Media literacy program and material for adult educators

ANNEX 5:
SERIOUS SURFING

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

Project APRICOT:
Attentive parental education for wise being and co-being in changing times

This intellectual output has been conceived and developed by the Strategic Partnership in APRICOT project under the coordination and responsibility of *Šiuolaikinių didaktikų centras*/ *Modern Didactics Centre* (LT).

Thanks to all partners for their precious contributes:

Apricot Training Management Ltd. (UK)
ItF Institut Kassel e.V. – Frauencomputerschule (DE)
Planeta Ciencias (ES)

Editorial coordinator: Daiva Penkauskienė

Authors: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Editorial Board: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė

Month/ Year: November 2021

9.5 Annex 5: Serious surfing

1. Features of a reliable internet source[12]

1. Enter the name of the website you are looking for into a search engine, for example Google search engine. A preliminary decision can be made based on the results. User ratings from popular sites are shown in the search results above. See reviews and feedback from sources unrelated to the website.
2. If a website starts with "https", it is usually more secure and therefore more trustworthy than a page with "http". Nevertheless, an "https" connection can still be unreliable. It is best to check whether the website uses other means. Make sure that the payment page of the website in particular is an "https" page.
3. "Secure" websites display a lock to the left of the website URL. Check the security status of the website in the address bar. By clicking on the lock, you can check further details about the website, e.g. the certification and the type of encryption used.
4. Even after determining that the connection is secure, you should watch out for the following warning signs:
   a. Multiple hyphens or symbols in the domain name.
   b. Domain names that imitate real companies (e.g. “Amaz0n” or “Nike Outlet”).
   c. Unique pages that use the templates of credible pages (e.g. "visihow").
   d. Domain endings like ".biz" and ".info". These sites tend not to be reliable.
   e. Also keep in mind that ".com" and ".net" sites are the easiest domain names to obtain, even if they are not necessarily dubious. However, they do not have the same credibility as a website with the domain ending ".edu" (for educational institutes) or ".gov" (government).
5. Pay attention to the language on the website. Many incorrectly spelled (or missing) words, generally poor grammar or oddly phrased sentences indicate dubious pages. Question these pages, even if, from a technical point of view, the looks professional.
6. Ads can also indicate dubious sites. Be careful if you notice the following types of ads:
   a. Ads that cover the entire page.
   b. Ads where you must complete a survey (or do something else) before continuing.
   c. Ads where you are redirected to another page.
   d. Adult advertisements or offensive advertisements
7. Make sure that a "Contact" page is available. Most websites have a contact page where you can reach the website owner. If possible, call the number provided or write to the email address to verify the seriousness of the website. If the website does not have a contact page, this is an immediate warning sign.
8. Use a “who is who” page to find out who registered the domain of the website. Previously, all domains had to have contact information of the person or company.

[12] https://de.wikihow.com/Herausfinden-ob-eine-Webseite-seriös-ist from 26.05.2020

This information can be found at most domain registration sites or at https://whois.check-domain.net//

(English: https://who.is/). However, due to the European General Data Protection Regulation (EU-GDPR), only the status of the domain is displayed when queries are made.

9. A missing or incomplete imprint is also an indication. According to § 5 of the Telemedia Act, commercial providers are obliged to state their name and address and, in the case of legal entities, the legal form in the imprint. Any person who displays a single paid ad on his website shall be considered a commercial provider.
10. Layout[13] and navigation can give hints about a dubious provider. Reliable sites tend to have a clear and concise layout and the navigation allows you to find your way around the site quickly and largely intuitively. A confusing website could also lead to you clicking on a link for which a fee is charged. Therefore, pay attention to your gut feeling.

Do not click on links from unknown or dubious sources! Only download from secure sources!

2. Recognizing and avoiding dangers

The Internet has become an indispensable part of everyday life. However, the dangers that the Internet holds are often repressed. These dangers can have serious negative effects, especially for younger children. In particular, anonymity poses a great danger. On the Internet, a different identity can be assumed. Adults can pretend to be children or teenagers in chats and communicate with children. Minors can then become victims of (sexual) harassment. If a perpetrator persuades minors to send inappropriate photos of themselves or to meet the person they do not know, it can be very dangerous.

One consequence of this anonymity can be cyberbullying, sexting and hate speech. Unfortunately, there are no filters or apps for this. Critical thinking and the media competence of parents and children are particularly important in situations such as these.

3. Rights on the Internet

It is very easy to copy texts from the internet, download music and movies or use foreign pictures. However, this is not legally permitted.

To publish photos or videos on the Internet, you need to get permission from everyone in the photos or videos. This also applies to people who have only been filmed or photographed from behind or have been distorted with filters.

[13] https://karrierebibel.de/unseriose-webseiten-erkennen/#Unserioese-Webseiten-erkennen from 25.04.2020

If you discover pictures of you or your child that have been published illegally on the web, you should keep them as evidence and ask the website operators to delete them.

All pictures, music or movies are protected by copyright. If copies of cinema films are published on the Internet, the downloading and distribution of these films is also illegal and will be prosecuted. Unfortunately, many people do not see this as theft since nothing physical is stolen. Nevertheless, it is a theft of intellectual property. Download your music/movies from legal streaming services, even if they are usually not free. In Germany, copyright infringement is punishable by heavy fines or even imprisonment.

Check the copyright in your country.

4. Cost trap: advertising

Another danger is advertisements. These advertisements are not immediately visible in apps or on certain websites. With a wrong or unconsidered click you can land on offers or you will be asked to provide your own data. Subscriptions or purchases can also be hidden behind the click, e.g. ringtones or wallpapers. Additional functions or new levels can be activated in free games. These purchases are billed via your mobile phone provider, so-called WAP billing. Criminals also use this type of payment very often. Because for many users WAP Billing is not clear enough.

5. Internet addiction

The Internet offers a very large number of services that can be used around the clock. There is no distinction between day and night. But if you spend too much time in the digital world you may lose connection to the real world. Pay attention to usage times and set a good example for your children.

6. Privacy

Everybody has to take care of their own privacy. Photos or telephone numbers are shared too quickly on the Internet. Always remember the saying, "The Internet never forgets." Every uploaded content will probably be stored there forever. Before uploading photos or personal information, always consider whether your counterpart really needs this content or whether you might regret sharing it later. Do not enter your private address or account number anywhere without due consideration. In the worst case, the content may incur costs or negative effects later.

7. Cookies

Cookies are text information that the browser automatically saves when websites are visited. Cookies are personal information and settings of visited websites. The cookies in the browser have both positive and negative aspects. If a web page is used repeatedly, cookies are advantageous since it is not necessary to log in again and enter long

passwords on the visited page. The disadvantage is that personal data is also stored. A visit to an online shop where items have been viewed will result in matching advertisements being offered on other websites afterwards.

Since cookies have both advantages and disadvantages, the question arises "Accept or block cookies?

Although cookies are not always advantageous, they are still used in many areas. There are the so-called "Tracking Cookies" and the "Session Cookies". Tracking cookies are used to switch to personalized advertising and "session cookies" are used, for example, in online banking for the current session. As soon as the user logs out, they are deleted immediately. Many online contents are based on the use of cookies. Some pages can only be used to a limited extent or almost not at all without cookies.

In the settings of the browser, cookies can be completely blocked or only those from visited websites or all cookies can be allowed. Third party cookies can be blocked without hesitation. Allowing cookies from visited websites is a healthy balance between privacy and taking advantage of the benefits of accepting them.

8. Recommendations for parents

All these dangers deter people from using the Internet. One might prefer to forbid children to use the Internet. But this is not possible, because the Internet has become an integral part of our everyday life. It would also make no sense. Networking brings many simplifications and advantages. But can parents deal with these dangers?

One recommendation here is the combination of technical restrictions (see Chapter 7.2) and parental education. But technology also has its limits, so it is important to strengthen the media competence of children.

In order to strengthen media competence and the awareness of children, one should understand the world of children.

- What applications does the child use?
- How does he/she deal with these applications?
- What games does he/she like to play?
- Which series is he/she interested in?
- Which series/movies is he/she interested in?

These questions can best be answered if parents show their children their interest in all digital trends. The child should be able to show and explain freely and without fear what they are doing on the Internet. It would be a mistake for parents to follow their children on social networks or try to crack the next computer game level together.

Their own media behavior serves as a template for children. Parents should not spend all day in front of the TV or using their smartphones. If media use plays a very important role in parents' lives, then the child will orientate itself accordingly.

Parents should not scold if the child has fallen into a cost trap but should provide preventive support. They should talk to the child about the above-mentioned dangers on the Internet and give practical examples that are comprehensible to the child. You should encourage the child to critically examine content and not to believe everything that can be read on platforms or websites. Children learn in real life how to deal with their fellow human beings. Exactly these social principles also apply in the digital world.

Parents should be the first person to whom the child confides if he/she does not feel safe or is attacked by others. They are the most important persons of trust for the child.