HINTS FOR TRAINERS/TEACHERS

STEP 1 - ORIENTATE

Hints for the trainers/teachers: This activity can be carried out both in students and teachers. Instructions for trainers in this part will consider both scenarios. Thus, in this part trainees can be equally referred to as participant teachers or students and the trainer may refer to as the teacher trainer or the teacher itself when the activity is conducted in a classroom.

At the very beginning, the context of 'Google spying on us' is presented. Ask trainees if they have heard these statements before, and in which contexts, and if they have evidence to believe in them. Afterwards, present the case of Google spying through the non-encrypted routers: https://www.wired.com/2012/05/google-wifi-fcc-investigation/https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data

You can ask trainees if they understand the content and its implications by asking them what they know about routers and encryption. Provide appropriate explanations in case needed, according to the knowledge and age of trainees (teachers or students).

Afterwards, ask trainees (teachers or students) if they are aware of what kind of information can be accessed from WiFis which are detected (as done in the previous Let's STEAM activities). You can invite trainees to perform a small brainstorm on the type of information they share online. (*optional: Discuss with trainees how they could prevent someone to have access to the information you transfer through your WiFi and briefly introduce the different encryption protocols. Try to foresee if the WiFi's detected with previous Let's STEAM activities.*)

STEP 2 - CONCEPTUALISE

Hints for the trainers/teachers: The trainer introduces to trainees that the information shared through routers can be gathered from the activity of using the Internet for different purposes.

The trainer can ask trainees different questions to trigger the discussion about potential risks of using the Internet, with:

- **What do you use the internet for? What searches do you do? What pages do you visit?**
- **Do you usually accept cookies? why? (if it is needed, briefly explain to trainees what are cookies and their uses).**
- **Do you know what type of information is shared (and can be stored about you), when surfing the internet? (examples: Location, Date // Year of birth, Mobile number, email address, Gender, Personal information...)**
- **How could you know which data about you have been stored? If trainees are teachers, you can also shift the discussion towards the kind of data that their students share on the Internet.**

Trainers are also encouraged to review the privacy policy of Internet resources that they have used in previous Let's STEAM activities, for example, Scratch. Try to direct the discussion towards if they knew which type of information was stored and the purposes of the storage of this information.

As well, if they agree or not with the purposes of the use, how it makes them feel and which actions they might consider undertaking in consequence. After some minutes, try to make a list with the trainees sorting the types of information that can be stored when using the Internet based on their potential risk (harm/ sensibility).

This activity sheet is part of the Let's STEAM project funded with support from the European Commission through the Erasmus + Strategic Partnership programme. Its content 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. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

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

STEP 3 - INVESTIGATE

Hints for the trainers/teachers: Trainees will be asked to search their full names on the Internet. See what results come up. Ask trainees: **Do you think that the results reflect who you are and/or what you do? How? Which image of you that information is projecting?** Invite trainees to search for one or two close friends (or peers who they already know). Discuss with them: **Do you think that the results reflect who they are and/or what they do? Have you contributed to providing more information about them on the Internet? How? Which information do you think your friends share about you?** Trainees can update the list of types of information and potential risks if it is needed. Encourage trainees to evaluate again the impact of sharing sensitive information that can easily put their privacy and security at risk if it is shared by mistake, thoughtlessness, or misleading prompts. Continue encouraging the discussion with new questions: **Do you think that sharing information is good? Are there any examples of positive sharing online? How about negative ones? Do you think you have given consent to share this information? Have you ever received a spam email or call without knowing how they had your data?**

The aim is that trainees become more aware of the potential risks of sharing information, especially sensible information. You can also introduce broader challenges and opportunities at a societal level concerning privacy and security in the Internet-of-Things era, the commercialization of data, the needs for top-down and bottom-up regulation and standardization, etc. will be considered. The internet knows everything and never forgets, which also there is a need to have rules for a right to oblivion. Content posted online can last forever and could be shared publicly by anyone.

Being aware of the super-exposure of private data in online environments, trainees will be invited to identify best practices to reduce the risks of sharing information and keep privacy in personal data shared online. For example: Which actions could we undertake to keep our information private? (Is it better to have a public profile on social media or a private profile? // download any app from the AppStore // navigate on the internet logged in on your Google account...). To do so, trainees will work in groups of 3 or 4 people identifying 10 different actions. As a trainer, try to foster the dialogue prompting different situations, such as:

- **You want to add your close friend to a group chat. - You take a funny picture of your neighbour's dog and want to post it online.**
- **You've just got a new boyfriend/girlfriend and want to change your relationship status.**
- **You see someone asleep on the bus and want to take a photo and share it online.**
- **You want to share your location and tag your friends.**
- **You find an old photo of you and your sibling and want to share it online.**
- **You want to wish your friend a happy birthday by posting on their social media account.**
- **You're sent a photo of yourself and a friend and you look really good in it. Your friend doesn't but you want to post it online anyway.**
- **You're on your holidays with your family and want to share a photo and tag them in it along with sharing the place you are staying.**

Trainees can search on the Internet for other examples if needed it.

Afterwards, the group of 3 or 4 trainees will merge with another small group, trying to: identify which guidelines are similar between groups and merge them; discuss the relevance of the different guidelines trying to order them from more relevant to less relevant. This procedure can be repeated at different times to reach a consensus with the whole group.

STEP 4 - CONCLUDE

Hints for the trainers/teachers: Discuss with the whole group the most important actions/best practices to reduce the exposure of private data. You can additionally ask trainees to elaborate on infographics with these guidelines to distribute to other peers from other groups.