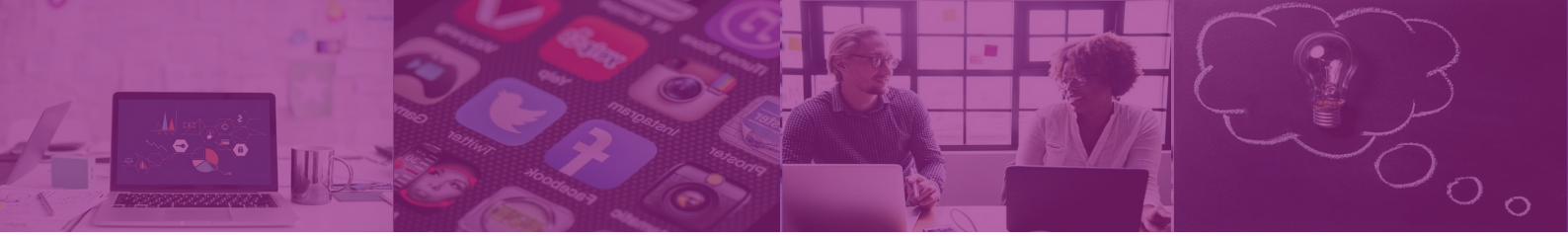
d. *Group wrap-up activity* (≈15 minutes): as a final activity, create in a group the 'top ten rules to manage your online personal accounts safely'. Start brainstorming and narrow down the rules mentioned to a list of the 10 essential things to take into account when managing your online accounts.



Topic 2:

Be safe online and secure your PC

GENERAL INDICATIONS	
Time load	2-3 hours
Target group	Adult learners
Objectives of this unit	○ Explain to learners the concepts and implications of computer security, IT security and Cybersecurity; ○ Explore with learners the different faces of PC security; ○ Explore with learners the different faces of Cybersecurity; ○ Raise awareness on social engineering phenomenon explaining the different threats such as, vishing, phishing, scamming etc.
Group size	5-15 people (recommended: 10)
Educator's competences required	○ Be familiar with issues such as, PC security, Cybersecurity; ○ Be able to relate and contact authorities or experts in the field of Online security and Social engineering.
Main topics and content	○ General framework about cybersecurity and pc security; ○ Privacy issues on the main online account (encryption, cryptography and anonymity); ○ Cookies and spam; ○ Viruses and other threats to the pc security; ○ Internet Security software, Firewalls; ○ Social Engineering concept and threats.



Development of the didactic unit

LEARNING OUTCOMES

✓ Learners know about the difference between pc security, IT security and cybersecurity;
✓ Learners are aware of the different implication of privacy issues;
✓ Learners can decide upon cookies or detect spam threats;
✓ Learners are able to defend themself from viruses and other pc security threats;
✓ Learners are able to choose the best internet security software for their needs;
✓ Learners knows about social engineering;
✓ Learners are able to recognise an online threats and can protect themselves and their device.

INTRODUCTION AND INITIAL EXPLORATION

This section is important to understand the level of knowledge among learners of this topic (estimated time: 1h).

Introduction

Learners' self-assessment: ask them some initial general questions like:

» Have you ever heard about cybersecurity?
» Do you secure your pc? How?
» Have you ever had your pc infected by a virus?

Collect their answers on sheets or on the flip chart so you can keep it for the end of the session.

Elicitation

Use some videos to start introducing some concepts like cybersecurity and social engineering and to trigger discussion among the group.

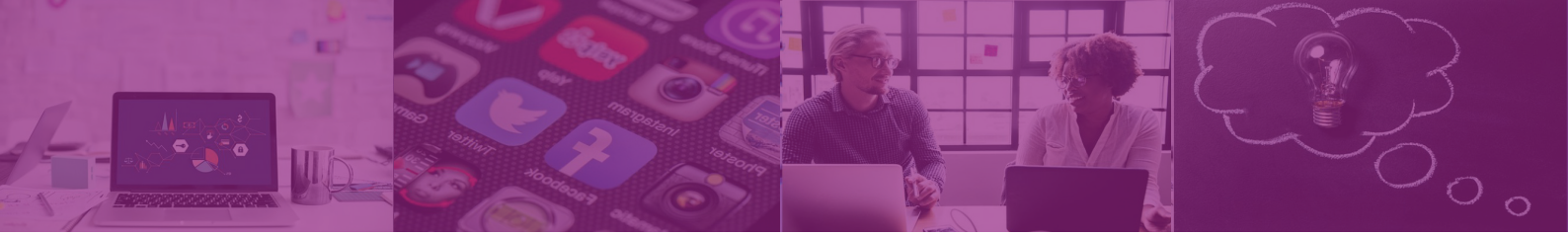
Selection of videos on the topics of hackers' attacks, cyber security, social engineering:

- Top hacker shows us how it's done | Pablos Holman | TEDxMidwest
- Cybersecurity: Crash Course Computer Science
- Cybersecurity 101
- Cybersecurity Basics

Promoting investigation

Divide learners in small groups and give them real cases of cyber security and PC security threats. Some video examples:

- Vishing
- Spam
- Ransomware



Ask them to discuss the cases and tell if they had some similar issues.

(Self) Evaluation

Ask the learners to answer the initial questionnaire again to self evaluate their stance and attitudes so far on the topics discussed.

DEVELOPMENT AND APPLICATION

This part of the session should allow learners to acquire precise information about the topic and to deepen what they have learned in the introduction phase.

a. Introduce to the learners some theory about PC security, cybersecurity and Social Engineering.

» You can use this platform to make it more attractive (EN only): ENISA Threat Landscapes (20 minutes).

b. Invite an expert from the law enforcement agency from your country or IT sector to talk about security implications and adoption of evolving technology (risk associated with the growth of mobile computing, cloud technology, outsourcing, management processes and practices) (30 minutes).

c. Show some real case studies and analyse them through discussion sessions.

» Alternatively, ask learners to research reliable sources of information for real case studies and how they were handled, and ask them to present their findings to the class.
» Relate to ENISA website for general approach: ENISA | What is "Social Engineering?"; Europol | 15 ways you could be the next victim of cybercrime.
» Famous social engineering cases: Gatefy | 7 real and famous cases of social engineering attacks.

d. Discussion with learners and eventual sharing of experiences among them (15 minutes).

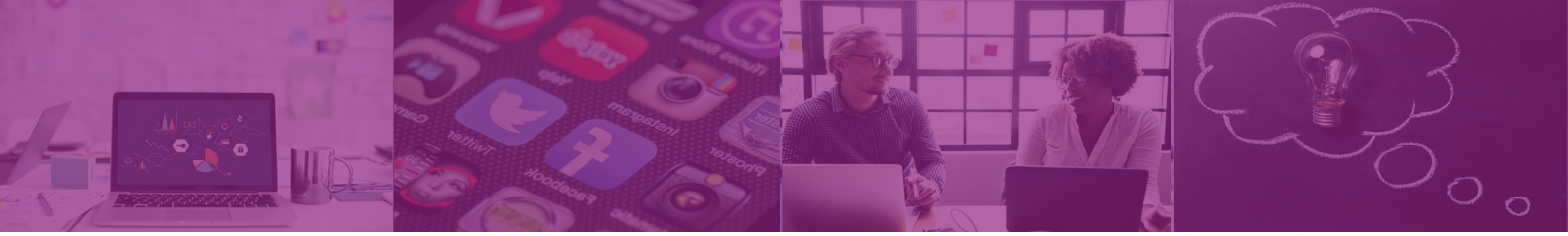
CONCLUSION

This is the final phase of the unit. The estimated duration is 10-20 minutes.

For the last 10-20 minutes of the session, summarise the main points discussed and refer to further learning resources. It is also a time for learners to share their impressions and provide some feedback.

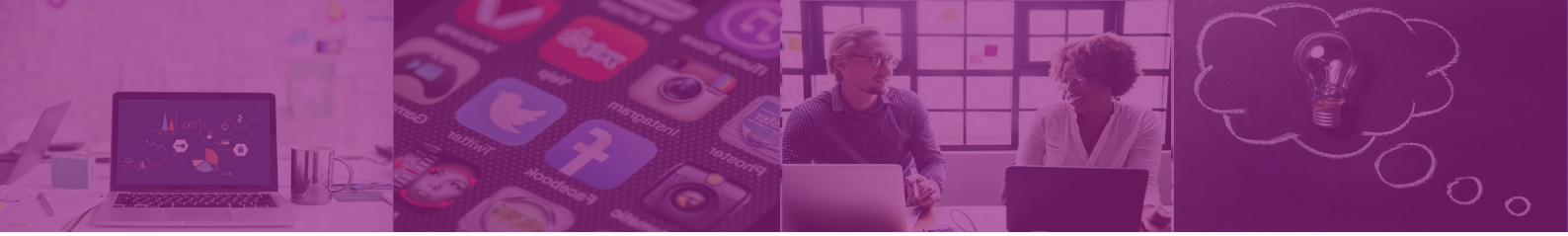
Suggested **practical activities**:

a. *Self-reflection activities* (≈15 minutes): ask



the students what they would change about their behaviours online after this session and encourage them to share their ideas.

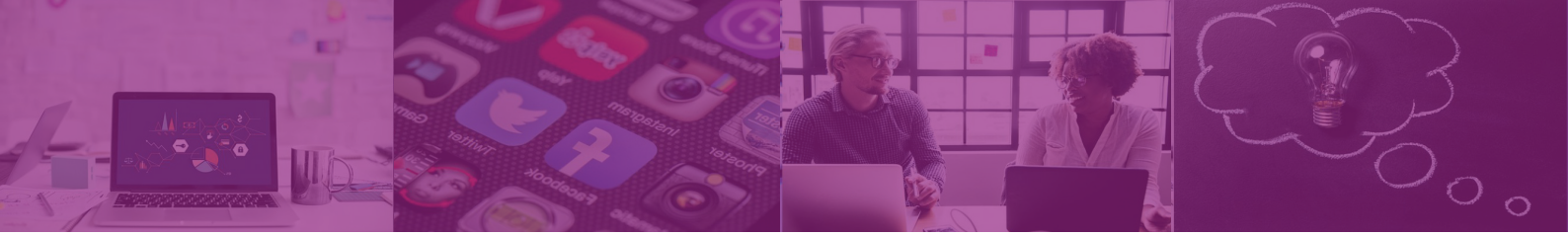
b. *Post-assessment test* (≈15 minutes): check if all concepts and terms discussed have been understood, give your students an assessment test with exercises such as defining vocabulary, yes/no questions or multiple choice. Correct the test as a group or by peer-reviewing it.



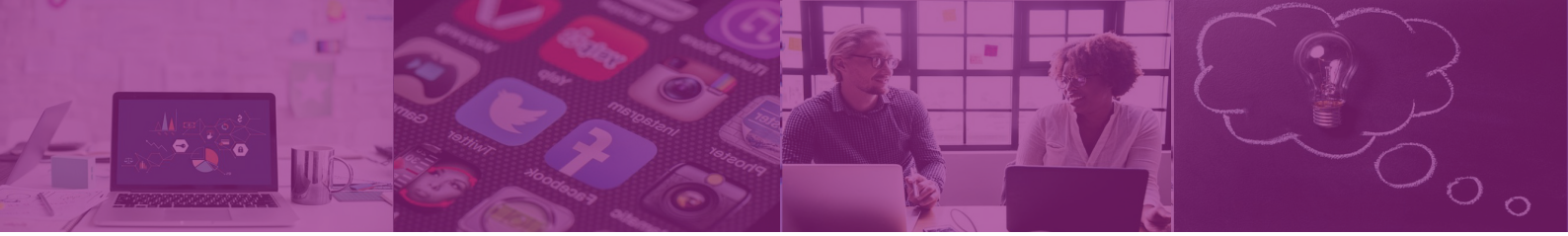
Topic 3:

Be a responsible digital citizen

GENERAL INDICATIONS	
Time load	2-3 hours
Target group	Adult learners
Objectives of this unit	○ Better understanding of the concept and issues related to digital citizenship; ○ Discuss and debate the implications of being a citizen in a digital world (challenges, risks, opportunities...); ○ Raise awareness of learners about the digital dimensions of citizenship (rights, law, identity, participation to politics, etc); ○ Raise awareness about other emerging issues: fake news, cyberbullying, hate speech, etc; ○ Enhance the knowledge of and access of participants to the digital citizenship tools and services (e.g. e-administration); ○ To learn the national or regional frameworks, ecosystem (law and public or private entities) that govern their rights, or can give them advice; ○ How to engage in politics online: the different forms, channels, the differences with offline participation, etc.
Group size	5-15 people (recommended: 10)



Educator's competences required	○ Regular user of Social Media; ○ Digital literacy; ○ Understanding of the concept of digital citizenship and related issues.
Main topics and content	○ Digital citizenship; ○ Digital Freedom, law, rights and responsibilities; ○ Digital Etiquette; ○ E-Democracy/e-governement: transformation of democracy and policy-making through the use of digital technologies that leads to new forms of democracy (for instance, liquid democracy); ○ E-administration: Access and use of online administration procedures and identity documents; ○ Web neutrality; ○ Echo chambers & filter bubble.



Development of the didactic unit

EXPECTATIONS AND LEARNING OUTCOMES

✓ Learners are aware of the concept of digital citizenship;
✓ Learners are aware of their digital rights and responsibilities and of the laws that protect them;
✓ Learners understand what "Digital Etiquette" is;
✓ Learners are familiar with "E-Democracy" and online "policy-making" issues and opportunities (e.g. what apps to use to participate in politics, online movements and campaigns);
✓ Learners are familiar with the concept of new forms of democracy (for instance, liquid democracy);
✓ Learners are informed of the concept of "e-administration";
✓ Learners are aware of how to access and use online administrative procedures and identity documents;
✓ Learners are aware of the issues connected to "web neutrality";
✓ Learners understand the concepts of "Echo chambers" and "filter bubble" as well as their related issues;
✓ Learners are informed of emerging issues such as fake news, hate speech, cyberbullying, etc. and aware of their rights relative to such issues.

INTRODUCTION AND INITIAL EXPLORATION

This is an introductory phase. The estimated duration is 20-30 minutes, depending on how much your students already know about the topic.

After making sure that learners' expectations and learning goals of the unit are on the same line, start introducing the topic. An important aspect is to introduce the vocabulary you are going to deal with: collect all terms and concepts that might be new to learners and go through them as a class. It is also important to give learners an overview of the topics you are going to deal with and explain their relevance to their life.

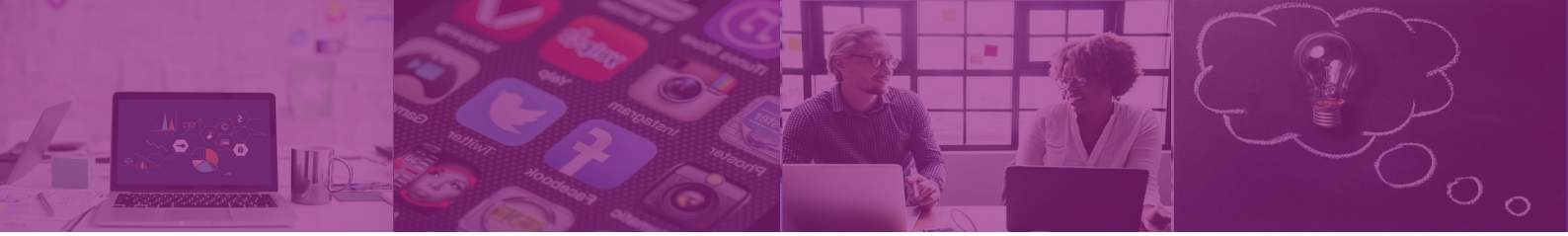
Suggested **practical activities**:

a. *Questions to the participants* (≈15 minutes) to evaluate the learners' level of awareness regarding the topic:

» What do you think "digital citizenship" is? What does it mean to be a "digital citizen"? Definition of the concepts and their scopes.
» Do you post, comment, share political-related topics on the Internet?

---

b. *Teacher's short presentation* of the context and issues (≈10 minutes): provide some statistics, present the general context and



set aside some time for Q&A.

Exploration:

a. Exercise on information/media access, processing/analysis and research (≈ 15 minutes): how to detect fake news, which are their recurrent channels, impact of fake news and examples.

b. Activity: knowledge exploration with the learners knowledge exploration - "Connect/ Extend/Challenge" exercise[1] (≈10 minutes).

Methodology

The aim of this introductory activity is to explore what connections learners make between new concepts such as digital citizenship, and how they connect them with prior knowledge. This will allow the facilitator to adapt the training delivery, if needed.

» *Connect*: how does the ideas and information on digital citizenship connect to what you already knew?
» *Extend*: is the digital citizenship topic extending your thinking in new directions?
» *Challenge*: how is the digital citizenship topic challenging or confusing for you to wrap your head around? What questions, wonderings or puzzles do you now have?

c. Watching and commenting a video (≈ 10-15 minutes); find other resources on the topic if needed.

▷ Example (in English): Lessons On Digital Citizenship From Charlie Brown | Marialice Curran | TEDxYouth@BHS (13 minutes)

DEVELOPMENT AND APPLICATION

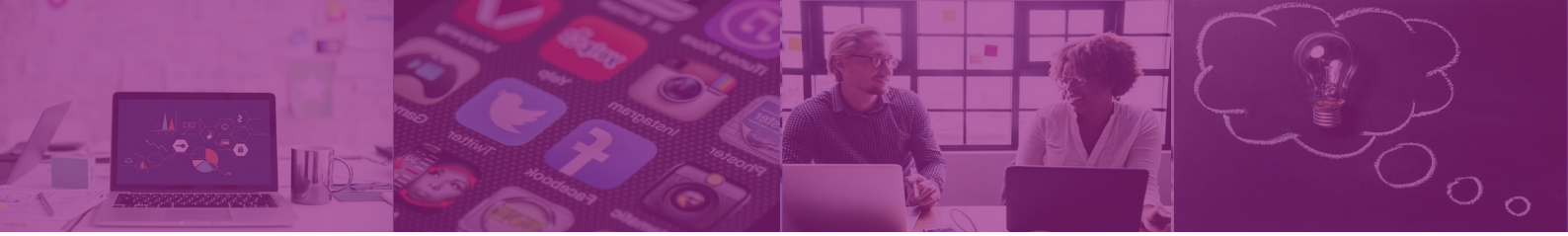
In this phase, learners develop and build up their knowledge on the topic. The estimated duration is 60 to 120 minutes.

Now it is the learners' turn to use their previous experience and the information gathered in the exploration phase to build up new knowledge and to apply it. It is important to engage them in group discussions and make them share ideas. Educators should encourage peer-work to get the most out of every individual in order to show students how to identify problems about this topic in different contexts (at studies/work, in their personal lives, in the educational community) and in different types of groups (teenagers and young people, adults, elderly people...). In addition, they are acquainted with and/or suggest possible solutions to the challenges presented to them.

Suggested **practical activities**:

a. *Small groups discussion* (≈15 minutes): how

[1] Other resources on the Connect/Extend/Challenge exercise: http://www.visiblethinkingpz.org/VisibleThinking_html_files/03_ThinkingRoutines/03d_UnderstandingRoutines/ConnectExtendChallenge/ConnectExtend_Routine.html



to digitally engage in politics and the 'spaces' of participation (online platforms, social media, blogs); tools (apps, petitions, online campaigns, communication, multimedia). Check which ones already exist and invent new forms of participation.

b. *Group work*: provide your students with a printed copy or a link to the "EU General Data Protection Regulation (GDPR) Portal" (https://www.eugdpr.org) and ask them to read the GDPR Key Changes section. Learners should make a list of the most relevant points. Other official documents on this issue can be used, such as national ones.

c. *Case analysis* (≈10 minutes): how the web has had an impact on politics/politicians. Search and discuss examples of politics or politicians being affected by Internet.

d. *Presentation by the educator and/or online research* (≈ 15 minutes): presenting the main legal instruments applicable to the learners, their legitimate rights as well as the organisations concerned with he protection of digital citizenship rights. Possible topics: hate speech, European regulation and law (GPDR, e-privacy: Privacy and Electronic Communication Regulations (PECR)); the role of Internet service providers and social media.

e. *Build a campaign to defend digital citizenship rights*: divided in mini-groups, the learners will have to create a campaign or join one. For instance, a campaign against bullying, online hate speech, etc. Educators may use Canva as a tool to create a poster for the campaign. Can be linked to the following activity (f).

f. *Look for and at examples of national, regional or local campaigns on digital citizenship-related topic* (≈ 20 minutes), individually or in groups of maximum three learners, with the use of a computer. Possible topics: online hate speech, cyber-bullying, etc.

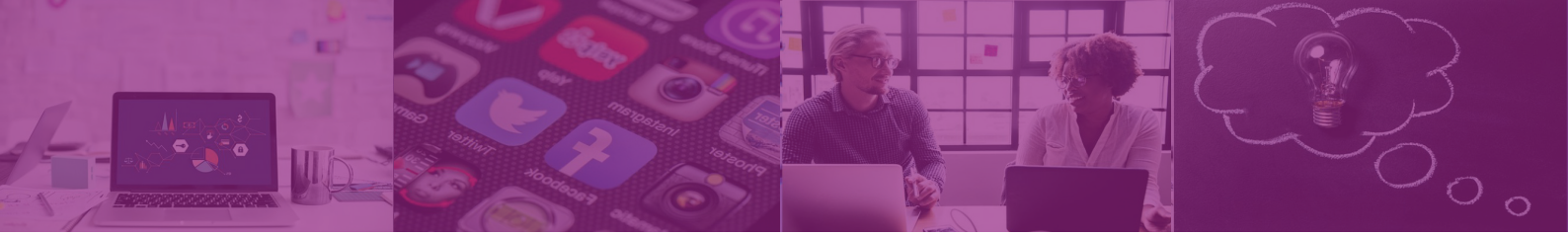
Possible exercise:

Create your own "campaign" by designing a poster about digital citizenship issues - learners can use free resources and user friendly platforms such as Canva.

Topic examples:

» Campaign against bullying
» Campaign against hate speech

These posters can then be printed out, adult learners can show them to their children, etc.



g. *Open discussion on new forms of democracy* (≈ 20 minutes): is the Internet a tool for "direct democracy"? The teacher can also inform their learners about new concepts (e.g. apps, liquid democracy) and discuss it with them.

---

h. *Debate: pros and cons* (≈ 25 minutes): after dividing the class in two groups, the educator will task one with finding arguments for the "pros" and the other with finding arguments for the "cons". Possible topics: free speech, digital democracy, … .

---

i. *Activity: "6 Thinking Hats"* (≈ 30 minutes , including 10 min. to explain the exercise and 20 min. of discussion).

Methodology:

This methodology allows to look at a topic from all points of view - it eases the conversations since every perspective is valid. Turn by turn, all participants will wear the different "hats" and deliver a different point of view on a topic/issue. The different hats are:

» *White hat*: neutral objective: focusing on facts, data, figures;
» *Red hat*: emotional view: intuition, feeling;
» *Yellow hat*: logical, positive, looking for the benefits;
» *Green hat*: creativity, looking for new ideas, growth;
» *Blue hat*: planning, process oriented from start to finish points of an idea;
» *Black hat*: judgemental, logical.

Possible topics:

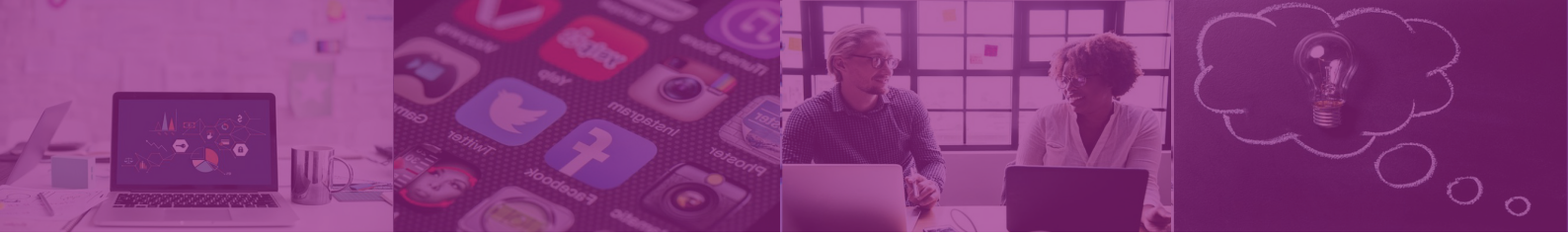
» E-democracy, e.g. online voting: "how can we vote online? What are the risks, the opportunities?…"
» Digital responsibility, e.g. anonymity and responsibilities, cyber-bullying: "how can we prevent cyberbullying? How to talk about cyber bullying?…"

This exercise can be adapted to different topics according to the learners' interest in and knowledge of the topic.

CONCLUSION

This is the final and concluding phase of the unit. The estimated duration is 20-30 minutes.

For the last 20-30 minutes of the session, summarise the main points discussed, reflect on what the learners have learned and refer to further learning resources. It is also time for learners to share their impressions and provide some feedback. Encourage them to ask questions or express their doubts about any issues that are still not clear to them.



Suggested **practical activities**:

a. *Activity: Wrap Up Exercise* (30 minutes)

Methodology:

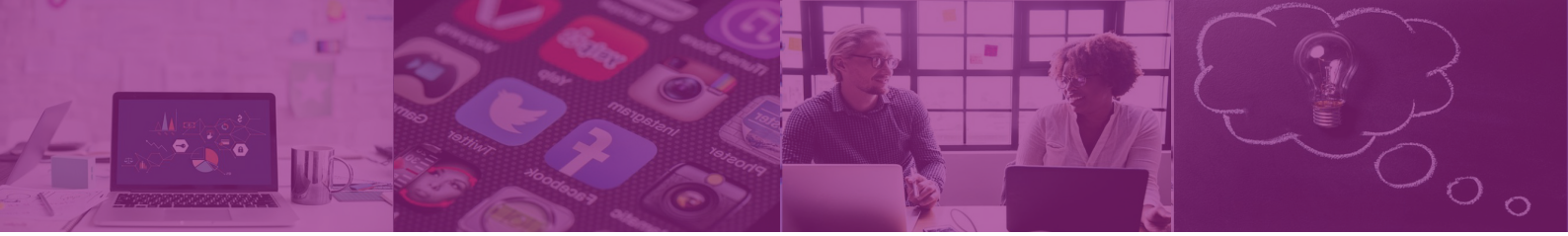
This exercise is based on the Johari Window model. On a printable template, learners complete the following table:

What I learned about the topic: - - - -	What surprised me about this topic: - - - -
How has my perspective changed based on today's discussion? - - -	What I would like to learn: - - - -

This exercise will allow to wrap up the training activities, summarise the learning outcomes and gain feedback on the learners' expectations vs. achievements.

b. Quiz or assessment test.

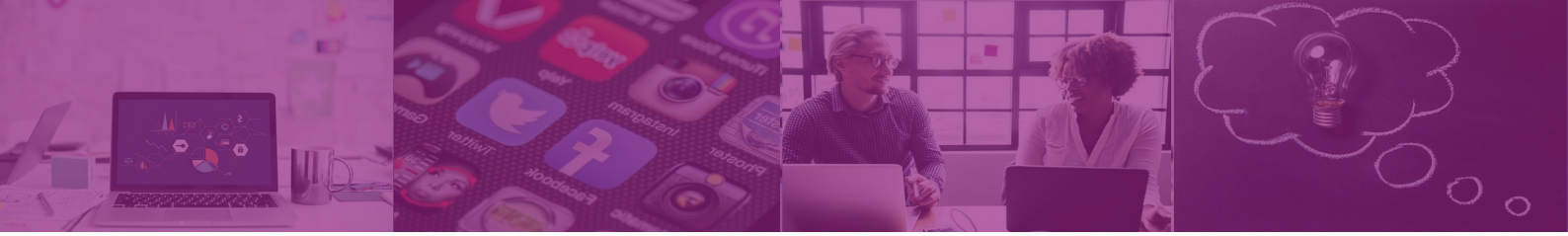
c. Provide a resource sheet ('to know more' about the topic.



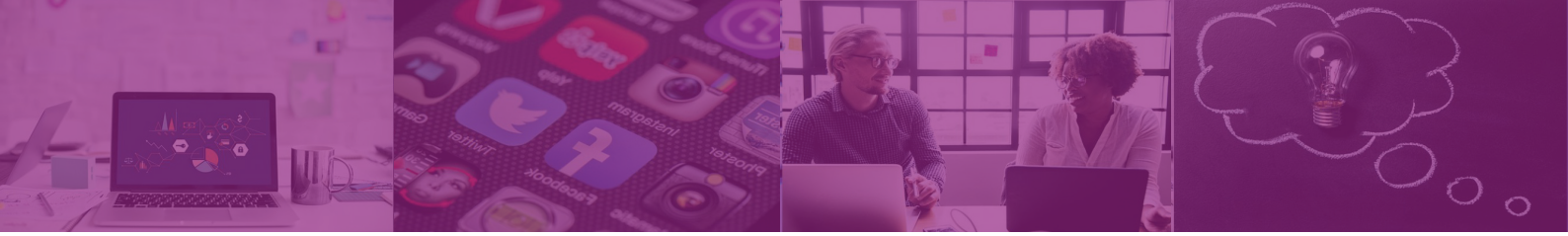
Topic 4:

Be aware of the side effects of excessive Internet use

GENERAL INDICATIONS	
Time load	2-3 hours
Target group	Adult learners
Objectives of this unit	Make learners aware of potential negative effects of excessive Internet use through: ○ sensitizing them to the first signs of Internet addiction; ○ making them aware of the consequences of the Internet excessive use; ○ presenting possible threats of excessive use of the Internet; ○ introducing different types of potential negative effects of the Internet use; ○ advising on how to prevent the addiction from the Internet, Social Media; ○ emphasizing the importance of developing soft skills such as communication, teamwork and time management in XXI century; ○ showing strategies for preventing harmful use of the Internet; ○ suggesting solutions that can be helpful for preventing mental health problems, overstimulation, sleep deprivation and social withdrawal.



Group size	5-15 people (recommended: 10)
Educator's competences required	Preferential/desired: ○ Social Media user; ○ Basic knowledge of psychology/sociology; ○ Basic mental health knowledge; ○ Basic digital safety skills.
Main topics and content	○ Potential consequences of the Internet overuse; ○ First signs of Internet addiction; ○ Possible threats of the Internet excessive use; ○ Different types of potential negative effects of the Internet (excessive) use and how to prevent them (in relation to for example Social Media, gaming, pornography, etc.); ○ Strategies for preventing harmful use of the Internet; ○ Preventing mental health problems - the Internet use; ○ Solutions connected with overstimulation, sleep deprivation and social withdrawal.



Development of the didactic unit

LEARNING OUTCOMES

The learner:

✓ can present the possible threats of excessive Internet use;
✓ is aware of the consequences of excessive Internet use;
✓ is aware of the first signs of Internet addiction;
✓ can introduce and characterize different types of addiction to the Internet;
✓ is familiar with several strategies/ techniques that can be helpful to prevent mental health problems caused by Internet use;
✓ is familiar with terms and concepts such as overstimulation, sleep deprivation, social withdrawal and FOMO (Fear of Missing Out).

INTRODUCTION AND INITIAL EXPLORATION

This is an introductory phase. The estimated duration is 30-40 minutes, depending on how much your learners already know about the topic.

Introduction (15 min)

Short discussion – checking the group's initial knowledge about the negative effects on the Internet use:

» Is the Internet safe for our health?
» Is all information on the Internet reliable?
» What negative effects of Internet use do you know? (physical, mental, relational, emotional)
» Have you noticed any of these negative effects in your family/environment?
» What are the potential consequences of such negative effects?
» How to prevent Internet overuse?

Watching a video (5 min)

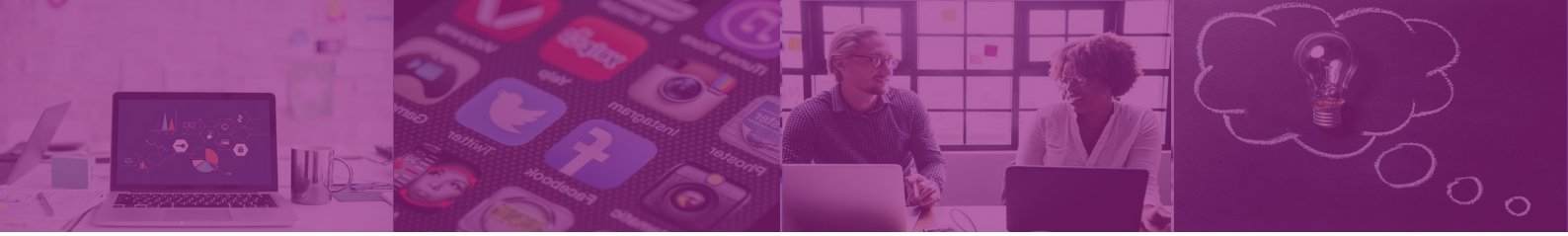
Please select one of the videos suggested below or identify a similar one in your national language:

▷ What the Internet is Doing to Our Brains

Knowledge check – questions (15 min)

Asking participants to list the main conclusions/information from the video. In further conversation, distributing them cards with questions to answer (in groups of 2-3):

» What is overstimulation? How can we feel it?
» How the Internet causes distraction?
» Which activities make us become more compulsive?
» How does the Internet affect our Short Term Memory (STM)?
» Why is the process of consolidation



disturbed when using the Internet?
» How can we increase our attention level in everyday life?

▷ 5 Crazy Ways Social Media Is Changing Your Brain Right Now

Knowledge check:

» Name 3 main ways Social Media is affecting our brain.
» Does using the Internet and Social Media intensively improve our multitasking?
» Which of our needs can Social Media fulfil? How could we fulfil these needs in more healthy way (offline)?
» What is your experience?
» Ask participants to give some examples from their life - what role Social Media plays in their life?

On a basis of these questions ask students to fill in a table:

Need	Social Media activity (-)	Real life activity (+)

DEVELOPMENT AND APPLICATION

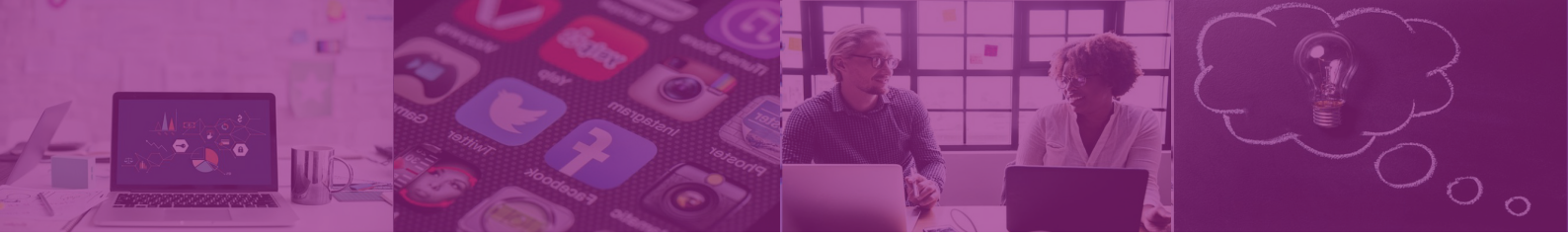
In this phase, learners develop and build up their knowledge on the topic. The estimated duration is 60-80 minutes.

At this stage it is important to engage all participants in group discussions and make them share ideas, as well as encourage peer-work.

A customised approach to each group is crucial, and it is important to help participants identify (and deal with) problems related to this topic in different contexts (at work, in their personal lives, in the educational community) and in different types of groups (teenagers and young people, adults, elder people...). In addition, they are acquainted with and/or suggest possible solutions to presented challenges.

Mini-lecture (20 min)

» Some statistics regarding number of people affected by the Internet over-exposition and which social/occupational and age groups are the most susceptible to it?
» Internet use vs mental health issues (mood disorders/self-esteem disorders: depression, anxiety, FOMO – fear of missing out, jealousy, etc.)
» Cyberbullying
» STM – Short Term Memory



» Delayed gratification and example of the Marshmallow test (Walter Mischel). What the Internet does to our brains – overstimulation and immediate gratification. See The Boston Globe | Instant gratification is making us perpetually impatient.
» Problems with building strong and long-lasting relationships with people.

Brainstorming exercise (10 min)

» How could one deal with overuse of the Internet on a daily basis?
» What can we do, as a society, to prevent it?
» What are the solutions for building meaningful relationships with people in the age of digital society?

The participants answer the questions on flipchart sheets in groups or pairs, depending on size of a group. Each flipchart makes a round so all participants have the opportunity to answer the same questions and gather all ideas. At the end each group reads and discusses the answers.

Case study (20 min)

This activity could be implemented by dividing participants into small groups (2-4). Each group receives a short "real case" to work on. Each case presents a profile of a person who is somehow affected by the one or more problems related to excessive use of the Internet. Suggested cases include for example:

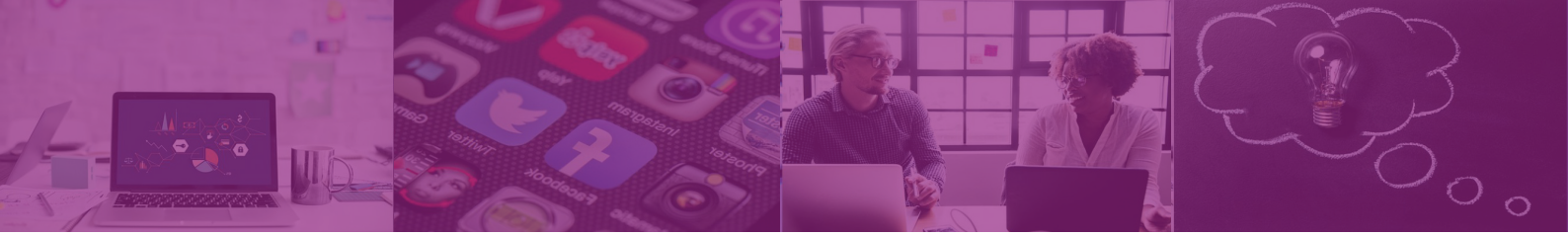
» Marta, 35, who is an online shopping addict (see her case below as a sample);
» Robert, 15, who is a victim of cyberbullying;
» Sarah, 6, young internet addict;
» Adrian, 28, who is socially withdrawn;
» Greg, 65, who is addicted to online gambling.

The cases need to be prepared and customised in advance, to reflect realities familiar to participants (e.g. names could be replaced by the trainer/facilitator with names typical from a respective country, and some other elements of description could be modified to be more realistic for each group)

Each small group is given one such "real case" and is asked to analyse it and propose solutions regarding a situation described in each case using the knowledge from the mini-lecture, video and brainstorming. Each group can present briefly for the whole audience.

Debate (15 min)

Split the group in two and give them a chart to complete with pros and cons of different statements (How to balance positive sides of the Internet use and minimise negative). Afterwards, share the groups' ideas and encourage a debate about it.



Short mindfulness practice (5 min)

The act of using the Internet, especially Social Media and its easy availability is not supportive for our mental health. Changing our level of digital mindfulness may be helpful but requires altering the way we respond to discomfort. Instead of turning to our phones while feeling restlessness (e.g. when you're waiting in a queue, meeting people you don't know, etc.), you can change your response to questions which are helpful to build your awareness: what's this restlessness about? How am I feeling right now? What am I hoping to gain from doing this? What need am I trying to meet? Moving your attention away from distractions and coping mechanisms while choosing to focus on our core needs is something you can develop through mindfulness practices.

Such practices can be found on the following websites:

» Pocket Mindfulness | 6 Mindfulness Exercises You Can Try Today;

» Mindfulness Exercises | 3 Mindful Breaths.

We recommend using some apps helpful for monitoring and limiting the Internet use.

» For example: Space App.

CONCLUSION

This is the final and concluding phase of the unit. The estimated duration is 10-20 minutes.

For the last 10-20 minutes of the session, summarise the main points discussed and refer to further learning resources. It is also time for learners to share their impressions and provide some feedback. Encourage them to ask questions or express their doubts about any issues that are still not clear to them.

Self-reflection activity: ask the participants how daily activities on the Internet affect their close environment and their relationships. Ask them to list potential problems in one column of the table and solutions in the other. Then, discuss the conclusions.

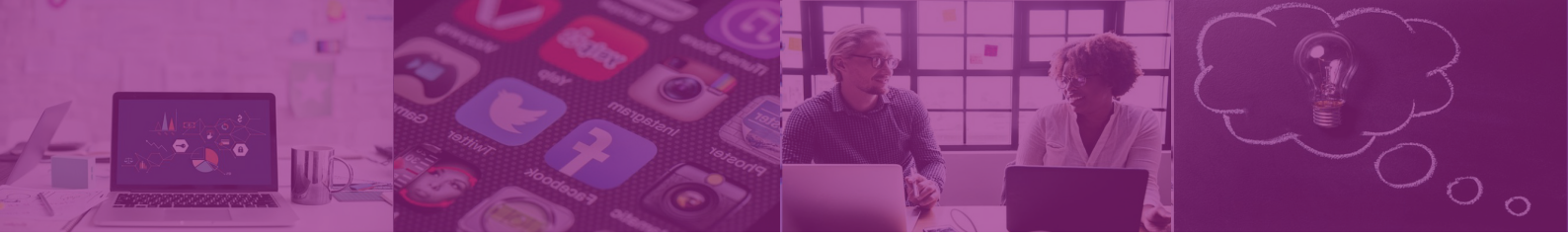
Other suggested **practical activities**:

a. *Assessment test/quiz*

Check if all concepts and terms discussed have been understood, give your students an assessment test with exercises such as defining vocabulary, yes/no questions or multiple choice. Correct the test as a group or by peer-reviewing it.

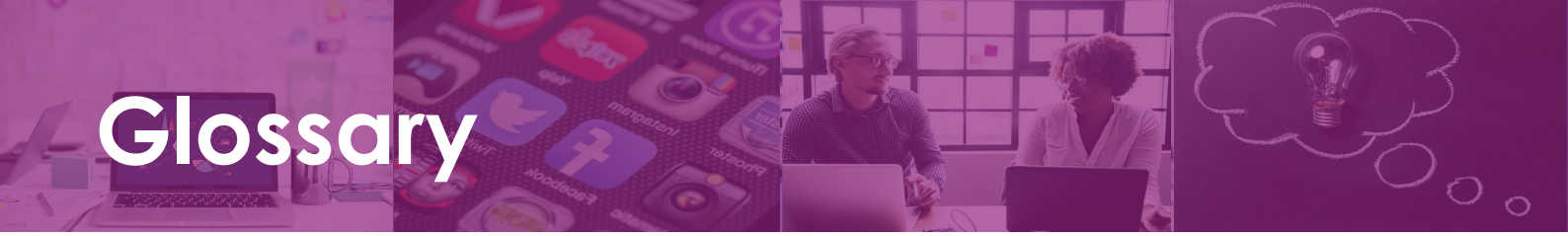
b. *Group wrap-up activity*

As a final activity, create in a group the 'Top ten solutions for excessive Internet use'.



Start brainstorming and narrow down the rules mentioned to a list to the 10 most essential.

At the end of the workshop distribute 1-page handouts including basic information about prevention of excessive Internet use and promoting healthy habits, short mindfulness practice instruction and contacts to institutions dealing with Internet addiction and mental health problems.



Glossary

A Avatar

An icon or figure visually representing a particular person in a video game, Internet forum, etc. (Source: https://en.oxforddictionaries.com).

B Big data

Data sets that are so voluminous and complex that traditional data processing application software are inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating and information privacy. There are five dimensions to big data known as Volume, Variety, Velocity and the recently added Veracity and Value. (Source: https://en.wikipedia.org/wiki/Big_data).

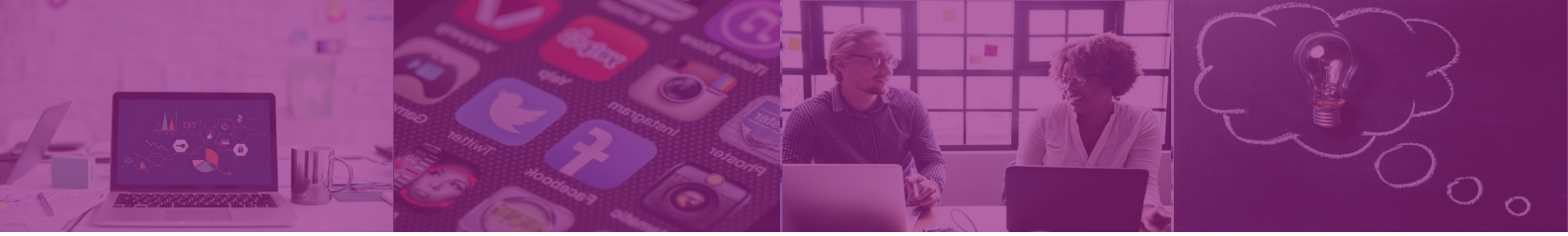
C Cyber bullying

Cyberbullying or cyber harassment is a form of bullying or harassment using electronic means. It has become increasingly common, especially among teenagers. Harmful bullying behavior can include posting rumors, threats, sexual remarks, a victims' personal information, or pejorative labels (i.e. hate speech). Finally, much of the abusive behaviour that takes place within offline relationships may also take place in online spaces or be abetted by digital technology.

Cyberbullying is traumatic: one-third of students who were bullied online reported symptoms of depression, a figure which rose to nearly one-half for those who experienced both online and offline bullying. Unfortunately, youth typically underestimate how harmful online bullying can be. Jennifer Shapka, a researcher specialising in bullying at the University of British Columbia, found while young people believe most of the negative behaviour that happens online was meant as a joke, "students need to be educated that this 'just joking' behaviour has serious implications". (Source: http://mediasmarts.ca/cyberbullying/cyberbullying-overview).

Catfishing

A catfish is someone who creates a false online identity. Catfishing is common on social networking and online dating sites. Sometimes a catfish's sole purpose is to engage in a fantasy. Sometimes, however, the catfish's intent is to defraud a victim, seek revenge or commit identity theft. (Source: http://whatis.techtarget.com/definition/catfish).



D

Digital citizen

A person who develops the skills and knowledge to effectively use the Internet and other digital technology, especially in order to participate responsibly in social and civic activities. (Source: https://www.dictionary.com/browse/digital-citizen).

Digital citizenship

Digital citizenship is the norms and rules we follow to act appropriately when using technology. (Source: https://study.com/academy/lesson/what-is-digital-citizenship-definition-themes.html).

E

Echo chambers

In news media, echo chamber is a metaphorical description of a situation in which beliefs are amplified or reinforced by communication and repetition inside a closed system. By visiting an «echo chamber», people are able to seek out information which reinforces their existing views, potentially as an unconscious exercise of confirmation bias. This may increase political and social polarization and extremism. (Source: https://en.wikipedia.org/wiki/Echo_chamber_(media)#cite_ref-barbera_1-0).

F

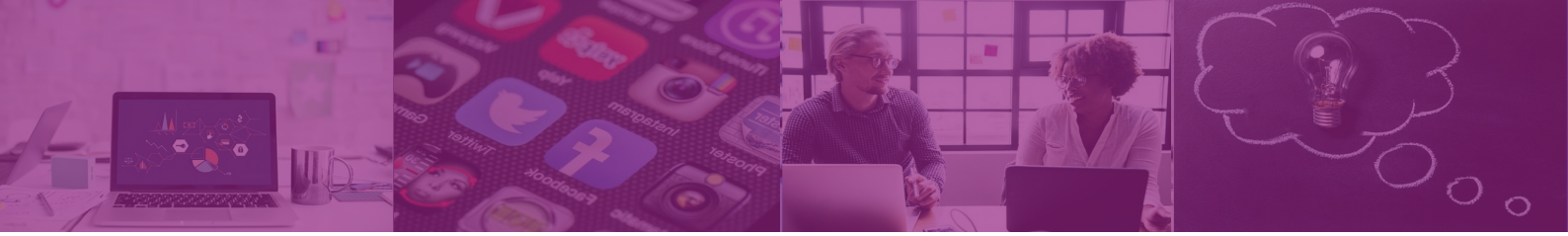
Filter bubble

A filter bubble is an algorithmic bias that skews or limits the information an individual user sees on the internet. The bias is caused by the weighted algorithms that search engines, social media sites and marketers use to personalize user experience (UX). (Source: https://whatis.techtarget.com/definition/filter-bubble).

H

Hashtag

A hashtag is a tag used on a variety of social networks as a way to annotate a message. A hashtag is a word or phrase preceded by a “#» (i.e. #InboundMarketing). Social networks use hashtags to categorize information and make it easily searchable for users. (Source: https://blog.hubspot.com/marketing/social-media-terms).



Identity theft

It is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. (Source: https://en.wikipedia.org/wiki/Identity_theft).

Internet Addiction Disorder

A behavioural addiction, which is defined as losing the ability to stop going online to the point where it negatively impacts other areas of your life, including relationships, emotions, social life, school, and so on.

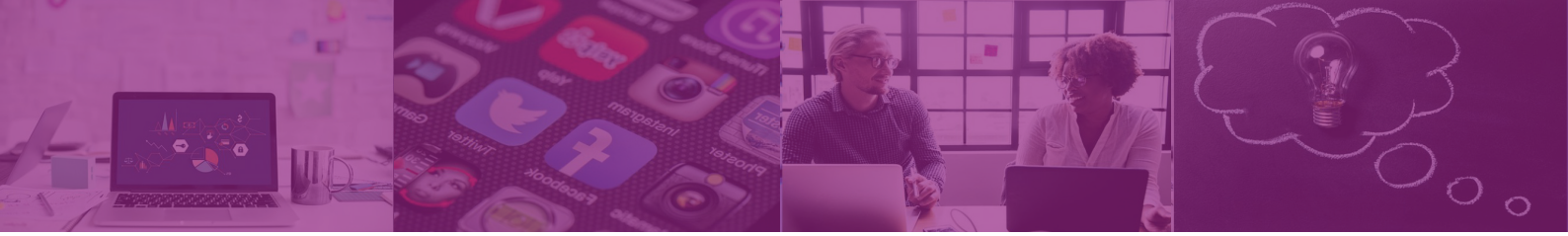
It is also now recognized that there are different forms of addiction based on the type of Internet activity:

- downloading
- forming online relationships
- compulsive shopping
- accessing pornography
- gaming

For young people, online role-playing games lend themselves particularly well to excessive use because these games have no end and there is always someone available to play with. In addition, in role-playing games players are often members of groups, which means they need to stay engaged so everyone can advance. However, keep in mind that research shows only five to twelve percent of gamers have a problem with excessive playing. (Source: mediasmarts.ca/excessive-internet-use/excessive-internet-use-overview).

Liquid democracy (or delegative democracy)

«Liquid Democracy is the combination of networks and democracy. It is a term designed to capture a more fluid and responsive participation of citizens in the democratic process through the use of both online and offline networks. Votes flow through networks of trusted relationships and in this way a range of types of "delegation" can be created, from



forms we are familiar with such as conventional representative democracy, to fluid parties and direct democracy». (Source: http://liquiddemocracy.org/)

Netiquette

Netiquette is short for «Internet étiquette». Just like etiquette is a code of polite behaviour in society, netiquette is a code of good behaviour on the Internet. This includes several aspects of the Internet, such as email, social media, online chat, web forums, website comments, multiplayer gaming, and other types of online communication. (Source: https://techterms.com/definition/netiquette).

Newsletter

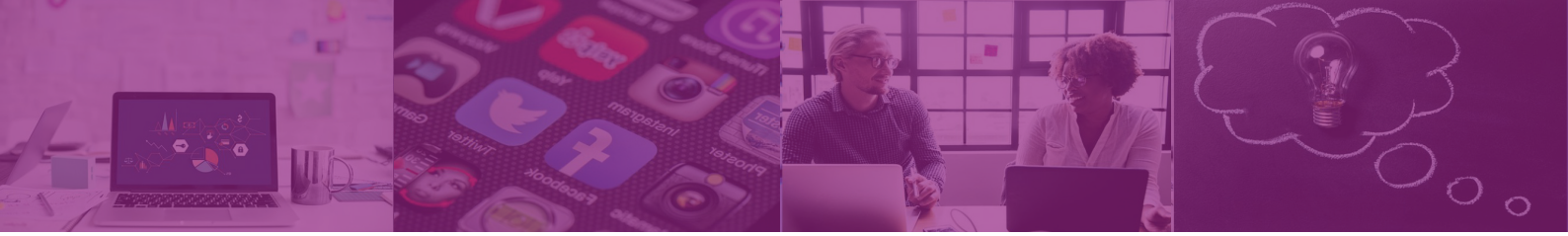
«A periodically published work containing news and announcements on some subject, typically with a small circulation. Newsletters may be distributed by electronic mail». (Source: encyclopedia2.thefreedictionary.com/newsletter).

Online advertisement

«Online advertising is a marketing strategy that involves the use of the Internet as a medium to obtain website traffic and target and deliver marketing messages to the right customers [...] Examples of online advertising include banner ads, search engine results pages, social networking ads, email spam, online classified ads, pop-ups, contextual ads and spyware». (Source: https://www.techopedia.com/definition/26362/online-advertising).

Online hate speech

It is hate speech communicated via the Internet. The Online Hate Prevention Institute (OHPI) focuses on online hate speech, with a primary focus on hate speech in social media. This is because the main social media platforms such as Facebook, YouTube and Twitter have the largest online engagement and the greatest ability to take a message of hate viral. Hate speech becomes embedded in 'the permanent visible fabric of society', and this is even more true online where the online world is made entirely of speech. Online messages will remain embedded in the environment, be it a hate page that appears in search results on Google, a hate page on Facebook or a hate video returned by a search on YouTube. This is part of the online environment people must live within as they conduct their life online. (Source: http://ohpi.org.au/learn-about-online-hate).



Online identity

Internet identity (IID), also online identity or internet persona, is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself. Although some people choose to use their real names online, some Internet users prefer to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally identifiable information. An online identity may even be determined by a user's relationship to a certain social group they are a part of online. Some can also be deceptive about their identity. (Source : https://en.wikipedia.org/wiki/Online_identity).

Overstimulation

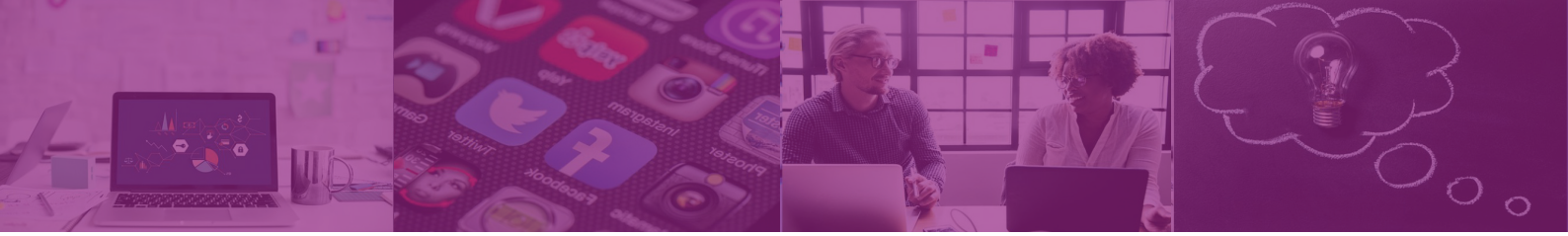
It means that the brain must give most of its attention to short-term decisions. The vast availability of information on the World Wide Web overwhelms the brain and hurts long-term memory. The availability of stimuli leads to a very large cognitive load, which makes it difficult to remember anything.

Using the Internet can lead to a lower attention span and make it more difficult to read in the traditional sense (that is, read a book at length without mental interruptions). Moreover, it is more difficult to concentrate and read whole books, even if you read a great deal when you were younger (that is, when they did not have access to the Internet).

Ease of access to the Internet can increase escapism in which a user uses the Internet as an «escape» from the perceived unpleasant or banal aspects of daily/real life. Because the internet and virtual realities easily satisfy social needs and drives, according to Jim Blascovich and Jeremy Bailensen, «sometimes [they are] so satisfying that addicted users will withdraw physically from society». (Source: en.wikipedia.org/wiki/Psychological_effects_of_Internet_use).

Reputation management

Sometimes referred to as rep management, online reputation management or ORM, is the practice of attempting to shape public perception of a person or organization by influencing online information about that entity. (Source: http://whatis.techtarget.com/definition/reputation-management).



P

Phishing

It is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. (Source: en.wikipedia.org/wiki/Phishing).

Privacy policy

The policy under which a company operating a website handles personal information collected about visitors to the site. (Source: www.icicibank.com/online-safe-banking/glossary.page?id=glossary).

S

Scam

«A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person. With the world becoming more connected thanks to the Internet, online scams have increased, and it's often up to you to help stay cautious with people on the Internet». (Source: https://www.computerhope.com/jargon/s/scam.htm).

Smishing

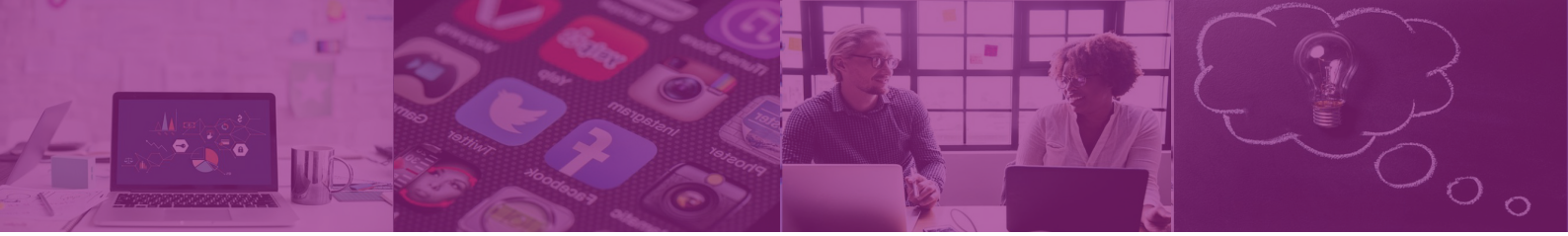
«Smishing» is SMS phishing where text messages are sent trying to encourage people to pay money out or click on suspicious links. Sometimes attackers try to get victims on the phone by sending a text message asking them to call a number, in order to persuade them further. Unsolicited text messages from unknown numbers should raise alarm bells, but often banks do text their customers for a variety of reasons. (Source: http://www.bbc.com/news/business-35201188).

Social engineering

In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional «con» in that it is often one of many steps in a more complex fraud scheme. (Source: https://en.wikipedia.org/wiki/Social_engineering_(security)).

Spam

«To indiscriminately send large amounts of unsolicited e-mail meant to promote a product



or service. Spam in this sense is sort of like the electronic equivalent of junk mail sent to 'Occupant'».

Different types of spam can include:

- Advertisement, for example online pharmacies, pornography, dating, gambling;
- "Get rich quick and work from home" schemes;
- Hoax virus warnings;
- Hoax charity appeals;
- Chain emails which encourage you to forward them to multiple contacts.

(Source: https://encyclopedia2.thefreedictionary.com/spam).

Subscription

«Subscribe is an option offered by product vendors or service providers that allows customers to gain access to products or services. Many websites, product and service companies, etc. allow customers to subscribe to their newsletters, product/service-related blogs, press releases, etc. In order to subscribe, the customer has to add his/her email address to the company's mailing list. This means that the customer is subscribed to anything sent to that mailing list». (Source: https://www.techopedia.com/definition/22374/subscribe).

T

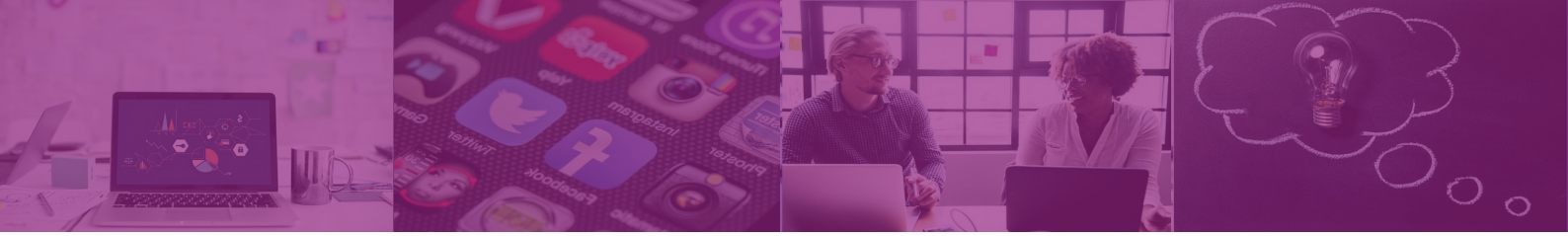
Tag

Tagging is a social media functionality commonly used on Facebook and Instagram that allows users to create a link back to the profile of the person shown in the picture or targeted by the update. (Source: https://blog.hubspot.com/marketing/social-media-terms).

U

Username (or user name)

It is the name given to/chosen by a user on a computer or computer network. (Source: https://www.computerhope.com/jargon/u/username.htm).



V Vishing

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. (Source: http://searchunifiedcommunications.techtarget.com/definition/vishing).

Additional resources

Netiquette
Education.com | Netiquette Rules
www.education.com/reference/article/netiquette-rules-behavior-internet/

Copyright for kids
Copyright Kids | Copyright Basics
www.copyrightkids.org/cbasicsframes.htm

Creative Commons (share your work and quote others')
Creative Commons | What we do
https://creativecommons.org/about/

Youth Protection Roundtable Toolkit
Youth Protection Roundtable | YPRT Toolkit
https://www.digitale-chancen.de/transfer/assets/final_YPRT_Toolkit.pdf

The Web We Want
The Web We Want | Handbook for Educators
http://www.webwewant.eu/es/web/guest/handbook-for-educators

Internet Addiction Disorder
Wikipedia | Internet Addiction Disorder
https://en.wikipedia.org/wiki/Internet_addiction_disorder

Social Engineering
Webroot | What is Social Engineering?
https://www.webroot.com/ie/en/resources/tips-articles/what-is-social-engineering

Safe Internet Organization
SafeInternet.org | Welcome page
http://www.safeinternet.org/

Consortium

INnCREASE Sp.z O.O (Poland) is a high-quality provider of innovation services, business consultancy and partner for the implementation of international projects, including in the education and training field.

Dlearn (Italy) is the European Digital Learning Network and aims to minimize the current gap in digital skills and learning opportunities through local and transnational bottom-up initiatives.

Platon Schools (Greece) is a modern educational institution designed to foster the education of learners from kindergarten to adult education and develop formal and informal methods for learning and teaching.

UPI (Slovenia) is a public, non-profit institution for the education and training of adults specialised in both formal and non-formal education programmes and a center for guidance and counselling in adult education.

DomSpain Consulting (Spain) is an adult education and training centre specialised in occupational, social and intercultural skills, languages and new technologies.

Inova Consultancy Ltd (UK) provides a flexible consultancy service that responds to the needs of organisations and individuals internationally in the area of diversity, equal opportunities and entrepreneurship.

The **Lifelong Learning Platform** (Belgium), European civil society in the field of education and training, is an umbrella organisation that gathers 43 networks covering formal, non-formal and informal education sectors.

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

For info on this publication
please contact:

DSCONSULTING
educational services

Raval Sant Pere 1-3 Entresol 43201
Reus, Spain
tel: +34 660 115 104
e-mail: international@domspain.eu