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

Unit	Social Media
Sub-unit	The risk of social media
Title	Social Media as self-expression tool *Digital: Me*
Short summary	These three awareness raising activities define different channels of social media and ask learners to reflect on their engagement online.
Learning Objectives	The student is able to: *describe important terms in the field of social media *explain the risks of social media * give at least three activities to minimize or avoid risks *reflect on digital:Me.
Method	**Who am I?** The method "Who am I?" is a creative method to describe and explain terms. Each student draws a term at random (eg twitter, YouTube etc) and tries to describe or explain the term without mentioning the term on the paper. While describing and explaining the term, the student explaining, chooses characteristics which this term consists of. The other students have to guess the term. **Mind mapping** "Mind mapping" is a graphical technique for visualizing connections between several ideas or pieces of information. It is often created around a single concept, drawn as an image in the center of a blank page, to which associated representations of ideas such as images, words and parts of words are added. Major ideas are connected directly to the central concept, and other ideas branch out from those major ideas.

Disclaimer

	Self-Reflection Self-reflection or introspection means self-observation and report of one's thoughts, desires, and feelings. It is a conscious mental process relying on thinking, reasoning, and examining one's own thoughts, feelings, and ideas. It is contrasted with extrospection, the observation of things external to one's self.
Material	See attachment 1-4
Target group	Students 15+
Duration	45 min
Introduction	1. Step: Common understanding of the terms used within the topic of social media. The classroom teaching starts with the method "Who am I?". The teacher cuts the terms provided in the attachment 1 and distributes them among the students. Each student draws a term at random and tries to describe or explain the term without mentioning the term on the paper. While describing and explaining the term, the student explaining will choose characteristics which this special term consists of. The other students have to guess the term. If the class consists of more than 8 students, the terms can be copied two or more times. In this case 2 or more students will work together (those who draw the same term) and will explain and describe the term as a group to the other students. Note: Implementing this method the teacher is able to determine the knowledge level of the students about the main social media terms.

Development	2. Step: Risks of social media Based on the input of the students in Step 1, the teacher discusses with the students the possible risks of social media. For this, the teacher uses the Mind mapping technique and interacts with the students to find out which risks students see using the mentioned social media platforms. In case not all risks have been mentioned by the students, the teacher adds to the list and summarizes the relationship between the risks and social media platforms (see attachment 2). 3. Step: Based on the input in Step 2, the teacher asks students how is it possible to minimize or avoid the mentioned risks? The answers of the students are written by the teacher to the white board respective are complemented by the teacher if any are missing (see attachment 3)
Assessment of learning outcomes	4. Step: Reflection and sum up How does my "digital:Me" look? Each student discusses his/her digital:Me based on the overview in the attachment 4. Finally, 2-3 students present his/her digital personality. The teacher asks additional questions and students add their own comments.

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

Attachment 1 Who am I?

Supportive material for the "Who am I?"

Term	Definition	Possible questions which can help students to better present the selected term.
Twitter	Twitter is an American microblogging and social networking service on which users post and interact with messages known as "tweets". Registered users can post, like, and retweet tweets, but unregistered users can only read them. Users access Twitter through its website interface, through Short Message Service (SMS) or its mobile-device application software("app").	Student could describe/characterize the selected term alongside these questions: What is typical for this term? How do people interact? What are people able to post here? Who are typical users? Why is it attractive? Why is it not so attractive for youth?
Facebook	The Facebook service can be accessed from devices with Internet connectivity, such as personal computers, tablets and smartphones. After registering, users can create a profile revealing information about themselves. They can post text, photos and multimedia which is shared with any other users that have agreed to be their "friend" or, with a different privacy setting, with any reader. Users can also use various embedded apps, join common-interest groups, buy and sell items or services on Marketplace, and receive notifications of their Facebook friends' activities and activities of Facebook pages they follow.	
Pinterest	Pinterest is an internet photo sharing and publishing service that allows users to "Pin" pictures they like and upload their own recommendations to their "pinboards". Users can visit other pinboards, 're-pin' images to their own pinboards, or 'like' photos.	

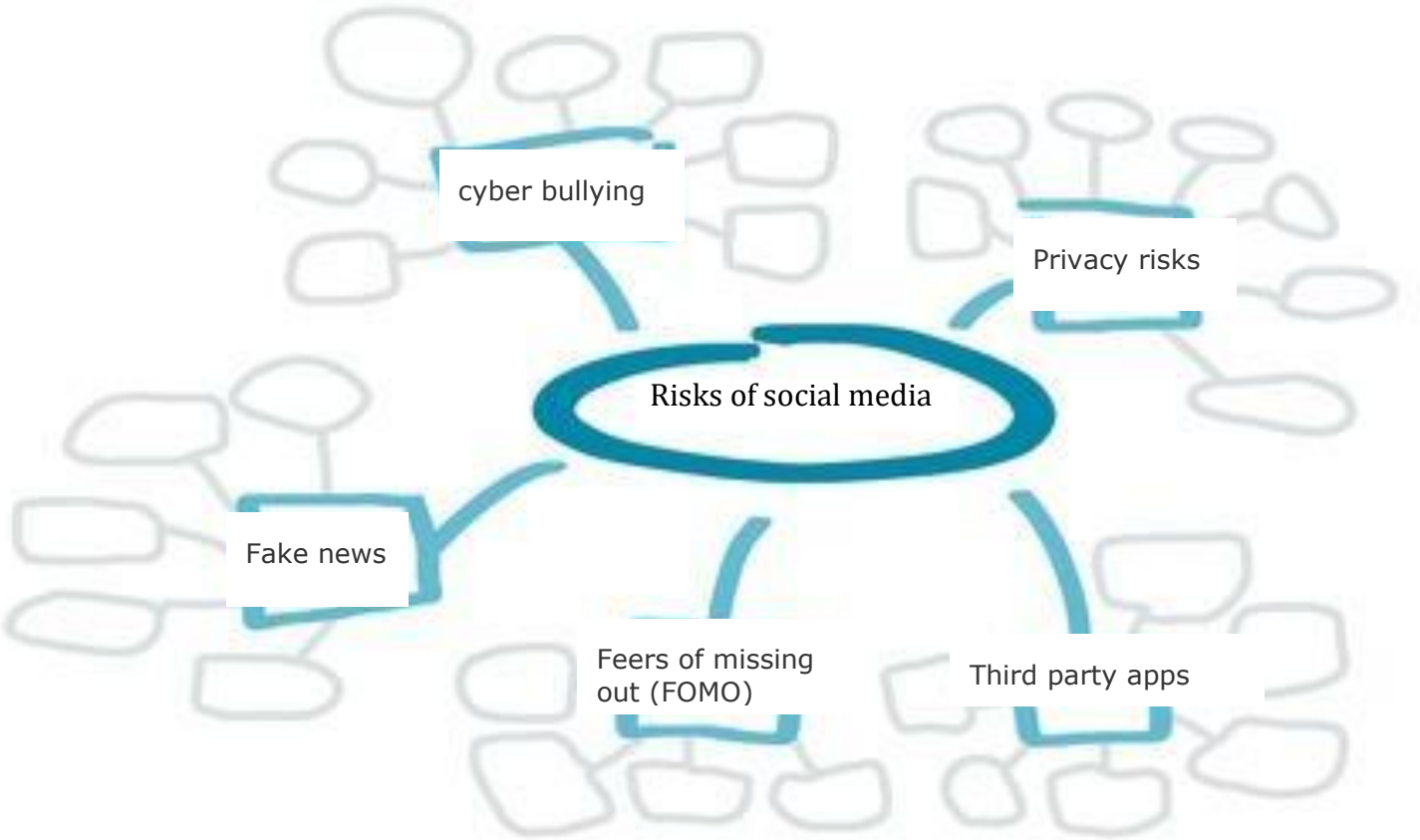
Instagram	Instagram is an American photo and video-sharing social networking service owned by Facebook. Users can upload photographs and short videos, follow other users' feeds, and geotag images with the name of a location. Users can set their account as "private", thereby requiring that they approve any new follower requests. Users can connect their Instagram account to other social networking sites, enabling them to share uploaded photos to those sites. In September 2011, a new version of the app included new and live filters, instant tilt-shift high-resolution photographs, optional borders, one-click rotation, and an updated icon. Instagram introduced hashtags to help users discover both photos and each other.	
YoutTube	YouTube is an American online video-sharing platform. YouTube allows users to upload, view, rate, share, add to playlists, report, comment on videos, and subscribe to other users. It offers a wide variety of user-generated and corporate media videos. Available content includes video, clips, TV show clips, music videos, short and documentary films, audio recordings, movie trailers, live streams and other content such as video blogging short original videos, and educational videos. Most content on YouTube is uploaded by individuals, but media corporations also offer some of their material via YouTube as part of the YouTube partnership program. Unregistered users can only watch (but not upload) videos on the site, while registered users are also permitted to upload an unlimited number of videos and add comments to videos.	
Vimeo	Vimeo is an American ad-free video platform providing free video viewing services as a competitor to YouTube. On August 1, 2019, Vimeo launched Vimeo Enterprise, a set of tools designed for large organizations that allow users to manage and share live and on-demand video across workspaces. Enterprise users are able to measure employee engagement with posted videos and view analytics	

Disclaimer

	to see how they interact with posted content. The new program represents the continuation of Vimeo's shift in strategy toward directly serving video creators and consumers, including large businesses, and away from streaming.	
SnapChat	Snapchat is a multimedia messaging app used globally. One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients. The app has evolved from originally focusing on person-to-person photo sharing to presently featuring users' "Stories" of 24 hours of chronological content, along with "Discover", letting brands show ad-supported short-form content. It also allows users to keep photos in the "my eyes only" which lets them keep their photos in a password-protected space. Snapchat has become known for representing a new, mobile-first direction for social media and places significant emphasis on users interacting with virtual stickers and augmented reality objects.	
WhatsApp	WhatsApp Messenger or simply WhatsApp is an American freeware, cross-platform, messaging and Voice over IP service owned by Facebook. It allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other media. WhatsApp's client application runs on mobile devices but is also accessible from desktop computers, as long as the user's mobile device remains connected to the Internet while they use the desktop app. The service requires users to provide a standard cellular mobile number for registering with the service.	

Disclaimer

Attachment 2 Risks of social media



Disclaimer

Attachment 3 Risk avoidance

Supportive material for "Risk avoidance"

Tips for dealing with the risks of social media

Social media provides various opportunities for connecting people and fostering interaction between them with the aim to discuss, share experiences or inform.

Despite the various positive effects of social media there are also risks and challenges the users have to deal with. Therefore, students are also exposed to possible risks, which we have introduced in this chapter.

To minimize risks when being active in social media, it is recommended to:[1]

1. Use different email addresses and secure passwords

If possible, use different e-mail addresses for the accounts of the different social networks. This can at least make it difficult for the information that you reveal about yourself on the respective pages to be compiled into a comprehensive profile about you. If you use freemail accounts for this, remember to call them up occasionally so that they remain activated. When choosing a provider, make sure that the email address does not expire and can be assigned to a new user. Otherwise there is a risk that another user will take over this email address and thus gain access to the assigned social network.

In addition, use different and secure passwords for the individual services such as Facebook or Twitter. The following applies to the password: the longer the better. It should be at least eight characters long, not appear in the dictionary and consist of upper and lower case letters as well as special characters and numbers. A password manager, such as B. keepass, can make handling different passwords easier. Under no circumstances should you pass on your password to third parties.

2. Use two-factor authentication

Use two-factor authentication to access your social media accounts. That means: The first factor is a strong password (knowledge category). The second factor for additional authentication is e.g. a security token, i.e. a hardware component such as

a key, a chip card or a special USB stick, is used (category ownership). An SMS sent by the provider can also be used. This provides much better protection for your user account. For unauthorized access, third parties would have to have both factors, i.e. both the knowledge of the password and the possession of the device.

3. Be careful when installing apps, add-ons or plug-ins

Many social networks allow third-party applications to be installed, such as games. You can add useful functions to your profile or adapt it to your personal needs. But online criminals also create or hijack such applications and use them to gain access to your profile. Therefore, check providers and sources for their trustworthiness. Share this with friends, for example, before installation or find out on the Internet which apps, add-ons or plug-ins are recommended or not.

4. Be especially careful with mobile use

Social networks are often used via mobile devices such as smartphones or tablets. The operators or third-party providers provide apps for this. They often use sensitive data on the mobile device that you may not want to disclose. These include the address book, photos, videos or location information. In addition, you are usually automatically logged into the social network afterwards. If your device is lost, this can be exploited by pretending to be the finder or thief. Therefore, you should avoid storing passwords on your mobile devices if possible and log in and out directly via the social network website instead of using the app.

5. Be picky about contact requests

Identity theft is one of the risks of the digital age. If you get dubious inquiries from friends, ask outside of social networks about the trustworthiness of these messages. In principle, only add people to your friend or contact list who you know from the real world. Unknowns could have malicious intentions. "False friends" can take over a foreign identity with the help of taken over or falsified accounts and possibly misuse them for crimes or illegal online business.

Disclaimer

6. Do not click carelessly on links or buttons

Online criminals use social networks to lure users with posts or links in chats to prepared websites, which they can use to access data or infect devices with malware.

A careless click can cause malware to install on your device. The malware can, for example, switch on the camera of your device unnoticed by you, record your conversations through the microphone or query your location. Your address book, your photos or your videos can also get into someone else's hands unnoticed.

7. Protect your privacy and don't reveal too much of yourself

Every social network offers numerous settings to protect your privacy. Use this, especially if you only want your friends to see your profile and postings. You can also set search engines to ignore your profile. Familiarize yourself with the possible settings and use them to protect your privacy.

Also consider the close integration of social network operators with other Internet services. This enables a very extensive profile to be created about you. From time to time, do an online search for your name or that of family members to find out what information about you or your children can be found online. Also check the security settings of your social media accounts at regular intervals. Pay particular attention to the link to other accounts. Social network providers could change these settings on their own. Very personal information just doesn't belong on the net. Information published on the Internet quickly develops a life of its own and can only be deleted with difficulty or never again. Check critically which personal information you want to publish and limit the group of recipients accordingly. The less personal data you have published, the less you fall back on. This also applies to confidential information about your employer and your work. Information about activities and people in the workplace should - if at all - only be published after consultation with the employer.

8. Report cyberstalkers and hate comments

Disclaimer

operator of the social network people who harass or insult you or others. The operators can investigate the abuse and delete dubious profiles. Ask the police for advice on obvious or suspected crimes, inform those affected and report them if necessary.

9. Delete your account when you no longer need it

If you want to shut down an account, save your data outside the network if necessary and then delete it in the account. In addition, follow the provider's procedure for deleting the user account. In some cases this also means that you do not have to log in again within a certain period of time.

10. Read the data protection regulations and the general terms and conditions and inform yourself about your rights and obligations

Social networks are operated by profit-oriented companies, which are mostly financed by advertising. The terms and conditions provide information on how the provider handles your personal data and how it is passed on to the advertising industry. Familiarize yourself with the general terms and conditions and data protection regulations - before you create a profile.

Some social networks grant rights of use to your publications. In this way, for example, you transfer the rights to use your photos and videos to the operator of the social network. It is also quite common for granted usage rights to remain in effect even if you leave the network and delete your profile. Before publishing, consider whether you want to share the rights to your images and texts. Also make sure that you do not violate the rights of third parties by posting pictures, texts or videos.

Social networks also have rules of conduct (netiquette) that must be observed.

A regular and open dialog with your students focused on the risks of social media can provide useful information about possible risks which students are exposed to.

Attachment 4 “digital:Me”

Please copy it and distribute it among your students. Each student gets one copy and works with this picture to elaborate their own “digital:Me”.

Disclaimer

Disclaimer

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

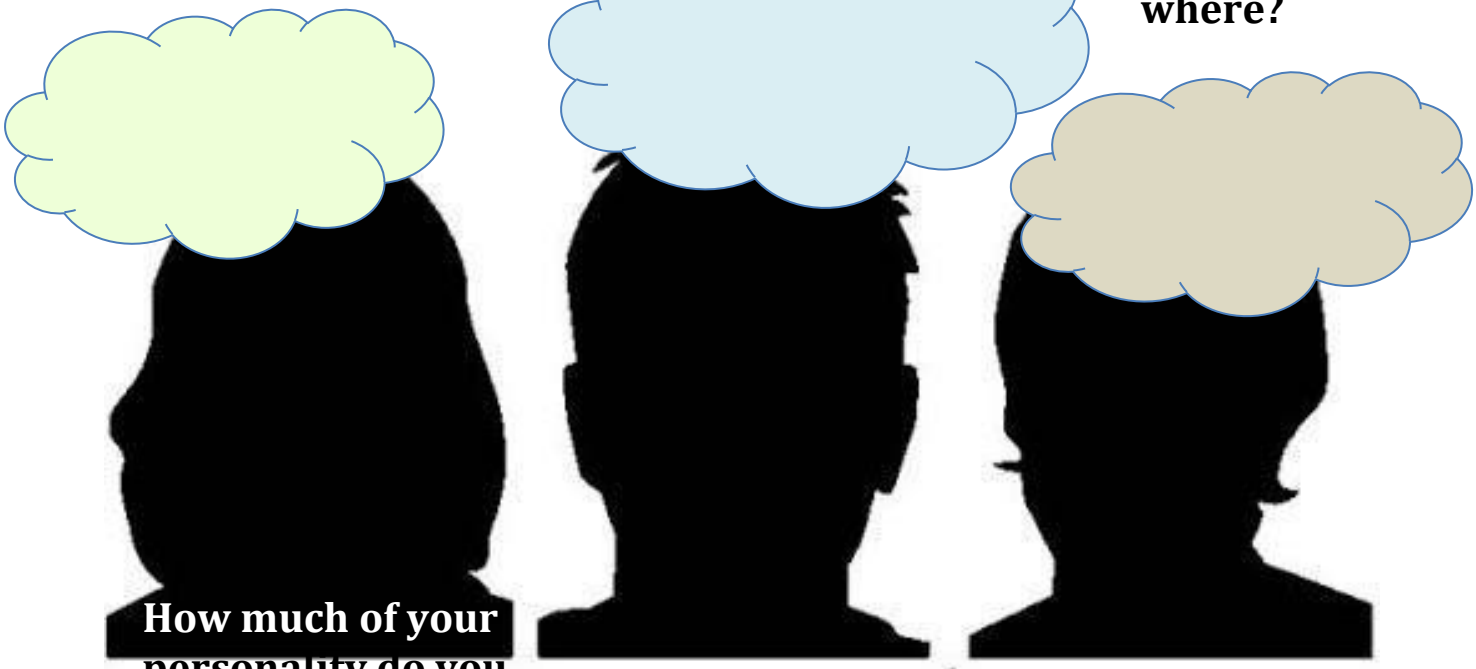
MEDIA EDUCATION WITHOUT BOARDERS

It is my digital:Me

How do you present yourself in social networks?

Wherever are you present in the Internet?

What are you posting and where?



How much of your personality do you reveal in social media?

How often do you post?

How many followers do you have?

What are your last 5 # (Hashtags) you have posted?

Do you often repost? If yes, what kind of information do you repost?

What kind of people/organisations/topics/others are you following?

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

Disclaimer