**Media Literacy**
**Youth lecture**

**Format:**
**The lecture is divided into 2 parts:**

1. **Basics of Media Literacy, a short introduction into the digital world**
2. **Basics of Digital security, how to protect yourself in the cyberspace**

**Aims of the lecture:**

- to stop taking everything online at face value
- to protect ourselves from privacy and security infractions
- to learn to research independently
- quick identification of most common misinformation and media manipulation tactics online

**Part 1: Basics of Media Literacy**

This lecture introduces the students to the concepts of ‘’media literacy’’ and ‘’critical thinking’’, teaching them about the downsides of social and mass media and giving them a basis for a more conscious absorption of information.

**Terms learned:**

*Disinformation* - a term that denotes probably false information that is created, presented and disseminated in order to gain someone’s benefit or deliberately discourage the public

*Media literacy* - the ability to identify different types of media and understand the messages they're sending.

*Fake news* - false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke

*Clickbait* - content whose main purpose is to attract attention and encourage visitors to click on a link to a particular web page.

*Fact* - a thing that is known or proved to be true.

*Fact-checking tools* - Fact checking tools are sites that check the accuracy of information in a public space.

**Script:**

The lecturer should use the accompanying presentation, which gives visual examples and interactive exercises, which are important for keeping the attention of young students. This is also important for associating already seen examples of disinformation, with examples proven to be disinformation, for easier identification in the future.

The lecturer has also the option of using the accompanying video lecture.

## Part 2: Basics of digital security and safety

This lecture aims to teach the students about the simpler inner workings of the internet and give them a head start on setting up their security measures. It will also give them a basis on the principles of privacy and cyber-security, and try to widen their world view and opinions on such topics.

**Terms learned:**

*Holistic security* - Holistic security is an approach to the security and protection of human rights defenders, defined in the Holistic Security Manual as integrating “self-care, well-being, digital security and information security into traditional security management practices.

*Multi-factor authentication* - when a user must provide two or more pieces of evidence to verify their identity to gain access to an app or digital resource.

*DNS* - the Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet. The ‘’phonebook of the internet’’.

*Deep web* - the part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks.

*Dark web* - World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access.

**Script:**

The lecturer should use the accompanying visual presentation or give some examples from his personal life, as to better explain some concepts which might be too abstract depending on the average age of the students. Terms like Privacy (which connects to free-speech) and Digital security might be too complex topics, so it would be best if simplified terms and examples based on experiences are used (ex. comparing cyber security to house security, etc.)