**CLASS 15**

|  |  |  |
| --- | --- | --- |
| **TOPIC** | Media literacy and the safe use of digital media: Digital Identity | |
| **LEARNING CONTENT - DETAILED CHARACTERISTICS** | This class focusses on the way media literacy becomes essential when confronted with one of the most commonly faced problems in the use of digital media, namely the risk of having your digital identity misused or stolen. Digital identity is usually defined as the relation between you and your digital presence, which can consist of numerous accounts, credentials and entitlements you are associated with. Being media literate helps us protect our digital identity in a much better way avoiding risks and facing challenges that have been the product of the new digital age in live in.  On the basis of the examples collected by the students, we discuss the major issues of preserving our digital identity and how being media literate can help us in that. | |
| **KEY WORDS** | Safe use of media; digital identity; media literacy | |
| **SUGGESTED TOOLS** | Power-point presentation  Videos and readings that can serve as examples for discussion  Discussion | |
| **TIPS / METHODOLOGICAL REMARKS**  **(if applicable)** | The “flipped classroom” method is used. Students are assigned readings and videos to watch and then a class discussion is carried out. All steps are detailed in the description | |
| **IMPLEMENTATION OF THE CLASSES** | **STEP 1** | The students are assigned to read the power-point presentation and think of possible questions to discuss. |
| **STEP 2** | The students are assigned to find examples of misuse of digital identity and ways of combating that  See Work Card 1 and Work Card 2. |
| **STEP 3** | Discussion: the students come to class and discuss the way one’s digital identity might become misused or stolen and the key factors for preventing such things from happening. They ask questions based on their getting acquainted with the presentation of the lecturer. |
| **STEP 4** | The lecturer clarifies the different points of view and makes students critically assess the role of media literacy for safeguarding one’s digital identity. |
| **STEP 5** | Learners discuss the different examples they have found illustrating the way digital identities can be misused or stolen and the ways of preventing that. |

**ADDITIONAL MATERIAL - WORK CARD 1**

**WORK CARD 1 – MEDIA LITERACY AND DIGITAL IDENTITY**

**Task 1:** There are different ways in which your privacy might be breeched on the Internet. What do you know about thiese? Say whether these statements are TRUE or FALSE.

**Privacy settings**

On Facebook and other social media platforms, you can choose yourself with whom you share information. TRUE/FALSE

**Streaming**

Streaming is always free of charge. TRUE/FALSE

**Cookies**

Cookies are used to add advertisements on the basis of your surfing behavior on the Internet. TRUE/FALSE

**Geolocation**

Your smartphone knows where you are. TRUE/FALSE

**Sharenting**

It’s OK to post photos from your children online. TRUE/FALSE

**Searching online**

Google shows the same information to everyone if they use the same search terms. TRUE/FALSE

**User terms**

It’s not important to know the content in the user terms of social media platforms. TRUE/FALSE

**Personality rights**

If somebody agrees to being photographed, he/she also agrees to the publication of that photo. TRUE/FALSE

**Internet of Things**

Devices connected to the Internet can record my conversations and use them for advertising. TRUE/FALSE

**Phishing**

If your bank sends you an email and asks you for the code of your bank card, you give it to them. TRUE/FALSE

**ANSWERS AND COMMENTS**

**Privacy settings**

On Facebook and other social media platforms, you can choose yourself with whom you share information. TRUE

COMMENT: It’s important that you know about the most important privacy settings. Go through the different privacy settings together with your child. Privacy settings allow you to choose with whom you share information.

**Streaming**

Streaming is always free of charge. FALSE

COMMENT: When streaming online music or movies, they are not stored on your local computer. They are broadcasted from the online platform to your computer. Sometimes you have to pay for it or listen to advertisements. Only use legal streaming services (Spotify, Netflix, Deezer, Apple Music…) because of copyright.

**Cookies**

Cookies are used to add advertisements on the basis of your surfing behavior on the Internet. TRUE

COMMENT: To make your web surfing experience more pleasant, you have to accept cookies on most websites. A cookie is a file that is stored on your computer, tablet or smartphone during your visit to a website. This way, when you visit the website again later, it better matches your preferences. For example, cookies are used for specific advertising, or to store your language choice or your online purchases in your shopping cart.

You may watch this video about how online advertisements work: <https://youtu.be/qgmeOJ-_hT4> *Movie produced by AdLit, an interdisciplinary research project about advertising literacy by 20 researchers from 4 Flemish Universities and diverse stakeholders.*

**Geolocation**

Your smartphone knows where you are. TRUE

COMMENT: Location information is used to check where you are, from where you are emailing, from where you are posting a photo or checking in, which route you take…More and more apps use geolocation. Via GPS signals, they know where you are. Only activate geolocation in apps that really need it.

**Sharenting**

It’s OK to post photos from your children online. FALSE

COMMENT: Set a good example and respect your child’s privacy. Don’t share just anything. Is your child old enough to have a conversation with? Then ask permission to spread the images. Sharenting is a contraction of sharing and parenting. It refers to parents who share all details of their children’s lives on the Internet.

**Searching online**

Google shows the same information to everyone if they use the same search terms. FALSE

COMMENT: Google has been personalizing its search results for years.

When you search online, the order of the search results is adjusted on the basis of your collected data (e.g. search history, location…). Watch out for sponsored search results (label ‘adv’). Advertisers pay every time someone clicks the sponsored link.

**User terms**

It’s not important to know the content in the user terms of social media platforms. FALSE

COMMENTS: It is important to properly read the user terms. In the user terms, you can find the conditions to use the service. To get access to the service, you have to accept those conditions. By accepting, you conclude a legal agreement with the company of that service.

**Personality rights**

If somebody agrees to being photographed, he/she also agrees to the publication of that photo. FALSE

COMMENT: Personality rights (right of publicity) give photographed people the right to object to the publication of their portrait. Teach your child to always ask other people if they agree to the publication of their photo. According to the law, in the case of minors, permission of their parents or guardian is necessary. When the child is a bit older, parents must still give their permission together with the minor. But if you agree to be photographed, that still doesn’t give anyone the right to publish the photo.

**Internet of Things**

Devices connected to the Internet can record my conversations and use them for advertising. TRUE

COMMENT: More and more devices and toys are connected to the Internet. For example, smart speakers, televisions, thermostats and talking dolls which communicate with you and adjust themselves to your preferences. This is called the Internet of Things. Those smart devices collect information (sound fragments, images…) about you and. Be aware that this information is also used by the manufacturer of these devices!

**Phishing**

If your bank sends you an email and asks you for the code of your bank card, you give it to them. FALSE

COMMENT: Companies do not ask for sensitive information via email. You should not give up bank information or other personal information just like that (code of your bank card, password, username…). In the case of phishing, a crook misuses your personal information. Check if the sender of the email really is who he/she pretends to be.

**ADDITIONAL MATERIAL - WORK CARD 2**

**WORK CARD 2 – MEDIA LITERACY AND DIGITAL IDENTITY**

**Task 1.** On the basis of your experience, order the risks having your digital identity misused or stolen starting from the most likely to happen. Illustrate that with examples you have come across.

1. **Tax identity theft**
2. **Social media impersonation**
3. **Financial identity theft**
4. **Child identity theft**
5. **Synthetic identity theft**
6. **Medical identity theft**
7. **Identity cloning**

 SUGGESTED ANSWER:

1. **Child identity theft** where attackers use a minor's identity for illegal personal gains. Children’s social security numbers provide clean records thieves use to secure employment, establish lines of credit, get driver's licenses, or even buy property. This type of fraud has long-term damaging effects and is more prevalent than you realize, with 1 in 10 minors affected in a [Carnegie Mellon study](https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf) of 40,000 children.
2. **Identity cloning** where a thief impersonates you to conceal their own identity for fraudulent purposes. Examples include concealing an individual’s illegal status, hiding from creditors, even discrediting you in front of employers and business partners, along with other unlawful activities
3. **Financial identity theft** in which the malicious actor uses your financial details to apply for and obtain credit, loans, goods, and services. This is the most common type of identity fraud with both online and offline ramifications.
4. **Medical identity theft** where your medical records are used to steal your health insurance, seek medical attention posing as you, alter your medical history or benefit from medical aid schemes.
5. **Tax identity theft** in which the attacker files a tax return with false information to claim and get the refund into a bank account they control.
6. **Social media impersonation** of both individuals and brands consists of cloning your identity and using it to defraud your connections, extort you to regain access, and many of the threats included in this list.
7. **Synthetic identity theft** in which the malicious actor fabricates an identity to pass various authentication tests government or private organizations enforce. This type is especially insidious because it involves combining real and fake elements (e.g. real social security number plus fake name and birth date) and it can go undetected by both anti-fraud systems and the victim itself.