

GODIGITAL
Digital tools for work



4. Safety & Problem Solving

Lead Organisations: IDEC, FEUZ, DLEARN, RCCI



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

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



REVISION HISTORY

Version	Date	Author	Description	Action	Pages
1.0	24/06/2020	Orestis Ntagiantas	Creation of the document	C	55
2.0	03/07/2020	Orestis Ntagiantas	Activity cards with quizzes became the “assessment” sections. Activity cards with videos and reflections, were added into the extra material of their respective units. “Expert” cards were changed to “Advanced”	R, D	43
3.0	23/07/2020	Orestis Ntagiantas	Transfer of activity cards to other modules and vice versa	I, R, D	46
4.0	27/7/2020	Karl Donert	Content check for language	U	46
5.0	03/08/2020	Orestis Ntagiantas	Replacement of “using guideyourtalent.com” with “using Pathways for Employ” in activity card 11	R	58
6.0	08/08/2020	Karl Donert	Content check of replacement Activity Card	U	58
7.0	07/10/202-	Karl Donert	Revision for language – content (along with the DLEARN-RCCI revision)	U	65
8.0	08/10/2020	Orestis Ntagiantas	Incorporation of revisions done by DLEARN & RCCI into their original content	I, U	65
9.0	14/10/2020	Orestis Ntagiantas	Addition of descriptions below images and delete of certain parts of activity cards 3 & 5	I, D	64
10	11/02/2021	Isabel Nuez	Content check	U	64

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

REFERENCED DOCUMENTS

ID	Reference	Title

APPLICABLE DOCUMENTS

ID	Reference	Title

Contents

1. Protecting personal data and privacy.....	4
1.1 Unit Introduction	4
1.2 Activity cards	5
1.2.1 Beginners Level	5
Activity card 1 - Data protection while searching for a job online	5
Activity card 2 - Data protection during a video interview	7
1.2.2 Intermediate Level.....	10
Activity card 3 - Digital footprint.....	10
Activity card 4 - Best practices on protecting your data online	14
1.2.3 Advanced Level.....	17
Activity card 5 - The privacy issue	17
Activity card 6 - The Right to be Forgotten.....	20
Activity card 7 - Privacy policy for your website	23
Activity card 8 - Blockchain	25
2. Creatively using digital technology.....	27
2.1 Unit Introduction	27
Safety and Problem Solving IDEC, FEUZ, DLEARN, RCCI	2

2.2 Activity cards	29
2.2.1 Beginners Level.....	29
Activity card 9 - Digital job seeking problems	29
2.2.2 Intermediate Level	32
Activity card 10 - Video interview problems	32
2.2.3 Advanced Level	35
Activity card 11 - Problems in your website	35
3. identifying digital competence gaps	39
3.1 Unit Introduction	39
3.2 Activity cards	40
3.2.1 Beginners Level.....	40
Activity card 12 - Identifying your digital skills gap	40
3.2.2 Intermediate Level	43
Activity card 13 - Skills Gap vs Signaling Gap.....	43
3.2.3 Advanced Level.....	45
Activity card 14 - Using Pathways for Employ	45

1. PROTECTING PERSONAL DATA AND PRIVACY

1.1 Unit Introduction

The below card will be visible to users of all levels when they click on the respective block (see design document)

PROTECTING PERSONAL DATA AND PRIVACY
DESCRIPTION OF THE TOPIC
<p>In this unit we learn about how to protect personal data and privacy in digital environments.</p> <p>In the digital world, it is crucial to understand how to share personal information and protecting our privacy and safety at the same time, as well as that of others.</p>
EMPLOYABILITY SKILLS
<p>-Critical skills</p> <p>-Caution and responsibility</p>
LEARNING OUTCOMES
<ul style="list-style-type: none"> • Know about what personal data is. • Know how to protect your personal data. • Know how to take care of your privacy. • Know how to protect the personal data and privacy of others. • Be aware of the importance of protecting your personal data and privacy. • Be aware of the importance of helping others in protecting their personal data and privacy.
DIGCOMP FRAMEWORK
<p>Competence area 4: Safety</p> <p>4.2 Protecting personal data and privacy</p>
REFERENCES (if applicable)
<p>APA style</p>
ADDITIONAL RESOURCES (if applicable)

<https://drive.google.com/drive/folders/1-1xmY7Bo0jyVubrIOpxHKaSm-g90SOfl?usp=sharing>

1.2 Activity cards

1.2.1 Beginners Level

Activity card 1 - Data protection while searching for a job online

Tips on how to protect your data while searching for a job online

LEVEL

Basic

DESCRIPTION OF THE ACTIVITY

A **European Union** platform, like **Eures**, has strong and specific **regulations** regarding the storage, processing and overall privacy of their users **personal data**.

But despite the fact that you are not in much danger of identity theft from the official platforms themselves, **there are great perils when you are dealing with web sites and their users**.

Job hunting may sound like a “serious and professional” sector where no mischievous, harmful or illegal actions take place, but that couldn’t be further from the truth.

Due to the simple fact that you share your **resume**, with a detailed list with the most of your personal data that could fit into 3 pages, means you need to be **really careful** what to include and what to omit.

More specifically, you should keep these **5 rules** in mind:

-Limit your contact information

It may sound obvious that you want yourself to be as reachable as possible by a potential employer, but in reality, not all contact information is essential.

- Never mention your home phone number

It is pretty much a straightforward way to reveal where you are living and you should be careful about doing that.

Your **place of residence** could be important information for a potential employer (e.g. in case they prefer you to be in close proximity to the company), however keep in mind that **you can just mention it through a phone call or at interview**.

It is recommended to provide your cell phone number (be also sure to have a voicemail account) and for even further security, you could use a [Google Voice](#) number.

- **Never give information about your home address.** It is almost never necessary for a potential employer to know your exact address. Note that by providing your home phone number, you may be providing details of where you are living.

- **Create an email account that you'll use only for job hunting.** Although giving away your personal email address is not considered very risky, it is still **recommended to create an email account specifically for your job hunting.**

Needless to say that since it should be a professional email account and you should **avoid strange names** such as hell_raiser@gmail.com or unicorn_kitty@hotmail.com.

Don't write your real birthdate. Whether you are a Capricorn, a Virgo or a Gemini shouldn't bother your potential employer.

Therefore, **avoid giving away your day, month and birth year all at once.** Instead, it is better to mention just your birthyear or age. No matter how important your age range might be for a potential job, **a potential employer will not need for an exact birthdate until you have been employed.**

Don't give away names of close people. You should **not mention the names of persons from your inner family** that have nothing to do with your job seeking.

Remember. it's a resume, not an identity card.

Don't reveal your ID number. You do not need to include your ID number in your CV.

Such data should only be provided after you have completed your interview and it's time for work contracts to be signed. **A legitimate employer would never ask to see your ID at interview stage.**

Never include your bank account details. This is a piece of information that is **only needed when your employment contract has been agreed and signed.** At this point it is time to define your payment situation.

A potential employer asking you for such information from the very beginning should be considered a scammer.

TOOLS & RESOURCES NEEDED

Job searching platform account

TIME REQUIRED

15 minutes

ASSESSMENT



1. **Which of the following should you NOT include in your CV?**
 - A) Your full name
 - B) **Your birthdate**
 - C) Your former employer's name
 - D) Your birth year

2. **Which of the following email types is mostly recommended for job seeking?**
 - A) Your personal
 - B) The one from your last job
 - C) **One that you made specifically for finding a job**
 - D) One with a weird name that draws attention

3. **If a potential employer asks you for your exact home address in person, you:**
 - A) Give it to him/her since it is safe because you are not in an online environment
 - B) Ask the reason it's needed
 - C) Say that you will give it only after you're hired
 - D) **Never give it**

4. **Which cellphone number is mostly recommended for job seeking?**
 - A) Your personal
 - B) A Google Voice number
 - C) **A and B**
 - D) A professional one from a former job

IMAGE

<https://pixabay.com/illustrations/job-search-hr-cv-opportunity-3681036/>

Activity card 2 - Data protection during a video interview

Tips on how to not give away sensitive/personal data during a video interview

LEVEL

Basic

DESCRIPTION OF THE ACTIVITY

Video interviews are getting more and more popular nowadays and, particularly following the coronavirus pandemic, their popularity will probably rise steeply.

Just like any Internet related action, such interviews have their **safety do's and don'ts**, since especially through video, there is a danger of **giving away sensitive data**.

Fortunately, none of these rules is very complicated, and they all fall into the category of "common sense".

Here are **5 key behaviors** that you should keep in mind:

1. Safety regulations of CVs, apply also here

The same kind of data that you should avoid writing down on your resume, **shouldn't be "caught on camera"**.

We are once again talking, about **not giving away** your:

- Full birthdate
- Home address
- Home phone number
- Identity card number
- Bank account number
- Parent or other close relative names

2. Have control of your camera and mic

Regardless of the video conference software that will be used for the interview, you should take a couple of minutes beforehand in order to familiarize yourself with the ways of turning on and off our camera and your microphone.

It may sound simple, but you should have it handy at the beginning of the interview since trying to find them on the spot may create an awkward pause.

And of course, they are crucial for hiding or muting yourself whenever it may be needed.

3. Keep an eye on screen recording

Most employers will probably want to **record your session** in order to be able **to examine it more thoroughly later**.

Of course, **you shouldn't reject an interview just because it will be recorded**, but it's recommended to ask beforehand whether this will be the case. In fact it is an **obligation of the employer to mention it** even if you don't ask, and doing so shows professionalism and creates a better sense of trust.

So after knowing that the session will be recorded, you know that you should be **even more cautious** about not giving away the aforementioned data.

But even if you're said that it should not be recorded, **you should still be careful**. Some video conference software has a feature where a symbol shows up (usually a **red dot**) in case the discussion is recorded.

If an employer tells you that there will be no recording of your session, and then you realize that it is being recorded, it's needless to say that this should be **huge warning** about the person interviewing you.

Finally, keep in mind that a session can be recorded with **external screen capturing software**. Unfortunately, you cannot be sure whether such actions are happening, so the best advice is to **always behave as if your interview was being recorded**, even if you have been told the opposite.

4. Beware of screen sharing



While it is rare practice to screen share for a job interview, there is a chance of them asking you to share your screen for some reason (or perhaps you yourself will need to do that).

In this case, make sure that **all your program tabs and pop-up notifications are closed**, and that **there is no sensitive data present on your screen** (e.g. as a desktop font or shortcut).

Also, during your screen sharing, never go through your **email inbox**, your **social media chats** and your **web banking**.

Finally, instead of going through your files in order to find the one you want to open, make sure that you **have it already open and ready**, before the conference begins.

5. Keep your software up to date

No matter if it's Skype, Zoom or any other video conference software, it is wise to **make sure that the version installed on your device is the latest one**.

This will ensure that the edition's security **protocol and threat defense system is the most up to date**, in the rare case of you facing an external "attack" during your conference.

Needless to say, that having **your firewall turned on** while at the same time using an **antivirus software**, further strengthens your security.

TOOLS & RESOURCES NEEDED

Video conference software

TIME REQUIRED

15 minutes

ASSESSMENT

5. If you are asked to share your screen during a video interview you:

- A) Deny it no matter what
- B) Ask for the reason
- E) Do it after having first taken all necessary precautions**
- F) Do it no matter what

6. What type of things should not be visible during your screen sharing?

- E) Your web banking
- F) Your documents
- G) Your email inbox
- H) All the above**

7. Which of the following video conference software should always be up to date?

- E) Skype
- F) Zoom**

- G) Go to Meeting
- H) Any software

8. In case you are warned beforehand that your video interview will be recorded

- E) You deny going through the interview
- F) You ask for the reason
- G) You accept it and are careful not to give away sensitive data**
- H) You leave the chat

IMAGE

<https://pixabay.com/illustrations/video-conference-video-call-skype-5048823/>

1.2.2 Intermediate Level

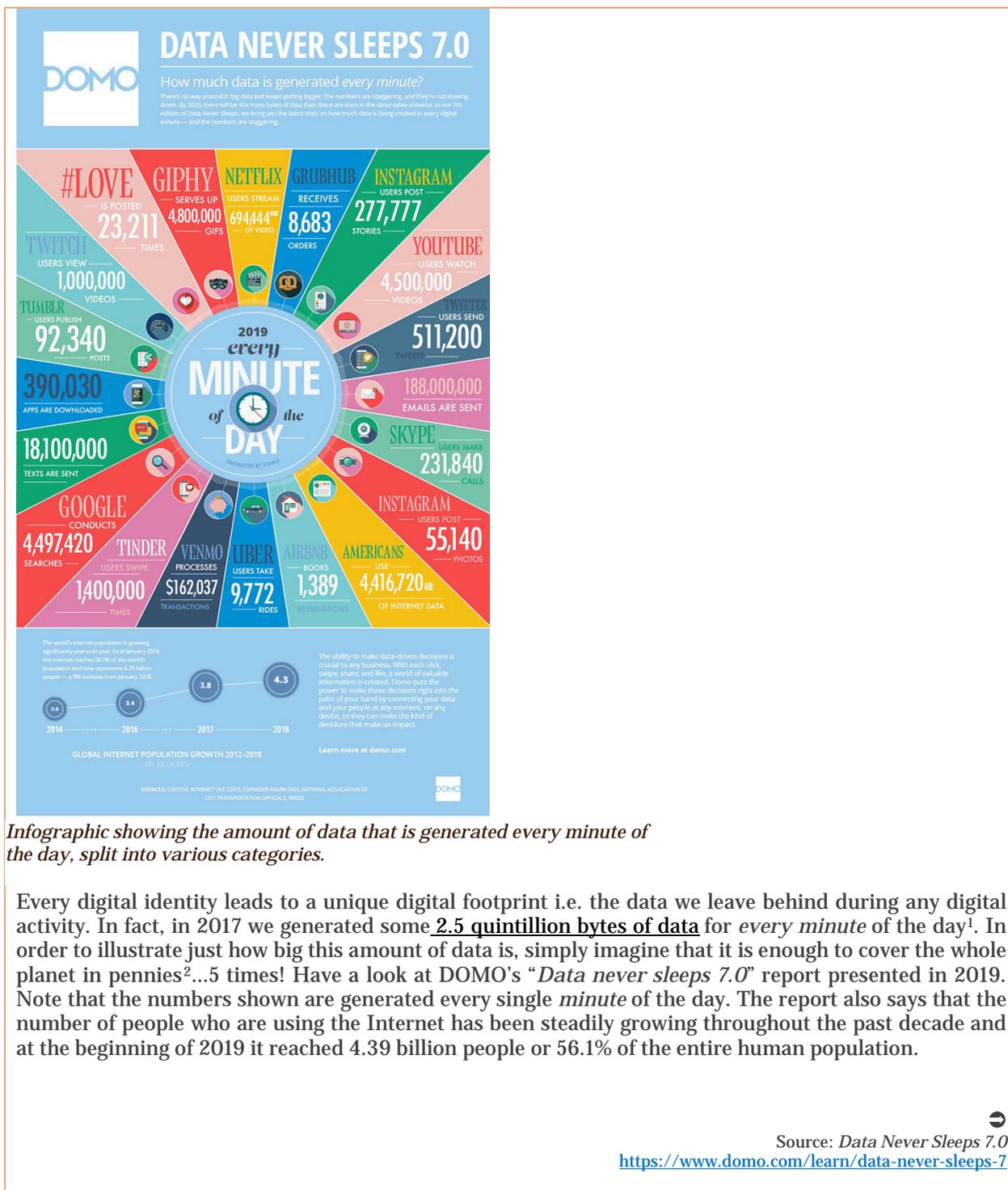
Activity card 3 - Digital footprint

Digital footprint

LEVEL

Intermediate

DESCRIPTION OF THE ACTIVITY



Infographic showing the amount of data that is generated every minute of the day, split into various categories.

Every digital identity leads to a unique digital footprint i.e. the data we leave behind during any digital activity. In fact, in 2017 we generated some **2.5 quintillion bytes of data** for every minute of the day¹. In order to illustrate just how big this amount of data is, simply imagine that it is enough to cover the whole planet in pennies²...5 times! Have a look at DOMO's "Data never sleeps 7.0" report presented in 2019. Note that the numbers shown are generated every single minute of the day. The report also says that the number of people who are using the Internet has been steadily growing throughout the past decade and at the beginning of 2019 it reached 4.39 billion people or 56.1% of the entire human population.

Source: *Data Never Sleeps 7.0*
<https://www.domo.com/learn/data-never-sleeps-7>

¹ Data never sleeps 5.0. <https://www.domo.com/learn/data-never-sleeps-5>

² A Penny's Worth of Data. <https://www.tdworld.com/smart-utility/data-analytics/article/20972851/a-pennys-worth-of-data>



Knowing all of this helps understand why managing your digital identity is important and same goes for being aware of your own digital footprint. In 2020, the European Digital Learning Network (DLEARN) carried out a year-long survey aiming to collect key information and data about general knowledge, awareness and consequently the attitudes of European citizens towards their digital footprint and all the information they – more or less consciously – disclose online. The survey came close to almost 20 000 respondents from 11 European countries and provided some very valuable insight regarding how digital awareness is perceived amongst the general public. When asked “Have you ever read a privacy policy in full before agreeing to it?”, 80% of respondents answered with “No”. In relation to digital footprint, digital identity and online reputation, the survey participants were asked to rate with “True/False” some statements, one of which was “I am in full control and I can manage my digital identity” to which 70% of the respondents answered with “False”. Would your answer be the same? Well, in case you did answer the same, then perhaps you might want to consider reviewing your browsing habits altogether. Read the whole [Report on Digital Awareness 2020](#) to learn more about digital footprint and understand its importance to you.

There are many examples to help you understand the concept behind this modern term called “digital footprint”, so here’s one composed specifically for this purpose:

Meet Emily – she is 20 and she just finished her freshman year in college and she’s wondering what she will be doing for the summer. Emily is an adventurous person and she likes travelling, so she goes to YouTube and starts watching videos (again) about her long-desired tourist destination – Bali, Indonesia. She likes the video and leaves a comment saying how big of a dream it is for her to be able to visit this paradise one day. Then, she logs into her Facebook account to scroll through some posts and runs into an ad, which in 4sec. hooks her up for a super nice discount at a 4 stars hotel if she did decide to finally go and stay in Bali in a couple of weeks from now. So, she clicks on the add, which takes her to a landing page, where she is lucky to have an option for additional 7% discount if she likes the tour operator’s social media page in Facebook. Back to Facebook to like the page and Emily is finally ready to book her reservation - she sits back to relax in excitement. Since, there are no cancellation fees the hotel booking she made, she now starts planning her trip: Emily needs to start looking for a flight ticket. After spending an hour googling and going through dozens of websites, she decides it is time for a quick social media brake, so she gets back to Facebook to check how her BFFs are doing. Before she realizes, Emily is again scrolling through her feed and now she runs in to another ad giving Emily a super sweet offer which is going to solve her logistics to Bali problem. A couple of more clicks and she now has her flight booked as well and that’s it – next stop Indonesia. But wait, what is she going to wear? Of course, her favourite jeans won’t fit her when she needs them, so she grabs her smartphone and opens up her favourite shopping app and after another hour in searching there it is – the perfect dress. Emily however, buys only cruelty free clothes, so she googles the brand to check their manufacturing practices. After thoroughly checking their website and watching a couple of videos on YouTube she decides that her standards are met and she can proceed to buy the dress. She grabs her smartphone again and she notices a message from her banking app and she finds out that she can get 5% cashback on items bought via her favourite shopping app. This is an absolute no brainer – the dress is now on the way, together with a new bag glasses and a bracelet. What a day for Emily!

So, what does Emily’s digital footprint tell us? If you thought she is lucky, think again. Perhaps, what everyone needs to accept and realize is the fact our personal data is an insight source with high potential, thus of great value to companies, because they profit from using and/or reselling that information. In Emily’s example above, her personal preferences were used to receive personalised ads, tailored according to her activity in a couple of Google’s platforms. By liking the video, she saw on YouTube, she responded to a particular ad targeting set by the advertisers i.e. they used that to present her a service according to her activity. The way it usually works is that social networks shows us content based on what you’ve previously liked, commented, shared or simply scrolled through in your feed. All of that information is directly stored and connected to your account. After a few hundred interactions over the internet a very accurate and detailed description of your preferences is created by analytical software: your very own

marketing profile. This profile may include personal information e.g. name, birthday, place of residence etc. or your political views, circle of friends, foods you like, clothes you like to wear, favourite brands and etc. Finally, based on the information captured within your profile, it can then be used for targeted campaigns by a multitude of stakeholders. It can even anticipate what you are going to need or buy something in the near future again based on your activity over the internet. It is what happened in the example with Emily when she was googling the available flights to Bali: that information was used to include her in a social media ad campaign which appeared directly within her social network feed. The same goes for choice of clothes, which became part of her “profile” when she googled the manufacturer of the dress she liked earlier. In her case, the information was used by her bank to stimulate her to use her credit card, which worked out pretty fine for her. You might be thinking that these things don’t work this fast, but it would be unwise to do so, because it’s an automated process. While not everything mentioned thus far is necessarily a bad thing, the real risk lies behind the point where *personal* information becomes *public* information i.e. having a small piece of your digital identity available to fraudsters means they can access even more of it. Figuring out your pet’s name won’t be much of a trouble – you already have it uploaded in Instagram, and how about your mothers’ maiden name – it is probably out there in Facebook...

Recognise yourself already? Well in case you did, you must know that having a digital footprint means at least two things: *first*, you should really pay attention about how you interact online and consider how your data is being stored and used; *second*, having a digital footprint is not necessarily a bad thing.

TOOLS & RESOURCES NEEDED

- A media device e.g. PC, Laptop, tablet, smartphone;
- Internet connection;

TIME REQUIRED

60-90 min

ASSESSMENT

1. What is a Digital footprint?
 - a) **The data we leave behind during any digital activity.**
 - b) It is when your fingers are being scanned at the airport security or law enforcement facilities.
 - c) Digital footprint in an online security measure which commercial websites use to verify your identity.
2. Choose the *correct* statement:
 - a) Digital footprint is unique to each person.
 - b) Not being aware of my digital footprint makes my online reputation vulnerable.
 - c) I should pay more attention when I agree to how I interact online.
 - d) **all are correct.**
3. Which of the following statements is *wrong*?
 - a) My digital footprint can be used for targeted ad campaigns.
 - b) **There’s nothing I can do to limit how my data is being used over the Internet.**
 - c) A few hundred interactions over the internet are enough for analytical software to create a very accurate profile of me and my preferences.

IMAGE

<https://pixabay.com/illustrations/finger-fingerprint-security-digital-2081169/>

Activity card 4 - Best practices on protecting your data online

Best practices on protecting your data online

LEVEL

Intermediate

DESCRIPTION OF THE ACTIVITY

At this point, we will take a break from the job focused material, and extend to the concept of **internet security** in general.

Our world is now more connected than ever, a state that offers countless privileges but also creates a significant number of dangers, with one of the most challenging ones being **data theft**.

There are safety measures and rules for the **physical world**, the same is the case for the **digital**.

The good news is that you don't need to be either a hacker or an expert to follow the most basic rules and these will offer you a **very adequate level of security**.

So without further ado, here is the.. **10 laws of Internet security**:

1. Passwords, passwords, passwords

The most classic security measure you can take.

As practically all Internet services that involves an account also requires you to set up a password, probably the **two most crucial tools** of your digital life, your **computer and your cell phone**, are paradoxically password optional!

So make sure **that both of them are password secured**, no matter how boring it is to input it every single time.

You should also **avoid allowing your browser memorize your login data for web pages**, since they pave the way for an intruder to access them all without even guessing them. Make also sure that you **don't forget to logout every time** you finish using a service, since in this case, the intruder doesn't even have to use the Login button!

Last but not least, don't forget the 2 golden rules of passwords:

- **Don't make them oversimple**
- **Don't use the same password everywhere**

Using "1234" on all your social media is unwise, and it makes it much easier for a potential hacker to break them.

It is logical to say that it's difficult keeping track of a large number of complicated passwords. For this reason, you should consider using a **Password Manager**. It is a type of software that not only helps you to **organize and keep track of your passwords**, but also to **automatically generate strong ones**.

2. Use Antivirus software

Perhaps the most obvious entry on this list, an Antivirus tool, can offer the most complete protection, that contains **defence against viruses, firewall, anti-spam tools** and, of course, **the ability to scan your system** for potential undetected threats (a process which should be done regularly).

3. Use an Ad-Block:

An increasingly popular "accessory for browsers", that usually comes into the form of an add-on for your browser and **prevents websites from "pushing" advertisements** in your face. Apart from **dodging annoying ads**, you also **remain secure from malware** that they may carry.

4. Avoid online storage

It may come as a shocker nowadays that cloud platforms are blooming, but the truth is that **you should avoid them for storing sensitive data**. This of course isn't the case for any material, but for the most private one such as, **passwords, e-banking, card numbers, social security numbers etc.** For this type of data, the traditional method of **storing them in a USB drive** hidden in your closet, could prove surprisingly safer.

5. Beware of public spaces

This has mainly to do with **public wifi** (e.g. in cafeterias, restaurants, hotels etc) which have **little to no security**, and a person being in the same network, could potentially access your data. When you are connected in such networks, **avoid trading sensitive data** with other devices while at the same time having as less of these data stored in your device as possible.

Unfortunately, the same goes for **internet cafes** where once again you should **avoid the circulation of personal data** while using their computers.

6. Keep your software up to date

Whether we talk about your **operating system, antivirus, conference software, web browser** etc... you should ensure they are all fully updated since this these help you to **keep up with the latest threats!**

7. Watch out for email spamming

The traits of a **fake email carrying a virus** or other malicious software may have .. bad grammar, spelling and punctuation mistakes, lack of logos, amateurish structure and weird sending email addresses.

Regarding their **content**, they are mostly concerned with supposed **pending obligations, prizes** that you must request, **job offers** for "making money while working from home",



dating offers and they frequently end with a request to **forward their mail** in order to win something (the so-called “**chain mails**”).

They almost always come with an attached file which you should **under no circumstances open** (thankfully, even if you do it accidentally, **your antivirus will most probably spot the threat** and prevent it from opening).

8. **Limit the amount of personal data you share on your social media**

Just as in the video, it is surprising how much information you may already have made publicly available through your social media accounts.

We are not suggesting completely giving up the use of social media, but we recommend **presenting as little information as possible** when using them.

You should **avoid** putting your **home address** and your **phone number(s)** there, while at the same time it would be recommended to **limit your friend list** to people you know reasonably well, **avoid check-in** since you automatically give away your current position and **make your profile viewable only by your friends** instead of having it public.

9. **Use an Anti-theft software**

It may sound sophisticated, but it's simpler than you think..

It is a type of **software** that, **in case your device is stolen**, you can **activate from distance enabling it to instantly erase all your personal data** (confidential contact lists, text messages, call history, browser history, bookmarks etc) from your device, before they are accessed by a thief.

Anti-theft software is not free, but it offers **a good solution in case of such an emergency**.

10. **Use a VPN (Virtual Private Network)**

Last but not least, this increasingly popular type of software, offers a wide array of solutions.

First, it **makes your Internet browsing private**, meaning it can't be accessed by your Internet Provider or by anyone else with access to your router. This is especially useful for people living in shared property, where the Internet connection is provided by the landlord, as well as residents of countries with heavy Internet censorship laws.

It is also an ideal for the **public places** where it offers the **security features that the public network may lack**.

VPN tools are not free, but since they cover a wide array of security needs at once, they should definitely be considered as a potential solution.

TOOLS & RESOURCES NEEDED

Computer/Laptop with Internet access

TIME REQUIRED

30 minutes

ASSESSMENT

1. **I ran a quick system scan and no threats were found. There's nothing else to do.**
 A) True
 B) **False (If you want to be 100% sure, you should perform a full system scan)**

2. **I received an email with an offer by a famous company, so it must be legit.**
 A) True
 B) **False (You should double cross it by googling the offer.)**

3. **Surfing in incognito mode is secure.**
 A) True
 B) **False (Incognito mode has nothing to do with security)**

4. **I should always use an Ad-Block.**
 A) **True**
 B) False

IMAGE

<https://pixabay.com/photos/tips-tricks-tips-and-tricks-4905013/>

1.2.3 Advanced Level

Activity card 5 - The privacy issue

The privacy issue

LEVEL

Advanced

DESCRIPTION OF THE ACTIVITY

Now that you are fully aware of having a digital footprint, how your personal information can be exploited and how important it is to maintain a good online reputation, is time to point you the core of managing your digital identity i.e. becoming in control of your own privacy.

So, how can you actually protect your privacy? Here are some of the steps we recommend doing:

1) Start using two factor authentications. Most of the popular digital platforms e.g. Google, Microsoft, Facebook, Apple, including banks and shopping websites, have this option available and this is

perhaps one of the most important steps you can take towards protecting your personal information. What two factor authentications does is asking you to confirm you are the owner of the account via another means of security. Usually it happens by logging into your account with your credentials and then the service provider would send a you a text message, a push notification through an app on your phone or an email containing a short code which you need to enter before you can actually login into your account. The reason why this is important is that, even if someone gets hold of your credentials for example, you still have another means of protection, which significantly lowers the chance for a successful attack on your personal data. So, go on and look for this security method and enable it wherever you can and whenever possible.

2) Stop using the same password for everything. We are aware that you've probably either heard this before or you've figured it out by yourself, but it is really the second-best thing you can do. There's a big chance that if you for example do online shopping, you probably have stored your credit card information somewhere online e.g. Google Pay, Amazon or eBay and surely you do not like the idea of becoming someone else's Santa Claus. Make sure to change your passwords regularly (and we already mentioned that is not a good idea to include you pet's name or you mother's maiden name in there etc.) and use different passwords for all your accounts. Difficult yes, but necessary.

3) Update your software regularly. This is probably the easiest one we recommend doing, simply because you can set it up as an automated process or simply do it at the time you are prompted to do so by your system. What you don't know it is that whether it is your computer with Windows or Apple on it, your smartphone, your tablet, your free or paid software (e.g. Microsoft Office, Adobe, Java), when there is an update available is usually related to an identified risk which hackers have figured out to get access to your device. Thus, keep your devices up to date and stop hitting that "snooze" button every time it pops up on your screen.

4) Pace yourself on how much information you reveal online. We have already touched on this one, but we can't stress enough how important this is, because what you do online e.g. your day-to-day activities, your spending habits, locations you reveal (tag yourself) or pictures you upload with location information are all exactly the things which hackers are looking for and can be used to know when you are out of your home or you are going to be away for a while. Do not login into newly discovered websites with already existing accounts e.g. Facebook, Google, Outlook, because then you are giving out much more of your information then you should.

5) Phishing attempts. This is a very common method used to obtain someone's personal data. There are various forms of it, but you can train your mind to recognise the risks and this minimize the chance for you to become a phishing attempt victim. Lookout for the sense of urgency i.e. an email you receive which says your account will get suspended if you don't confirm your identity by clicking a link provided to you in the same email. Also, emails starting with a reply and following something you can't recall e.g. if you receive an email with a subject saying "RE: order 188281ZR4 is cancelled" or "Confirm your PayPal account now", can be directly delete them, or at least double check on the dedicated application (if applicable) from your smartphone or simply by logging into your account from another browser or device. Be aware that such emails can appear 100% authentic and the provided link can lead you to a website which can also look completely legitimate to you, but it might be a phishing attempt so that you reveal your credentials and give someone access to your account. Phishing attempts also include phone calls, but same applies to them, and if you are asked to give credentials or any account information over the phone, tell them that you will call them back and visit the website of the company they say they represent, check the number and get in touch with an actual representative to confirm what you've been asked or told before. Do not except friend requests of people you do not know over social media, no matter how good-looking the profile picture might be.

6) Review your privacy settings. Make a list of the all the accounts you have and go into their settings for each one of them to change your privacy settings. Opt-out of any marketing consents you've

unintentionally signed up for. Some of those settings might be hidden under other names like “Personalisation” or “Allowed suggestions”, look them up as well. Limit how apps use your location and how you tick off the boxes asking you to provide information on how you use your devices.

7) Remove apps you don’t use. Another step you can take is to have a look at all the apps you have on your devices and ask yourself which ones are just sitting there without being actually used. The logic behind doing so, is that most of the apps are free, but you are required to create an account, which most likely is being used by third parties without you even knowing. The more the apps, the more you are vulnerable to phishing attempts and hacker attacks.

Learning how to manage your digital identity also means that you should know your rights and how you can use them. GDPR gives individuals more control over their privacy via the following 8 core rights:

- **The right to be informed:** this is the one that actually makes the most sense, because in order for you to do anything with your personal data out there, you need to know who has it in the first place. Thus, this right deals with you giving your explicit consent to controllers to use your data. It also means that you can ask who are other recipients of your data. GDPR forces data controllers to be completely transparent how they collect and use your personal data and therefore, to facilitate a process during which your consent is “freely given, specific, informed and unambiguous”. In addition, requesting your consent must be “*clearly distinguishable from the other matters*” and presented in “*clear and plain language*”. Finally, you can withdraw previously given consent whenever you want.
- **The right of access:** you have the right to know what data is being collected about you and how it is being processed.
- **The right to rectification:** in case you do use your right of access and you discover that there is something inaccurate about them, you have the right to ask the controller to have it corrected.
- **The right to erasure (right to be forgotten):** it is exactly what it sounds like: you have the “*right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*”. Additional conditions apply, but in general you can withdraw consent and ask for your personal data to be deleted.
- **The right to restrict processing:** additional rules apply, but basically you are given the right to limit processing of your data. This right also obliges the data collector to inform “*each recipient to whom the personal data have been disclosed*” if you have decided to take advantage of this right.
- **The right to data portability:** you have to right to transfer personal data personal data “*directly from one controller to another, where technically feasible*” without having to worry about any obstacles related to whom you’ve given your personal data at first.
- **The right to object:** Again, some additional conditions apply, but under this right you are entitled to object to have you your personal data being used (e.g. direct marketing purposes, scientific or historical research purposes or statistical purposes). This right has to be “*explicitly brought*” to your attention “*and shall be presented clearly and separately from any other information*”.
- **Rights in relation to automated decision making and profiling:** meaning that you have the right “*not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects*” or “*similarly significantly*” affects you. In other words, this right aims to protect you against a potential harm i.e. “decision” made without any human intervention.

There is much more which can be said about GDPR like the fact that in case of a data breach/data leak, the data collector must notify both you and the responsible national authority depending on the risk it may pose. You can have a further look into the GDPR and your rights [here](#), or in case you are interested in reading the original document yourself, you may access it [here](#). We also encourage you to watch the following [YouTube video](#), which will help you gain some more knowledge about how GDPR affects you.

TOOLS & RESOURCES NEEDED

- A media device e.g. PC, Laptop, tablet, smartphone;
- Internet connection;

TIME REQUIRED

90-120min

ASSESSMENT

1. I can have a one-for-all password as long it is fulfils all the necessary criteria
 - a) True.
 - b) **False.** Having strong but multiple passwords is the number one thing the majority of security experts recommend when talking about protecting your online credentials and personal information.
2. What is two-factor authentication?
 - a) It's a contract condition for using online services.
 - b) It's when the system asks me to enter my password again, after I've mistaken my credentials.
 - c) **It's an electronic method for additional identity verification via providing extra proof of ownership.**
3. What is the right of access granted by the General Data Protection Regulation (GDPR)?
 - a) **the right to know what data is being collected about you and how it is being processed.**
 - b) the right to enter a company's records and search freely about what information they possess about me.
 - c) the right to have access to free services if I don't what to pay the required fees

IMAGE

<https://pixabay.com/illustrations/hacker-computer-spirit-cyber-code-4031973/>

Activity card 6 - The Right to be Forgotten

The Right to be Forgotten

LEVEL



Advanced

DESCRIPTION OF THE ACTIVITY

The **Right to be Forgotten** is a practice which you will rarely need to use.

But in case you have to resort to it for your own reasons, it is very helpful for you know its **details**, and your **rights** that arise from them, in advance.

The Right to be Forgotten **can be used** in the cases that have been discussed earlier in this unit (**job search and video interviews**) and the companies from which you will request **data erase**, are **usually obliged** to fulfil it.

The term “usually” hides a lot of issues, and that’s exactly what we’re going to focus on:

First of all, in Article 15 of GDPR there are **3 main reasons** mentioned, which you can evoke in order to justify your request for erasing your data:

- 1) You no longer consent to the processing of your data
- 2) There are significant errors within the data
- 3) **You believe that they are being stored unnecessarily**

The third reason is the most viable one when it comes to **job searching websites** and companies with which you went through a **video interview**.

In both cases, you can claim **that since the reason you offered your data was for them to consider hiring you, if they ultimately didn’t, then there’s no reason for them to keep your information in in their database anymore.**

(Note that “information” in our case can mean your **CV** or the **record of your interview**).

Of course, there have been many claims that the above mentioned liberties, could very well be overused, hence ending up at the **limitation of free speech** and a **rewriting of history**.

That’s why, in Article 17 of GDPR there are some **counter arguments** from the company’s side, through which they could deny your request:

- The data is being used to exercise the **right of freedom** of expression and information.
- The data is being used to comply with a **legal ruling or obligation**.
- The data is being used to perform a task that is being carried out in the **public interest** or when exercising an organization’s **official authority**.
- The data being processed is necessary for **public health purposes** and serves in the public interest.
- The data being processed is necessary to perform **preventative or occupational medicine**. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
- The data represents important information that serves the public interest, **scientific research, historical research, or statistical purposes** and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing.

- The data is being used for the establishment of **a legal defense** or in the exercise of other legal claims.

Also note that, besides denying your request, companies also hold the right to **charge you a fee** in order to proceed your request.

The final **outcome** of such conflict is unfortunately **uncertain** since it depends on a variety of factors and is practically subject to law.

So just keep in mind the above factors and **make sure that it is absolutely necessary** to proceed to such request if and when you consider doing it, since in many cases it can take a **significant amount of time** for it to be resolved.

If you want to practice, click [here](#) in order to download an **official template** produced by the **European Union** which you can fill in based on a **hypothetical situation**.

TOOLS & RESOURCES NEEDED

Right to Erasure Request Form

TIME REQUIRED

30 minutes

ASSESSMENT

- 1. Which of these reasons is not a valid counterargument for a company who want to keep your data?**
 - A) Your data are useful for scientific research
 - B) They are going to be used in a court
 - C) **Your right to request delete has expired**
 - D) They will be used for public health projects
- 2. In which case you do not have the legal right to request erasing your data?**
 - A) The purpose for which they were offered to the company, is now over.
 - B) Your data is incorrect
 - C) You recall your consent to the company processing them
 - D) **You demand better terms of processing**
- 3. How long does it take for a request to erase data to be resolved?**
 - A) 1 week
 - B) 1 month
 - C) 2 months
 - D) **Depends on the case**
- 4. On which sector can you make a request to erase data?**
 - A) Private
 - B) Public
 - C) Non-profit



D) All of them

IMAGE

<https://pixabay.com/vectors/trash-trashcan-recycle-bin-shredder-97586/>

Activity card 7 - Privacy policy for your website

Privacy policy for your website

LEVEL

Advanced

DESCRIPTION OF THE ACTIVITY

All websites must typically contain a **Privacy Policy**, this is a **text document** that describes **what type of personal data may be collected** from its users and **the terms under which they are going to be processed**.

If you want to be legal and don't face any difficult situations, you should definitely **create your own Privacy Policy** for your web site.

At first, it may sound as a brain squeezer, but it is in fact a very formulaic process where almost **all its units are predefined**, and they come as following:

1. What type of information do you collect?

You must begin with a clear list of information that could potentially be collected by your website. This list depends on the services your site offers, but the main choices are the following:

Email, name, IP address, billing details, Identity Card Number, password, purchase history, credit card information, reviews, comments, feedback.

2. How do you collect information?

Then, you must explain the ways in which the aforementioned data will be gathered. Once again, the various options may be:

Creation of a profile, subscription to newsletter, purchases, message through contact form

3. Why do you collect information?

After "what" and "how", you have to focus on "why". The most frequent reasons are:

1) To **provide the services** from the website



- 2) To **assist and support** your users
- 3) To **personalise their experience** with the site
- 4) To **gather statistics** that will upgrade the website's services
- 5) To comply with **law regulations**

4. How you store this data?

You should point out the **server** on which they are stored and its **security level** (if it incorporates a specific **security system/technology**).

In case **transactions** take place, you have to mention the **security standard/protocol** that is applied.

5. How you communicate with your visitors?

Mention the possible ways of contacting your users (**email, telephone, postal mail, sms etc.**) along with the possible reasons for that (**problem troubleshooting, dispute resolution, payment collection, surveys, newsletters etc.**)

6. What about cookies?

In case your site uses cookies, you have to mention their **types**, the **kind of data** they collect, and the **reasons** for collecting them.

7. How can your visitors withdraw?

You must mention the alternative ways in which your users can **withdraw their consent** to their data being collected.

8. Policy updates

At the end, you have to highlight that **you hold the right to revise your privacy policy at any time**, providing that **you will notify your users** every time a revision takes place.

9. Questions

End with the **available methods through which visitors can reach you** in case they have any **questions regarding Privacy Policy and their stored data**.

You can now **practice by creating your own Privacy Policy** document for an imaginary website, or one that you aspire to create.

TOOLS & RESOURCES NEEDED

Text

TIME REQUIRED

45 minutes

ASSESSMENT

1. In your Privacy Policy, you should include the frequency at which you are going to communicate with your visitors.
A) TRUE
B) FALSE

2. If no transactions take place in your website, you don't have to mention any payment security protocol.
A) TRUE
B) FALSE

3. It is obligatory to have a cookie consent disclaimer at your homepage.
A) TRUE
B) FALSE

4. You can revise your Privacy Policy without necessarily notifying your users afterwards.
A) TRUE
B) FALSE

IMAGE

<https://pixabay.com/illustrations/privacy-policy-dsgvo-security-man-3415416/>

Activity card 8 - Blockchain

Blockchain

LEVEL

Advanced

DESCRIPTION OF THE ACTIVITY

Personal data should now mean much more to you than just having an ID and thus hopefully its value has also increased your perception for it. However, since technology is now moving at an ever-faster pace and pushing innovation in every direction, we are going to take the time and introduce you to a rather important topic – the Blockchain technology.

Most people connect Blockchain with Bitcoins, but the fact is, that its application is universal and can be used in many other areas like insurance, asset management, payments, smart appliances, healthcare and personal identification (e.g. passports) and therefore it has a lot to do with digital identity management.

Blockchain is perhaps the most radical and game-changing innovation of our generation and it isn't something we should wait to see in the near future – it is happening now. So, what exactly is Blockchain? Perhaps the first thing to learn here is that Blockchain is a software technology and as such there are different types of Blockchain depending on what is it being used for.



Watch the following [video](#) for an introduction in the topic.

So how does Blockchain affect digital identity? Digital identity has the potential to achieve real social transformation and Blockchain technology can help that happen. That is because Blockchain can put you in control of your own data, the way you do business, how you use services and how you interact with people in general. Let's have a look at some real-life applications of the Blockchain technology:

- Self-sovereign identity – this is probably the ultimate use case of Blockchain, where a complete identity system puts user in control of their own data. A good example is the city of Zug, Switzerland, which is one of the first cities in the world which leverages the power of Blockchain, by introducing a digital ID for their citizens. Another similar solution comes from Estonia, where unlike many other countries, every Estonian, irrespective of their location, has a state issued digital identity. Thanks to this Estonia is years ahead of countries still trying to work out how to authenticate people without physical contact. In Estonia, every person can provide digital signatures using their ID-card, Mobile-ID or Smart-ID, so they can safely identify themselves and use e-services. There are [1 billion people](#) in the world living their lives without being able to prove their identity. Can you imagine how their lives would change if they could benefit from such a solution?
- Authentication – this solution can exploit Blockchain technology to store and access authentication documentation, while maintaining data protection at its fullest and keeping data tampering at its lowest. It can also be used to identify us both online and offline, and use one set of credentials to access multiple services. For instance, consider notaries, local government authorities, lawyers etc. A good example comes from [India's West Bengal local government](#) where a Netherlands-based Blockchain company, helps them handle administrative operations such as processing requests and verifying legal identities (e.g. application for birth certificates).
- Payments – how comfortable are you when making purchases online or bank transfers to someone or somewhere at the other half of the world? Probably not so much. What if there was a way that you take trust out of the equation and simply focus on your main goal i.e. make things happen? Because Blockchain is built over on the idea of decentralization and trust therefor is handled for you, such an application can help both save money by eliminating the middle man and save time because its much faster than a banking transfer which can take days. Same goes for banking access in remote areas where not all people have access to banking services or they have to deal with uncertainties, country fluctuations, mistrust or simply can't afford it. In these cases, Blockchain can become a solution for a more stable form of currency, which would not use its value overnight and you

Blockchain applications are emerging literally everywhere in the world and various fields including its original creation cryptocurrencies – there are now more than 150 of them. In the future we can expect Blockchain technologies to become a larger part of our lives mainly due to its features we've already mentioned, trust and decentralization being the ones heading the list. Therefore if exploited under commonly agreed ethical standards, Blockchain could be most powerful and efficient tool for business, conducting fair trade, democratization of societies and economies.

We recommend that you take the time to learn more about Blockchain and its application by watching the following [free training course](#).

TOOLS & RESOURCES NEEDED

- A media device e.g. PC, Laptop, tablet, smartphone;
- Internet connection;

TIME REQUIRED

180 min

ASSESSMENT

3-4 Assessment questions based on what the user has learnt from the activity
The questions can be true or false and multiple choice
Each question should have only one correct answer

1. What is Blockchain?
 - a) It's a chain of data blocks, necessary to access online services.
 - b) **It is a software technology, which allows decentralised, secure and trust-enabled transactions.**
 - c) It is a recently discovered artifact, which many believe it testifies for the existence of aliens.

2. Blockchain is only used for cryptocurrencies (Bitcoins)
 - a) True.
 - b) **False.**

3. Which are some of the areas where Blockchain is being used
 - a) **payments, identification, healthcare and trade;**
 - b) it has a very limited use;
 - c) Blockchain currently not available, but it will be used in the future

IMAGE

Find an image that represents the activity from an open source website (e.g. pixabay.com, pexels.com, unsplash.com, freeimages.com., etc.) and copy paste the link here.

<https://pixabay.com/illustrations/bitcoin-currency-technology-money-3089728/>

2. CREATIVELY USING DIGITAL TECHNOLOGY

2.1 Unit Introduction

The below card will be visible to users of all levels when they click on the respective block (see design document)

CREATIVELY USING DIGITAL TECHNOLOGY

DESCRIPTION OF THE TOPIC



In this unit, we will learn how to use digital technology in order to solve problems, meet our needs and resolve issues in collaboration with others.

EMPLOYABILITY SKILLS

- Caution and responsibility
- Self-awareness
- Autonomous spirit
- Problem solving

LEARNING OUTCOMES

- Know how to solve problems and needs using digital tools.
- Know how to engage collectively to solve problems and needs using digital tools.
- Know how to help and guide other to solve their needs and problems using digital tools.

DIGCOMP FRAMEWORK

Competence area 5: Problem solving

5.3 Creatively using digital technology

REFERENCES (if applicable)

APA style

ADDITIONAL RESOURCES (if applicable)

https://drive.google.com/file/d/1RvesU1MRgDrXvFEbOPalhHG_2i95S6AV/view?usp=sharing



2.2 Activity cards

2.2.1 Beginners Level

Activity card 9 - Digital job seeking problems

How to face digital job seeking problems

LEVEL

Basic

DESCRIPTION OF THE ACTIVITY

Online job searching is a sector that has its own particular security problems, with the automation of the process offering both privileges and drawbacks.

The latter is what we are going to focus on this activity, enlisting **the most common problems** that may be faced when **searching for a job online** and, of course, **easy ways for limiting or resolving them completely**:

1. Your CV is not scannable

Nowadays, due to the **huge flow of resumes** that a company can receive digitally, most of them (especially the larger ones) use the **Applicant Tracking System (ATS)**.

This is a type of software that **automatically scans the received CVs and tries to spot certain keywords** inside them that are **related to the company's subject and qualifications that are required** for the position.

If a **sufficient number of words** is found, then the document is **promoted for review by a person**, otherwise it is **automatically rejected**. This may appear heartbreaking, but according to research almost **75% of resumes are rejected this way**.

Unfortunately, this list of "hot" words, is totally **different depending on your target field**. So use your **common sense** and try to **list as many potential important words as possible**, and then **incorporate them** carefully into your CV.

2. The same CV for everybody

It is one of the most classic traps that job seekers fall into, and it applies both to the digital and the physical world.

Sending **exactly the same resume** to each potential employer is a **big mistake** since, no matter how specific it is what you are looking for, there can always be some **deviations from**



what is required, therefore avoid giving **the impression that you send out resumes mechanically**.

So, for proper “customisation” keep in mind **3 things**:

- In a certain job ad, spot the requested elements that you possess but haven’t specifically included them in your CV and **add** them.
- **Subtract** elements that are not requested by the job ad.
- **Reorder** your skills in order to get the most important for the specific ad to the top.

3. Scammers

The general anonymity that the Internet provides, makes it a great field for scam artists, and unfortunately, job seeking is no exception.

Thankfully, there are some fairly **common traits** that can be found among scammers and these may prevent you from falling into their trap:

- **They contact you first:** A message starting with the claim that your resume was found by a job searching website, is a yellow (warning) flag. While at times it could be true, it is rare for companies to search job platforms for potential employees rather than receiving CVs through an advert.
- **Too good to be true:** Work from home, a few hours per week, high salaries and flexible schedules are the most classic warning for a scammer. While such great jobs might actually exist, they are almost always given to “insiders”.
- **Very quick reply:** If you ultimately go through an interview, and receive a positive answer right away or even the next day, then you probably shouldn’t proceed. The selection process between candidates usually takes much longer.
- **Vague job requirements and description:** When a job requires very essential elements that most people have, and at the same time refuses to describe in detail the duties of the position (“Don’t worry, we’ll train you”), they perhaps have a reason for avoiding it.
- **Unprofessional emails:** Capitalization, punctuation and grammatical errors, along with the lack of a logo or signature, are things that a real company would never leave unnoticed.
- **Asking you to pay for something:** If you are asked to pay just for having the right to be interviewed or to have your resume reviewed, is a huge red flag for con artists. This is one of their most “traditional” methods.
- **They ask you to give away personal information:** As mentioned in the previous unit, a legitimate company would never ask you for data like your bank account, identity card number, credit card number etc. before being hired. If this happens then avoid any further contact.

4. Lack of a cover letter

You may have heard it before, but the truth is that **a cover letter is more than welcome**, since it can summarise information from your CV, something which **makes your application friendlier to its reviewer**.

The problem when it comes to cover letters and job searching platforms, is that many of them do have a section for uploading your CV, but not for uploading a document with the cover letter.

There are 3 main alternatives:

- If there is a “message” section you can copy-paste your cover letter there.
- You can include the cover letter in the same file as your cv
- Instead of applying through the platform, you can send your cv and your cover letter by email

Keep also in mind that the same **customisation** rules that apply to your CV are also valid for your cover letter. The cover letter **can be even more tailor-made** than your resume, since you can **refer to the company by its name** and address the specific job advert that was posted.

5. Don't rely solely on online searching

Including such a statement here may sound ironic, but it is absolutely true.

The **“traditional”** methods of job searching have not vanished yet and in reality **they can prove really helpful**.

You can always find job adverts **in magazines and newspapers** that are not found online and, of course, trying to make **personal connections to potential** employers through your social circle, will help you **stick out** more than you just being another document in a vast digital pile.

TOOLS & RESOURCES NEEDED

Job platform account

TIME REQUIRED

15 minutes

ASSESSMENT

1. **Having the right keywords for the ATS in your CV means that it will be approved.**
A) TRUE
B) **FALSE (there are a lot of other elements that define its quality)**
2. **Receiving an email from a famous company means that it's not a scam.**
A) TRUE
B) **FALSE (a con artist can pose as a member of the company. You should double check the offer by contacting the company)**
3. **While welcome, a cover letter is not obligatory.**
A) TRUE
B) FALSE
4. **Sending to a large number of companies, guarantees you that at some point you will be picked.**
A) TRUE
B) **FALSE (it's all about the quality, not the quantity)**

IMAGE

<https://pxhere.com/el/photo/1449657>

2.2.2 Intermediate Level

Activity card 10 - Video interview problems

How to face video interview problems

LEVEL

Intermediate

DESCRIPTION OF THE ACTIVITY

Video interviews are relatively unexplored territory, since they have **only recently started to be used** and especially since the corona pandemic, where distant meetings are **preferred**.

Since we are dealing with digital tools here, there are always some possibilities that you might face **technical issues** and, of course, during and interview you may have “**traditional**” **problems** that are not concerned with technical issues.

In both cases, **being prepared is the best you can do**.

By reacting quickly to a problem that occurs, not only can you **keep the interview running**, but it can also demonstrate that you are a **skillful and well-prepared applicant**.

So keep in mind the following **potential scenarios and their solutions**:

1. There is a specific dress-code for video interviews

Not for fashion but for technological reasons, as the wrong attire won't interact well with the camera.

Although each camera is different, it is generally **recommended not to wear white or very brightly colored clothes** since in some case they can produce some **weird reflections**.

The same goes for stripes since, as you may have already noticed at some point, they tend to turn into **optical illusions when on camera**.

So prefer darker and preferably monochrome choices.

It is a common secret that some people don't wear trousers during video calls. You may be sure that it's safe, and in most cases it may be, but **there is always the danger of doing reflexive/mechanical movements** that you don't realise instantly, such as **standing up in order to pick something up**.



You definitely don't want your interviewers to evaluate your choice of underwear, so in order to be 100% secure, **make sure that you wear proper trousers**. It is better than having surprises.

2. **If you wear glasses, beware**

The above mentioned "dress code" is also the case for those of you that wear glasses, since **they can make reflections that will prevent your eyes from being clearly visible**.

If your glasses come with an **anti-glare coating**, then this is most probably OK since that is exactly what this coating has been for.

If you don't, then decide whether you should **switch to contact lenses**, or **take off your glasses** provided that you can still see the people on your screen.

3. **Watch your background**

The more **neutral** your background is, the better. An ideal case would be a **plain wall** but showing some **basic house elements** within your screen (as a couch, a door, a lamp, a small bookcase etc) will not do any harm.

On the other hand, you should avoid **overly complicated settings** since they are going to distract your interviewers and of course, they are not that pleasant to the eye.

Use your **common sense** about avoiding problem backgrounds like a pile of unwashed dishes.

Finally, **avoid having a window on your background during daytime**, since the sunlight can create a **"silhouette effect"** where you will appear dark.

4. **Make sure that you look at your interviewer**

It is one of the most common traps of video interviews. You spend too much time looking at the video box to keep track of your mannerisms, or looking at the box of your interviewer in order to check their reactions.

In both cases, **it will seem that you are constantly looking elsewhere**, which is a big drawback since eye contact is equally important during a video interview as it is during a traditional one.

So **make sure that you look straight into your computer's camera as long as possible**, taking only **small glimpses onto your screen** in order to check reactions.

5. **Don't be too relaxed**

Being **stressed and robotic can be negative**, but going to the opposite extreme by being **overly laid-back, can be wrong** as well.

While a **more relaxed attitude shows confidence**, you shouldn't overdo it and this is a trap of video interviews, since being in your own cozy home environment, can tempt you into this (especially if the interview is long). So bear this in mind.

6. **Practice, practice, practice**

As mentioned, preparation in everything, especially if it is going to be your first video interview.

First of all, make sure that you have **familiarized yourself with the software** that you are about to use.

You should know how to turn on and off your camera and microphone for security reasons, but it is also useful for all aspects of the interview.

Make sure that your **camera settings give a nice, clear image of you** and check that you are using **the latest version of the software**.

Finally, you could **make a practice call with a friend of yours**, in order to test both the **efficiency of the software**, and that **you know all the basic functions** that may be needed.

Needless to say, **all this should be done as far in advance as possible** and not just a couple of hours before the interview.

7. **Be prepared for the event of a tech issue**

Technology is very helpful but not perfect, and there can always be **unexpected technical problems**.

While you cannot avoid them, you can be **prepared** for them. This, in the case of a video interview, means that if your **software crushes** and you have to restart it, **you are able to call your interviewer on the phone** in order to inform him/her that you are restarting it and that, in worst case scenario, you could go on with a phone interview. **So make sure that you have your interviewer's number handy**.

You could also try to **call them from a second device** which could be **a second computer** (recommended) or **your cell phone**, but since they are generally less powerful than computers, you should try it only in case you are **confident that your phone will be able to connect**. So make sure that **"device b"** is **ready and set** before beginning your interview.

TOOLS & RESOURCES NEEDED

Video conference software

TIME REQUIRED

20 minutes

ASSESSMENT

1. **Which of these settings is not recommended for a video interview?**
 - A) A loud cafeteria
 - B) On public transport
 - C) On your bed
 - D) **All the above**

2. **Should you use your hands when talking during a video interview?**
 - A) Yes, because you seem more expressive
 - B) Yes, because it gives more energy to the discussion
 - C) **No, because while they show expression during a face-to-face session, they distract during video conference.**
 - D) No, because there is the danger of bumping into objects around you.

3. **In case there is a software crash while on interview, you must**



- A) Restart it until it works
 B) **Restart it, and while doing it, call your interviewer on the phone. If the software doesn't recover, try to run it on your device b. If it doesn't run there either, you continue your interview through the phone.**
 C) Restart it and if it doesn't recover, go to your device b. If it doesn't recover there either, call your interviewer.
 D) None of the above
4. **Which of these should you check before a video interview?**
 A) The basic functions of the software
 B) Your camera settings
 C) The quality of your connection through a practice call
 D) **All the above**

IMAGE

<https://www.publicdomainpictures.net/en/view-image.php?image=289426&picture=video-conference>

2.2.3 Advanced Level

Activity card 11 - Problems in your website

How to face problems in your website

LEVEL

Advanced

DESCRIPTION OF THE ACTIVITY

Even when **websites** are personal and fairly basic (as it might be the situation in your case) they can still be a **source of various troubles**.

These issues are literally countless and could vary from **highly specialized subjects** that need the assistance of an expert, to **more simple cases** where the owner of the website can solve it him/herself.

For us we're going to focus on the second category, highlighting the **most common problems** that you can get into, along with their **recommended solutions**, should they be technical or practical:

1. Outdated design



A sky with clouds as a background, 5 types of Word Art fonts together, pictures with a resolution of 640x480 and glowing colors everywhere, might have been acceptable in 1998, but not today.

Nowadays where **graphic standards are very high**, having such a sloppy looking website instantly **gives the impression that it was created by an amateur**.

And while this could might as well be the case (since you are not a professional web designer) that's exactly why **ready-to-use themes** exist.

Whether you use **Wordpress, Wix** or any other popular website creator, it is certain that you will find **premade themes** where **colors, visual identity, design and overall style are pretty much ready**, and the only thing you have to do is **fill them with content**.

They are a **valuable tool for all beginners in website creation**, and therefore you should definitely consider using them.

2. Lack of updates

When it comes to a personal website, you will most probably not have a lot of regular news to post. But **a web site does need to be updated and up-to-date** in order to generate traffic since users need a reason to keep on visiting it.

Try **to update your web site at least once a week** and even if you don't feel like there is something worth mentioning, **create a news item!**

The ideas for such "content fillers" vary depending on your subject, but the safest method is to **upload news regarding your professional sector** since they can be both **interesting for your visitors** and, of course, **they are endless!**

3. Cluttered homepage

Your main page acts as a preview of the content that the user can explore in your website, and not the content itself.

You should therefore try to keep it **as simple as possible**, because getting into a vast amount of information from your first click discourages users to go on.

A recommended structure for a personal homepage is:

- A welcome banner
- A brief biographical note
- A bullet point list of what can be found on the site
- A newsfeed
- A contact form along with your contact details

4. Complicated structure

A structural issue, like being lost into a labyrinth of folders and subfolders, lowers the surfing experience.

The structure of your main menu could be:

- Home
- About
- A dropdown list of your site's main points

- News
- Contact

The difference is that while on the **homepage** there are the **previews** of these elements, the **menu** is used the access to the **actual contact**. Think of it like the showcase of a shop and its interior.

5. **Broken links**

Coming across “404 page not found” frequently is a sign of the **website being abandoned and not receiving proper care**. Not to mention a **poorer ranking in Google** since its algorithm assesses that a great number of dead links with the website being inactive (even if it’s not).

Put into your agenda to do a regular “**dead links check**”, especially when you make **structural changes** to your web pages.

6. **Slow speed**

A slow web site triggers a huge discussion about the potential reasons, some of which are very technical.

But one of the most common causes, that is easy to correct, is the **overload of the server with unnecessary content**, with the most noteworthy being large **photos**.

It is surprising how much space you can spare just by **compressing** your photos while at the same time **the difference to the eye will be almost unnoticeable**.

7. **Lack of contact details**

One of the main targets for running a personal website is to **get in contact with users** who can **help you fulfill your goal**.

Having them perform detailed research in order to reach you, is certainly something that won’t help.

As mentioned previously, make sure that **at least your email is clearly visible** on your homepage while using a **contact form** would be even better.

The same applies to your **social media** pages. Make sure that **a set of buttons linking to all your social media is at the top of your homepage**, and it would be even better if they were present on all the pages of your site.

TOOLS & RESOURCES NEEDED

A personal website

TIME REQUIRED

20 minutes



ASSESSMENT

1. **In case your website is slow, compressing your photos will definitely solve the problem**
A) TRUE
B) FALSE

2. **It is obligatory to have a set of buttons to your social media in every single page of your website**
A) TRUE
B) FALSE

3. **As long as your contact details are visible, it is not necessary to have a contact form**
A) TRUE
B) FALSE

4. **You need to be or to know a graphic designer in order for your website to look appealing**
A) TRUE
B) FALSE

IMAGE

<https://pixabay.com/vectors/monitor-404-error-problem-page-1350918/>

3. IDENTIFYING DIGITAL COMPETENCE GAPS

3.1 Unit Introduction

The below card will be visible to users of all levels when they click on the respective block (see design document)

IDENTIFYING DIGITAL COMPETENCE GAPS
DESCRIPTION OF THE TOPIC
The so-called skill gap, is the difference between the set of skills that employers want/need and the skills that you actually possess. In this unit we will learn to identify which digital gaps you may have and where to seek opportunities to develop them.
EMPLOYABILITY SKILLS
<ul style="list-style-type: none"> - Self-awareness - Autonomous spirit - Problem solving - Helping others - Collaborating with others
LEARNING OUTCOMES
<ul style="list-style-type: none"> - Know how to explain where your digital competences need to be improved or updated. - Know where to find opportunities for self-development to keep up to date with the digital revolution. - Know how to assess the digital skills of others. - Know how to guide others to update their digital skills - Know how to use guideyourtalent.com
DIGCOMP FRAMEWORK
Competence area 5: Problem solving



5.4 Identifying digital competence gaps

REFERENCES (if applicable)

APA style

ADDITIONAL RESOURCES (if applicable)

<https://drive.google.com/file/d/1D9VThYkvBfiv4WDuWPdJoG3KozSdQJcC/view?usp=sharing>

3.2 Activity cards

3.2.1 Beginners Level

Activity card 12 - Identifying your digital skills gap

Identifying your digital skills gap

LEVEL

Basic

DESCRIPTION OF THE ACTIVITY

The first step when identifying your digital competences is **to know the list of competences you can choose from.**

While the term “digital competences” may sound quite vague, in reality a specific list of them has been created. It is called the **Digital Competence Framework for Citizens (DigiComp)**.

The structure of the GoDigital project and this training course has been based on the Framework. The list of competence areas and dimensions can be found on page 11 of the Framework.

Use this list of **20 digital competences**, split into **5 competence areas**, to identify your digital competence strengths and gaps through the following **3 simple steps**:

1. Write a list of the skills that you already possess

This means that you should only include those that you consider to hold a **level 3 or higher**. You can check the level descriptions from **page 23** onwards.



2. Write a list of the skills you wish to acquire

Spot the competences that you don't yet hold (those with a **level up to 2**) but feel confident that **at some point you could upgrade them** and that you have the natural talent to do so.

3. Write a list of the skills that you think you are not able to achieve

It is not possible to be good at everything, so it should be acceptable to identify your **weak spots** and it can **save you a lot of time** when searching for jobs.

So identify those competences that, either due to **lack of a natural talent** and/or **a lack of willingness to explore**, you are **not going to develop** at this point in time.

It can be even easier for you write the above lists, if you take the digital competences assessment test by [Pathways for Employ](#) the results of which can guide you through this process.

Now that you hold these 3 lists, you can take the following steps every time you consider a job advert in order to evaluate **how likely it is for you to be hired** (in terms of skillset) and also **which competences you should consider developing first**:

1. Identify the digital competences that the position requires

Read carefully the job description and try to **identify which of the 20 competences of DigiComp are sought, along with their required levels**. If you think that this is not clear in the job description **you can Google the digital competences** that are usually needed for the sector of the position you are interested in.

If there are **competences from the list you will not achieve** among those needed for the position, it would be advisable for you not to **consider applying for this position** and therefore try to find more suitable opportunities.

2. Do the maths

For each of the required skills for the job, subtract the level you have on it from the level you think is required. The number you get is **your skill's score**.

For example, if the job requires **level 5** Netiquette, and your Netiquette **level is 3**, then **your Netiquette score is 2**.

You will get a **negative score** in cases where **your level surpasses** the one that is required by the job. For example, if the job needs "Developing digital content" at **level 2** and you hold it at **level 6**, then **your score would be -4**.

Finally, if the job needs a skill that you don't possess at all, then your score is the level that the company is seeking. For example if the company needs "Protecting Devices" at **level 3** and **you don't possess** Protecting Devices at all, then **your score is 3**.

As you may have already guessed, **the lower the score in each skill, the better**.

3. Find your proximity to getting the job

Sum the levels of all the skills that are required for the job and this is the **job score**.

Sum the skill scores that you gathered from the previous step and you get your **personal job score**.

Subtract the personal from the job score, and you get the **final score**.

The lower the final score is, the better!

The closer your personal score is to the job score, the worse for you. If it is **0** then it means that you hold the exact level of competences that are required and finally, if it's negative, it means that you are overqualified for the job.

4. Prioritize the competences that will be developed

Finally, you should create a list of your competences for this job, based on their **urgency for development**.

This is simply done by **arranging them based on their skill score**. The one that holds the **highest** (and therefore has the **biggest gap** from the level that is needed) **is placed first**, while the one with the **lowest is placed last**.

TOOLS & RESOURCES NEEDED

Text

TIME REQUIRED

40 minutes

ASSESSMENT

1. **A skill score of -5 means that you lack the skill level that is needed**
A) TRUE
B) FALSE
2. **A personal score of zero means that you are just as qualified as it's needed**
A) TRUE
B) FALSE
3. **A skill score can never be higher than the required level for that particular skill**
A) TRUE
B) FALSE
4. **The final score only shows how qualified you are for the digital competences that are required for the job, without referring to any other type of requirement that may be sought.**
A) TRUE
B) FALSE

IMAGE

<https://pixabay.com/photos/mind-the-gap-london-underground-1876790/>

3.2.2 Intermediate Level

Activity card 13 - Skills Gap vs Signaling Gap

Skills Gap vs Signaling Gap

LEVEL

Intermediate

DESCRIPTION OF THE ACTIVITY

While the term “Skills Gap” grabs all the attention, there is another similar one that is not well known is the “**Signaling Gap**”.

While the former refers to **not having certain skills**, the latter is about **not knowing what skills are required** by employers.

It is ironic that the **Signaling Gap** is not that known, **since it precedes the Skills Gap**, hence **you must first know what skills are in demand and then you try to upgrade them**.

While it is easy to understand the skills that are demanded from a single job advert, it is **more challenging to have an understanding of the overall job market**.

Additionally, the **digital world is rapidly changing**, and as a result so is the ranking of the most sought-after skills. In 2020 the top 10 digital skills is the following:

**At the end of each entry, you can see the corresponding DigiComp Framework codes for the heading skill.*

1. Coding

This is perhaps most important traditional activity in the digital world. It fits into a large number of digital projects.

The most popular coding languages right now are **PHP/JavaScript, MySQL jQuery and Angular**.

Unfortunately, such a **highly requested skill**, is inevitably **highly demanding**, with the teaching of coding being **more applicable within organized courses rather than self-teaching**.

DigiComp codes: 1.3, 3.1, 3.2, 5.1

2. Digital Business Analysis

“Are we going to choose digital solution A or B?”

If you are able to guide a company through this choice (and of course to justify your opinion) this will be a **boost for your career!**

When considering the almost constant technological evolution, companies need to know how they are going to evolve digitally in order to compete with others.

DigiComp codes: 1.1, 1.2, 5.2

3. Website and Application development

Web developers are in high demand since **all businesses and organisations**, from the smallest to the largest, need to **have a well branded website** that is used as the **main reference point** for any potential customer.

DigiComp codes: 3.1, 3.3

4. Digital Marketing

Digital marketing has grown and is here to stay.

New methods and techniques to manage clients and their behaviours are constantly being implemented, and the **budget** that goes into persons that devise marketing campaigns is **increasing**.

Special mention should be given to **social media marketing** which is a separate category of marketing, with many companies dedicating a significant portion of their marketing strategy to it.

DigiComp codes: 2.1, 2.2, 2.6, 3.1

5. Data Analysis

Enterprises collect large amounts of data every day which, if not processed properly, is useless. This where **data analysts** work, to use the data and **derive valuable information, offer advice and provide recommendations** that can assist the company in moving forward.

At the moment the demand for data analysts far outweighs their supply, and choosing such a career path, can open a lot of doors.

DigiComp code: 1.1, 1.2, 1.3

TOOLS & RESOURCES NEEDED

-

TIME REQUIRED

10 minutes

ASSESSMENT



1. **What is the definition of “Skills Gap”?**
 - A) **The difference between the skills you own and the skills that are required**
 - B) Not knowing what skills are required
 - C) Upgrading your skills
 - D) Lowering your skills

2. **What is the definition of “Signaling Gap”?**
 - A) The difference between the skills you own and the skills that are required
 - B) **Not knowing what skills are required**
 - C) Upgrading your skills
 - D) Lowering your skills

3. **What is a DigiComp code?**
 - A) The skill of coding
 - B) An app
 - C) **The digital skill areas that are defined by the Digital Competence Framework**
 - D) A code of ethics in digital professions

4. **What is data analysis?**
 - A) **Deriving information and recommending solutions through the process of data that are collected by a company**
 - B) Programming a computer software
 - C) Creating a database for archival reasons
 - D) A mathematical formula

IMAGE

<https://www.pxfuel.com/en/free-photo-epjgi>

3.2.3 Advanced Level

Activity card 14 - Using Pathways for Employ

Using Pathways for Employ

LEVEL

Advanced

DESCRIPTION OF THE ACTIVITY



Pathways for Employ is a digital tool that detects and evaluates your digital skills gap.

Through a **series of questions**, it identifies your **strong and weak points**, and presents you with a **report** that explains these points in further detail.

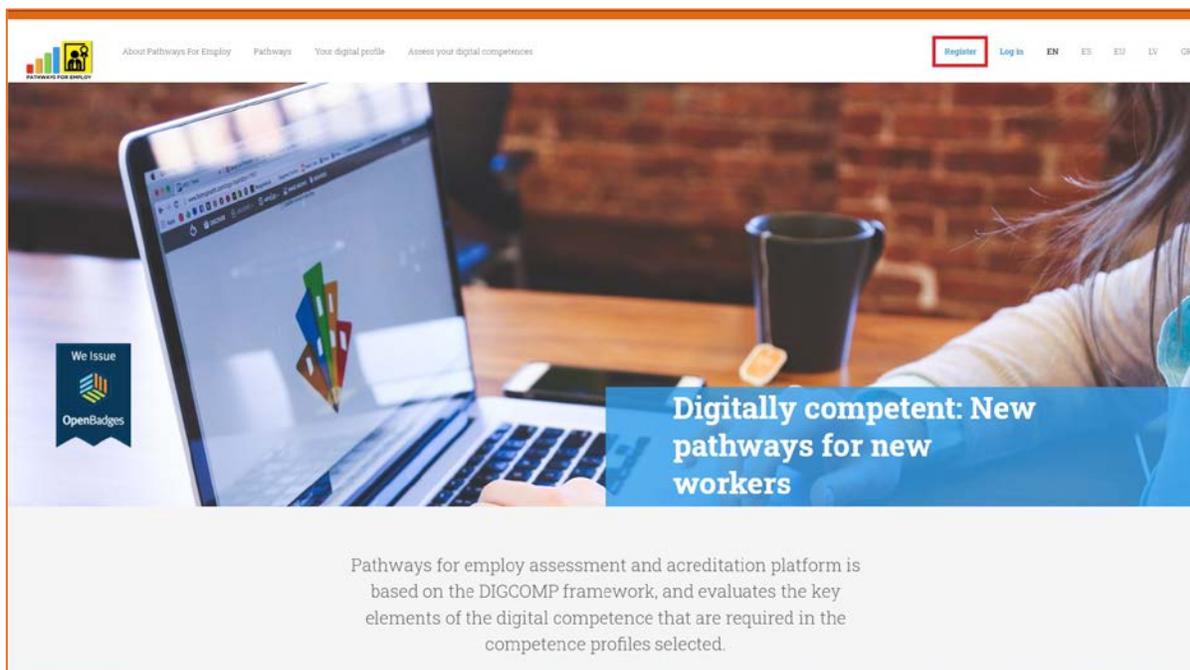
An important feature of this tool is that **it follows the structure of DigiComp Framework**, and it therefore presents its results in accordance to 21 skills and 5 competence areas of the Framework.

It is **easy to use** and since you take the test as a registered user, your **results are stored** and you can **check your digital skills gaps whenever you want**.

Click [here](#) in order to access its website where you can read more details about the **Pathways for Employ** project, its partners and the potential it has in supporting your future professional life.

Taking the test:

In order to go through the test, **you must be a registered user**. Go to the **Pathways for Employ** homepage and click on **Register** at the upper right.



Register button in the Homepage of Pathways for Employ

You will need to complete a form where you have to provide the following information:

- Email
- Name (it is recommended to use a nickname)
- Gender
- Employment status
- Age range
- Town & country



-
- The level of education that you possess (low-medium-high). Click on the cross at the right of each option, in order to get more details about which qualifications it includes.
 - Finally, you have to set a password.

After ticking the box about data protection at the bottom of the page, click **Save the data** on the bottom right.



Personal information

E-mail: (*)	<input type="text" value="example@email.com"/>
Name: (*)	<input type="text" value="Jonathan"/>
Surname: (*)	<input type="text" value="White"/>
Second surname:	<input type="text"/>
Gender: (*)	<input checked="" type="radio"/> Male <input type="radio"/> Female
Employment status: (*)	<input type="text" value="Employee"/>
Age(in completed years): (*)	<input type="text" value="25-54"/>
Highest level of your education: (Successfully completed) (Tick only one): (*)	<input type="radio"/> Low formal education level (±) <input type="radio"/> Medium level education (±) <input checked="" type="radio"/> High level education (±)
Town: (*)	<input type="text" value="Athens"/>
Country: (*)	<input type="text" value="Greece"/>

Password:

Password: (*) (?)



The GDPR (General Data Protection Regulation) seeks to create a harmonised data protection law framework across the EU and aims to give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world. The Regulation also introduces rules relating to the free movement of personal data within and outside the EU. P4E is committed to providing our users with data privacy and security to assist them on their journey to GDPR compliance.

(*) By registering, you accept the terms of service and P4E's privacy policy.

Save the data

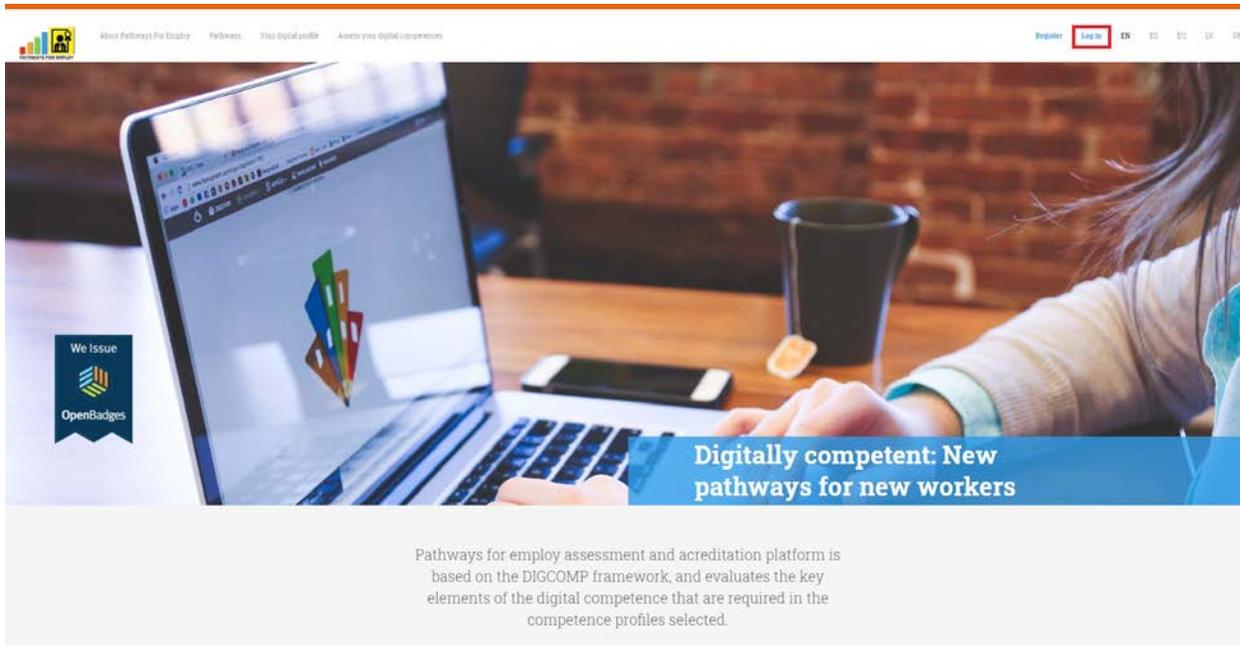
Registration form

Upon successful registration you will receive the following **notification email**



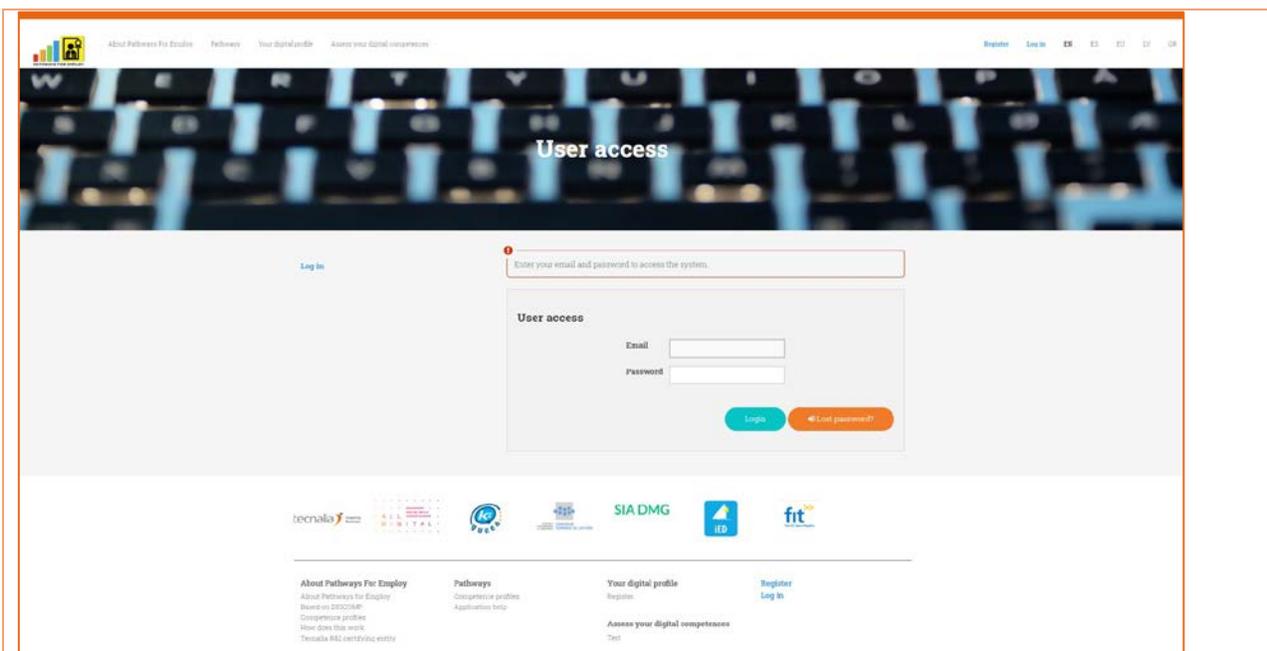
Email notifying successful registration

You should then return to the Homepage, and this time click on **Log In** on the upper right.



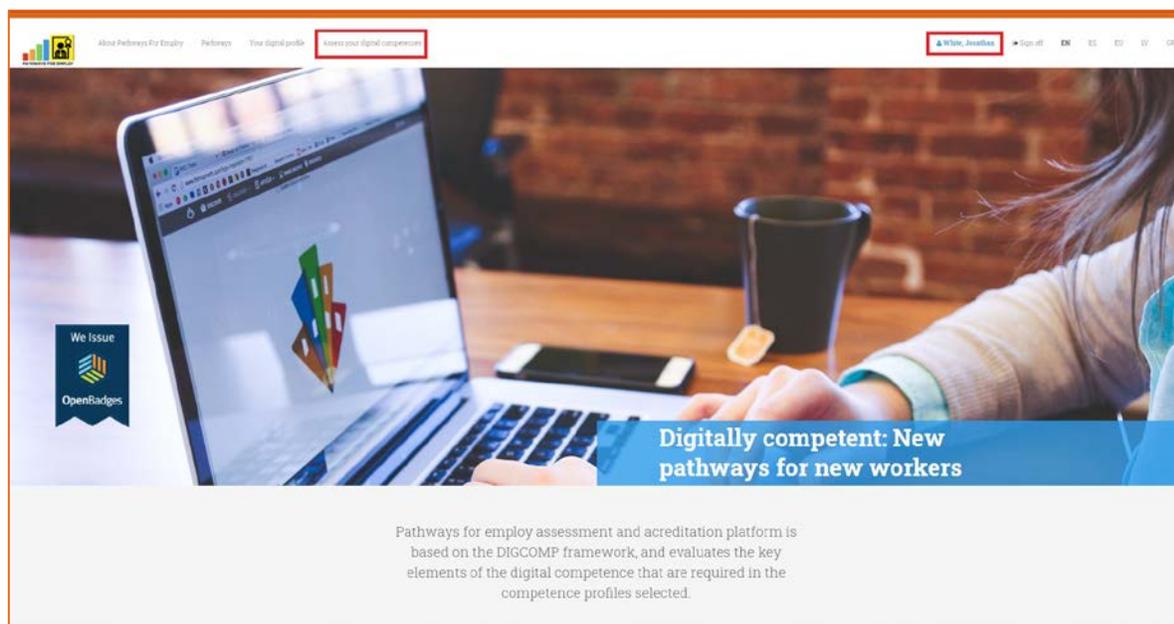
Log In button in the Homepage of Pathways for Employ

Put your email and password in the form that will show up, and Login.



Login screen

Upon successful login, you will notice that the Register button on the upper right has changed to the name of your account. You can now take the test by clicking on **Assess your digital competencies** at the upper left.



Assess your digital competencies button

On the next screen, you will get some basic information about the test. Click **Let's go**.

The screenshot shows the website's main interface. At the top, there are navigation links: "About Pathways For Employ", "Pathways", "Your digital profile", and "Assess your digital competences". A user profile "Wijn_Joostan" is visible in the top right corner. The main heading is "Are you ready for assessing your digital competences?". Below this, there are four informational cards: "Before the test" (with a play button icon), "Test" (with a heart icon), "Time" (with a battery icon), and "At the end" (with a computer icon). A red box highlights the "Let's go" button located below these cards. At the bottom, there are logos for "tecnalia", "DIGITAL", "KE", "SIA DMG", and "fit".

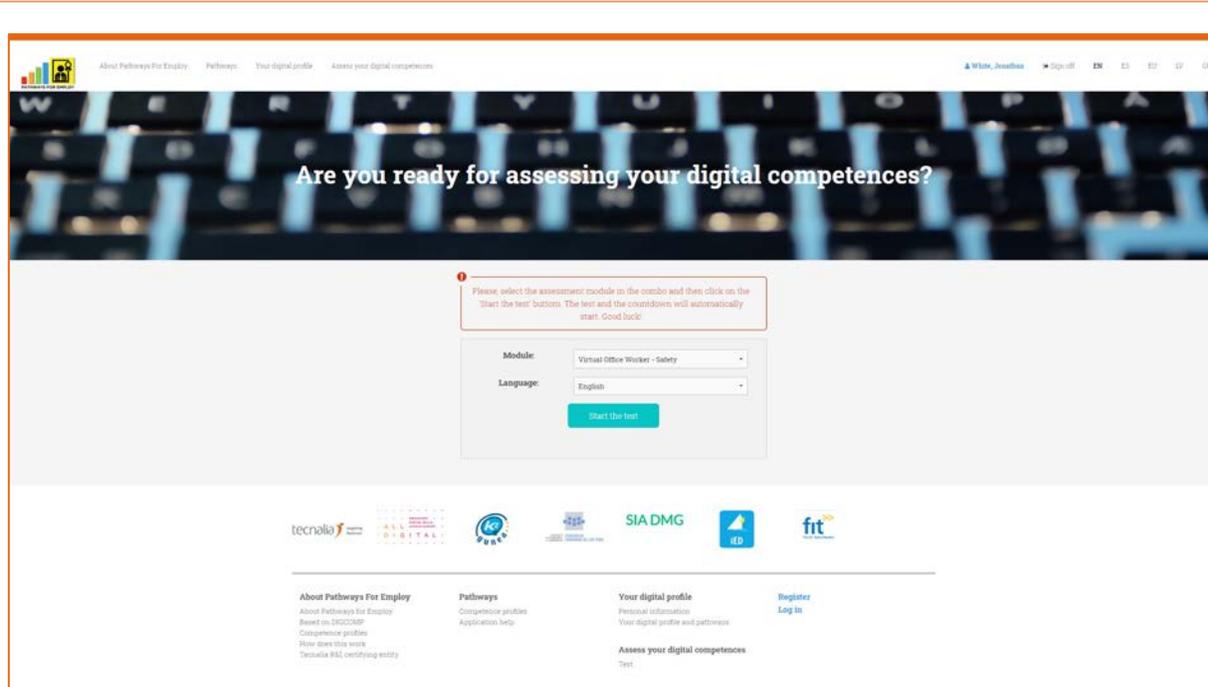
Let's go button

Open the dropdown menu of **Module** and there, choose **the competence area on which you want to be tested**. You will notice that for each of area, there are 2 options.. either from the aspect of an **Entrepreneur** or the aspect of a **Worker**.

This screenshot shows the same website interface but with a dropdown menu open. A red box highlights a message: "Please, select the assessment module on the option and then click on the 'Start the test' button. The test and the countdown will automatically start. Good luck!". The dropdown menu is titled "Module:" and lists several options, including "Virtual Office Worker - Safety" (which is highlighted in blue), "Entrepreneur - Information and data literacy", "Entrepreneur - Communication and collaboration", "Entrepreneur - Digital content creation", "Entrepreneur - Safety", "Entrepreneur - Problem solving", "Virtual Office Worker - Information and data literacy", "Virtual Office Worker - Communication and collaboration", "Virtual Office Worker - Digital content creation", and "Virtual Office Worker - Problem solving". Below the dropdown, there is a "Language:" label. The rest of the page content is identical to the previous screenshot.

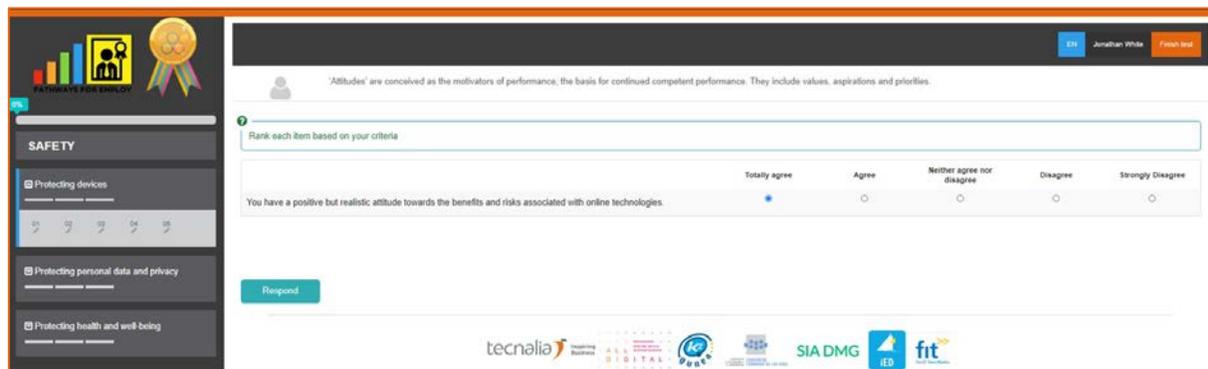
Choosing your preferred language

You then choose your preferred language and click **Start the test**



Ready to start the test

While doing the quiz, you may encounter various types of questions such as self-reflections..



Self reflection

multiple choice

The screenshot shows a simulation interface with a sidebar on the left containing icons for 'SAFETY', 'Protecting devices', 'Protecting personal data and privacy', and 'Protecting health and well-being'. The main content area has a header with a user profile 'Jonathan White' and a 'Finish test' button. Below the header, a message reads: 'You are at the airport and want to connect to the WiFi network... but all the WiFi networks are not safe.' A dropdown menu is open with the text 'Select one of the following options'. The question asks to 'Indicate which of the following statements is CORRECT'. There are four radio button options:

- Public WiFi networks that are protected with a username and password are secure. The dangerous ones are those that do not require an authentication process.
- We can connect to a public-WiFi network as long as we do not login into our bank account or other personal accounts.
- Connecting to a public WiFi network is dangerous if it is done from desktops or laptops. However, smartphones and tablets are not at risk.
- As a general rule, we must be very careful of the information we use when we connect to an unsecured WiFi network since we do not know if our personal information, can be seen, and/or analyzed by others.

 A large question mark icon is positioned to the right of the options. At the bottom, there is a 'Respond' button and a row of logos including tecnalnia, ALL DIGITAL, SIA DMG, and fit.

Multiple choice

clicking on the right spot of an image

The screenshot shows a simulation interface similar to the one above. The main content area has a message: 'You use email daily, so it's important to adopt security measures in order to avoid problems with devices that you are accessing your mail from.' Below this, a note states: 'Please note that you need to click very precisely on the exact spot in the image where the required action needs to be carried out. Then the simulation will lead you to the next step. If you click anywhere else, the simulation will not work. You will have to do it without overpassing the maximum quantity of clicks and time allowed.' The question asks to 'Mark the last email as SPAM'. The image shows a Gmail inbox with several emails. The last email in the list is from 'Google' with the subject 'New sign-in from Chrome on Windows...'. A red dot is placed on the 'Mark as spam' icon of this email. At the bottom, there is a 'Respond' button and a row of logos including tecnalnia, ALL DIGITAL, SIA DMG, and fit.

Clicking on the right spot of an image

or giving an answer in text form



Answers in text form

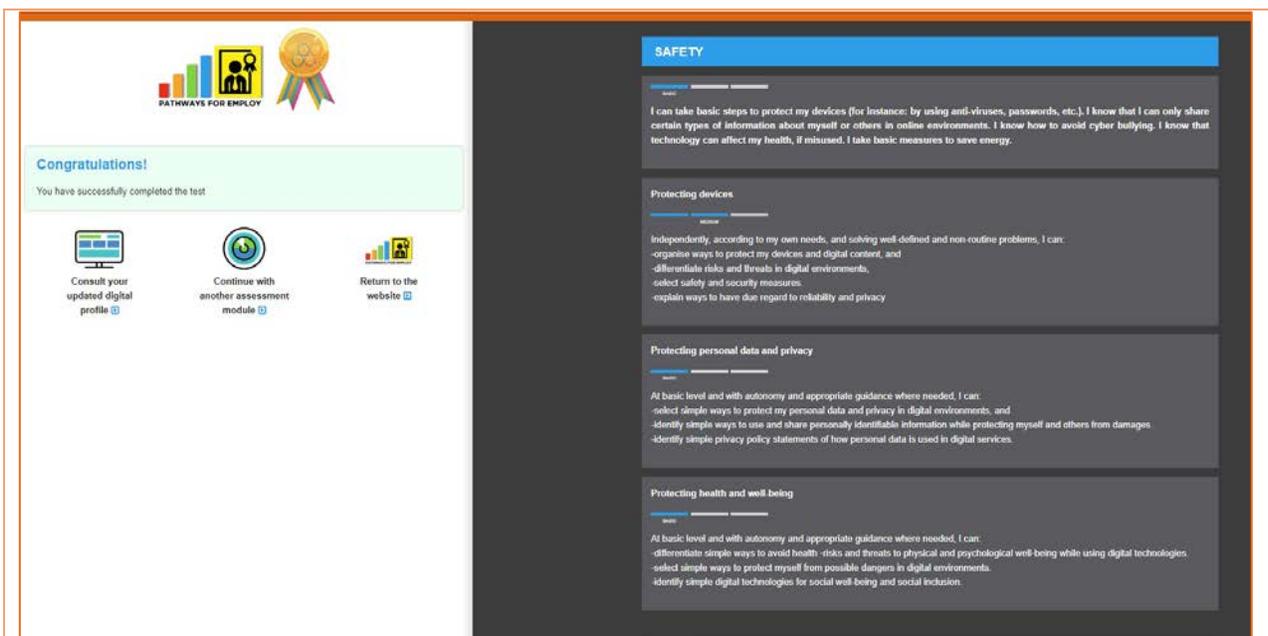
On the left, there is always a **column** where you can check elements such as:

- Your **progress** up to that point
- The **competence area** and the **skill(s)** on which you're being tested
- The **skill level** that you have achieved so far (depending on your answers)
- Right below the skill level, you can see the **numbers of its questions**. Under each number there is either a **tick** or an **'x'** depending on whether you answered it **correctly or wrongly**, or a **pencil** in case you **haven't answered it yet**.



Column on the left

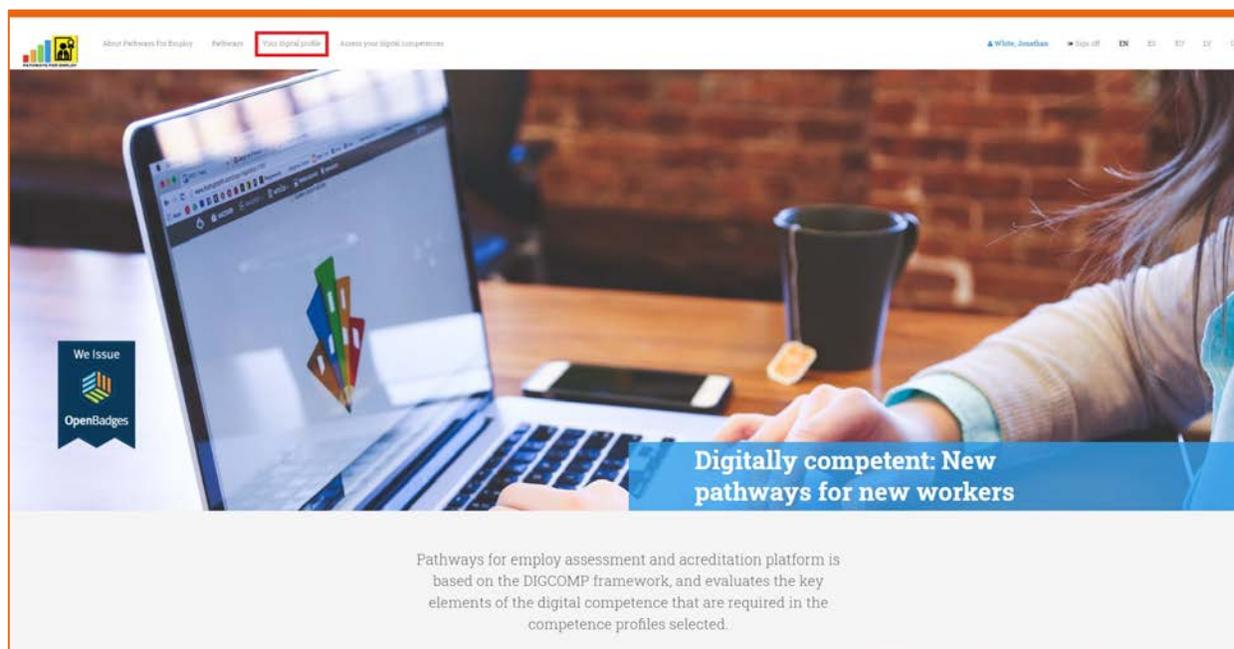
At the end, you will be presented with a **report of your results**, where you can see the **level that you achieved in each of the competence area's skills**, along with a text that describes your capabilities in each case.



Results report

Keeping track:

If you want to check your activity on the website, go to the **Pathways for Employ Homepage** and click **Your digital profile** on the upper left.



Your digital profile button

You will be able to edit your personal information. On the left column, click on **Your digital profile and pathways**.

Personal information

Your digital profile and pathways

i Note: All fields marked with an asterisk (*) are required.

Personal information

Name (*)	<input type="text" value="Jonathan"/>
Surname (*)	<input type="text" value="White"/>
Second surname	<input type="text"/>
Gender (*)	<input checked="" type="radio"/> Male <input type="radio"/> Female
Employment status: (*)	<input type="text" value="Employee"/>
Age(in completed years): (*)	<input type="text" value="16-24"/>
Highest level of your education: (Successfully completed) (Tick only one): (*)	<input type="radio"/> Low formal education level (±) <input type="radio"/> Medium level education (±) <input checked="" type="radio"/> High level education (±)
E-mail (*)	<input type="text"/>
Town (*)	<input type="text" value="Athens"/>
Country: (*)	<input type="text" value="Greece"/>

Password

Your digital profile and pathways button on the left

On the **Tests performed** tab, you can see a list of your tests, from the latest to the oldest, along with the **time and date** that you began each one, whether you have **completed or not**, and finally whether you have received its corresponding **badge** (in this case the badge icon is in colour).

White, Jonathan

Tests performed

Digital profile

Competence profiles

History of tests performed

Badge	Test	Date	Status	More details
	Entrepreneur - AREA 4: Safety	03/08/2020 (08:22)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (10:03)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (10:08)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (10:12)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (10:26)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (11:03)	✓ Completed	View more details
	Virtual Office Worker - AREA 4: Safety	03/08/2020 (11:05)	? Not completed	View more details
	Entrepreneur - AREA 1: Information and data literacy	03/08/2020 (11:27)	✓ Completed	View more details

History of tests performed

From the **Digital profile** tab you can see **the highest level that you have achieved in each of the 21 skills** (if you haven't taken the test of a certain skill yet, there will be hyphens instead of ticks)

White, Jonathan

██████████

Tests performed

Digital profile

Competence profiles

Download a certificate (Compatible with Europass)

Areas	Competences	BASIC	MEDIUM	ADVANCED
<p>Information and data literacy</p>	1.1 Browsing, searching and filtering data, information and digital content	-	-	-
	1.2 Evaluating data, information and digital content	-	-	-
	1.3 Managing data, information and digital content	-	-	-
<p>Communication and collaboration</p>	2.1 Interacting through digital technologies.	-	-	-
	2.2 Sharing through digital technologies	-	-	-
	2.3 Engaging in citizenship through digital technologies	-	-	-
	2.4 Collaborating through digital technologies	-	-	-
	2.5 Netiquette	-	-	-
	2.6 Managing digital identity	-	-	-
<p>Digital content creation</p>	3.1 Developing digital content	-	-	-
	3.2 Integrating and re-elaborating digital content	-	-	-
	3.3 Copyright and licences	-	-	-
	3.4 Programming	-	-	-
<p>Safety</p>	4.1 Protecting devices	-	✓	-
	4.2 Protecting personal data and privacy	-	✓	-
	4.3 Protecting health and well-being	✓	-	-
	4.4 Protecting the environment	-	-	-
<p>Problem solving</p>	5.1 Solving technical problems	-	-	-
	5.2 Identifying needs and technological responses	-	-	-
	5.3 Creatively using digital technologies	-	-	-
	5.4 Identifying digital competence gaps	-	-	-

Download a certificate button

Additionally, you can click on **Download a certificate** at the upper left, in order to download a pdf file in which the aforementioned skill achievements are enlisted.

DIGITAL PROFILE: *Jonathan White*

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

Project No 2019-1-ES01-KA204-064269. This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	AREAS	COMPETENCES	BASIC	MEDIUM	ADVANCED
	INFORMATION AND DATA LITERACY	1.1 Browsing, searching and filtering data, information and digital content 1.2 Evaluating data, information and digital content 1.3 Managing data, information and digital content			
	COMMUNICATION AND COLLABORATION	2.1 Interacting through digital technologies 2.2 Sharing through digital technologies 2.3 Engaging in citizenship through digital technologies 2.4 Collaborating through digital technologies 2.5 Netiquette 2.6 Managing digital identity			
	DIGITAL CONTENT CREATION	3.1 Developing digital content 3.2 Integrating and re-elaborating digital content 3.3 Copyright and licenses 3.4 Programming			
	SAFETY	4.1 Protecting devices 4.2 Protecting personal data and privacy 4.3 Protecting health and well-being 4.4 Protecting the environment	X	X X	
	PROBLEM SOLVING	5.1 Solving technical problems 5.2 Identifying needs and technological responses 5.3 Creatively using digital technologies 5.4 Identifying digital competence gaps			

Achieved levels of competence along the 5 areas

From the Competence profiles tab, click on the **play sign** at the end of the “Virtual office worker” description...





White, Jonathan

Tests performed Digital profile **Competence profiles**

Available profiles



Entrepreneur

Most important digital competences, transversal and complementary digital competences of the Entrepreneur profile, based on the European Framework DIGCOMP [a](#)



Virtual office worker

Work skills, proficiencies and abilities required a virtual office worker across any jobs and work settings [a](#)

Play sign button at the bottom right of the virtual office worker button

...and you will come up with the requirements necessary for acquiring the badges of the 5 competence areas. You will notice that in almost all cases you have to achieve an advanced level in the area's respective skills.

White, Jonathan

Tests performed

Digital profile

Competence profiles

Virtual office worker

Badge not achieved

Profile: Virtual office worker

Main tasks:

- General and digital skills considered needed by a virtual office worker profile like, Sensemaking; ability to determine the significance of what is being expressed;
- Social intelligence: ability to connect to others in a deep and direct way, to sense and stimulate reactions and desired interactions;
- Cross-cultural competency: ability to operate in different cultural settings;
- Computational thinking: ability to translate vast amounts of data into abstract concepts and to understand data-based reasoning;
- New-media literacy: ability to critically assess and develop content that uses new media forms, and to leverage media forms for persuasive communication;
- Virtual collaboration: ability to work productively, drive engagement, and demonstrate presence as a member of a virtual team, and so on.

Areas	Competences	BASIC	MEDIUM	ADVANCED
<p style="font-size: small; text-align: left;">Information and data literacy</p>	1.1 Browsing, searching and filtering data, information and digital content			✘
	1.2 Evaluating data, information and digital content			✘
	1.3 Managing data, information and digital content			✘
<p style="font-size: small; text-align: left;">Communication and collaboration</p>	2.1 Interacting through digital technologies.			✘
	2.2 Sharing through digital technologies			✘
	2.4 Collaborating through digital technologies			✘
	2.5 Netiquette			✘
	2.6 Managing digital identity			✘
	2.3 (Not visible in image)			✘

Badge requirements 1



 Digital content creation	3.1 Developing digital content	x
	3.2 Integrating and re-elaborating digital content	x
	3.3 Copyright and licences	x
 Safety	4.1 Protecting devices	x
	4.2 Protecting personal data and privacy	x
	4.3 Protecting health and well-being	x
 Problem solving	5.1 Solving technical problems	x
	5.2 Identifying needs and technological responses	x
	5.3 Creatively using digital technologies	x
	5.4 Identifying digital competence gaps	x








About Pathways For Employ

About Pathways for Employ
Based on DIGCOMP
Competence profiles
How does this work
Tecnalia R&I, certifying entity

Pathways

Competence profiles
Application help

Your digital profile

Personal information
Your digital profile and pathways

Assess your digital competences

Test

[Register](#)
[Log in](#)

Badges requirements 2

After you have achieved all 5 of them, you will get the **Virtual Worker badge!**

TOOLS & RESOURCES NEEDED

Pathways for Employ

TIME REQUIRED



20 min

ASSESSMENT

1. The report that you get at the end of the test is based on how many questions you answered correctly
A) True
B) False
2. There is a premium version of the website
A) True
B) False
3. All questions have right and wrong answers
A) True
B) False
4. You can take the test regularly (e.g. every month) in order to track your progress on job searching
A) True
B) False

IMAGE

<https://pxhere.com/en/photo/1443493>