DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Let’s get started!

Management of personal accounts and images

Project number: 2017-1-PL01-KA2014-038433

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

Let’s start!

What is a Digital Footprint?

Digital footprint is one’s trace, trail of data, which is created while using the Internet. It is known as the set of traceable digital activities, actions, contributions and communications that we leave on the Internet or on digital devices. It refers to the records and traces we leave behind us as we use the Internet.

It can be divided into two types of footprint:

✓ *Passive digital footprint* (unintentional), which is created when the owner is not aware about his/her information.

✓ *Active digital footprint* (intentional) when the owner releases and shares his/her personal data deliberately.

Let’s start!

Online habits

We all use the Internet on a daily basis but, are we aware of what actions leave a trace and how much information we are revealing?

▶ **You are revealing information!**

Visiting any website provides its owner with your IP address, which may include your geographic location, your web browser type and operating system, and, often, the last web site you visited. However, these data is relatively innocuous and even fairly anonymous. If these are footprints, they are not very relevant, as many people can be using the same IP address at the same time.

Source: www.internetsociety.org

▶ Online Commerce, Social Networks and Web Mail:

For some types of online sites or platforms, IP addresses do not provide enough information; this is why they set up a cookie!

Most websites set a cookie in your browser automatically when you first visit the site. In this cookie, profile and preference information about you can be stored.

As a result, websites that can access the cookies in your browser (even if it is to improve your experience) end up holding information about you.

Source: [*www.internetsociety.org*](http://www.internetsociety.org)

Profiling companies:

Based on the raw data you are revealing, profiling companies can link all information they can track about you online and make inferences about …

- Your habits
- Your preferences
- Your values
- Your aspirations
- Your intentions
- Your future behavior

Source: www.internetsociety.org

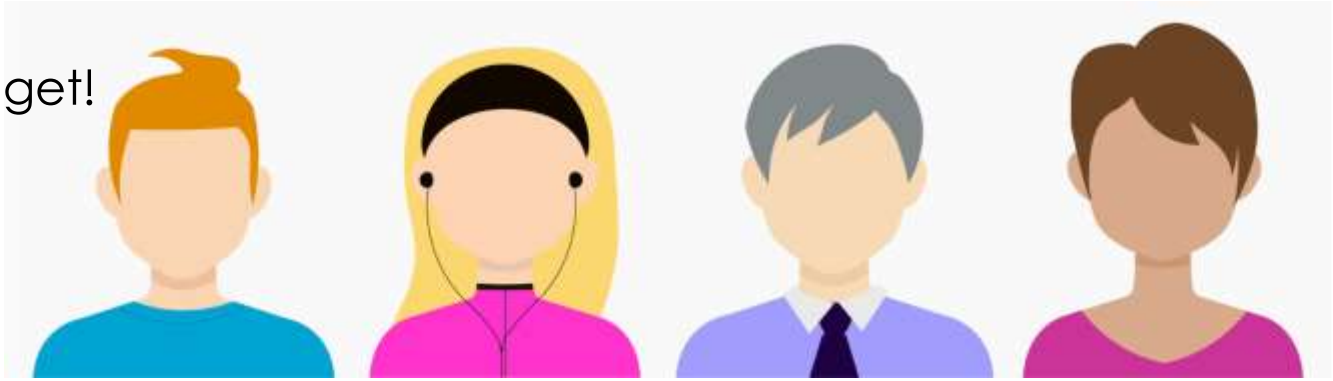
Linkability:

This concept refers to the act of linking or putting together all individual footprints onto a complete online profile about us. This fact occurs when websites or online platforms decide to share with each other personal data which apparently is stored in single contexts.

It limits users' ability to keep, and thus to manage, their own privacy.

Your online profile is built using your raw data, such as websites you have visited, products you have purchased, anything you have searched for, your address, and any kind of personal information you have given to any of the cooperating sites: gender, age, employment status, financial information…

It is unimaginable how long this list can get!



Source: www.internetsociety.org

Let’s start!

How much do you know?

We all have some general knowledge about internet related terms and concepts, but do we know their real and more accurate meaning?

Check the following definitions in order to have a deeper understanding of regularly used concepts:

Let’s start!

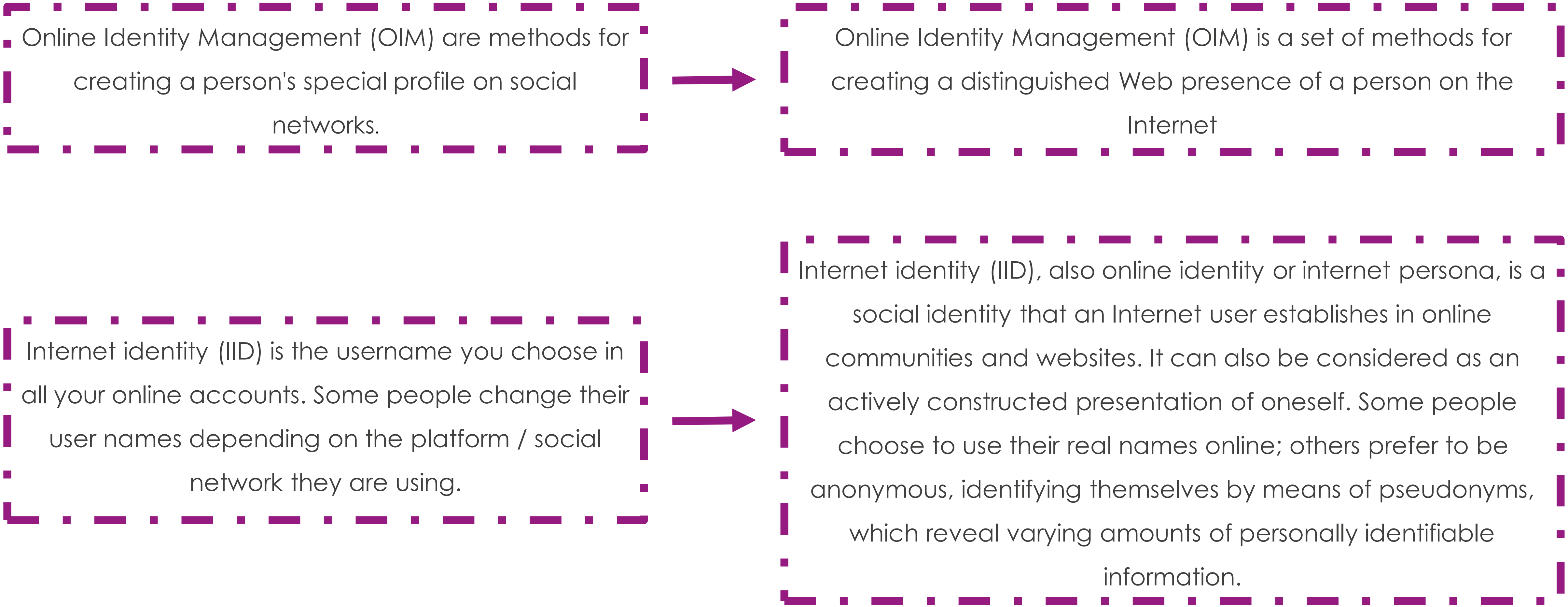
Digital Certificate is a password that allows a person to exchange data online.

→ It is correct, but not precise enough. Digital Certificate is an electronic ‘password’ that allows a person and organisation to exchange data securely over the internet using the public key infraestructura (PKI). Digital Certificate is also known as a public key certificate or identity certificate.

Netiquette refers to the way that people communicate with others online.

→ Netiquette is short for ‘Internet etiquette’. In the same way etiquette is a code of polite behaviours in society, netiquette is a code of good behaviour on the internet. This includes several aspects of the Internet such as email, social media, online chat, web forums, website comments, multiplayer gaming, and other types of online communication.

Let’s start!



Online Identity Management (OIM) are methods for creating a person's special profile on social networks.

Online Identity Management (OIM) is a set of methods for creating a distinguished Web presence of a person on the Internet

Internet identity (IID) is the username you choose in all your online accounts. Some people change their user names depending on the platform / social network they are using.

Internet identity (IID), also online identity or internet persona, is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself. Some people choose to use their real names online; others prefer to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally identifiable information.

Let’s start!

Link-jacking is when you click a link that is only in advertisement and you are redirected to a website where they sell the product that was being advertised.

Link-jacking is a practice used to redirect one website’s links to another which hackers use to redirect users from trusted websites to malware infected websites that hide drive-by downloads or other types of infections.

A newsletter is information that you receive in your email even if you do not want it or are not interested in what they advertise.

A newsletter is a periodically published work containing news and announcements on some subject, typically with a small circulation. Newsletters may be distributed by electronic mail.

Let's start!

Like-jacking is a virus that enters your computer when you click 'like' or 'follow' buttons in Social Media platforms.

→

Like-jacking is a phenomenon that occurs when criminals post fake Facebook or other Social Networks "like" buttons to web pages. Users who click the button don't "like" the page, but instead download malware.

Passive digital footprint is data trail that other people post about you on the internet, specially in Social Media Networks.

→

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

Let’s start!

To subscribe means to accept that they send you information about offers and discounts to your personal email.

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

Let’s start!

Take control of your personal data

Do you check your privacy settings when you sign-up for a website?

What are the consequences of not doing so?

List the reasons why people should check their privacy setting and limit access to their private information.

→ www.youtube.com/watch?v=5ByVaZ0rg8U

Let’s start!

Online Image Management (OIM)

Did you know that…

- In Companies’ recruitment procedures, applicants’ digital footprints (photos, online posts, etc.) play a major role.

- Cyberbullying is a usual practice in those sites that are more frequently visited by a large number of teenagers.

http://youtu.be/T6ulH2bWCnY

Let's start!

Youth Social Media Use

Watch this video and reflect about the following issues:

- What are the main ideas presented?
- Would you say he is pessimistic or realistic?
- Did you feel identified when he was talking?
- Do you thing most young people behave this way?

www.youtube.com/watch?v=SnweVUXEuEQ

Let’s start!

Protect your online privacy!

Tighten up your privacy by taking some small and useful precaution steps:

- Turn off location services to prevent any app from tracking your location.
- Don’t allow apps to know data stored in your phone (contact list, calls history…)
- Be careful when you log in social networks, as you may be allowing them to access certain information from your profile.
- Read the fine print to know what you are sharing!

Let’s start!

Research the following sites for detailed information about each Social Media Platform:

- ✓ Instagram Help Center
- ✓ Instagram Privacy and Safety Tips

- ✓ Twitter – Safety and Security
- ✓ Twitter – Rules and Policies

- ✓ Facebook Privacy Basics
- ✓ Facebook Help Centre - Privacy

- ✓ YouTube Policy Center - Protecting your privacy
- ✓ YouTube Safety Center - Safety

- ✓ Google+ Safety Center - Managing your digital reputation
- ✓ Google+ Safety Center - Privacy resources

Try to formulate a report with five top tips for protecting privacy or managing online reputation

Thank you for your attention!

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

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

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Dive in!

Management of personal account and image

Project number: 2017-1-PL01-KA2014-038433

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

Dive in!

Group discussion!

- ✓ Talk about our real and online identity.
- ✓ Give students a set of questions such as:
  - *What is identity?*
  - *Is it important for us?*
  - *Are real identity and online identity the same thing?*
  - *Do we lie when we are online?*
  - *Do we behave differently in each type of our Social Media profiles?*

Dive in!

Group presentations

✓ Divide your group in pairs or small groups.

✓ They should do online research about a close friend or a family member.

✓ Then they should prepare a short presentation (Power Point, Prezi …) about the data they were able to find online about their personal/private life.

✓ Encourage a debate/discussion about the type of data found and possible (negative) implications

Dive in!

Pro and contra debates

✓ Split the group in two smaller groups.

✓ Give each group a chart to fill in with pros and cons about different statements.

✓ Share the groups ideas and encourage a debate/discussion about them.

Dive in!

1

Pay with your phone

PROS	CONS

Mobile payment is easy to use

You can’t use it everywhere

Device failure in case of battery drain

Phone is prone to be theft

Mobile payments are very fast

It’s safer than plastic card

1

Pay with your phone

PROS	CONS
Mobile payment is easy to use	You can’t use it everywhere
Mobile payments are very fast	Device failure in case of battery drain
It’s safer than plastic card	Phone is prone to be theft

Dive in!

Do the groceries online

PROS	CONS

You can order anytime, 24/7

You don’t get to pick perfect produce

Some grocery store websites are poorly designed

Delivery is convenient

Avoid crowds and parking queues

Popular offers may sell out before your allotted delivery time

Do the groceries online

PROS	CONS
You can order anytime, 24/7	You don’t get to pick perfect produce
Delivery is convenient	Some grocery store websites are poorly designed
Avoid crowds and parking queues	Popular offers may sell out before your allotted delivery time

Case studies about identity theft

- ✓ Examples on http://nordvpn.com/blog/identity-theft-case-studies/.
- ✓ Divide your group in pairs or small groups.
- ✓ Discuss possible reasons for identity theft, the consequences and possible solutions.
- ✓ Learners should think of a similar case in their local environment or their country.
- ✓ Share opinion/experience with other groups.

Dive in!

Write down all your online daily activities

- ✓ List of activities students carry out using the Internet.
- ✓ Then split them in 2 groups:
  - *Activities they could carry out without Internet.*
  - *Activities impossible to carry out without Internet.*
  - *Start a debate: is using the internet for almost all our daily activities a choice or is it "forced"*

Dive in!

Work in groups

✓ Divide your class in pairs or small groups.

✓ Each pair or a group chooses an online platform or social network *(Facebook, Gmail, Drive, Instagram …)* and goes through the terms and conditions.

✓ Learners write down all those sentences which are complex, ambiguous and difficult to understand.

✓ Then start a debate:

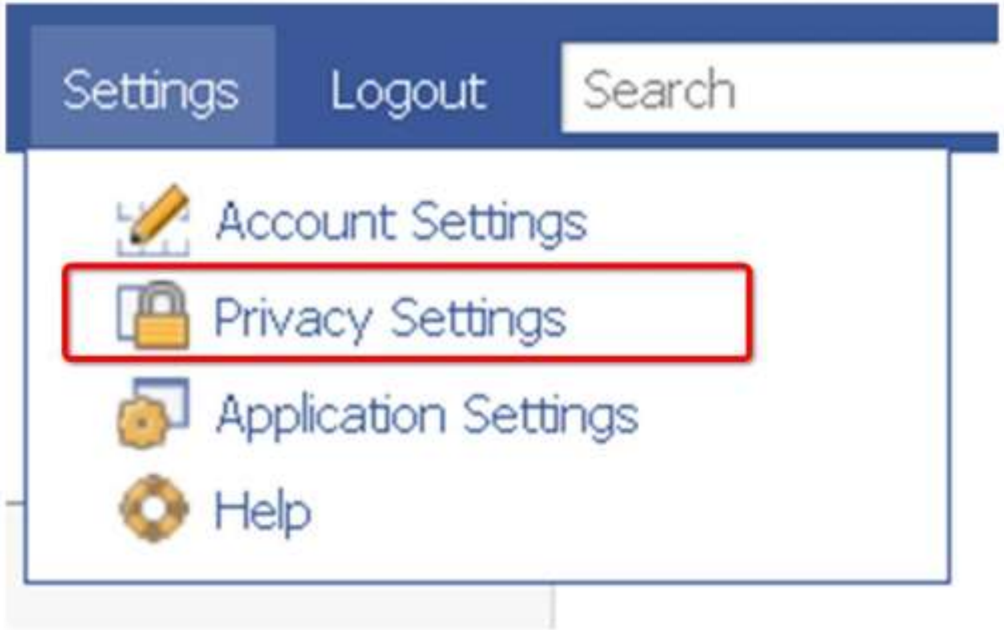
- *How users should be informed about terms and conditions?*

Dive in!

How to change privacy on Facebook

- ✓ Divide your class in pairs or small groups.
- ✓ Each group is given the task to adjust different settings.
- ✓ For help: Link to basic Facebook privacy settings:

  https://www.facebook.com/help/325807937506242
- ✓ To view and adjust your privacy settings:
  - ✓ Click ▾ at the top right of Facebook and select Settings.
  - ✓ Click Privacy on the left column.



Dive in!

Brainstorming about online banking

- ✓ Divide your class in 2 groups.
- ✓ One group should think about arguments for using online banking and one group should think about arguments against using online banking.
- ✓ Then each group present their arguments.
- ✓ Then start a debate about safe use of the online banking and try to turn students arguments again using online banking to positive.

Dive in!

Rotating Stations

- ✓ Create stations and divide your class in small groups.
- ✓ Each group moves to a station, where they take about ten minutes discussing an idea and recording the results of their discussion on a white board located at the station.
- ✓ As the groups move from station to station, they base their discussions on what previously has been recorded on the white board.
- ✓ Then start a debate.

Dive in!

Suggested topics to discuss

What are different types of digital certificates?	What is a digital certificate?	Why and where digital certificates are used for?
Why do we need authentication system?	What are certification authorities?	What is the process of obtaining a certificate?
What does a digital certificate contain?	Advantages of digital certificate	Disadvantages of digital certificate
How authentication is used	How authentication works	Types of authentication methods

Dive in!

The debate

Role play with your students. Present them with a situation (there has been a case of online theft via a fake Online Banking App) and they have to create a debate (moderated by a person who will be appointed by the teacher).

After each person receives their role, they will have 10 minutes to work with the people in their group and prepare arguments to defend their position.

After the debate, have a short group discussion.

Dive in!

Examples of characters (depending on the number of students):

In favor	Against
A person working in a bank	A victim of online theft
A person who sells his/her products online	A regular online customer
A regular online customer	An old person
A person in a wheelchair	A person working a regular shop
[…]	[…]

Dive in!

Online shopping

Hand out to your students small cards with the following vocabulary. Pair them up or organise them in small groups and let them discuss for 10/15 minutes about these concepts. Then, each group will define some of the concepts and will provide examples, showing them on the screen, of online platforms where these concepts apply *(Amazon, Ebay, Walmart, Aliexpress, Etsy, Wish…)*

Cart	Encryption	Return policies	Order status	Basket	A complaint
Encryption	Personally identifiable information (PII)	Checkout	Delivery	A full refund	Sign in
Cookies	Security enabled	Merchandise credit	Stock	Watch Lists	Advertisement

Dive in!

Did you know that…?

“An annually carried out report, found that **8%** of global **malicious email attachments** were **_docm_ files** (*a type of Microsoft Word XML file that executes macros*).” *(source)*

“**Mobile platforms** are one of the fastest-growing targets for cyber criminals. In just one year (2015 to 2016) there was a **105% increase** of **malware detections**: almost 18.4 million!” *(source)*

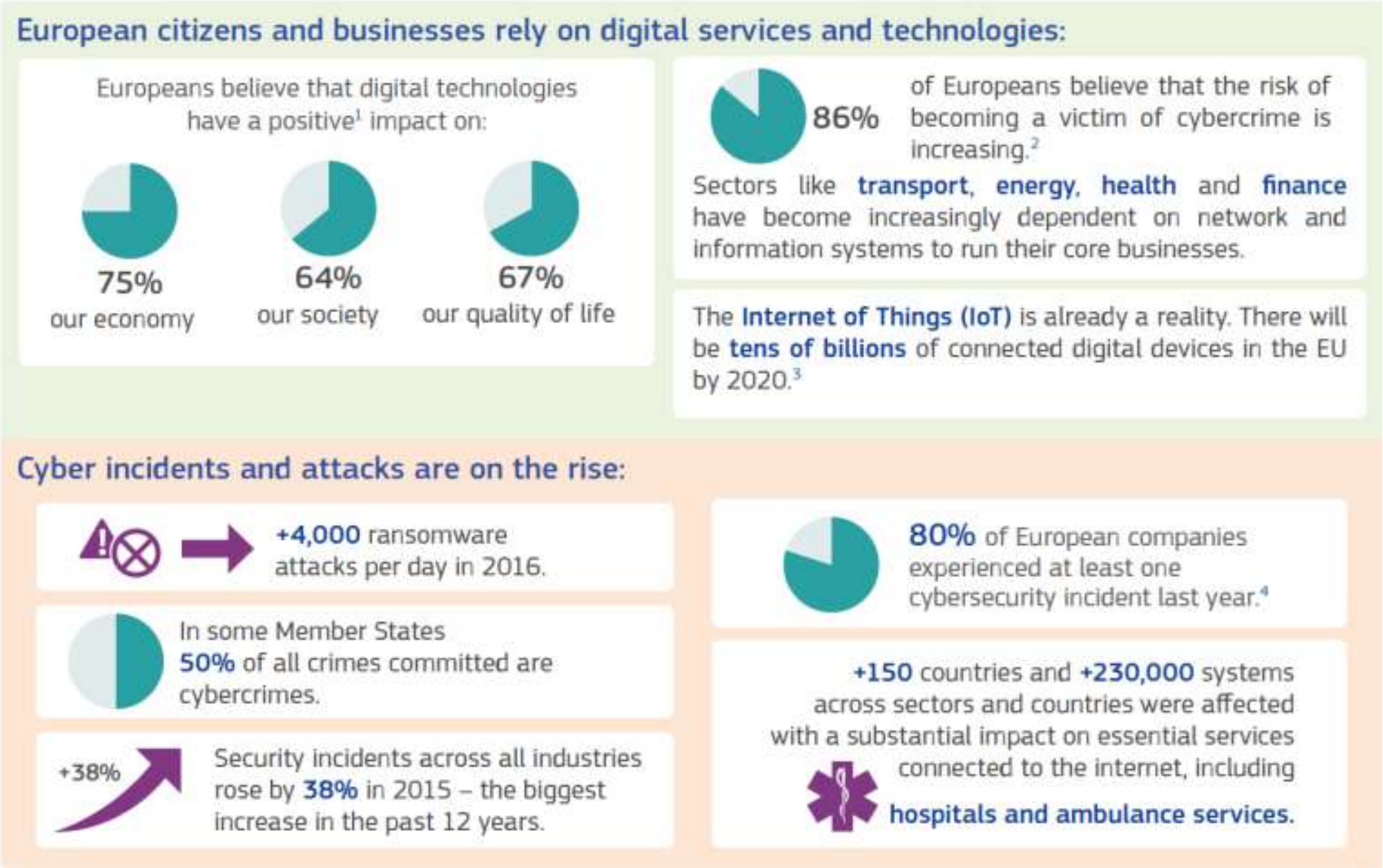
Dive in!

“A survey carried out in 21 countries, showed that although 76% of consumers acknowledge the importance of keeping their account information secure, many still **share their passwords** and **have other risky behaviors with their data** – a further 35% allow some devices to go **unprotected** and **vulnerable** to all forms of **viruses and malware**”. *(source)*

“**Fileless attacks** are on the raise! Rather than attempting to download large executables, now fileless attacks exploit software already installed on the victim's computer, executing, for instance, in a browser plug-in. In 2017, a **77%** of compromised attacks **were fileless.**” *(source)*

“According to report, **92% of malware** is still delivered by **email**, being **phishing attacks** one of the most common methods which are also becoming **increasingly targeted**.” *(source)*

Dive in!



European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive[1] impact on:

75%	64%	67%
our economy	our society	our quality of life

86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing.[2]

Sectors like **transport**, **energy**, **health** and **finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.[3]

Cyber incidents and attacks are on the rise:

+4,000 ransomware attacks per day in 2016.

In some Member States **50%** of all crimes committed are cybercrimes.

+38% Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

80% of European companies experienced at least one cybersecurity incident last year.[4]

+150 countries and **+230,000** systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including **hospitals and ambulance services.**

Sources: Cybersecurity "State of the Union 2017", European Commission. (1) Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017. ; (2) Eurobarometer on Cybersecurity (EBS 464); (3) Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014; (4) PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.

Dive in!

"Usually, users of Social Networks trust their circles of online friends, which results in **more than 600.000 Facebook accounts being compromised every single day**! According to some surveys, 1/10 social media users reported having been a victim of a cyber attack –and figures are on the rise!" *(source)*

"169 million Europeans between 16 and 74 years – a surprising **44%** of the total– **do not have basic digital skills**." *(source)*

"In 2016, at a global level, **cybercrime** was the **2nd most reported crime.**" *(source)*

"Microsoft estimated that, globally, in 2016 the total potential **cost of cybercrime** was around **$500 billion**!" *(source)*

Thank you for your attention!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

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

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Wrap-up!

Management of personal accounts and images

Project number: 2017-1-PL01-KA2014-038433

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

Wrap-up!

✓ In the final phase the teacher should:

- *Summarise the main points discussed.*
- *Refer to further learning resources.*
- *Encourage students to share their impressions, feedback and express their doubts about any issues that are still not clear.*

Wrap-up!

Self-reflection activities

✓ Ask the students if they would change their behaviors online after this session.

Why? Why not?

✓ Encourage your students to share their ideas.

Wrap-up!

Quiz

✓ Make a quiz for your students.

✓ Think about the sort of questions you can ask your students to check their understanding of the main concepts.

✓ You can use an online tool: www.kahoot.com.

- *Divide the students in groups.*
- *Questions need to be displayed on a shared screen.*

Wrap-up!

Post-assessment test

- ✓ Give your students an assessment test with exercises such as:
  - *Vocabulary*
  - *Yes/No questions,*
  - *Multiple choice questions*
- ✓ Correct the test as a group or by peer-reviewing it.
- ✓ Check if all concepts and terms discussed have been understood.

Wrap-up!

Group wrap-up activity

- ✓ Encourage your learners to think about essential things to take into account when managing your online account.
- ✓ Create the **top 5 rules** to manage your online personal accounts safely.

Thank you for your attention!

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

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

Dive in!

Online habits Quiz

How much do you know about online habits and online behaviour?

Let’s check it!

Dive in!

1

What is your digital footprint?

a) A scanned image of your foot

b) A photograph of your shoe

c) All the information online about a person that is stored online

d) Having a blog, facebook or twitter page

Source

Dive in!

1

What is your digital footprint?

a) A scanned image of your foot

b) A photograph of your shoe

c) All the information online about a person that is stored online

d) Having a blog, facebook or twitter page

Source

Dive in!

2

Which of the following would indicate that a website is secure and safe to use?

a) https

b) A locked padlock symbol before the urls address

c) A green background in the address bar

d) A .com or .org suffix to the web address

Source

Dive in!

2

Which of the following would indicate that a website is secure and safe to use?

a) https

b) A locked padlock symbol before the urls address

c) A green background in the address bar

d) A .com or .org suffix to the web address

Source

Dive in!

3

You have received a friend request from someone who works for the company where you have an interview next week – what should you do?

a) Accept the friend request, they will need to accept you just the way you are

b) Refuse the request because if they see what sort of content is on your profile they won't want you working there

c) Go through your profile deleting all of the content which could be deemed offensive by other people

d) Configure your privacy settings so that your new friend is only able to see the content that you want him/her to be able to

Source

Dive in!

3

You have received a friend request from someone who works for the company where you have an interview next week – what should you do?

a) Accept the friend request, they will need to accept you just the way you are

b) Refuse the request because if they see what sort of content is on your profile they won't want you working there

c) Go through your profile deleting all of the content which could be deemed offensive by other people

d) Configure your privacy settings so that your new friend is only able to see the content that you want him/her to be able to

Source

Dive in!

4

Everything that is posted online is saved for how long?

a) Forever

b) Until I remove it

c) 48 hours

d) 1 year

Source

Dive in!

4

Everything that is posted online is saved for how long?

a) Forever

b) Until I remove it

c) 48 hours

d) 1 year

Source

Dive in!

5

What is a good way to maintain a positive digital footprint?

a) Don't overshare

b) Use privacy settings

c) Only post things that you would want everyone to see

d) All of the above

Source

Dive in!

5

What is a good way to maintain a positive digital footprint?

a) Don't overshare

b) Use privacy settings

c) Only post things that you would want everyone to see

d) All of the above

Source

Dive in!

6

Who can see or use data from my digital footprint?

a) Only the police have access to the possible private information a digital footprint can hold

b) Your digital footprint is potentially visible to anyone

c) It is visible to professional but they need special permission to go through the data

d) Data from your digital footprint can not be used for commercial purposes by others

Source

Dive in!

6

Who can see or use data from my digital footprint?

a) Only the police have access to the possible private information a digital footprint can hold

b) Your digital footprint is potentially visible to anyone

c) It is visible to professional but they need special permission to go through the data

d) Data from your digital footprint can not be used for commercial purposes by others

Source

Dive in!

7

What is "personal data"?

a) Information which nobody else can access other than you personally

b) A secret that only you know about

c) Information that could identify you as who you are

d) Data concerning personnel working for a company

Source

Dive in!

7

What is "personal data"?

a) Information which nobody else can access other than you personally

b) A secret that only you know about

c) Information that could identify you as who you are

d) Data concerning personnel working for a company

Dive in!

8

Which of the following could help to protect your online reputation?

a) Only be “friends” with people you know and trust

b) Deleting all social networking profiles

c) Regularly review privacy on social networking profiles to ensure that you are in control of what is being shared

d) Only using professional social networks such as LinkedIn

Source

Dive in!

8

Which of the following could help to protect your online reputation?

a) Only be “friends” with people you know and trust

b) Deleting all social networking profiles

c) Regularly review privacy on social networking profiles to ensure that you are in control of what is being shared

d) Only using professional social networks such as LinkedIn

Source

Thank you for your attention!

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

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