Teaching cybersecurity & cybersafety in high school

The CONCORDIA Methodology and Guidelines in support of teachers
Work package 3: Community impact and sustainability

Teach-the-Teachers in high-school
Methodology and Guidelines

Abstract: This paper is part of the WP3 task T3.4. It describes a methodology and associated guidelines in support of the teachers when preparing to teach cyber-security and cyber-safety to high-school students.

<table>
<thead>
<tr>
<th>Contractual Date of Delivery</th>
<th>---</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Date of Delivery</td>
<td>---</td>
</tr>
<tr>
<td>Report Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Editors</td>
<td>Felicia Cutas, EIT Digital Pantelitsa Leonidou, CUT Lama Sleem, UL Ivana Butnic-Obor, CODE</td>
</tr>
<tr>
<td>Contributors</td>
<td>Nikos Salamanos, CUT Marin Vukovic, FER Borka Jerman Blazic, IJS Tatjana Welzer Druzovec, UM Kostas Lampropoulos, UP</td>
</tr>
</tbody>
</table>

1 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.
## The CONCORDIA Consortium

<table>
<thead>
<tr>
<th>UniBW/ CODE</th>
<th>University Bundeswehr Munich / Research Institute CODE (Coordinator)</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORTH</td>
<td>Foundation for Research and Technology - Hellas</td>
<td>Greece</td>
</tr>
<tr>
<td>UT</td>
<td>University of Twente</td>
<td>Netherlands</td>
</tr>
<tr>
<td>SnT</td>
<td>University of Luxembourg</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>UL</td>
<td>University of Lorraine</td>
<td>France</td>
</tr>
<tr>
<td>UM</td>
<td>University of Maribor</td>
<td>Slovenia</td>
</tr>
<tr>
<td>UZH</td>
<td>University of Zurich</td>
<td>Switzerland</td>
</tr>
<tr>
<td>JACOBSUNI</td>
<td>Jacobs University Bremen</td>
<td>Germany</td>
</tr>
<tr>
<td>UI</td>
<td>University of Insubria</td>
<td>Italy</td>
</tr>
<tr>
<td>CUT</td>
<td>Cyprus University of Technology</td>
<td>Cyprus</td>
</tr>
<tr>
<td>UP</td>
<td>University of Patras</td>
<td>Greece</td>
</tr>
<tr>
<td>TUBS</td>
<td>Technical University of Braunschweig</td>
<td>Germany</td>
</tr>
<tr>
<td>TUDA</td>
<td>Technical University of Darmstadt</td>
<td>Germany</td>
</tr>
<tr>
<td>MU</td>
<td>Masaryk University</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>BGU</td>
<td>Ben-Gurion University</td>
<td>Israel</td>
</tr>
<tr>
<td>OsloMET</td>
<td>Oslo Metropolitan University</td>
<td>Norway</td>
</tr>
<tr>
<td>Imperial</td>
<td>Imperial College London</td>
<td>UK</td>
</tr>
<tr>
<td>UMIL</td>
<td>University of Milan</td>
<td>Italy</td>
</tr>
<tr>
<td>BADW-LRZ</td>
<td>Leibniz Supercomputing Centre</td>
<td>Germany</td>
</tr>
<tr>
<td>EIT DIGITAL</td>
<td>EIT DIGITAL</td>
<td>Belgium</td>
</tr>
<tr>
<td>TELENOR ASA</td>
<td>Telenor ASA</td>
<td>Norway</td>
</tr>
<tr>
<td>AirbusCS-GE</td>
<td>Airbus Cybersecurity GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>SECUNET</td>
<td>secunet Security Networks AG</td>
<td>Germany</td>
</tr>
<tr>
<td>IFAG</td>
<td>Infineon Technologies AG</td>
<td>Germany</td>
</tr>
<tr>
<td>SIDN</td>
<td>Stichting Internet Domeinregistratie Nederland</td>
<td>Netherlands</td>
</tr>
<tr>
<td>SURF</td>
<td>SURF bv</td>
<td>Netherlands</td>
</tr>
<tr>
<td>CYBER-DETECT</td>
<td>Cyber-Detect</td>
<td>France</td>
</tr>
<tr>
<td>TID</td>
<td>Telefonica I+D SA</td>
<td>Spain</td>
</tr>
<tr>
<td>RUAG</td>
<td>RUAG AG (as replacement for RUAG Schweiz AG)</td>
<td>Switzerland</td>
</tr>
<tr>
<td>BITDEFENDER</td>
<td>Bitdefender SRL</td>
<td>Romania</td>
</tr>
<tr>
<td>ATOS</td>
<td>Atos Spain S.A.</td>
<td>Spain</td>
</tr>
<tr>
<td>SAG</td>
<td>Siemens AG</td>
<td>Germany</td>
</tr>
<tr>
<td>Flowmon</td>
<td>Flowmon Networks AS</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>TÜV TRUST IT</td>
<td>TUV TRUST IT GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>TI</td>
<td>Telecom Italia SPA</td>
<td>Italy</td>
</tr>
<tr>
<td>Efacec</td>
<td>EFACEC Electric Mobility SA (as replacement for EFACEC Energia)</td>
<td>Portugal</td>
</tr>
<tr>
<td>ARTHUR'S LEGAL</td>
<td>Arthur’s Legal B.V.</td>
<td>Netherlands</td>
</tr>
<tr>
<td>eesy-inno</td>
<td>eesy-innovation GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>DFN-CERT</td>
<td>DFN-CERT Services GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>CAIXABANK SA</td>
<td>CaixaBank SA</td>
<td>Spain</td>
</tr>
<tr>
<td>BMW Group</td>
<td>Bayerische Motoren Werke AG</td>
<td>Germany</td>
</tr>
<tr>
<td>GSDP</td>
<td>Ministry of Digital Policy, Telecommunications and Media</td>
<td>Greece</td>
</tr>
<tr>
<td>RISE</td>
<td>RISE Research Institutes of Sweden AB</td>
<td>Sweden</td>
</tr>
<tr>
<td>Ericsson</td>
<td>Ericsson AB</td>
<td>Sweden</td>
</tr>
<tr>
<td>SBA</td>
<td>SBA Research gemeinnutzige GmbH</td>
<td>Austria</td>
</tr>
<tr>
<td>IJS</td>
<td>Institut Jozef Stefan</td>
<td>Slovenia</td>
</tr>
<tr>
<td>UiO</td>
<td>University of Oslo</td>
<td>Norway</td>
</tr>
<tr>
<td>ULANC</td>
<td>University of Lancaster</td>
<td>UK</td>
</tr>
<tr>
<td>ISI</td>
<td>ATHINA-ISI</td>
<td>Greece</td>
</tr>
<tr>
<td>UNI PASSAU</td>
<td>University of Passau</td>
<td>Germany</td>
</tr>
<tr>
<td>RUB</td>
<td>Ruhr University Bochum</td>
<td>Germany</td>
</tr>
<tr>
<td>CRF</td>
<td>Centro Ricerche Fiat</td>
<td>Italy</td>
</tr>
<tr>
<td>ELTE</td>
<td>EOTVOS LORAND TUDOMANYEGYETEM</td>
<td>Hungary</td>
</tr>
<tr>
<td>Utimaco</td>
<td>Utimaco Management GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>FER</td>
<td>University of Zagreb, Faculty of Electrical Engineering and Computing</td>
<td>Croatia</td>
</tr>
<tr>
<td>ICENT</td>
<td>Innovation Centre Nikola Tesla</td>
<td>Croatia</td>
</tr>
<tr>
<td>Utilis</td>
<td>Utilis d.o.o</td>
<td>Croatia</td>
</tr>
<tr>
<td>Polito</td>
<td>Politecnico di Torino</td>
<td>Italy</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction ........................................................................................................................................ 6

2. The Methodology - our proposed approach ...................................................................................... 10

3. Guidelines .......................................................................................................................................... 16
   Modules fiches A. Cybersafety ............................................................................................................ 17
   A0. Why discussing cybersafety ........................................................................................................ 18
   A1. Personal / Sensitive Data and Privacy .......................................................................................... 19
   A2. Cyberbullying and Sexual Harassment ......................................................................................... 21
   A3. Inappropriate Content .................................................................................................................. 22
   A4. Hate speech ................................................................................................................................ 23
   A5. Fake profiles, Fraud and Phishing ............................................................................................... 24
   A6. The importance of Strong Passwords .......................................................................................... 26
   A7. Addiction ....................................................................................................................................... 29
   A8. Keep my online account safe......................................................................................................... 30
   A9. Stay safe in Online Social Networks ........................................................................................... 31
   A10. Online Games ............................................................................................................................... 32
   A11. Fake News ..................................................................................................................................... 33
   A12. Transparency of Recommendation Algorithms ............................................................................ 35
   Modules fiches B. Cybersecurity ......................................................................................................... 37
   B0. Why study cybersecurity ............................................................................................................... 38
   B1. OSI Model ..................................................................................................................................... 39
   B2. Operating systems (OS), Computer Hardware and how does a computer work ..................... 41
   B3. Protection of Data: concerns .......................................................................................................... 44
   B4. Network Standards & Protocols .................................................................................................... 45
   B5. Essentials in Cyber security .......................................................................................................... 48
   B6. Attacks, threats, vulnerabilities ...................................................................................................... 51
   B7. Defense against Cyber threats (Cyber Hygiene) .......................................................................... 54
   B8. Cryptography ................................................................................................................................. 55
   B9. Individual Incidents Responses .................................................................................................... 58
   B10. Capture the Flag ......................................................................................................................... 59
   B11. Penetration testing ....................................................................................................................... 62
   B12. Roles in Cyber security and Top Certifications .......................................................................... 63

Annex – Education related initiatives in Europe ..................................................................................... 64
1. Introduction

Cybersecurity does not only challenge researchers and industry but is a major concern for our society at large. It is therefore of highest importance that new generations are made aware and kept updated about the major cyber threats, new technologies as well as appropriate individual and collective behaviors to reduce risks. Teachers have an important role in building and consolidating the cybersecurity culture at all levels. By helping children and young adults grasp the basics of cyber, discover the domain, or develop more advanced skills in the area, they contribute in the medium term to reducing the skills gap. This effort is specifically important at the high-school level, the period when the young adults reflect on their future careers.

As mentioned in the 2022 EURYDICE report\(^2\) on “Informatics Education at school in Europe”, informatics is still a relatively new discipline in school education; and cybersecurity is even newer. The current generations of teachers covering informatics topics at school, in their vast majority, have never studied cybersecurity as a separate discipline. Efforts are put in place at national level to deploy specialised programmes to prepare teachers on the informatics topics as the availability of appropriate continuous teacher training. Therefore, various teaching materials are the necessary conditions for good-quality teaching and learning. Many education systems have also developed a wide range of teaching materials for informatics teachers. Yet there is still a few cyber-specific documentation to support current teachers preparing the classes.

Within the CONCORDIA project we grasp this challenge under what we call the “Teach-the-Teachers” activity, hereby proposing high-school teachers teaching methodology and materials for them to adopt with their pupils. This Methodology takes into consideration results that were collected via an online survey and in-person interviews with teachers from different European countries, scouting the needs in terms of teaching cybersecurity and cybersafety subjects at high-school level. Based on our findings and considering the growing importance of the topics, we strongly encourage the management of the high-schools to consider organizing specific classes as part of ICT subjects or specific extracurricular activities. In view of supporting this endeavor, we propose an approach and a set of materials, subject of this document. Importantly, the present methodology and associated guidelines address teachers having a medium level of knowledge in ICT.

The Methodology proposes to best match the different cyber related knowledge level of the high-school students with their interest on specific topics. Thus, through the availability of different options, any teacher may participate in this effort and progressively learn and teach more advanced topics and courses. Among our priorities is the use of existing -and already validated- resources, systems and tools. Such tools will address various objectives like e.g., helping teachers and students evaluate their cybersecurity skills, offering online courses from multiple eLearning platforms, providing access to online testing infrastructures and facilities for hands-on tests and experiments etc.

This work will focus on two major aspects, cybersafety and cybersecurity. With cybersafety we are targeting a more supportive and theoretical approach to the current threats that high-school students are facing today, also teaching ways to handle difficult situations as well as informing the proper people and authorities to get help in case of an incident. With the cybersecurity courses we are looking to advance

the technical skills of students and at the same time incentivize them to learn more about jobs and career paths in cybersecurity that they might want to follow in the future.

---

**Outcome of the Survey and Interviews**

In order to identify the current needs in terms of content and delivery methodologies fit for the high-school level, we have decided to apply a funnel approach by starting with collecting structured data via an EU-wide survey, followed by interviews with a small group of survey participants. The identified needs have been further validated in a live event before moving to the next step in the process, the design of the methodology for teaching cybersecurity in high-school and some materials.

The objectives of this Survey were three-fold:

**RELEVANCE**: To select the most needed topics to be covered in the materials.

**EFFECTIVENESS**: To define the most appropriate format for the materials to be developed.

**NOVELTY**: To identify areas not (enough) covered by existing programs.

In order to collect relevant input, we looked into collecting input from the following audience:

- European high-school Teachers,
- European high-school Students
- European Parents of high-school students
- European school Management

The analysis performed on the survey and interviews answers was captured in a specific report[^3] and could be concluded as follows:

1. **the most in need topics** to be covered in the materials are: “Being safe in online social platforms”, “Recognizing fake accounts”, “Ensuring their privacy in online activities”, “Creating strong passwords”, “Using email applications in a secure way”, based on the topics-to-be-discussed ranking we obtained from parents, teachers, and students through the survey. Moreover, the lower confidence level mentioned by the students in “Secure online shopping”, “Sharing files online”, and “Securely Downloading” adds those topics to the list of the most in-need topics to be covered.

2. **the most appropriate format** for the materials to be developed would be the videos, interactive presentations, and games/platforms. The interviewed teachers and the parents strongly suggest having interactive instruments where real facts are presented to the students followed by discussions between the students and the teachers on the topics covered by exchanging prior related experiences. Paper material is mentioned marginally, for the use of disseminating contact information of special organizations offering support for students experiencing an online risk. The additional research performed on the latest studies in the education field have shown that cybersecurity education requires innovative approaches like the use of cyber ranges and serious games that have proven to be more effective in developing cyber-related skills.

Indeed, these approaches enable interactivity in the training process and lead the learner to take decisions in a safe but real life-like environment thus helping accelerate the learning process.

(3) **the areas not (enough) covered** by existing programs are how to detect and handle the online risks when they occur. The limited time spent in relevant courses and seminars and the lack of the students' experiences with real threats makes it difficult to adequately cover detecting and handling the online risks and make the students feel confident less in such tasks. Increasing the time and the frequency of such courses and presenting the threats in a more practical than theoretical way can help in improving the effectiveness of existing programs. Additionally, during the interviews, the conclusion has been drawn that cybersafety topics (e.g. cyberbullying, sexual grooming, privacy, etc.) are more discussed than cybersecurity topics (e.g. cyber-attacks, spams, viruses). This can be an indicator that the existing programs focus more on spreading awareness on cybersafety topics and less on cybersecurity topics.

These findings were considered when proposing the list of modules and the content of the associated fiches in chapter 3. Guidelines.

---

**Mapping similar initiatives**

For almost a decade in most of the EU member states general awareness of cybersafety and cybersecurity topics has grown in its importance. Therefore, numerous organizations, mostly NGOs, with the generous support of their national governments have started specialized campaigns and initiatives toward strengthening the literacy on cybersafety and cybersecurity among children, youth and young adults. With time, further initiatives, running under the support of the European Union, have managed to attract additional partners and participating organizations, not only from the public or NGO sector but also from the IT industry.

Based on information available on their web pages, most of the initiatives approach the topics related to the “safe use of the internet in everyday life”. Available information is usually very well structured and presented in a way understandable by the targeted audience, e.g. younger children or youth. They describe the situations that children and youth might face when using their connected electronic devices, explain the threats and consequences, in a way adapted to a certain age, and give guidelines (sometimes providing hotlines in case of critical situations, like cyber harassment) on how to proceed in specific circumstances.

Some initiatives even go a step further addressing not only children and youth but also parents, legal guardians and teachers. They offer different types of information and advices on how to behave, explain the danger of certain activities on the internet as well as how to give support to children and youth in such cases. Most of the provided material is available in written electronic form (brochures, posters or presentations, typically in pdf). Nevertheless, some of them turn to the use of interactive content, trying to make it attractive and interesting for the target audience.

Specially customized guidance and material related to cybersafety and cybersecurity which can be used by the teachers during the classes are offered in a limited way across EU member states. When existing, these contents are often developed with the help or support of responsible national public bodies and aligned with national strategies on digitalization and the development of a digital society.
In the Annex of this document, teachers, students, and their parents can find a non-exhaustive set of initiatives currently existing across several EU member states. This collection of initiatives is structured in a way to help the readers grasp quickly the topic addressed, the language of the document, and the main target audience, while also providing a direct link to the resources. It is meant to complement the content presented in Chapter 3. Guidelines.
2. The Methodology - our proposed approach

The CONCORDIA Methodology we propose is based on the following main assumptions:
- The high-school teacher has a background in the ICT area
- The school management recognizes the importance of teaching cybersecurity and cybersafety-related subjects at the high-school level thus allowing covering these topics during IT classes and/or offering this option as part of the non-compulsory curricula
- The school class (the lab) is equipped with computers and/or the students are allowed to use their own devices during the classes, for educational purposes

When it comes to design and delivery, the CONCORDIA Methodology extrapolates The Dynamic Teaching Model\(^4\) and is looking to involve the students from the design stage of the course. We consider that students learn tech topics such as cyber easier if they are interested and find their learning relevant. It is said that when students are emotionally invested in their learning, cognition peaks.

Structure-wise, the content of the fiches part of the Methodology is inspired from the existing European initiatives such as the DigComp\(^5\), a detailed framework for the development of digital competence of all citizens. The DigComp document includes also a self-assessment grid consisting of five areas of digital competence and three proficiency levels, going from A (foundation level), over B (intermediate level) to C (advanced level). This grid is later backed by an interactive user-friendly DigComp tool\(^6\) to be used at an individual level. The DigComp framework was also referred in a Eurydice report on Digital education at school in Europe\(^7\) published in 2019. The report shows that teaching digital competencies also means preparing young people to use digital technologies effectively and safely. Some of the risks posed to students’ personal well-being, such as through cyberbullying and internet addiction, as well as the loss of privacy, signaled the need to make safety an essential part of digital education. Famous cases related to the misuse of personal data, web-tracking, and the spreading of fake news have put the spotlight on the crucial role that education can play in preparing young people to be digitally mature.

Based on the DigComp framework, schools have started developing their own guidelines on how to teach digital competences by adapting them to their needs. For instance, the Digital Competence Framework (DCF) for the European Schools\(^8\) follows the five competence areas and the twenty-one sub-competences of DigComp. It is structured using cycle progression statements for each of the sub-competences, to address all learners from Nursery to Secondary school and proposes six proficiencies levels. Finally, the DCF also proposes the teachers some task ideas to be used during the class.

\(^4\) https://mgiep.unesco.org/article/the-dynamic-teaching-model
\(^6\) https://digcomp.digital-competence.eu/
\(^7\) https://op.europa.eu/o/opportal-service/download-handler?identifier=d7834ad0-ddac-11e9-9c4e-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=
\(^8\) https://www.eursc.eu/BasicTexts/2020-09-D-51-en-2.pdf
§. The model

The CONCORDIA Methodology process is structured in three main stages as depicted below. When describing the stages and the associated steps we will refer to several elements detailed in Chapter 3. Guidelines such as the topic fiches and their components.

Assess
- Step 1. Kickstart the discussion on the cybersafety and cybersecurity topics
- Step 2. Test the group knowledge level
- Step 3. Build the class portfolio

Plan
- Organize the curricula for the semester/year

Deliver
- Step 1. Get yourself ready (prepare the specific topic)
- Step 2. Deliver specific topic
- Step 3. Test the knowledge acquired by the students
§. Model phase ASSES

Step 1. - Introduce the general topic

Before addressing any specific subject, we propose to first discuss with the group of students the importance of addressing cybersafety/cybersecurity topics (by using fiches A0 / B0).

**Cybersafety** means protecting users from harmful online content. It concerns the emotional and psychological impact of what you see, read and hear online. Being cyber-safe means meeting appropriate standards of behavior in the content we put on the internet, knowing how to avoid harmful interactions online, and being equipped to seek help if things aren’t right. *Examples of cybersafety incidents:* e.g., cyberbullying, sexual harassment, exposure to hate speech/inappropriate content (violent, sexual, etc.), and leakage of sensitive information.

**Cybersecurity** means protecting data and information. It refers to the physical operation of the networks and computers over which the internet is delivered. *Examples of cybersecurity incidents:* Viruses, DOS- denial of service attacks (company’s network fails because it receives a huge amount of requests), hacked accounts/profiles, Man-in-the-middle attacks (an attacker can have access to your communication channel and can see/modify information you send), social engineering (where a person tries to know your credentials by asking simple questions).

During this step, an introduction to "what a career in cybersecurity means" could be done (see fiche B12). Apart from presenting the different role profiles in the industry ([ENISA - European Cybersecurity Skills Framework](https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf)), we suggest inviting industry representatives/role models to share experiences/inspire the students to consider building a career in cyber such as:

- School Parents working in the cyber domain, willing to share their career path and job satisfaction
- police officer that can bring real incidents/reports/statistics (cybercrime department)
- representatives of organizations specialized in cybersafety and cybersecurity topics, e.g., [EU Safer Internet Centers](https://digital-strategy.ec.europa.eu/en/policies/safer-internet-centres)

A special attention should be paid on presenting the cybersecurity career option as a gender inclusive one. Different resources and databases are available online to support this endeavor, such as the [CONCORDIA role models](https://www.concordia-h2020.eu/meet-the-women-in-concordia/), [Women4Cyber Chapters](https://women4cyber.eu/w4c-chapters), and the [Women Know Cyber: The Documentary](https://www.youtube.com/watch?v=Kpc31WJ6l2M&t=439s).

Step 2. - Test the knowledge on specific topics

The second step of the Asses phase is about checking the group knowledge-level per topic. In view of doing that, we propose applying two tests, one on cybersafety and one on cybersecurity subjects. Each
test contains a series of multiple-choice questions, 4-5 questions per topic proposed in this methodology, with different levels of difficulty.

The tests are developed under an open-source platform. They are designed in such a way allowing the teachers to receive statistics per question. The tests are meant to be applied in an anonymous way since their purpose is to offer information about the level of knowledge of the group, and not of the individuals. The tests are not time-bound. Yet, we suggest allocating about 40 minutes per test, thus running one test within one class session.

We recommend applying the same test at the end of the class year. Comparing the results of these two tests would help assess the extent to which the classes increase the group knowledge on the different topics, while also providing an indication of the future topics (and associated levels) to be addressed.

| IMPORTANT: Teachers interested in getting access to the tests are invited to send an email to contact@concordia.eu by mentioning their name, the name of the school they are representing, and the location of the school (city and country). |

**Step 3.- Build topics portfolio**

In our view, it would be beneficial for the teachers to discuss with the class students the statistical results of the cybersecurity and cybersafety-related tests. This would help with building together the list of priority topics to be covered during the school year. Since in most of the schools around Europe the cybersecurity and cybersafety subjects are not officially part of a curricula, this offers flexibility in choosing the content to be covered in the class. Involving the students in building the class topics portfolio shall develop a sense of ownership which in turn shall be reflected in an increased level of participation of the students when running the lessons.

---

§. Model phase PLAN

Within the framework of this methodology, we pledge for a Needs-based & Knowledge-level-based approach with lessons clustered in a modular portfolio.

**Needs-based**

The Guidelines chapter lists 12 topics on Cybersafety area and another 12 topics on Cybersecurity area. Yet, some of them might have already been addressed within the class and are not of specific interest. The teacher is advised to work with the students on the topics of the group interest as described in the Assess - Step 3 while also considering the prerequisites mentioned in the specific fiches.

**Knowledge-based**

Some of the fiches included in the guidelines cover one topic on different levels (Foundation / Intermediate / Advanced). As such, if the group test results show a good level of understanding of a specific topic, we
suggest spending less time on the Foundation related content and building the lesson mainly on the Intermediate / Advanced related content.

**Modular**
The course portfolio shall bring together a set of cyber-related topics at different levels of difficulty as identified by the teacher following the assessment test and in agreement with the students. When deciding on the order of covering the topics, we propose alternating cybersafety-related topics with cybersecurity-related topics. By periodically shifting from emotional/psychological topics addressed in the cybersafety classes to more technical ones covered in the cybersecurity classes would positively change the dynamic of the cyber classes, thus preserving the interest of all the students, irrespective of their interest in specific topics.

---

**§. Model phase DELIVER**

Once the course portfolio is ready, we move to the Deliver stage. Within this stage, we propose 3 steps that should be repeated for each of the topics of the portfolio.

**Step 1. Get yourself ready (prepare the specific topic)**

When preparing a class, we suggest covering all the activities related to one topic to be deployed in one class interval. This also includes the small test presented in Step 3. below.

**The storyline**
Part of this methodology we included in Chapter 3. Guidelines, a series of fiches per individual cybersecurity and cybersafety topics. These fiches are meant to support the teachers in their effort to prepare the class and build the storyline. They contain information about the prerequisites to be fulfilled before covering a specific topic at a specific level, describe the main learning objectives (LO) to be achieved at the end of the lesson, list the main messages (M) important to be passed to the students in relation to the specific topic addressed.

In addition to the specific content listed in the fiche, for more general content, we recommend checking Annex regarding Existing initiatives in Europe.

**Using examples**
In order to help the students in understanding the different concepts we recommend teachers to use practical examples such as the ones listed in the fiches (E). The examples could be complemented with local news on the topic, inspirational talks of different experts, etc.

Besides, we suggest teachers consider incorporating the bring-your-own-example (BYOE) tactic. This approach is an invitation for the students to check in advance the lesson to be covered in the next class and look for (personal) cases they would like to share and discuss with the teacher and their peers.
Step 2. Deliver specific topic

When delivering a class, a high degree of interaction with the students is advisable. This could start already at the beginning of the hour by inviting 1-2 students to briefly introduce the examples they have prepared (BYOE).
For optimal impact, the class should be delivered in a classroom equipped with computers and an internet connection. Alternatively, the students should be allowed to use, for educational purposes, their own smartphones/tablets. This would allow searching for/checking/testing the different resources planned to be exemplified/used during the class.
A class should end with the small test described in Step 3. below and by announcing the topic for the next session.

Step 3. Test the knowledge acquired by the students

For most of the topics part of this methodology, the content covered allows testing the knowledge acquired (except content from fiches B11, B12). We thus recommend allocating about 10 minutes at the end of each class to ask topic-specific questions to the students. Depending on the number of students attending, they can answer the questions individually or work in groups. The same questions could be asked also at the beginning of the class to help kick-start the discussions.
Some examples of questions (Q) are listed in the topic fiches under the heading “Example of questions to be asked”.

3. Guidelines

The chapter includes a collection of fiches in support of high-school teachers interested in addressing cybersecurity and/or cybersafety-specific topics with their students.

The fiches are built around specific topics and include information about:
- The level of knowledge addressed (Foundation / Intermediate / Advanced)
- The prerequisites per difficulty level
- The main learning objectives (LO) per difficulty level
- Suggestions of questions to be asked during the class
- Suggestions of examples to be used during the class
- Link(s) to resources to be used for preparing the class

It is the role of the teacher to build the storyline of the lesson based on the information provided in the fiche.

An overview of the modules presented in the document is depicted in the visual below.

<table>
<thead>
<tr>
<th>A. Cybersafety topics</th>
<th>B. Cybersecurity topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0. Why discussing cybersafety</td>
<td>B0. Why study cybersecurity</td>
</tr>
<tr>
<td>A1. Personal / Sensitive Data and Privacy</td>
<td>B1. OSI Model</td>
</tr>
<tr>
<td>A2. Cyberbullying and Sexual Harassment</td>
<td>B2. Operating systems (OS), Computer Hardware, and how does a computer work</td>
</tr>
<tr>
<td>A3. Inappropriate Content</td>
<td>B3. Protection of Data: concerns</td>
</tr>
<tr>
<td>A4. Hate speech</td>
<td>B4. Network Standards and Protocols</td>
</tr>
<tr>
<td>A5. Fake profiles, Fraud, and Phishing</td>
<td>B5. Cyber security essentials (CIA triad)</td>
</tr>
<tr>
<td>A8. Keep my online account safe</td>
<td>B8. Cryptography</td>
</tr>
<tr>
<td>A10. Online Games</td>
<td>B10. Capture the Flag</td>
</tr>
</tbody>
</table>
Modules fiches A. Cybersafety

This chapter describes 12 cybersafety-related modules. Most of them are introduced at the foundation level with some exceptions, like the topics related to data privacy, fake profiles and fake news, and the transparency of recommendation algorithms. Besides, the subject linked to the importance of a strong password is addressed on all three levels.

<table>
<thead>
<tr>
<th>Module code</th>
<th>Cybersafety Module title</th>
<th>Module levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>Why discussing cybersafety</td>
<td>-</td>
</tr>
<tr>
<td>A1</td>
<td>Personal / Sensitive Data and Privacy</td>
<td>x</td>
</tr>
<tr>
<td>A2</td>
<td>Cyberbullying &amp; Sexual harassment</td>
<td>x</td>
</tr>
<tr>
<td>A3</td>
<td>Inappropriate content</td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>Hate-speech</td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>Fake profiles, Fraud, and Phishing</td>
<td>x</td>
</tr>
<tr>
<td>A6</td>
<td>The importance of Strong Passwords</td>
<td>x</td>
</tr>
<tr>
<td>A7</td>
<td>Addiction</td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>Keep my online account safe</td>
<td>x</td>
</tr>
<tr>
<td>A9</td>
<td>Stay safe in Online Social Networks</td>
<td>x</td>
</tr>
<tr>
<td>A10</td>
<td>Online games</td>
<td></td>
</tr>
<tr>
<td>A11</td>
<td>Fake news</td>
<td></td>
</tr>
<tr>
<td>A12</td>
<td>Transparency of Recommendation Algorithms</td>
<td></td>
</tr>
</tbody>
</table>

Most of the cybersafety modules are not dependent of one to each other with few exceptions depicted in the table below.

<table>
<thead>
<tr>
<th>PREREQUISITES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
</tr>
<tr>
<td>A1</td>
</tr>
<tr>
<td>A2</td>
</tr>
<tr>
<td>A3</td>
</tr>
<tr>
<td>A4</td>
</tr>
<tr>
<td>A5</td>
</tr>
<tr>
<td>A6</td>
</tr>
<tr>
<td>A7</td>
</tr>
<tr>
<td>A8</td>
</tr>
<tr>
<td>A9</td>
</tr>
<tr>
<td>A10</td>
</tr>
<tr>
<td>A11</td>
</tr>
<tr>
<td>A12</td>
</tr>
</tbody>
</table>
## A0. Why discussing cybersafety

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Students can define and explain what is cybersafety  
LO2: Be able to list the most common online risks and understands the harm they can cause  
LO3: Understand the importance of being safe, responsible, respectful online |
| Main messages (M) | M1: Cybersafety is important for the online user's mental & physical health  
M2: Anyone, even an expert online user can experience online risks  
M3: Acting safe and responsible online is as important as acting safe and responsible in real life |
| Example of questions to be asked (Q) | Q1: What is Cybersafety?  
Q2: List the online risks they know  
Q3: Do they feel comfortable and safe with your online activities? |
| Practical example (P) | P1: Give real statistics (time spent, ages of users, reported risks, etc.) for online activities and risks.  
- EU Kids Online 2020\(^{14}\)  
- 18 Chilling Privacy Statistics in 2022\(^{15}\)  
- Online risks are everyday events for teens—but they rarely tell their parents\(^{16}\)  
- The Dangers of the Internet\(^{17}\)  
- Teen Voices: Who You’re Talking to Online\(^{18}\) |
| Resources [links] | - Safe Web Surfing: Top Tips for Kids and Teens Online\(^{19}\)  
- How to be safe online, from a young person | Aurelia Torkington\(^{20}\)  
- Is Social Media Hurting Your Mental Health? | Bailey Parnel\(^{21}\)  
- Cyber Safety Week Lesson Resources\(^{22}\)  
- Digital Literacy: Staying safe online\(^{23}\) and What is digital literacy?\(^{24}\)  
- Helping young people manage their online identity | Internet Matters\(^{25}\)  
- My Family's Digital Toolkit\(^{26}\) |

---

\(^{14}\) [https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf](https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf)  
\(^{15}\) [https://legaljobs.io/blog/privacy-statistics/](https://legaljobs.io/blog/privacy-statistics/)  
\(^{17}\) [https://www.youtube.com/watch?v=uuqeRzrcwA18](https://www.youtube.com/watch?v=uuqeRzrcwA18)  
\(^{18}\) [https://www.youtube.com/watch?v=Dh8Lj0_TGQ](https://www.youtube.com/watch?v=Dh8Lj0_TGQ)  
\(^{19}\) [https://www.youtube.com/watch?v=yrln8nyVBLU&ab_channel=watchwellcast](https://www.youtube.com/watch?v=yrln8nyVBLU&ab_channel=watchwellcast)  
\(^{20}\) [https://www.youtube.com/watch?v=hV1sigh6WKA&ab_channel=TEDxTalks](https://www.youtube.com/watch?v=hV1sigh6WKA&ab_channel=TEDxTalks)  
\(^{21}\) [https://www.youtube.com/watch?v=Czg_9C7gw0o&ab_channel=TEDxTalks](https://www.youtube.com/watch?v=Czg_9C7gw0o&ab_channel=TEDxTalks)  
\(^{22}\) [https://www.youtube.com/watch?v=iVTuAS_DE5A](https://www.youtube.com/watch?v=iVTuAS_DE5A)  
\(^{23}\) [https://www.youtube.com/watch?v=eyQeUwqCDWg](https://www.youtube.com/watch?v=eyQeUwqCDWg)  
\(^{24}\) [https://www.youtube.com/watch?v=LEIwqX7Ag&list=PLcetZ6gSk9682A7ZAZq2s9Qb-y8Ng63e](https://www.youtube.com/watch?v=LEIwqX7Ag&list=PLcetZ6gSk9682A7ZAZq2s9Qb-y8Ng63e)  
\(^{25}\) [https://www.youtube.com/watch?v=RnHOFlxQf](https://www.youtube.com/watch?v=RnHOFlxQf)  
\(^{26}\) [https://www.internetmatters.org/digital-family-toolkit/#explore-further](https://www.internetmatters.org/digital-family-toolkit/#explore-further)
## A1. Personal / Sensitive Data and Privacy

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Learn what not to share  
LO2: Discover what are the consequences of sharing sensitive data  
LO3: Learn about what is the digital footprint |
| Main messages (M) | M1: Whatever goes online stays online forever  
M2: Be critical for what you post online  
M3: Respect your own and others’ privacy |
| Example of questions to be asked (Q) | Q1: What do they consider as private/sensitive data?  
Q2: What are the risks when people disclose private data?  
Q3: Have they ever experienced/heard about private data disclosure? Describe the incident. (When/Which application they used/What did they do?) |
| Practical example (P) | P1: Lesson 1. The threat of personal data leaks.  
P2: Cyber Safety Lesson Plan  
P3: Movie: The Great Hack |
| Resources [links] | - How to Protect Your Digital Privacy  
- What is personal data?  
- Data protection and online privacy  
- 5 tips to protect your privacy online  
- Microsoft shares tips on how to protect your information and privacy against cybersecurity threats  
- 8 ways to protect your private information online  
- What is a digital footprint? And how to protect it from hackers  
- Online safety - it is not about the internet... |
# A1. Personal / Sensitive Data and Privacy

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-F</td>
</tr>
</tbody>
</table>

## Learning objectives (LO)

- **LO1**: Learn about the purpose of setting up cookies and role of cookies to enhance user experience on a website.
- **LO2**: Learn to check for and decline third-party cookies
- **LO3**: Understand that cookies are reversible

## Main messages (M)

- **M1**: Websites can track the users’ behaviors using cookies
- **M2**: Do not accept all the cookies
- **M3**: Users can manage their cookies through their browsers settings

## Example of questions to be asked (Q)

- **Q1**: Do they know what cookies are?
- **Q2**: What are the benefits of cookies?
- **Q3**: What is the bad thing about cookies?

## Practical example (P)

- **P1**: Open a website for the first time and explore the cookie notice with the students
- **P2**: Visit a browser and set the cookie settings - Clear, enable, and manage cookies in Chrome - Computer[^39],
- **P3**: Managing Cookie Settings in Your Browser Article - dummies[^40]

## Resources [links]

- Should you accept cookies? 5 times you definitely shouldn’t | Norton[^41]
- Cookies: What Do They Do? - Free Privacy Policy[^42]
- AllAboutCookies.org[^43]
- How Browser Cookies Help You[^44]
- A Complete Guide to Web Tracking (and How to Avoid It)[^45]

[^39]: https://support.google.com/chrome/answer/95647?hl=en&co=GENIE.Platform%3DDesktop
[^41]: https://us.norton.com/internetsecurity-privacy-should-i-accept-cookies.html
[^42]: https://www.freeprivacypolicy.com/blog/cookies/
[^43]: https://allaboutcookies.org/
[^44]: https://youtu.be/x5Gv8rY5y8U
[^45]: https://www.avast.com/c-web-tracking
## A2. Cyberbullying and Sexual Harassment

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Learn to detect signs of cyberbullying and online sexual harassment  
LO2: Understand the importance of reporting such incidences to a trusted adult  
LO3: Learn how to support the victim and not the predator |
| Main messages (M) | M1: No cyberbullying or sexual harassment is accepted  
M2: Cyberbully and Sexual Harassment are illegal  
M3: It is not a shame to report being a victim of cyberbullying or sexual harassment |
| Example of questions to be asked (Q) | Q1: What is cyberbullying?  
Q2: What is sexual harassment?  
Q3: Share experiences they had or heard about |
| Practical example (P) | P1: Sexual harassment:  
Emily’s Story - Online Grooming  
Online Sexual Abuse Can Happen  
P2: Cyberbullying:  
Is it Cyberbullying?  
Heart-Breaking Cyberbullying Statistics for 2022  
P3: Movies: Bully; Audrie and Daisy (16+); Submit the documentary |
| Resources [links] | - Cyberbullying among young people  
- Quiz for cyberbullying  
- Bullying and advice on coping and making it stop  
- What is Cyberbullying, its bad effects and how to stop it  
- Peer to peer sexual harassment  
- Lesson Plans to address sexual harassment  
- Digital Predators | Full Episode | Dateline  
- Online Predators  
- Bad Behavior Online: Bullying, Trolling & Free Speech | Off Book | PBS Digital Studios |

---

46 https://www.youtube.com/watch?v=GQsgOhtmvaUQ&ab_channel=ThinkUKnowAUS  
47 https://www.youtube.com/watch?v=CEivufW2lWs&ab_channel=FightChildAbuse  
48 https://www.youtube.com/watch?v=vtfMzmkYp9E&ab_channel=StopBullyingGov  
49 https://dataprot.net/statistics/cyberbullying-statistics/  
51 https://www.childnet.com/resources/step-up-speak-up/teaching-toolkit/quiz/  
54 https://www.childnet.com/resources/step-up-speak-up/teaching-toolkit/films/  
55 https://www.childnet.com/resources/step-up-speak-up/teaching-toolkit/step-up-speak-up.lesson-plans/  
56 https://www.youtube.com/watch?v=RnKlo0EJaqc&ab_channel=SBSDateline  
57 https://www.infosecawareness.in/concept/children/online-predators  
58 https://www.youtube.com/watch?v=RVSAFhTjAdc
### A3. Inappropriate Content

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1 - F</td>
</tr>
</tbody>
</table>

#### Learning objectives (LO)
- **LO1:** Learn to define the different types of inappropriate content (i.e., violent, sexual, hateful, extremist)
- **LO2:** Understand the negative effect of inappropriate content on young people
- **LO3:** Learn how to react to inappropriate content

#### Main messages (M)
- **M1:** Exposure to inappropriate content can be dangerous for our physical and mental health
- **M2:** Sharing inappropriate content is illegal
- **M3:** Reporting and blocking content to protect ourselves and the others

#### Example of questions to be asked (Q)
- **Q1:** What kind of inappropriate content they can find online?
- **Q2:** Did they find any inappropriate content online? In what applications?
- **Q3:** What do they do when they find online inappropriate content?

#### Practical example (P)
- **P1:** Teach and encourage students to report/block/hide inappropriate content they find online using the platforms settings and options
- **P2:** TikTok restricted mode in settings ([Is TikTok Safe for Kids? Here’s What Parents Should Know](https://www.pandasecurity.com/en/mediacenter/family-safety/ir-tiktok-safe-for-kids/))
- **P3:** TECH - Here’s Facebook’s once-secret list of content that can get you banned ([https://www.cnbc.com/2018/04/24/facebook-content-that-gets-you-banned-according-to-community-standards.html](https://www.cnbc.com/2018/04/24/facebook-content-that-gets-you-banned-according-to-community-standards.html))

#### Resources [links]
- [Inappropriate or explicit content | NSPCC](https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/)
- [Inappropriate content | Cyber Safety Pasifika](https://www.cybersafetypasifika.org/stay-safe-online/inappropriate-content)
- [Inappropriate Content - Cyber Safety](http://cybersafetyed.weebly.com/inappropriate-content.html)
- [Four ways to report inappropriate content online](https://www.youtube.com/watch?v=iOF7Txx0Kzk&ab_channel=ThamesValleyPolice)
- [Find your local child helpline](https://childhelplineinternational.org/helplines/)
- [How to protect children and teens from inappropriate content online](https://www.youtube.com/watch?v=alXhRabFJAc)
## A4. Hate speech

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

| LO1 | Learn to recognize hate speech |
| LO2 | Understand the impact of hate speech |
| LO3 | Learn ways to get away from hate speech |

### Main messages (M)

| M1 | Hate speech can lead to extreme actions |
| M2 | You can help take hate speech content down by reporting and blocking actions |
| M3 | Be critical before you post or comment, try not to generate hate speech |

### Example of questions to be asked (Q)

| Q1 | Where hate speech can be found online? |
| Q2 | At what level do they feel exposed to such content? |
| Q3 | How do they react to such content? |

### Practical example (P)

| P1 | Facing Facts: What is hate speech? |
| P2 | STARTING POINTS FOR COMBATING HATE SPEECH ONLINE |
| P3 | The Datafication of Hate: Expectations and Challenges in Automated Hate Speech Monitoring |

### Resources [links]

- What is Freedom of Expression and what is hate speech?
- How to Recognize Online Hate Speech
- Teen Voices: Hate Speech Online
- Hate speech has ability to alter our minds, faiths, convictions and compel us to reject rule of law
- What Is Hate Speech? We Asked College Students
- Hate Speech - Survey example 1
- Hate Speech - Survey example 2

---

67 [https://www.youtube.com/watch?v=n7p112mU-I8&ab_channel=FacingFacts](https://www.youtube.com/watch?v=n7p112mU-I8&ab_channel=FacingFacts)
70 [https://www.youtube.com/watch?v=BZBP8JZOLSU&ab_channel=CivicsAcademySA](https://www.youtube.com/watch?v=BZBP8JZOLSU&ab_channel=CivicsAcademySA)
71 [https://www.youtube.com/watch?v=on-y1yOmm4&ab_channel=SofiaDA](https://www.youtube.com/watch?v=on-y1yOmm4&ab_channel=SofiaDA)
72 [https://www.youtube.com/watch?v=8vUdWpwLv10&ab_channel=CommonSenseEducation](https://www.youtube.com/watch?v=8vUdWpwLv10&ab_channel=CommonSenseEducation)
74 [https://www.youtube.com/watch?v=skuLK0YpksI](https://www.youtube.com/watch?v=skuLK0YpksI)
75 [https://www.surveymonkey.com/r/6L3BZW](https://www.surveymonkey.com/r/6L3BZW)
76 [https://www.surveymonkey.com/r/QJLTYG8](https://www.surveymonkey.com/r/QJLTYG8)
## A5. Fake profiles, Fraud and Phishing

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Learn to identify fake profiles, online fraud, and fishing  
LO2: Understand the intentions of these malicious practices  
LO3: Learn to report fake profiles, fraud or phishing |
| Main messages (M) | M1: Fake activities online are illegal  
M2: Be careful and critical when being online  
M3: Report and block such profiles or actions |
| Example of questions to be asked (Q) | Q1: What is a fake profile, and how malicious users can use it?  
Q2: What is phishing?  
Q3: What experiences do they have with these incidents? |
| Practical example (P) | P1: What Is Phishing? Examples and Phishing Quiz - Cisco  
P2: Phishing Statistics (Updated 2022) - 50+ Important Phishing Stats - Tessian  
P3: Fake Instagram Account Generator  
P4: Random Person Generator | User Identity, Account and Profile Generator |
| Resources [links] | - 6 social media scams to avoid in 2022, plus red flags | Norton  
- 10 Social Media Scams and How to Spot Them - Panda Security Mediacenter  
- What Is Phishing? Examples and Phishing Quiz - Cisco  
- Fake Profiles - Student - ISEA |

79 [https://generatestatus.com/fake-instagram-account-maker/](https://generatestatus.com/fake-instagram-account-maker/)  
80 [https://fakepersongenerator.com/](https://fakepersongenerator.com/)  
81 [https://us.norton.com/internetsecurity-online-scams-social-media-scams.html](https://us.norton.com/internetsecurity-online-scams-social-media-scams.html)  
84 [https://infosecawareness.in/concept/student/fake-profiles](https://infosecawareness.in/concept/student/fake-profiles)
### A5. Fake profiles, Fraud and Phishing

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A5-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | **LO1:** Learn to analyze email messages to determine legitimacy  
**LO2:** Get yourself familiar with common frauds  
**LO3:** Learn to detect fake profiles on social media |
| Main messages (M) | **M1:** Emails can easily be forged; learn how to detect fake emails  
**M2:** Don't trust offers that seem too good to be true  
**M3:** Fake profiles are usually easy to detect |
| Example of questions to be asked (Q) | **Q1:** How would they analyze an email to see where it was really sent from?  
**Q2:** What are the main characteristics of typical frauds?  
**Q3:** How could they determine that the social media profile contacting them is fake? |
| Practical example (P) | **P1:** 5 Ways to Detect a Phishing Email: With Examples[^85]  
**P2:** Detect Fakes[^86] |
| Resources [links] | - Phishing Quiz[^87]  
- Fake account profile quiz[^88]  
- Behind the Screen Quiz | Scam Spotter[^89]  
- How to Detect Fake Profiles – Understanding Phishing[^90]  
- How to check a suspicious e-mail sender | Kaspersky official blog[^91] |

[^85]: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email  
[^86]: https://detectfakes.media.mit.edu/  
[^87]: https://phishingquiz.withgoogle.com/  
[^88]: https://spotthetroll.org/profile/1  
[^89]: https://scamspotter.org/quiz/  
[^90]: https://www.cybintsolutions.com/detect-fake-profiles-phishing/  
[^91]: https://www.kaspersky.com/blog/analyzing-mail-header/42665/
### A6. The importance of Strong Passwords

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning objectives (LO)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LO1:</td>
<td>Learn the ‘ingredients’ to create a strong password</td>
</tr>
<tr>
<td>LO2:</td>
<td>Learn the methods mostly used to attack a password</td>
</tr>
<tr>
<td>LO3:</td>
<td>Learn managing your passwords safely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main messages (M)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>M1:</td>
<td>Password needs to be long</td>
</tr>
<tr>
<td>M2:</td>
<td>Passwords must also contain special characters, and numbers, not only letters</td>
</tr>
<tr>
<td>M3:</td>
<td>Password is private data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example of questions to be asked (Q)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1:</td>
<td>How do they create passwords?</td>
</tr>
<tr>
<td>Q2:</td>
<td>Do they use the same password in many applications?</td>
</tr>
<tr>
<td>Q3:</td>
<td>Who knows their password?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practical example (P)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P1:</td>
<td>Password Check</td>
</tr>
<tr>
<td>P2:</td>
<td>How to Create a Strong Password[^93]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resources [links]</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Strong Password Tips</td>
<td>Create a strong password in 2022[^94]</td>
</tr>
<tr>
<td>- How to Remember a Unique Password For Everything[^95]</td>
<td></td>
</tr>
<tr>
<td>- Password Guidelines • European University Institute[^96]</td>
<td></td>
</tr>
<tr>
<td>- 6 Types of Password Attacks &amp; How to Stop Them</td>
<td>OneLogin[^97]</td>
</tr>
<tr>
<td>- RBC Cyber Security - Powerful Passwords[^98]</td>
<td></td>
</tr>
<tr>
<td>- How Do Password Managers Work[^99]</td>
<td></td>
</tr>
</tbody>
</table>

[^92]: https://password.kaspersky.com/
[^93]: https://www.youtube.com/watch?v=aEmF3Jy1v44&ab_channel=SafetyinCanada
[^94]: https://www.youtube.com/watch?v=Cg2Cs_E6fS1&ab_channel=LanguageTechSolutions
[^95]: https://www.youtube.com/watch?v=HrMHS8EGPc4&ab_channel=ExperimentalJack
[^97]: https://www.onelogin.com/learn/6-types-password-attacks#:~:text=Password%20attacks%20are%20one%20of%20the%20most%20frequent%20types%20of%20password%20attacks%20and%20were%20due%20to%20compromised%20credentials
[^98]: https://www.youtube.com/watch?v=IhlXtBNNuKs&ab_channel=RBC
[^99]: https://www.youtube.com/watch?v=Df72oBhMgWs
## A6. The importance of Strong Passwords

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A6-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Understand how passwords are brute forced  
LO2: Understand the entropy of a password and how it affects “guessability”  
LO3: Learn how passwords are stored and how they can be stolen |
| Main messages (M) | M1: Passwords need to be long and unpredictable  
M2: Passwords are typically brute forced (guessed)  
M3: Use different password across services in case they are stolen |
| Example of questions to be asked (Q) | Q1: How could they attack a password?  
Q2: How would they estimate password complexity?  
Q3: Why is it important to use different passwords across services? |
| Practical example (P) | P1: Password Strength Meter[^100]  
P2: Check if your password is already leaked[^101] |
| Resources [links] | - [Password Entropy Calculator][^102]  
- [Correct Horse Battery Staple Review - Password Advice - Virtual CISO][^103]  
- [Brute Force Attack - Meaning, Examples and Prevention][^104]  
- [Why Is It So Important to Use Different Passwords for Everything][^105]  
- [Password Complexity vs Length][^106]  
- [Strong Passwords – How to Create & Benefits][^107] |

---

[^100]: https://www.passwordmonster.com/
[^101]: https://haveibeenpwned.com/
[^102]: https://www.omnicalculator.com/other/password-entropy
[^103]: https://fractionalciso.com/correct-horse-battery-staple-review/
[^104]: https://crashtest-security.com/brute-force-attacks/
[^105]: https://www.youtube.com/watch?v=lUAgmkdVws&ab_channel=AskLeo%21
[^106]: https://www.lepide.com/blog/password-complexity-vs-length/
[^107]: https://www.kaspersky.com/resource-center/threats/how-to-create-a-strong-password
### A6. The importance of Strong Passwords

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A6-I</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Understand why biometrics can be more secure than passwords  
LO2: Learn the methods biometrics are attacked  
LO3: Define the Cryptography and passwords terms: Hash, Salt, and Pepper |
| Main messages (M) | M1: Biometrics are unique  
M2: Biometrics can still be hacked  
M3: Developers can use cryptography methods to secure your passwords |
| Example of questions to be asked (Q) | Q1: How do they unlock your phone?  
Q2: Is their fingerprint unique?  
Q3: How are passwords stored on the application side? |
| Practical example (P) | P1: Biometric Authentication  
P2: Password Hashing, Salts, Peppers | Explained! |
| Resources [links] |  
- How secure is Biometric Authentication Technology and Biometric Data? | Biometric Security  
- Hash, Salt and Pepper: How cooking a password makes it safer | Gearbrain  
- Salting, peppering, and hashing passwords |

108 [https://www.youtube.com/watch?v=J5n630AMLbE](https://www.youtube.com/watch?v=J5n630AMLbE)  
109 [https://www.youtube.com/watch?v=--tnZMuK3E&ab_channel=Seytonic](https://www.youtube.com/watch?v=--tnZMuK3E&ab_channel=Seytonic)  
110 [https://www.youtube.com/watch?v=ZPG3XQhZVII](https://www.youtube.com/watch?v=ZPG3XQhZVII)  
112 [https://www.youtube.com/watch?v=FvstbO787Qo&ab_channel=mCoding](https://www.youtube.com/watch?v=FvstbO787Qo&ab_channel=mCoding)
### A7. Addiction

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>

| Learning objectives (LO) | LO1: Detect the signs of an online addicted person  
LO2: Understand the methods used by platforms that can cause addiction  
LO3: Understand the negative effect of addiction |
|--------------------------|--------------------------------------------------|
| Main messages (M) | M1: Stop missing out the real world to be online  
M2: Control the time and the quality of your online activities |
| Example of questions to be asked (Q) | Q1: How much time do they spend online?  
Q2: How often do they check their phone when they are alone/you are with other people?  
Q3: Do they cancel going out/meeting friends to stay online? |
| Practical example (P) | P1: Internet Addiction Test (Self-Assessment)¹¹³ |
| Resources [links] | - Social Media Addiction¹¹⁴  
- Social Media Addiction | Definition, Signs, Contributing Factors¹¹⁵  
- Addiction to social media: main causes and symptoms¹¹⁶  
- Psychology of Social Networks: What makes us addicted? - Learn UX¹¹⁷  
- Trapped - the secret ways social media is built to be addictive (and what you can do to fight back)¹¹⁸  
- What Makes Social Media So Addictive?¹¹⁹  
- The Bitter Reality Of Video Game Addiction¹²⁰  
- Video Game Addiction - Treatment, Symptoms, and Causes¹²¹  
- Video Game Addiction Symptoms and Treatment¹²²  
- How I Cured My Social Media Addiction [Easiest Way]¹²³  
- How I Cured My Phone Addiction¹²⁴  
- Movie: The Social Dilemma¹²⁵ |

---

¹¹³ [https://www.psycom.net/internet-addiction-test-quiz](https://www.psycom.net/internet-addiction-test-quiz)  
¹¹⁹ [https://www.youtube.com/watch?v=VK4PwT9fc&ab_channel=DownwardThrust](https://www.youtube.com/watch?v=VK4PwT9fc&ab_channel=DownwardThrust)  
¹²⁰ [https://gamequitters.com/video-game-addiction/](https://gamequitters.com/video-game-addiction/)  
¹²¹ [https://americanaddictioncenters.org/video-gaming-addiction](https://americanaddictioncenters.org/video-gaming-addiction)  
¹²² [https://www.youtube.com/watch?v=j2MERFltRns](https://www.youtube.com/watch?v=j2MERFltRns)  
¹²³ [https://www.youtube.com/watch?v=Qk5f7UMJ3M](https://www.youtube.com/watch?v=Qk5f7UMJ3M)  
¹²⁴ [https://www.netflix.com/gr/title/81254224](https://www.netflix.com/gr/title/81254224)
## A8. Keep my online account safe

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A6-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO)                   | LO1: Learn to check for the Security and Safety Settings in the applications  
|                                            | LO2: Learn about and set up the multi-factor authentication mechanism  
|                                            | LO3: Learn about and enable the inappropriate content blocking mechanism  |
| Main messages (M)                         | M1: Use the applications security & privacy mechanisms to keep you safe  
|                                            | M2: Look for the multi-factor authentication in each application and enable it  
|                                            | M3: You can always choose the more advanced security settings and not the default selection to enhance your security  |
| Example of questions to be asked (Q)       | Q1: Have they ever used a One-Time-Password? Why do you think it is used?  
|                                            | Q2: What security and safety features do they apply for their online accounts?  
|                                            | Q3: What security and safety features do they know is there but do not use?  |
| Practical example (P)                      | P1: Go through apps the students use and set together security and privacy  
|                                            | P2: 12 Simple Things You Can Do to Be More Secure Online126  |
| Resources [links]                          | - **Google**: [Google Safety Center]127  
|                                            | - **Tiktok**: [TikTok Social Media Parental Control and Safety settings] - [Internet Matters]128  
|                                            | - **Facebook**: [Your Privacy | Facebook Help Center]129  
|                                            | - [Lesson 5. How to configure privacy in Facebook]130  
|                                            | - [What's Privacy Checkup and how can I find it on Facebook? | Facebook Help Center]131  
|                                            | - **Instagram**: [Managing Your Privacy Settings | Instagram Help Center]132  
|                                            | - [Lesson 7. How to configure privacy in Instagram]133  
|                                            | - [What is a one-time password (OTP)? Definition from SearchSecurity]134  
|                                            | - [Set Two-Factor Authentication to your - Google Account Help]135  
|                                            | - **Microsoft**: [How to help keep your Microsoft account safe and secure]136  
|                                            | - [What is antivirus and why is it important?]137  |

126 [https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online](https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online)  
127 [https://safety.google/](https://safety.google/)  
131 [https://www.facebook.com/help/443357099140264](https://www.facebook.com/help/443357099140264)  
134 [https://www.techtarget.com/searchsecurity/definition/one-time-password-OTP#:~:text=A%20one%2Dtime%20password%20(OTP)%20is%20an%20automatically%20generated%20or%20reused%20across%20multiple%20accounts](https://www.techtarget.com/searchsecurity/definition/one-time-password-OTP#:~:text=A%20one%2Dtime%20password%20(OTP)%20is%20an%20automatically%20generated%20or%20reused%20across%20multiple%20accounts)  
135 [https://support.google.com/accounts/answer/185833?hl=en](https://support.google.com/accounts/answer/185833?hl=en)  
137 [https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/](https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/)
A9. Stay safe in Online Social Networks

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td>A1-F, A2, A3, A4, A5-I, A6-F, A7, A8</td>
</tr>
</tbody>
</table>

| Learning objectives (LO) | **LO1**: Understand what it is okay to share and what not  
**LO2**: Understand how to decide you are your friends online  
**LO3**: Understand when to avoid third party applications and logging |

| Main messages (M) | **M1**: Think before you post  
**M2**: Your online actions stay online forever  
**M3**: Do not log in with your social media accounts to untrusted applications |

| Example of questions to be asked (Q) | **Q1**: How often do they post online?  
**Q2**: What do they post (video/image/text/combination of those), and who can see their posts?  
**Q3**: Do they use their online profile to log in to other applications (e.g., games)? |

| Practical example (P) | **P1**: Social Media Safety Tips[^138]  
**P2**: Youth And Violent Extremism On Social Media[^139]  
**P3**: Preventing The Deaths That Are Driven By Social Media[^140] |

| Resources [links] | - Social Media Data Privacy Awareness[^141]  
- What are the dangers of oversharing on social media?[^142]  
- Mental Health and Social Media[^143]  
- How Social Media Is Destroying Our Brains[^144]  
- Metaverse: how to regulate a space yet to be invented?[^145] |

---

[^138]: https://www.youtube.com/watch?v=VPIWDfP0T0&ab_channel=SEONorth  
[^139]: https://unesdoc.unesco.org/ark:/48223/pf0000260382  
[^140]: https://www.newsy.com/stories/preventing-the-deaths-that-are-driven-by-social-media/  
[^141]: https://www.youtube.com/watch?v=UhhYSrUHnao&ab_channel=TechnologyServicesAtIllinois  
[^142]: https://www.youtube.com/watch?v=e2xm5fc5MQk&ab_channel=ShowtimeProductions  
[^143]: https://www.youtube.com/watch?v=QDiQspkwI&ab_channel=PsychHub  
[^144]: https://www.youtube.com/watch?v=fouSmgZBXSU&ab_channel=TopThink  
## A10. Online Games

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-F, A2, A3, A4, A5-I, A6, A7-F</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

- **LO1:** Define Online Game addiction as a fact
- **LO2:** Learn to recognize Phishing in online games
- **LO3:** Learn to recognize toxic behaviors (cyberbullying, sexual harassment, etc.) in online games environment

### Main messages (M)

- **M1:** Online games encounter dangers
- **M2:** The age limits for games are there for a reason
- **M3:** You can develop secure habits when playing online

### Example of questions to be asked (Q)

- **Q1:** How much time they spend in online gaming?
- **Q2:** Do they play with strangers?
- **Q3:** Do they have any online risk experience during playing online?

### Practical example (P)

- **P1:** Is Online Gaming Safe? Tips for Online Gaming Security \(^{146}\)
- **P2:** Recent FIFA 22 Incident and Phishing Attacks in the Gaming industry \(^{147}\)
- **P3:** Boy’s suicide triggers debate over banning PlayerUnknown’s Battlegrounds in India \(^{148}\)

### Resources [links]

- **Games and security** \(^{149}\)
- **Lesson 1. Games and security** \(^{150}\)
- **Online gaming | Childline** \(^{151}\)
- **How to Protect Your Child from the Top 7 Dangers of Online Gaming** \(^{152}\)
- **Cyber Safety Video: Online Gaming Safety** \(^{153}\)
- **Twitch Safety Center** \(^{154}\)

---

146. [https://www.youtube.com/watch?v=60PSb00T3Kc&t=121s](https://www.youtube.com/watch?v=60PSb00T3Kc&t=121s)
149. [https://www.youtube.com/watch?v=QEP7kMMVjo&ab_channel=Kaspersky](https://www.youtube.com/watch?v=QEP7kMMVjo&ab_channel=Kaspersky)
152. [https://usa.kaspersky.com/resource-center/threats/top-7-online-gaming-dangers-facing-kids](https://usa.kaspersky.com/resource-center/threats/top-7-online-gaming-dangers-facing-kids)
### A11. Fake News

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A5-F</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1: Learn what is fake news  
LO2: Understand what is the impact of fake news  
LO3: Learn about fake profiles, bots |
| Main messages (M) | M1: Online information can be false  
M2: Don’t believe everything you find online  
M3: Be critical when believing in/sharing with others online information |
| Example of questions to be asked (Q) | Q1: Have they ever come across online fake news?  
Q2: What can fake news cause?  
Q3: Why does fake news spread fast? |
| Practical example (P) | P1: What Is Fake News?  
P2: The Impact Of Fake News On The World As Mistruths Continue To Spread  
P3: How Online Bots Spread Fake News | Young Scot  
P4: Fact Check: How to decipher online news and information: Identifying Fake News  
P6: EUfactcheck |
| Resources [links] | - What is fake news and misinformation? | Internet Matters  
- How Fake News Spreads  
- How false news can spread - Noah Taylin  
- How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting | Center for Information Technology and Society  
- 10 Examples of Fake News from History - The Social Historian  
- Fake News: Separating Truth From Fiction  
- Game: Get bad news |

---

155 https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise  
156 https://www.youtube.com/watch?v=5biqhnWucew&ab_channel=TheProject  
158 https://academicguides.waldenu.edu/library/fakenews/idfakenews  
159 https://www.avg.com/en/signal/what-is-fake-news  
160 https://eufactcheck.eu/  
162 https://libguides.uvic.ca/fakenews/how-it-spreads  
163 https://www.youtube.com/watch?v=cSKGa_7XJkg&ab_channel=TED-Ed  
164 https://www.cits.ucsb.edu/fake-news/spread  
165 https://www.thesocialhistorian.com/fake-news/  
166 https://libguides.valenciacollege.edu/c.php?g=612299&p=4251520  
167 https://www.getbadnews.com/books/english/
## A11. Fake News

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A11-F</td>
</tr>
<tr>
<td>Learning objectives (LO)</td>
<td>LO1: Learn about the main (measurable) characteristics of fake news  &lt;br&gt; LO2: Understand how social media profiles are related to fake news  &lt;br&gt; LO3: Learn about available fact-checking tools</td>
</tr>
<tr>
<td>Main messages (M)</td>
<td>M1: Fake news has specific parameters that can be detected  &lt;br&gt; M2: Some social media profiles are prone to spreading fake news  &lt;br&gt; M3: Use your critical thinking and fact-checking tools to prevent the spread of fake news</td>
</tr>
<tr>
<td>Example of questions to be asked (Q)</td>
<td>Q1: How do they identify a fake new post?  &lt;br&gt; Q2: What are the characteristics of social media profiles that are more prone to sharing fake news?  &lt;br&gt; Q3: Have they ever used/heard someone used a fact-checking tool/website?</td>
</tr>
</tbody>
</table>
## A12. Transparency of Recommendation Algorithms

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A1-I</td>
</tr>
<tr>
<td>Learning objectives (LO)</td>
<td>LO1: Understand how a recommendation algorithm works&lt;br&gt;LO2: Understand what is a filter bubble&lt;br&gt;LO3: Understand the importance of algorithms transparency</td>
</tr>
<tr>
<td>Main messages (M)</td>
<td>M1: There is a logic behind the recommendations delivered to us&lt;br&gt;M2: Recommendations are supposed to give the users more content they are interested in&lt;br&gt;M3: Platforms should give explanatory information about the recommendations we get</td>
</tr>
<tr>
<td>Example of questions to be asked (Q)</td>
<td>Q1: How often they get recommendations when you are online? (accounts you may know, movies you may like, other people who bought this also ordered that)&lt;br&gt;Q2: Why do people require transparency?&lt;br&gt;Q3: How do they believe Facebook recommends friends to add?</td>
</tr>
<tr>
<td>Practical example (P)</td>
<td>P1: How Recommender Systems Work (Netflix/Amazon)&lt;br&gt;P2: How news feed algorithms supercharge confirmation bias</td>
</tr>
<tr>
<td>Resources [links]</td>
<td>- Presentation - Algorithmic Mediation in Information Access Services&lt;br&gt;- What is a Filter Bubble? - Definition from Techopedia&lt;br&gt;- Recommender system - Wikipedia&lt;br&gt;- Recommender Systems&lt;br&gt;- Algorithmic bias explained&lt;br&gt;- Show me the algorithm: Transparency in recommendation systems — Schwartz Reisman Institute</td>
</tr>
</tbody>
</table>

---

180 [https://www.youtube.com/watch?v=n3RKsY2H-NE&ab_channel=ArtoftheProblem](https://www.youtube.com/watch?v=n3RKsY2H-NE&ab_channel=ArtoftheProblem)
181 [https://www.youtube.com/watch?v=prx9bzns3g&ab_channel=BigThink](https://www.youtube.com/watch?v=prx9bzns3g&ab_channel=BigThink)
183 [https://www.techopedia.com/definition/28556/filter-bubble](https://www.techopedia.com/definition/28556/filter-bubble)
185 [https://www.youtube.com/watch?v=Eez1DEeWUjA&ab_channel=CS50](https://www.youtube.com/watch?v=Eez1DEeWUjA&ab_channel=CS50)
186 [https://www.youtube.com/watch?v=bWOUw8omUVg&ab_channel=TRTWorld](https://www.youtube.com/watch?v=bWOUw8omUVg&ab_channel=TRTWorld)
# A12. Transparency of Recommendation Algorithms

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>A12-F</td>
</tr>
</tbody>
</table>

## Learning objectives (LO)

- **LO1**: Learn how user profiling is done on the web
- **LO2**: Learn how recommendation algorithms work based on your profile

## Main messages (M)

- **M1**: When you are surfing on the web, services are profiling you
- **M2**: They recommend services and products based on your profile
- **M3**: Several algorithms determine how offers should be made according to your profile to maximize clicks or purchases

## Example of questions to be asked (Q)

- **Q1**: What do the services “know” about you when you are online?
- **Q2**: How can they use that information to offer personalized services or products?
- **Q3**: How can they protect themselves from tracking?

## Practical example (P)

- **P1**: Introduction to recommender systems - Things Solver[^188]
- **P2**: Online Targeting and Tracking[^189]

## Resources [links]

- [Online Profiling | Encyclopedia.com][^190]
- [How TikTok’s Algorithm Figures You Out | WSJ][^191]
- [Netflix Research: Recommendations][^192]
- [How TikTok recommends videos #ForYou][^193]
- [Meta Company (Facebook, Instagram) Our approach to ranking | Transparency Center][^194]
- [Advertisement and Online Profiling, Protecting Data][^195]

[^188]: https://thingsolver.com/introduction-to-recommender-systems/
[^189]: https://www.youtube.com/watch?v=6pVSLgH-3kw&ab_channel=CommonSenseEducation
[^190]: https://www.encyclopedia.com/books/educational-magazines/online-profiling
[^191]: https://www.youtube.com/watch?v=nfczi2cI6Cs&ab_channel=WallStreetJournal
[^192]: https://www.youtube.com/watch?v=f8OK1HBEgn0
[^194]: https://transparency.fb.com/features/ranking-and-content/
Modules fiches B. Cybersecurity

Within this chapter there are 12 cybersecurity related modules. Most of them are covering all three levels, from foundation to advanced, with some exceptions like the topics related to the OSI model, protection of data, and Defense against cyber threats, which stays at the Foundation level we consider appropriate to be studied in high school. We are suggesting a foundation level for introductory talk on Why study cybersecurity (B0) to kick-off the course. On the other hand, the fiches B11 and B12 are of a different nature since they address subjects linked to prospects if building a career path in cybersecurity, so they are classified at the Advanced level.

<table>
<thead>
<tr>
<th>Module code</th>
<th>Cybersecurity Module title</th>
<th>Module levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>Why study cybersecurity</td>
<td>---</td>
</tr>
<tr>
<td>B1</td>
<td>OSI Model</td>
<td>x</td>
</tr>
<tr>
<td>B2</td>
<td>Operating systems (OS), Computer Hardware and how does a computer work</td>
<td>x x</td>
</tr>
<tr>
<td>B3</td>
<td>Protection of Data: concerns</td>
<td>x</td>
</tr>
<tr>
<td>B4</td>
<td>Network Standards &amp; Protocols</td>
<td>x x x</td>
</tr>
<tr>
<td>B5</td>
<td>Essentials in Cyber security</td>
<td>x x</td>
</tr>
<tr>
<td>B6</td>
<td>Attacks, threats, vulnerabilities</td>
<td>x x x</td>
</tr>
<tr>
<td>B7</td>
<td>Defense against Cyber threats (Cyber Hygiene)</td>
<td>x</td>
</tr>
<tr>
<td>B8</td>
<td>Cryptography</td>
<td>x x x</td>
</tr>
<tr>
<td>B9</td>
<td>Individual Incidents Responses</td>
<td>x</td>
</tr>
<tr>
<td>B10</td>
<td>Capture the Flag</td>
<td>x x</td>
</tr>
<tr>
<td>B11</td>
<td>Penetration testing</td>
<td>x</td>
</tr>
<tr>
<td>B12</td>
<td>Roles in Cyber security and Top certifications</td>
<td>x</td>
</tr>
</tbody>
</table>

Most of the cybersecurity modules are dependent of some previous one with few exceptions depicted in the table below.

<table>
<thead>
<tr>
<th>PREREQUISITES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>B1</td>
</tr>
<tr>
<td>B2</td>
</tr>
<tr>
<td>B3</td>
</tr>
<tr>
<td>B4</td>
</tr>
<tr>
<td>B5</td>
</tr>
<tr>
<td>B6</td>
</tr>
<tr>
<td>B7</td>
</tr>
<tr>
<td>B8</td>
</tr>
<tr>
<td>B9</td>
</tr>
<tr>
<td>B10</td>
</tr>
<tr>
<td>B11</td>
</tr>
<tr>
<td>B12</td>
</tr>
</tbody>
</table>
## B0. Why study cybersecurity

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>

| Learning objectives (LO) | LO1. Discover why cybersecurity is crucial to our data and personal life  
LO2. Learn what data can be affected in case of not properly secured  
LO3. Learn about the Cybercrimes which are rising every day  
LO4. Identify some of the attacks that are recently happening |
|--------------------------|-------------------------------------------------|
| Main messages (M) | M1. Different kinds of attacks can occur in case of lack of security (access to data, loss of credentials, access to credit cards etc.)  
M2. The main reasons to learn about cybersecurity are: (1) Protect from Cyber-attacks, (2) Ensure privacy of information, (3) Provide guidelines for data security  
M3. Learning cyber security can give you a good career for the future |

| Example of questions to be asked (Q) | Q1: What is cyber security?  
Q2: Where do we use cybersecurity in our daily use?  
Q3: Do you download any game from any source?  
Q4: What are the sectors that you can work in? |
|-------------------------------------|-------------------------------------------------|
| Practical example: (P) | - Introduction to Cybersecurity\(^{196}\)  
- Why Is Cybersecurity Important?\(^{197}\)  
- Website Hacking Statistics You Should Know in 2022\(^{198}\)  
- Try the Gorilla example\(^{199}\), an exercise on “Inattentional blindness”.  
- Smart Home Security: Security and Vulnerabilities\(^{200}\) |

| Resources [links] | - Cyber Security In 7 Minutes | What Is Cyber Security: How It Works?\(^{201}\)  
- Why Cybersecurity is Important! | Romeo Farinacci | TEDxGrandCanyonUniversity\(^{202}\)  
- Cybersecurity Tutorial for Beginners | Introduction to Cybersecurity | Invensis Learning at 1:28 min and 11:12 min  
- Cybersecurity Training for Kids\(^{203}\)  
- How the smart home could be at risk from hackers\(^{204}\)  
- Top 10 Reasons to Learn Cybersecurity in 2021 | Edureka\(^{205}\) |

196 [https://www.youtube.com/watch?v=ULGILG-ZaQ0](https://www.youtube.com/watch?v=ULGILG-ZaQ0)  
197 [https://cybersecurityonline.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/](https://cybersecurityonline.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/)  
198 [https://patchstack.com/articles/website-hacking-statistics/](https://patchstack.com/articles/website-hacking-statistics/)  
199 [http://viscog.beckman.illinois.edu/flashmovie/15.php](http://viscog.beckman.illinois.edu/flashmovie/15.php)  
201 [https://www.youtube.com/watch?v=inWWhr5tnEAl](https://www.youtube.com/watch?v=inWWhr5tnEAl)  
202 [https://www.youtube.com/watch?v=JIJslcA8Q5g&ab_channel=TEDxTalks](https://www.youtube.com/watch?v=JIJslcA8Q5g&ab_channel=TEDxTalks)  
203 [https://www.youtube.com/watch?v=ZLyFt6BdxD4&ab_channel=Malwarebytes](https://www.youtube.com/watch?v=ZLyFt6BdxD4&ab_channel=Malwarebytes)  
205 [https://www.youtube.com/watch?v=ZlyFt6BdxD4&ab_channel=edureka%21](https://www.youtube.com/watch?v=ZlyFt6BdxD4&ab_channel=edureka%21)
# B1. OSI Model

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>----</td>
</tr>
</tbody>
</table>

| Learning objectives (LO) | LO1: Learn about the layers of the OSI model and their purpose  
LO2: Understand how devices use layers to communicate across the Internet  
LO3: Learn to differentiate between two types of transmitted information: (1) allow the controlling of the data and (2) data itself. |
| Main messages (M) | M1: OSI Model is a conceptual framework used to describe the functions of a networking system.  
M2: Data is transmitted within the layers of the OSI model  
M3: Physical layer can be cable, wireless medium etc. |
| Example of questions to be asked (Q) | Q1: Why is the OSI Model broken into separate layers?  
Q2: Why are there different layers in the OSI model?  
Q3: What do you know as connection mediums at the physical layer? |
| Practical example (P) | P1: Discuss the different physical layers available.  
P2: Give the Man in the Middle attack example and discuss what happens at the network layer |

| Resources [links] | - OSI Model Explained | Real World Example | 206  
- Attacks on various OSI Model layers | by Ehsan Ahmadi | Medium | 207  
- OSI Model Explained | OSI Animation | Open System Interconnection Model | OSI 7 layers | TechTerms | 208  
- TCP vs UDP: Key Difference Between Them | 209  
- Online quiz: OSI Model Game | 210 |

---

206 https://www.youtube.com/watch?v=LANW3m7UzWs&ab_channel=CertBros  
207 https://medium.com/@e.ahmadi/attacks-on-various-osi-model-layers-bd2fac5ab985  
208 https://www.youtube.com/watch?v=vv4y_uOneC0&t=5s&ab_channel=TechTerms  
210 https://samsclass.info/123/quiz/osi.htm
## B1. OSI Model

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1-F</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

- **LO1:** Discover the difference between TCP and UDP and the purpose of each layer alone
- **LO2:** Know that security attacks can take place at different OSI layers

### Main messages (M)

- **M1:** Network layer is the reason for Internet to exist
- **M2:** This phrase can be useful to memorize the seven layers: "Peter Dances Near The Soft Pink Apples".
- **M3:** TCP is a connection-oriented protocol and UDP is a connectionless protocol.
- **M4:** The application layer of the seven-layer OSI model is the top layer that approaches protocols for application interaction with the network.

### Example of questions to be asked (Q)

- **Q1:** What is the difference between TCP and UDP?
- **Q2:** When is TCP used? UDP? State some of their applications.
- **Q3:** Why is the OSI model useful?

### Practical example (P)

- **P1:** Give an example where the Application layer is exploited (ex: attacks on websites)
- **P2:** Propose a scenario where UDP and TCP are used and state the differences

### Resources [links]

- [OSI Model: A Practical Perspective - Networking Fundamentals - Lesson 2a](https://www.youtube.com/watch?v=LkolbURtTs&ab_channel=PracticalNetworking)
- [Physical layer in OSI Model | Physical layer Protocols | Physical Layer Tutorial | networking tips](https://www.youtube.com/watch?v=qSk5SLrg7Yg&ab_channel=ISOTrainingInstitute)
- [OSI Model - A Real World Example:::InetDaemon.Com](https://www.inetdaemon.com/tutorials/basic_concepts/network_models/osi_model/real_world_example.shtml)
- [OSI Model Explained](https://www.youtube.com/watch?v=O_rsqVtul0&ab_channel=DeeRa)
# B2. Operating systems (OS), Computer Hardware and how does a computer work

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>----</td>
</tr>
</tbody>
</table>

## Learning objectives (LO)
- **LO1**: Introduce Basic parts of a Computer
- **LO2**: Know what is a software and what is Hardware
- **LO3**: Learn a short history of the computer

## Main messages (M)
- **M1**: Each internal hardware component has a basic function (CPU, GPU, Hard Disk, RAM, Motherboard etc.)
- **M2**: Hardware can be internal or external (like motherboards, hard drives, memory, and internal peripherals such as a CDROM drive, CD-R)

## Example of questions to be asked (Q)
- **Q1**: Can a computer operate with software or hardware alone?
- **Q2**: What does CPU stand for?

## Practical example (P)
- **P1**: Assemble a computer in a real-life experiment showing the students the components inside
- **P2**: Explain the Motherboard to the students stating the function of the basic parts.

## Resources [links]
- Computer Basics: Basic Parts of a Computer[^216]
- EXTERNAL HARDWARE AND INTERNAL HARDWARE[^217]
- History of computers: A brief timeline | Live Science[^218]
- History of Computers – How were Computers Invented Short Documentary Video[^219]
- Computer Science Unplugged - The Show[^220]

[^216]: https://www.youtube.com/watch?v=mLgTnkw558w&ab_channel=GCFLearnFree.org
[^217]: https://www.youtube.com/watch?v=KioTAi90CPM&ab_channel=MarkAnthonyDacullo
[^218]: https://www.livescience.com/20718-computer-history.html
[^219]: https://www.youtube.com/watch?v=Aqg6LxGCz44&ab_channel=Technology%3APast%2CPresentandFuture
[^220]: https://www.youtube.com/watch?v=VpDDPWVn5-Q&t=3151s&ab_channel=UCComputerScienceEducation
## B2. Operating systems (OS), Computer Hardware and how does a computer work

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B2-F</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

- **LO1**: Define the Binary format
- **LO2**: Understand what an Operating system is
- **LO3**: Learn how a computer works
- **LO4**: Learn to define the basic roles of each hardware

### Main messages (M)

- **M1**: Hardware is the bottom-level component of the systems
- **M2**: An operating system is the most important software that runs on a computer and without an operating system, a computer is useless.

### Example of questions to be asked (Q)

- **Q1**: What is the structured bottom level component of computers?
- **Q2**: What is binary language?
- **Q3**: What are some of the available operating systems?

### Practical example (P)

- **P1**: Give an example for changing a binary exercise
- **P2**: Good practical sheet: [Binary.pdf](https://corbettmaths.com/wp-content/uploads/2019/04/Binary.pdf) and [Worksheet 1: Binary Numbers 2 00010 5 3 12 19 8 15](http://csunplugged.mines.edu/Activities/Binary/BinaryWorksheets.pdf)

### Resources [links]

- [5 main components of computer system and their functions](https://sciencerack.com/components-of-computer/)
- [Components of Computer System](https://www.tutorialspoint.com/computer_concepts/computer_concepts_components_of_computer_system.htm)
- [Why Do Computers Use 1s and 0s? Binary and Transistors](https://www.youtube.com/watch?v=Xpk67YzOn5w&ab_channel=BasicsExplained%2CH3Vtux)
- [ExplGame: tagged "computer parts"](https://matchthememory.com/computer-components1)
- [Computer Basics: Understanding Operating Systems](https://www.youtube.com/watch?v=fkGCLIQx1MI&t=2s&ab_channel=GCFLearnFree.org)
- [Binary Bonanza! Binary Number game - Fun, Free, Online Way to Learn Binary](https://games.penjee.com/binary-bonanza/)
- [Binary Numbers | Classic CS Unplugged](https://classic.csunplugged.org/activities/binary-numbers/)
- [Why Do Computers Use 1s and 0s? Binary and Transistors Explained](https://www.youtube.com/watch?v=Xpk67YzOn5w&ab_channel=BasicsExplained%2CH3Vtux)
## B2. Operating systems (OS), Computer Hardware and how does a computer work

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B2-F, B2-I</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

- **LO1**: Relate between Cyber security and Operating Systems
- **LO2**: Learn about the importance of the basic knowledge of operating systems work to have a secure device

### Main messages (M)

- **M1**: Power outages and theft are some consequences of software and hardware vulnerabilities
- **M2**: It is very important to update the operating systems frequently.
- **M3**: Operating systems will be vulnerable to (virus) attacks if not patched frequently (by the users)

### Example of questions to be asked (Q)

- **Q1**: State some recent system cyber attacks (Spectre and Meltdown)
- **Q2**: Do you think security is affected by the operating system?
- **Q3**: What are the main differences between types of malware?

### Practical example (P)

- **P1**: Show how to update an operating system.
- **P2**: Use different versions of operating systems and see the differences
- **P3**: Do research for different kinds of attacks on infrastructure or software

### Resources [links]

- [Operating Systems & Virtualisation Security Knowledge Area Version]({link})
- [Meltdown & Spectre vulnerabilities - Simply Explained]({link})
- [Spectre Explained - The Attack that took the world by surprise in 2018]({link})
- [Different Operating Systems - GeeksforGeeks]({link})
- [CISCO Learning - Binary Game]({link})

---

232 [https://www.youtube.com/watch?v=bs0xswK0eZk&ab_channel=SimplyExplained](https://www.youtube.com/watch?v=bs0xswK0eZk&ab_channel=SimplyExplained)
233 [https://www.youtube.com/watch?v=Phmt8UrofDY&ab_channel=HusseinNasser](https://www.youtube.com/watch?v=Phmt8UrofDY&ab_channel=HusseinNasser)
234 [https://www.geeksforgeeks.org/different-operating-systems/](https://www.geeksforgeeks.org/different-operating-systems/)
# B3. Protection of Data: concerns

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>----</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning objectives (LO)</th>
</tr>
</thead>
</table>
| **LO1**: Learn what is data security  
| **LO2**: Realize what can be learned from someone’s data, and how could a hacker leverage this information.  
| **LO3**: Know what is a cyber warfare  
| **LO4**: Know how is data protected  
| **LO5**: Learn about the confidentiality of data and its importance |

<table>
<thead>
<tr>
<th>Main messages (M)</th>
</tr>
</thead>
</table>
| **M1**: Personal data can reveal all information about a person (places he/she visited, his/her family, thoughts and sensitive information)  
| **M2**: Cybersecurity impacts our life (positively and negatively)  
| **M3**: Social engineering is the term used for a broad range of malicious activities carried out through human interactions.  
| **M4**: Cybersecurity events opened the door for new career paths. |

<table>
<thead>
<tr>
<th>Example of questions to be asked (Q)</th>
</tr>
</thead>
</table>
| **Q1**: Ask the students if any have been attacked, if their social media account was taken or if any personal data was breached.  
| **Q2**: What kind of information do they share on social media accounts?  
| **Q3**: What are possible solutions to face attacks?  
| **Q4**: What do updates and patches help with? |

<table>
<thead>
<tr>
<th>Practical example (P)</th>
</tr>
</thead>
</table>
| **P1**: Two Scenarios: Your Children Could Open You to Attack | DigiCert.com  
| **P2**: Real example: This is how hackers hack you using simple social engineering  
| **P3**: Real Experiment: Amazing mind reader reveals his 'gift'  
| **P4**: A challenge: Hacking challenge at DEFCON |

<table>
<thead>
<tr>
<th>Resources [links]</th>
</tr>
</thead>
</table>
| - 2022 ForgeRock Consumer Identity Breach Report  
| - Watch Out! 5 Most Common Social Engineering Attacks  
| - Understanding and assessing risk in personal data breaches | ICO  
| - What Is Cyber Warfare? | Fortinet  
| - Social Engineering- The art of hacking humans | Prasad Sawant |  
| - TEDxElproIntlSchool |  

---

236 [https://www.digicert.com/blog/children-online-attacks](https://www.digicert.com/blog/children-online-attacks)  
237 [https://www.youtube.com/watch?v=lc7scvxKQOo&ab_channel=oraclemid](https://www.youtube.com/watch?v=lc7scvxKQOo&ab_channel=oraclemid)  
238 [https://www.youtube.com/watch?v=F7pyHN9jC9l&ab_channel=DuvalGuillaume](https://www.youtube.com/watch?v=F7pyHN9jC9l&ab_channel=DuvalGuillaume)  
239 [https://www.youtube.com/watch?v=hHiNWdKw0hY&ab_channel=ConflictInternational](https://www.youtube.com/watch?v=hHiNWdKw0hY&ab_channel=ConflictInternational)  
241 [https://www.youtube.com/watch?v=j5fc0Bfc6&ab_channel=DemakisTechnologies](https://www.youtube.com/watch?v=j5fc0Bfc6&ab_channel=DemakisTechnologies)  
243 [https://fortinet.com/resources/cyberglossary/cyber-warfare](https://fortinet.com/resources/cyberglossary/cyber-warfare)  
244 [https://www.youtube.com/watch?v=lEK84Iv6dxs&ab_channel=TEDxTalks](https://www.youtube.com/watch?v=lEK84Iv6dxs&ab_channel=TEDxTalks)
# B4. Network Standards & Protocols

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>---</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | **LO1**: Learn about what is a network protocol and what is a network standard  
**LO2**: Discover some protocols at the Physical Layer  
**LO3**: Know about basic network components |
| Main messages (M) | **M1**: A protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers.  
**M2**: A standard is a formalized protocol accepted by most of the parties that implement it.  
**M3**: Standards vs Protocols: Protocols are like languages, while Standards are like dictionaries. |
| Example of questions to be asked (Q) | **Q1**: What medium do you use when using your computer connected to the Internet?  
**Q2**: Do you think all protocols are open source? |
| Practical example (P) | **P1**: Bring an RG45 cable in class to define one of the physical mediums.  
**P2**: Give an example of how people can communicate using different languages - It is important to define some guidelines to understand each other and the same goes to network standards.  
**P3**: Activity: **Activity 11 - Tables of Stone—Network Communication Protocols** |
- Physical Layer | Layer 1 | The OSI-Model](https://www.educaplay.com/printablegame/3212017-map_osi_and_tcp_ip_layers.html)  
- Computer network Facts for Kids](https://osi-model.com/physical-layer/)  
- [How The Internet Works? | What Is Internet? | Dr Binocs Show | Kids Learning Video | Peekaboo Kidz](https://www.youtube.com/watch?v=UXsomnDkntI&ab_channel=PeekabooKidz)  
- Network Protocol | TechTerms](https://www.youtube.com/watch?v=BnWn18qUYvA&ab_channel=TechTerms) |
# B4. Network Standards & Protocols

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B3, B4-F</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)

| LO1: | Learn about Protocols at the Network layer |
| LO2: | Learn about Protocols at the Transport layer |
| LO3: | Understand the logic of routing and how packets are transmitted through internet |
| LO4: | Understand what an IP address is |

### Main messages (M)

| M1: | The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. |
| M2: | The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite are commonly categorized as layer-4 protocols within OSI. |
| M3: | An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network, for communication. |
| M4: | Routing is the process of selecting a path for traffic in a network or between or across multiple networks. |

### Example of questions to be asked (Q)

| Q1: | Do you think there are protocols for routing? |
| Q2: | What is the difference between TCP and UDP? |
| Q3: | What is an IP in your own words? |

### Practical example (P)

| P1: | How can an attacker be caught using what you know from this lesson? |
| P2: | Which of the following are possible through network protocols? |
| | - Sending a text message to your friend. |
| | - Visiting [www.google.com](https://www.google.com) |
| | - Connecting your tablet to a wireless network. |
| | - All of these answers are correct. |
| P3: | Activity: Activity 10 - The Orange Game—Routing and Deadlock in Networks |

### Resources [links]

- [tcp vs udp compared and explained in simple terms | CCNA 200-301](https://classic.csunplugged.org/documents/activities/routing-and-deadlock/unplugged-10-routing_and_deadlock.pdf)
- [What is an IP Address? Everything You Need to Know](https://www.youtube.com/watch?v=bDjP6bQLv3M&ab_channel=NETWORKINGWITHH)
- [Understanding Routing! | ICT#8](https://www.youtube.com/watch?v=gQtgtKtvRdo&ab_channel=Lesics)
### B4. Network Standards & Protocols

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B3, B4-F, B4-I</td>
</tr>
</tbody>
</table>

#### Learning objectives (LO)

- **LO1**: Discover some protocols at the Application layer
- **LO2**: Learn about the importance of open-source protocols
- **LO3**: Gain the ability to understand a small network example and define which protocol is acting at which OSI layer
- **LO4**: Learn about protocols used in Cyber attacks

#### Main messages (M)

- **M1**: There are several Application layer protocols: SMTP, HTTP, FTP, POP3, SNMP, DHCP etc.
- **M2**: DNS is a useful protocol used for navigating websites without knowing their IP address.
- **M3**: SMTP is used to send and receive emails.
- **M4**: Protocols can be a target for cyber criminals
- **M5**: TCP can be leveraged for SYN flood attack

#### Example of questions to be asked (Q)

- **Q1**: What would happen if we don’t have DNS?
- **Q2**: Is it good to use a secret protocol? Explain why.
- **Q3**: What is the purpose of HTTP? (provide web pages)
- **Q4**: What is the purpose of FTP? (transfer files)

#### Practical example (P)

- **P1**: Give an example for watching a YouTube video (using which protocols)
- **P2**: What protocol is used when sending an email?
- **P3**: Give a real scenario (like sending an email) and state which protocols are being used

#### Resources [links]

- DNS: Domain Name System - Explained![^256]
- Types of Network Protocols and Their Uses[^257]
- Explaining FTP for Dummies[^258]
- Application Protocols in Computer Network[^259]

[^256]: https://www.youtube.com/watch?v=FJYa6C-MXno&ab_channel=SimplyExplained
[^257]: https://www.w3schools.in/types-of-network-protocols-and-their-uses
[^258]: https://www.youtube.com/watch?v=U0LzX_rTiNw&ab_channel=WidyaLestari
[^259]: https://www.tutorialspoint.com/data_communication_computer_network/application_protocols.htm
## B5. Essentials in Cyber security

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | **LO1:** Learn to Define the CIA Triad  
**LO2:** Understand the Confidentiality  
**LO3:** Understand the Integrity  
**LO4:** Realize the importance of Availability |
| Main messages (M) | **M1:** CIA triad is essential for an organization’s security infrastructure to set the goals and objectives for every security program.  
**M2:** Confidentiality means that only authorized users and processes should be able to access or modify data.  
**M3:** Integrity means that data can be trusted. Prevent unauthorized parties to alter the data.  
**M4:** Availability means that Authorized parties can access and use data anytime. |
| Example of questions to be asked (Q) | **Q1:** What does the CIA stand for?  
**Q2:** Why is the CIA important? |
| Practical example (P) | **P1:** When paying through a credit card, and receiving a Pin number, this is a real example of confidentiality.  
**P2:** The ATM provides availability as it is for public use and is accessible at all times. |
| Resources [links] | - [Cybersecurity Tutorial for Beginners | Introduction to Cybersecurity | Invensis Learning](https://www.youtube.com/watch?v=agnDpN961xU&ab_channel=InvensisLearning) at 9:24 min (Confidentiality), at 9:50 min (Integrity), at 10:15 minute (Availability)  
- [3 Steps to Protect Your Reputation Online](https://www.youtube.com/watch?v=rwigKjEsdTc&ab_channel=ProjectAres)  
- [What is the C.I.A. Triad?](https://www.youtube.com/watch?v=BrjqLE4fiSc&ab_channel=IntellectualPoint)  
- [What is the CIA Triad? Confidentiality, Integrity, Availability](https://www.youtube.com/watch?v=11_Hp5Dvx5E)  
- [Ways to Ensure Data Integrity | Google Data Analytics Certificate](https://www.youtube.com/watch?v=9qCfJv-zoyE)  
- [Quiz: Code-HS Flashcards | Quizlet](https://quizlet.com/627578434/code-hs-flash-cards/)  
- [Cyber Security Full Course for Beginner](https://www.youtube.com/watch?v=U_P23JsJaDc)  
- [Introduction to Cybersecurity Essentials](https://www.coursera.org/learn/introduction-to-cybersecurity-essentials) |
## B5. Essentials in Cyber security

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B4</td>
</tr>
</tbody>
</table>

**Learning objectives (LO)**

- **LO1:** Understand the role of Cryptography in ensuring confidentiality and integrity.
- **LO2:** Understand the scope of Denial of service attacks
- **LO3:** Be able to list some of the attacks linked to CIA triad

**Main messages (M)**

- **M1:** Cryptography secures information by protecting its confidentiality.
- **M2:** Cryptography can also be used to protect information about the integrity and authenticity of data
- **M3:** The CIA is affected by the fact that laws are different all over the world.
- **M4:** A denial-of-service (DoS) attack is a tactic for overloading a machine or network to make it unavailable.
- **M5:** Software vulnerabilities themselves can result in a loss of confidential data including breaches

**Example of questions to be asked (Q)**

- **Q1:** What does DoS attack aim at?
- **Q2:** Do you know other kinds of attacks and what exactly they threaten?
- **Q3:** Why is cryptography used?

**Practical example (P)**

- **P1:** Some software vulnerabilities: (Equifax)- breach of credit card information in 2017
- **P2:** Healthcare information (Anthem) hack: The data was stolen over a period of weeks the month before the data breach was discovered.
- **P3:** Breach of Government records (OPM data breach) 2015
- **P4:** Home assistants attack (Amazon Echo hacks)

**Resources [links]**

- [What Do We Mean By Security Anyway](https://www.brookings.edu/opinions/what-do-we-mean-by-security-anyway/)
- [The CIA Triad: Confidentiality, Integrity, Availability - Panmore Institute](https://panmore.com/the-cia-triad-confidentiality-integrity-availability)
- [TOP 10 biggest data breaches in history](https://www.youtube.com/watch?v=ihOY5I8oPOc&ab_channel=SurfsharkAcademy)
- [5 of the biggest data breaches ever](https://www.youtube.com/watch?v=fIR-RbA-R4s&ab_channel=CNNBusiness)
- [The 66 Biggest Data Breaches (Updated August 2022) | UpGuard](https://www.upguard.com/blog/biggest-data-breaches)
### B5. Essentials in Cyber security

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B4</td>
</tr>
</tbody>
</table>

#### Learning objectives (LO)

- **LO1:** Know the four Elements of Network Security:
- **LO2:** Identify the reason for Network access control.
- **LO3:** Understand why it is important to have Firewall Security.
- **LO4:** Know what is Intrusion prevention system (IPS)

#### Main messages (M)

- **M1:** Network Access Control allows the network admin to control who can/cannot access the network.
- **M2:** Security Firewall defines if a specific traffic should be allowed or blocked in the network
- **M3:** Intrusion Prevention System is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.
- **M4:** Network security is to protect the network, its infrastructure and all its traffic from cyberattacks.

#### Example of questions to be asked (Q)

- **Q1:** Why do we need network security?
- **Q2:** What is a firewall?
- **Q3:** Who takes action in case of an attack?

#### Practical example (P)

- **P1:** If a computer is running without a firewall, it is giving open access to other networks. It is like having your house open for any kind of visitor.
- **P2:** Worksheet: Firewalls worksheet

#### Resources [links]

- Cybersecurity Tutorial for Beginners | Introduction to Cybersecurity | Invensis Learning at 11:30 min
- CIA Triad
- Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data
- What Is a Firewall? - Cisco
- What is Network Security?
- What Is A Firewall? | Firewall Explained | Firewall Tutorial

---

275 https://www.liveworksheets.com/qa2928338ag
276 https://www.youtube.com/watch?v=agnDpN961xU&ab_channel=InvensisLearning
277 https://www.youtube.com/watch?v=gsx0rIrpFlnc&ab_channel=NesoAcademy
280 https://www.paloaltonetworks.com/cyberpedia/what-is-network-security
281 https://www.youtube.com/watch?v=9GZlVOafYTg&ab_channel=Simplilearn
### B6. Attacks, threats, vulnerabilities

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B5</td>
</tr>
</tbody>
</table>

**Learning objectives (LO)**

- **LO1:** Understand what is an adversary and know their types
- **LO2:** Know the difference between vulnerability, threat and attack.
- **LO3:** Learn the objectives of different attacks (ex: Password attack)

**Main messages (M)**

- **M1:** An adversary conducts malicious activity (cyber espionage, crime etc.)
- **M2:** Adversary can be classified into passive/active or Insider/outsider.
- **M3:** A threat could harm an asset while a vulnerability is a weakness that makes a threat possible.
- **M4:** Cyber attacks have different aims (disable, disrupt, destroy etc.)

**Example of questions to be asked (Q)**

- **Q1:** What can be the aim of an attacker?
- **Q2:** What is the difference between insider and external attacker?
- **Q3:** What is the difference between a vulnerability and a vulnerability and a threat?

**Practical example (P)**

- **P1:** Use [haveibeenpwned](https://haveibeenpwned.com/) to check passwords
- **P2:** Games with animation:
  - [ikeepsafe](https://ikeepsafe.org/faux-paw-the-techno-cat/)
  - [Cyber-Five Internet Safety • ABCya](https://www.abcya.com/games/cyber_five_internet_safety)
  - [thinkuknow](https://www.thinkuknow.co.uk/8_10/)
  - [BREACH a data loss prevention game](https://www.educationarcade.co.nz/breach)
- **P4:** Activity [CyberSprinters Wordsearch](https://www.ncsc.gov.uk/files/CyberSprinters-Wordsearch.pdf)

**Resources [links]**

- [Threats, Vulnerabilities, and Attacks](https://www.uobabylon.edu.iq/eprints/publication_3_25852_324.pdf)
- [Videos | NOVA Labs | PBS](https://www.pbs.org/wgbh/nova/labs/videos/#cybersecurity)
- Detailed resource: [Teaching Security](https://teachingsecurity.org/)
- [Attackers and Type of attackers](https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks)
- [15 Types Of Cyber Attacks To Look Out For](https://www.youtube.com/watch?v=NDcEOW8r0xc)
- [What is Malware](https://www.youtube.com/watch?v=QozdEbyMK5E)
### B6. Attacks, threats, vulnerabilities

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B4, B5, B6-F</td>
</tr>
</tbody>
</table>

#### Learning objectives (LO)

- **LO1**: Learn about different kinds of attacks.
- **LO2**: Know what is a malware, Man in the Middle, SQL injection attack.
- **LO3**: Get familiar with Phishing attacks and know how to avoid them.

#### Main messages (M)

- **M1**: Malware refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.
- **M2**: Phishing attack is a type of social engineering attack where an attacker impersonates a trusted contact and sends the victim fake emails.
- **M3**: Password attack is when a hacker cracks your password with various programs and password-cracking tools.
- **M4**: SQL injection attack is the number 1 OWASP attack and it consists of the insertion of a SQL query by the input data.

#### Example of questions to be asked (Q)

- **Q1**: What is a phishing attack?
- **Q2**: What is ransomware?
- **Q3**: What does an SQL injection attack affect in the CIA triad?

#### Practical example (P)

- **P1**: Crack the Code: Breaking a Caesar Cipher | Science Project
- **P2**: An Online experiment Have you taken phishing IQ test?

#### Resources [links]

- [Cybersecurity Tutorial for Beginners](https://www.sciencebuddies.org/science-fair-projects/project-ideas/Cyber_p005/cybersecurity/crack-caesar-cipher) from 13:14 min
- [SQL Injection | OWASP Foundation](https://owasp.org/www-community/attacks/SQL_Injection)
- [Threats to Information Security - GeeksforGeeks](https://www.geeksforgeeks.org/threats-to-information-security/)
- [defending your organisation from email phishing attacks](https://youtu.be/gGoPNrRVUQ)
- [Active games: Free Cyber Security Games | Education Arcade](https://www.educationarcade.co.nz/game-time)
- [Phishing attacks: defending your organisation - NCSC.GOV.UK](https://www.ncsc.gov.uk/guidance/phishing)
## B6. Attacks, threats, vulnerabilities

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B4, B5, B6-F, B-I</td>
</tr>
</tbody>
</table>

**Learning objectives (LO)**

- **LO1:** Realize the different outcomes of security vulnerabilities at the different OSI layers.
- **LO2:** Understand that an adversary can gain information on remote systems and can control the system.
- **LO3:** Learn that both hardware and software are important for security.

**Main messages (M)**

- **M1:** At the physical/link layer, an adversary can observe, modify or jam messages on the link.
- **M2:** At the network layer an attacker may impersonate an address (spoofing) or disrupt communication (Denial of Service)
- **M3:** At the transport layer adversaries can hide their intentions by using port numbers incorrectly or may prevent a device from delivering data to the application.
- **M4:** At the application layer messages sent by the attacker may make the applications stop working or behave in a way that serves the goal of the attacker.

**Example of questions to be asked (Q)**

- **Q1:** What is the relation between the OSI model and the different attacks?
- **Q2:** Where is the Man in the middle attack performed in the OSI model?
- **Q3:** When someone attempts to compromise a target by flooding it with requests from multiple systems that is called a: (choose one answer) 1-DDoS Attack 2-Phishing Scam 3-Virus 4-SSL/TLS layer

**Practical example (P)**

- **P1:** Discuss What Is A Man-in-the-Middle Attack? |
- **P2:** Discuss the different kind of attacks at the application layer

**Resources [links]**

- Cyber security in schools: Practical tips
- Threats, Attacks, and Vulnerabilities | Cyber.org
- internet-traffic-light
- Man in the Middle Attack: Tutorial & Examples | Veracode
- Malware+projects: Course materials for Malware Analysis by RPISEC

---

305 https://www.youtube.com/watch?v=DgqID9k83oQ&ab_channel=Hacksplaining
306 https://resources.infosecinstitute.com/topic/man-in-the-middle-demystified/
308 https://cyber.org/cybersecurity/threats-attacks-and-vulnerabilities
310 https://www.veracode.com/security/man-middle-attack
311 https://github.com/RPISEC/Malware
## B7. Defense against Cyber threats (Cyber Hygiene)

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B2, B3, B5</td>
</tr>
<tr>
<td>Learning objectives (LO)</td>
<td>LO1: Be aware of cyber hygiene practices and their importance. LO2: Know what password hygiene is. LO3: Define what is a Digital Identity.</td>
</tr>
<tr>
<td>Main messages (M)</td>
<td>M1: Cybersecurity hygiene is a set of practices to maintain the health and security of the users, their devices, existing networks and data. M2: Some cyber hygiene practices:  - Patch and update software and use an antivirus  - Avoid giving your sensitive personal information on social media  - Use Multi-Factor Authentication (MFA) and strong passwords  - Use encryption and file encryption protects sensitive data.  - Do not download software from untrusted sources. M3. A digital footprint is data left behind when users have been online.</td>
</tr>
<tr>
<td>Example of questions to be asked (Q)</td>
<td>Q1: How often should you change your password? Q2: What is the importance of updating an application or a software? Q3: What is multi-factor authentication?</td>
</tr>
<tr>
<td>Practical example (P)</td>
<td>P1. Discuss digital footprint: Posting on social media, subscribing to a newsletter, leaving an online review, and what does it say about them P2: Activate the two-factor authentication and show its importance</td>
</tr>
</tbody>
</table>

[^14]: https://www.youtube.com/watch?v=RVX8ZSAR40Y&ab_channel=TEDxTalks
[^16]: https://security.berkeley.edu/education-awareness/back-school-cybersecurity-tips
[^17]: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
[^18]: https://www.pbs.org/wgbh/nova/labs/lab/cyber/
[^19]: https://www.thinkuknow.co.uk/8_10/
## B8. Cryptography

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B5, B6</td>
</tr>
<tr>
<td>Learning objectives (LO)</td>
<td></td>
</tr>
<tr>
<td>LO1:</td>
<td>Know the storyline of Cryptography and its importance.</td>
</tr>
<tr>
<td>LO2:</td>
<td>Understand simple cryptography.</td>
</tr>
<tr>
<td>LO3:</td>
<td>Identify the elements needed to encrypt/decrypt.</td>
</tr>
<tr>
<td>Main messages (M)</td>
<td></td>
</tr>
<tr>
<td>M1:</td>
<td>Cryptography is the art and science of concealing meaning.</td>
</tr>
<tr>
<td>M2:</td>
<td>Encryption is the process of encoding a message.</td>
</tr>
<tr>
<td>M3:</td>
<td>Decryption is the process of converting the encoded message.</td>
</tr>
<tr>
<td>M4:</td>
<td>The Encryption key is necessary for encryption and decryption.</td>
</tr>
<tr>
<td>M5:</td>
<td>Caesar Cipher is an encryption algorithm that shifts the alphabet.</td>
</tr>
<tr>
<td>Example of questions to be asked (Q)</td>
<td></td>
</tr>
<tr>
<td>Q1.</td>
<td>What is the aim of encryption?</td>
</tr>
<tr>
<td>Q2.</td>
<td>Why do we use a key for encryption/decryption?</td>
</tr>
<tr>
<td>Q3.</td>
<td>What is a Caesar cipher?</td>
</tr>
<tr>
<td>Practical example (P)</td>
<td></td>
</tr>
<tr>
<td>P1:</td>
<td>Explain how the enigma worked using The Imitation Game movie.</td>
</tr>
<tr>
<td>P2:</td>
<td>Propose this sentence on the board: “serr cvmmn va gur pnsrgrevn” Give students about 3-5 minutes to work on cracking the message. Answer: &quot;free pizza in the cafeteria&quot; - the A-Z alphabet is shifted to 13 characters.</td>
</tr>
<tr>
<td>P3.</td>
<td>Discuss that this encryption technique took a few minutes to decode a small message. Imagine with a computer how much it would take Resource.</td>
</tr>
<tr>
<td>Resources [links]</td>
<td></td>
</tr>
<tr>
<td>-Cryptographic Protocols</td>
<td><a href="https://www.imdb.com/title/tt2084970/">Classic CS Unplugged</a></td>
</tr>
<tr>
<td>-Activities Interactive: Caesar Cipher - <a href="https://curriculum.code.org/csp-18/unit4/7/">Interactivate</a></td>
<td></td>
</tr>
<tr>
<td>-Activities Interactive: Caesar Cipher II - <a href="https://classic.csunplugged.org/activities/cryptographic-protocols/">Interactivate</a></td>
<td></td>
</tr>
<tr>
<td>-Caesar Cipher II - <a href="http://www.shodor.org/interactivate/activities/CaesarCipher/">Interactivate</a></td>
<td></td>
</tr>
<tr>
<td>-Caesar Cipher III - <a href="http://www.shodor.org/interactivate/activities/CaesarCipherTwo/">Interactivate</a></td>
<td></td>
</tr>
<tr>
<td>-Cryptography: Crash Course Computer Science #33 <a href="http://www.shodor.org/interactivate/activities/CaesarCipherThree/">CrashCourse</a></td>
<td></td>
</tr>
<tr>
<td>-How to Explain Modern Security Concepts to your Children <a href="https://hal.archives-ouvertes.fr/hal-01397035/document">Children</a></td>
<td></td>
</tr>
<tr>
<td>B8. Cryptography</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Level</strong></td>
<td>Intermediate (I)</td>
</tr>
<tr>
<td><strong>Prerequisites</strong></td>
<td>B1, B2, B3, B4, B5, B6, B8-F</td>
</tr>
</tbody>
</table>
| **Learning objectives (LO)** | LO1: Relate the CIA triad with respect to cryptography.  
LO2: Understand key management.  
LO3: Differentiate between symmetric and asymmetric cryptography. |
| **Main messages (M)** | M1: Symmetric encryption involves one key for encryption and decryption.  
M2: Public key encryption/Asymmetric encryption involves two keys.  
M3: Key management is the management of cryptographic keys in a cryptosystem by generating, exchanging, storing, using and replacing keys. |
| **Example of questions to be asked (Q)** | Q1: What is the difference between asymmetric and symmetric cryptography?  
Q2: How are the cryptographic keys managed?  
Q3: Why do we need key management? |
| **Practical example (P)** | P1: Discuss the following: "How can two people send encrypted messages to each other if they can't communicate, or agree on an encryption key ahead of time, and the only way they have to communicate is over the Internet?"  
P2: Practical sheet online: U4L09 Activity Guide - Public Key Bean Counting  
P3: Make a comparison between private and public keys.  
P4: Discuss with students what would happen if a symmetric cipher used a different key to decrypt. |
| **Resources [links]** | - The Internet: Encryption & Public Keys  
- Sheets: Kid krypto—Public-key encryption  
- Presentation 6: Privacy and Encryption - Children and Technology  
- UNIT 16 Modern Encryption Teacher Resource Material  
- The Public Key  
- Public Key Cryptography - Computerphile  
- Digital Signatures  
- Games: Solve the Cryptoquote, RSA Encryption and Decryption, Difference between Symmetric and Asymmetric encryption |

333 https://docs.google.com/document/d/1l0KDF33-gWIsZGqfuHgD0QpF50Pdyqras46FeuNLgc/edit  
334 https://www.youtube.com/watch?v=ZghMPWGxexs&ab_channel=Code.org  
336 https://sites.google.com/site/childrenandtechnology/Home/presentation-6-privacy-and-encryption  
337 https://www.cimt.org.uk/resources/codes/codes_u16_tr.pdf  
338 https://nrich.maths.org/2184  
339 https://www.youtube.com/watch?v=GSIDS_JvRv4&ab_channel=Computerphile  
340 https://demonstrations.wolfram.com/SolveTheCryptoquote/  
341 https://demonstrations.wolfram.com/RSAEncryptionAndDecryption/  
342 https://www.youtube.com/watch?v=gRec1hWXFo0&ab_channel=KnowledgePowerhouse
## B8. Cryptography

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B4, B5, B6, B7, B8-F, B8-I</td>
</tr>
</tbody>
</table>

**Learning objectives (LO)**

- **LO1**: Learn what is a Hash function
- **LO2**: Know the relation of hash functions and passwords
- **LO3**: Be able to list some attacks done on ciphers

**Main messages (M)**

- **M1**: Hash functions are an important cryptographic primitive and they compute a digest of a message which is a short, fixed-length bit-string.
- **M2**: Hash functions are used to store passwords and then a hacker can just get access to the encrypted “hash” created by your password in case of an attack.
- **M3**: Chosen plaintext attacks are very famous and that was how Turing and his team broke the ENIGMA machine during the Second World War.

**Example of questions to be asked (Q)**

- Q1. How are passwords stored?
- Q2. What is the name of the output of a hash function?
- Q3. What was the attack that broke the Enigma?

**Practical example (P)**

- P1: Make the students check their passwords using [Password Checker](https://www.security.org/how-secure-is-my-password/)

**Resources [links]**

- A complete lesson with activity for: [Public Key Cryptography](https://curriculum.code.org/csp-18/unit4/9/)
- Advanced sheet: [Public Key Cryptography](https://www.nrich.maths.org/2200)
- [The Knapsack Problem and Public Key Cryptography](https://nrich.maths.org/2199)
- Course: [Code-Based Cryptography - Course - FUN MOOC](https://nrich.maths.org/2200)
- Book: (PDF) [Understanding Cryptography: A Textbook for Students](https://www.cimt.org.uk/resources/codes/codes_u1_tr.pdf)
- Worksheets: [Substitution Ciphers](https://www.nrich.maths.org/2200) [Encryption And Decryption](https://www.nrich.maths.org/2200)
- Advanced course: [NIH Information Security Awareness Course](https://www.healthit.gov/its-training/online-training/nihsaacertified-sa-awareness-course)
## B9. Individual Incidents Responses

<table>
<thead>
<tr>
<th>Level</th>
<th>Foundation (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B2, B6, B8-F</td>
</tr>
</tbody>
</table>

### Learning objectives (LO)
- **LO1**: Know the steps that could be done in case of an attack
- **LO2**: Understand what is the Incident Response (IR).
- **LO3**: Realize that every company/organization should have an IR

### Main messages (M)
- **M1**: Incident Response is the effort to identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.
- **M2**: Steps for IR are: Preparation, Detection, Containment, Recovery, and Lessons.
- **M3**: An individual should: Change passwords after an attack, use Two-factor authentication on all accounts, ask for help in case sensitive data was attacked (e.g. bank account) and alert the family and friends in case of a phishing attack.

### Example of questions to be asked (Q)
- **Q1**: What is the first step you take in case your social account was hacked?
- **Q2**: What is Two-factor authentication?
- **Q3**: Do you know what is the name of the plan done after a cyber attack?

### Practical example (P)
- **P1**: Discuss ideas presented here: [Security Tip: I'm Hacked, Now What?](https://www.shsu.edu/dept/it@sam/newsletter/july-2016/security-tip.html)
- **P2**: You can practice with them how to activate Two Factor Authentication

### Resources [links]
- [What is incident response in cyber security](https://www.youtube.com/watch?v=NL1ShMo4Gm4)
- [3 Benefits of an Incident Response Plan - Cybriant](https://cybriant.com/incident-response-plan/)
- [Good Practice Guide for Incident Management (ENISA)](https://studentprivacy.ed.gov/content/guidance-videos)
- [Student Guide for CyberSecurity Awareness](https://studentprivacy.ed.gov/content/guidance-videos)
- [A College Students Guide](https://www.cdse.edu/Portals/124/Documents/student-guides/CS130-guide.pdf?ver=00gYkCPZlAxxAVjUFdDQ5Q%3D%3D)
- [Cyber Security Threats: How Students Can Protect Their Data](https://www.security.org/resources/college-guide-data-cyber-protection/)
- [The 7 things you need to do if you get hacked](https://ivypanda.com/blog/cyber-security-threats/)
- [Online games: Cybersecurity Games](https://www.security.org/resources/college-guide-data-cyber-protection/)
- [NCSC - Cyber Sprinter](https://it.tamu.edu/security/cybersecurity-games/index.php)

---

357 [https://www.shsu.edu/dept/it@sam/newsletter/july-2016/security-tip.html](https://www.shsu.edu/dept/it@sam/newsletter/july-2016/security-tip.html)
358 [https://www.youtube.com/watch?v=NL1ShMo4Gm4](https://www.youtube.com/watch?v=NL1ShMo4Gm4)
360 [https://studentprivacy.ed.gov/content/guidance-videos](https://studentprivacy.ed.gov/content/guidance-videos)
362 [https://www.cdse.edu/Portals/124/Documents/student-guides/CS130-guide.pdf?ver=00gYkCPZlAxxAVjUFdDQ5Q%3D%3D](https://www.cdse.edu/Portals/124/Documents/student-guides/CS130-guide.pdf?ver=00gYkCPZlAxxAVjUFdDQ5Q%3D%3D)
364 [https://ivypanda.com/blog/cyber-security-threats/](https://ivypanda.com/blog/cyber-security-threats/)
365 [https://www.money.co.uk/guides/the-7-things-you-need-to-do-if-you-get-hacked](https://www.money.co.uk/guides/the-7-things-you-need-to-do-if-you-get-hacked)
# B10. Capture the Flag

<table>
<thead>
<tr>
<th><strong>Level</strong></th>
<th><strong>Foundation (F)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td>B1, B2, B4, B6</td>
</tr>
</tbody>
</table>

| **Learning objectives (LO)** | **LO1**: Get familiar with the term CTF and why it is important.  
**LO2**: Realize the different types of CTF.  
**LO3**: Build the courage to try new challenges. |

| **Main messages (M)** | **M1**: CTF provides the perfect opportunity to play around with vulnerabilities and better understand the context they operate in.  
**M2**: CTF gives the feeling of solving a particularly difficult task and seeing all the puzzle pieces click together.  
**M3**: There are two main types of CTFs: Jeopardy-style and Attack-Defense-style. |

| **Example of questions to be asked (Q)** | **Q1**: What does CTF stand for?  
**Q2**: How many types of CTF are there?  
**Q3**: What are the advantages of CTF? |

| **Practical example (P)** | **P1**: Some examples: [ctflearn](https://ctflearn.com/)  
**P2**: Start a team to work together for a CTF, or make the students search online for CTF teams (Hacking forums and infosec discord channels are also good for this) |

| **Resources [links]** | See Introduction to CTF at Google Developer Student Clubs  
Capture-The-Flag Competitions: all you ever wanted to know  
Full course: [Capture the Flag - Cyber Security Base 2022](https://cybersecuritybase.mooc.fi/module-6.1/index)  
Challenges: [Easy challenges](https://csb-capture-the-flag.cs.helsinki.fi/ctf/)  
Platform: [HackTheBox](https://www.hackthebox.com/)  
-Hacking-Lab  
Online CTF events: [CTFTime](https://ctftime.org/)  
-Capture the Flag - Cyber Security Base 2022 |
## B10. Capture the Flag

<table>
<thead>
<tr>
<th>Level</th>
<th>Intermediate (I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B4, B6, B7, B10-F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning objectives (LO)</th>
<th>LO1: Know some tools and platforms for CTF. LO2: Develop Team spirit and learn cooperative work</th>
</tr>
</thead>
</table>

| Main messages (M) | M1: CTF and wargame are good to maintain technical skills . M2: Jeopardy-style CTFs are a list of hacking challenges that you can complete for flags that are worth a certain number of points. M3 Attack-and-Defense-style CTF is when teams defend their own servers against attack, and attack opponents' servers to score (ex: DEFCON^377) M4: Attack-and-Defense-style CTF: Competitor needs to patch(fix) the vulnerability and exploit(attack) the other teams. |

<table>
<thead>
<tr>
<th>Example of questions to be asked (Q)</th>
<th>Q1: What is a flag? Q2: Why do we submit a flag?</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Practical example (P)</th>
<th>P1: Prepare a VM with different challenges. P2: Practical examples: Challenges » CyberTalents^378</th>
</tr>
</thead>
</table>

|-------------------|-------------------------------------------------------------------------------------------------|

---

^377 https://defcon.org/
^378 https://cybertalents.com/challenges
^379 https://tryhackme.com/
^380 https://trailofbits.github.io/ctf/
^381 https://cybersecuritybase.mooc.fi/module-6.1/index
^382 https://github.com/IgniteTechnologies/CTF-Difficulty#easy
^383 https://github.com/IgniteTechnologies/Vulhub-CTF-Writeups
^384 https://github.com/IgniteTechnologies/TryHackMe-CTF-Writeups
^385 https://github.com/IgniteTechnologies/HackTheBox-CTF-Writeups
^386 https://github.com/enaqx/awesome-pentest#ctf-tools
^387 https://github.com/moloch--/RootTheBox
^388 https://github.com/facebookarchive/lbctf
^389 https://ctfd.io
^390 https://picocft.com/
^391 https://github.com/OWASP/SecurityShepherd
^392 https://github.com/Nakiami/mellivora
^393 https://github.com/mcpa-stlouis/hack-the-arch
### B10. Capture the Flag

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1, B2, B3, B4, B5, B6, B7, B8, B10-F, B10-I</td>
</tr>
</tbody>
</table>

#### Learning objectives (LO)

- **LO1** Solve some CTF examples and challenges
- **LO2** Be familiar with CTFs steganography and Cryptography
- **LO3** Use some of the CTF famous tools with at least one known platform

#### Main messages (M)

- **M1**: CTFs challenges are typically divided into categories.
- **M2**: Some famous tools in CTF are: binwalk, burp suite, stegsolve, GDB and the command line
- **M3**: Some famous Advanced CTF competitions: DEFCON, PlaidCTF, CodeGate, SECCON, PHD Qals

#### Example of questions to be asked (Q)

- **Q1**: What do we call hiding a text in an image?
- **Q2**: What would help you in case you are blocked in a CTF?

#### Practical example (P)

- **P1**: More difficult exercises: [OverTheWire](https://overthewire.org/wargames/)
- **P2**: Practical examples: [Challenges » CyberTalents](https://cybertalents.com/challenges)
- **P3**: Mitre exercises: [MITRE Cyber Academy · GitHub](https://github.com/mitre/cyber-academy)

#### Resources [links]

- Full course: [Capture the Flag - Cyber Security Base 2022](https://cybersecuritybase.mooc.fi/module-6-1/index)
- List of challenges: [Easy challenges](https://github.com/SpiderLabs/CryptOMG)
- [CryptOMG CTF](https://github.com/Ignitetechnologies/Vulnhub-CTF)
- [Vulnhub-CTF](https://github.com/Ignitetechnologies/HackTheBox-CTF-Writeups)
- Online hacking competition designed to educate high schoolers in computer [HSCTF](https://github.com/Ignitetechnologies/Vulnhub-CTF-Writeups)
- GitHub - [Aksheet10/Cyber-Security-Resources](https://github.com/Aksheet10/Cyber-security-resources)
- A famous CTF: [Google CTF](https://capturetheflag.withgoogle.com/)
**B11. Penetration testing**

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1→B10</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1 Know the difference between harmful hacking and Ethical hacking/Pentesting  
LO2 Know what is the OWASP Top 10  
LO3 Get familiar with some of the tools and frameworks for pentesting. |
| Main messages (M) | M1: Pentesting helps to learn how to handle any type of break-in.  
M2: Penetration testers use an outlined scope (NIST 406, PTES 407, OWASP 408)  
M3: Gathering information about the target is the first step in Pentesting and can be done using different tools (Nmap, metasploit etc.) |
| Example of questions to be asked (Q) | Q1: What is the first step in Pentesting?  
Q2: Ethical hacking is something dangerous to do, is this correct?  
Q3: What is an SQL Injection? |
| Practical example (P) | P1: Use the hydra tool to crack a password Hydra Bruteforce Attack 409  
P2: Use wpscan to crack a WordPress page  
P3: Analyze a Wireshark packet (p:15 Defensive Hacking 410)  
P4: Additional worksheet for Password hacking: Pass 411 |
| Resources [links] | - Lessons: Lessons 412 PortSwigger 413  
- Root Me 414 devguru-1 415 pwned-1 416 cybox-1 417 razrsec 418  
- Pentesting Basics | Hacker101 419  
- Create the red team and blue team at home: hauser 421  
- Vulnerable Web (DSVW): DSVW 422  
- Vulnerable machine: Metasploitable 423  
- Events of hacking/training: Hacking-Lab 424  
- https://drive.google.com/file/d/1thlYoYnfsNgNuAh7v7rOxjKBvUQUWHyqNO/view  
- https://drive.google.com/file/d/1cMHo9JKeIwcvvqOH9bWLSNpPxkLL_U/view  
- https://www.youtube.com/watch?v=EA1H0QHZq8&ab_channel=TypicallyEthical  
- razrsec  
- https://www.hacker101.com/2021/03/04/creating-a-red-blue-team-home-lab/  
- https://github.com/stamparm/DSVW  
- https://github.com/rapid7/metasploitable3  
- https://www.hacking-lab.com/events/ |
## B12. Roles in Cybersecurity and Top Certifications

<table>
<thead>
<tr>
<th>Level</th>
<th>Advanced (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>B1→ B11</td>
</tr>
</tbody>
</table>
| Learning objectives (LO) | LO1 Realize that there is an increasing demand for people in Cybersecurity.  
LO2 Know the kind of posts and working domains in cyber security.  
LO3 Know some of the most famous certifications. |
| Main messages (M) | M1: The market is fast evolving to respond to a fundamental trend which is the digital transformation of companies and administrations [link](https://www.idc.com/getdoc.jsp?containerId=prEUR149609822).  
M2: There are many posts available in cybersecurity domain like: Security Engineer, Chief Information Security Officer, Security Analyst, Computer Forensics, Security Consultant, Digital Forensics, Cryptographer Security Administrator, Penetration Tester, etc.  
M3: All sectors need a cyber security employee to guarantee the security of the data and systems (Financial, Insurance Sector, Healthcare, Environmental, Energy, Government, Transportation, Food, and Agriculture)  
M4: Certifications are a good way to validate your security level and find a better post (CISA, CEH, CISSP, Pen Testing, etc.) |
| Example of questions to be asked (Q) | Q1: Do you think the demand for cybersecurity has decreased compared to the past years?  
Q2: What is the reason for an increasing demand in cybersecurity?  
Q3: Give some examples of security professional roles you know |
| Practical example (P) | P1: Do research about the available roles in cyber security and discuss them.  
P2: Discuss the different certifications available and their importance. |
| Resources [links] | - Popular Certifications: [Certifications](https://cybersecurityguide.org/programs/cybersecurity-certifications/cryptography/)  
- Cyber Security Career[link](https://www.coursera.org/articles/popular-cybersecurity-certifications)  
- Will Smith's Cybersecurity Career Map - Xmind[link](https://www.youtube.com/watch?v=BlsW9jp9NJM&ab_channel=Simplilearn)  
- Cybersecurity Domain Map ver 3.0[link](https://xmind.app/m/97mj/)  
- Cybersecurity education and workforce needs in Europe[link](https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/)  
- Cybersecurity HR Recruitment[link](https://ecs-org.eu/documents/publications/6202804a65a70.pdf)  
- How can I develop a career in Cybersecurity? [link](https://digital-skills-jobs.europa.eu/en/community/online-discussions/how-can-i-develop-career-cybersecurity) |
## Annex – Education related initiatives in Europe

<table>
<thead>
<tr>
<th>Title and link</th>
<th>Short description</th>
<th>Language</th>
<th>Age segment addressed</th>
<th>Topics addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safer Internet Centers</strong>[^435]</td>
<td>Inform, advise and assist children, parents, teachers, and carers on digital questions and fights against children’s online abuse. Co-funded by the European Commission and run over national awareness centres organised by Insafe[^436] and INHOPE[^437] networks.</td>
<td>EN</td>
<td>Children and youth</td>
<td>Cybersafety, cyberbullying, grooming and data privacy.</td>
</tr>
<tr>
<td><strong>Croatian Society of Young Informaticians</strong>[^438]</td>
<td>Croatian roof organisation of young informaticians running initiatives and campaigns on diverse cyber security topics, involving also teachers.</td>
<td>HR</td>
<td>Youth</td>
<td>Diverse cyber security topics</td>
</tr>
<tr>
<td><strong>SINI platform</strong>[^439]</td>
<td>Platform related to topics of safe internet for children and youth. The platform also offers webinars and related information for teachers and parents.</td>
<td>HR</td>
<td>Children and youth</td>
<td>Cybersafety, cyberbullying, grooming and data privacy.</td>
</tr>
<tr>
<td><strong>klicksafe</strong>[^440]</td>
<td>Klicksafe is a part of the German Awareness Centre under the initiative of the EU[^441].</td>
<td>DE</td>
<td>Children and youth</td>
<td>Save use of internet.</td>
</tr>
</tbody>
</table>

[^436]: [https://www.betterinternetforkids.eu](https://www.betterinternetforkids.eu)
[^437]: Educational resources available at [https://www.betterinternetforkids.eu/resources](https://www.betterinternetforkids.eu/resources)
[^438]: [https://hsin.hr/](https://hsin.hr/)
[^439]: [https://sini.hr/](https://sini.hr/)
[^440]: [https://www.klicksafe.de/](https://www.klicksafe.de/)
[^441]: [https://www.saferinternet.de/](https://www.saferinternet.de/)
<table>
<thead>
<tr>
<th>Platform</th>
<th>Description</th>
<th>Language</th>
<th>Target Audience</th>
<th>Cybersecurity Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberstart</td>
<td>Cyber security training (fee-paying) brought to life through real-world hacking challenges and puzzles.</td>
<td>EN</td>
<td>Youth, young adults</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>Microsoft Learn</td>
<td>Free curriculum, training, and tools for teaching.</td>
<td>EN</td>
<td>Not defined</td>
<td>Diverse cybersecurity topics</td>
</tr>
<tr>
<td>Internet Segura Kids</td>
<td>EU funded initiative in Spain on internet safety. Different information and material provided for children, youth, parents and teachers.</td>
<td>ES</td>
<td>Children and youth</td>
<td>Mostly cybersafety</td>
</tr>
<tr>
<td>Tonis Escape dem Hacker auf der Spur</td>
<td>Online game for youth that can be used as part of lectures. Part of the German national initiative funded by the BMBF where security topics are covered.</td>
<td>DE</td>
<td>Age 12-15</td>
<td>Cybersecurity, security in smart homes, authentication and security of AI.</td>
</tr>
<tr>
<td>CyberSchool</td>
<td>Program run by Foundation cyber school that organizes workshops for cyber safety and awareness in schools with the involvement of teachers.</td>
<td>NL</td>
<td>Children and youth</td>
<td>Cybersafety and cybersecurity awareness</td>
</tr>
<tr>
<td>DataDetox</td>
<td>Offers an 8-day program and game about data awareness, that is suitable for explanations and use during the lectures.</td>
<td>NL</td>
<td>Children and youth</td>
<td>Data privacy</td>
</tr>
</tbody>
</table>

442 https://cyberstart.com/
443 https://docs.microsoft.com/en-gb/learn/educator-center/programs/msle/
444 https://www.is4k.es/de-utilidad/recursos?utm_source=notas%20de%20prensa&utm_medium=mmcc&utm_campaign=IS4K
445 https://www.is4k.es/materiales-didacticos
446 https://tonis-escape.sichere-digitale-zukunft.de/v1.0/
447 https://www.sichere-digitale-zukunft.de/it-sicherheitsforschung-f%C3%BCr-den-unterricht
448 https://www.sichere-digitale-zukunft.de/
449 https://stichtingcyberschool.nl/
450 https://data-detox.nl/
<table>
<thead>
<tr>
<th>Project Name</th>
<th>Description</th>
<th>Language(s)</th>
<th>Age Group(s)</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DataDetoxKit</strong></td>
<td>Guide through everyday steps one can take to control digital privacy, security, and wellbeing.</td>
<td>Multilingual</td>
<td>Not defined</td>
<td>GDPR, Data privacy</td>
</tr>
<tr>
<td><strong>De baas op internet</strong></td>
<td>The programme &quot;The boss on the internet&quot; about internet safety offering also material for teachers.</td>
<td>NL</td>
<td>Children but also youth at age of 14</td>
<td>Internet safety</td>
</tr>
<tr>
<td><strong>It's up you</strong></td>
<td>Interactive video about cyberbullying that can be used in class.</td>
<td>NL</td>
<td>Youth</td>
<td>Cyberbullying</td>
</tr>
<tr>
<td><strong>CyberEDU</strong></td>
<td>Flexible and practical training solutions tailored to knowledge level. Users can learn how to identify vulnerabilities and/or react in incident response situations as a preparation for real-world situations.</td>
<td>EN</td>
<td>Youth, young adults</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td><strong>UNbreakable Romania</strong></td>
<td>Romanian national contest for high-school students and university students</td>
<td>RO</td>
<td>Youth, young adults</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td><strong>My Data done right</strong></td>
<td>Help in access, remove, correct, move your data from specific platforms</td>
<td>Multilingual</td>
<td>Not defined</td>
<td>GDPR</td>
</tr>
<tr>
<td><strong>Cybersafety</strong></td>
<td>National platform gathering different initiatives and bringing closer cyber safety topics to children.</td>
<td>EL</td>
<td>Mostly children</td>
<td>Cybersafety</td>
</tr>
<tr>
<td><strong>Education game “The Witch’s Secret”</strong></td>
<td>Interactive game teaching basics of cryptography methods.</td>
<td>EN</td>
<td>Youth, young adults</td>
<td>Cryptography</td>
</tr>
</tbody>
</table>

451 https://datadetoxkit.org/en/home  
452 https://debaasopinternet.nl/info  
453 https://debaasopinternet.nl/content/2-aan-de-slag/1-wie-mag-alles-van-me-weten/debaasopinternet-privacy-leerkrachtinstructie.pdf  
454 https://itsuptoyou.nu/  
455 https://cyberedu.ro  
456 https://unbreakable.ro/  
457 https://www.mydatadoneright.eu/  
458 https://cybersafety.cy/  
459 http://public.tel.fer.hr/witch/
<table>
<thead>
<tr>
<th><strong>E-LearningScape game</strong></th>
<th>Educational game developed by Sorbonne University</th>
<th>FR</th>
<th>youth</th>
<th>Cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybermalveillance</strong></td>
<td>Official governmental site with relevant information and guidelines.</td>
<td>FR</td>
<td>Children and youth</td>
<td>Cybersecurity and cybersafety</td>
</tr>
<tr>
<td><strong>E-Enfance</strong></td>
<td>Governmental supported initiative on spreading information targeted to different age groups.</td>
<td>FR</td>
<td>Children and youth</td>
<td>cybersafety</td>
</tr>
<tr>
<td><strong>Internet licence for children</strong></td>
<td>Educational information and material</td>
<td>FR</td>
<td>Children</td>
<td>cybersafety</td>
</tr>
<tr>
<td><strong>EDUSCOL</strong></td>
<td>Governmental official material and guidelines for teachers</td>
<td>FR</td>
<td>Children and youth</td>
<td>Cybersecurity and cybersafety</td>
</tr>
<tr>
<td><strong>Fables la fontaine cyberse</strong></td>
<td>4 fables of La Fontaine diverted to raise awareness of cyber security</td>
<td>FR</td>
<td>Children and youth</td>
<td>Cybersecurity and cyber safety</td>
</tr>
</tbody>
</table>

460 [https://webia.lip6.fr/~muratetm/elearningscape/?fbclid=IwAR3f8VUV7K3CCvMplW1AGmuylVbVfEj_yqFxbYgaUV0vChqAaq_SWhntJMKLA](https://webia.lip6.fr/~muratetm/elearningscape/?fbclid=IwAR3f8VUV7K3CCvMplW1AGmuylVbVfEj_yqFxbYgaUV0vChqAaq_SWhntJMKLA)
462 [https://e-enfance.org/](https://e-enfance.org/)
463 [https://permisinternet.com/](https://permisinternet.com/)
464 [https://eduscol.education.fr/](https://eduscol.education.fr/)
| **Cybersecurity: The 4 Hack Academy films CIGREF**<sup>466</sup> | Cybersecurity campaign films | FR | youth | Cybersecurity |
| Guide Des Bonnes Pratiques De L’informatique<sup>467</sup> | CPME ANSSI / 12 rules for security | FR | Youth and adults | Cybersecurity and cyber safety |
| **Game “1,2,3 Cyber”**<sup>468</sup> | Online free available material for the game developed by Centre de la Cybersécurité pour les Jeunes<sup>469</sup> and company Wavestone. | FR | 11-14 years | Cybersecurity |
| **Capitaine Cyber**<sup>470</sup> | 5 videos made for security hygiene | FR / by Belgium | Youth | Cybersecurity |
| **Cyber security games for school**<sup>471</sup> | Worksheet and examples for students | FR | Youth | Cybersecurity |
| **gca toolkit by Global Cyber Alliance**<sup>472</sup> | Free and effective tools that you can use now to take immediate action to reduce the risks to your business. | FR | Youth | Cybersecurity |
| **Commission nationale de l’informatique et des libertés**<sup>473</sup> CNIL | 5 cyber Modules with activities and attestation at the end. | FR | Youth | Cyber security |
| **L’essentiel de la securite numerique**<sup>474</sup> | A full guide for cyber security, written by the greatest minds in the Academia and Industry | FR | Professional s | Cyber security |

### Guide Cybersecurite 475
by Cyber Malveillance

A good guide with practical examples.

<table>
<thead>
<tr>
<th>FR</th>
<th>Managers of small and medium sized companies</th>
<th>Cyber security</th>
</tr>
</thead>
</table>

### Tous en ligne maintenancen 476 - Funded by the French government

Public and private players with one objective in mind: to support the success of small businesses through digital technology/ Online cyber security coaching

<table>
<thead>
<tr>
<th>FR</th>
<th>Youth</th>
<th>Cyber security</th>
</tr>
</thead>
</table>

### Project SAFE.SI 477

Inform, advise and assist children, parents, teachers and carers on digital questions and fights against online child sexual abuse. Offers (not regularly) courses and seminars, especially for teachers.

Co-funded by the European Commission and as national awareness centre

<table>
<thead>
<tr>
<th>SI</th>
<th>Children and youth</th>
<th>Cybersafety, cyberbullying, grooming and data privacy</th>
</tr>
</thead>
</table>

### Educational network 478

Slovenian roof organisation for education about the internet for youth. Seminars are offered, but not on regular basis. A platform for chatting module.

<table>
<thead>
<tr>
<th>SI</th>
<th>Youth (from secondary and primary school)</th>
<th>Basic knowledge about internet and safety</th>
</tr>
</thead>
</table>

### Slovenian education and research network education initiative 479

Regular educational platform providing webinars for school students and teachers about safe internet use.

<table>
<thead>
<tr>
<th>SI</th>
<th>Mostly youth</th>
<th>Safe internet use</th>
</tr>
</thead>
</table>

---

475 [https://www.cybermalveillance.gouv.fr/medias/2021/05/Guide-de-cybers%C3%A9curit%C3%A9-des-tarten-des-dirigeants-de-TPE-PME-et-EI.pdf](https://www.cybermalveillance.gouv.fr/medias/2021/05/Guide-de-cybers%C3%A9curit%C3%A9-des-tarten-des-dirigeants-de-TPE-PME-et-EI.pdf)
476 [https://tousen lignemaintenant.fr/](https://tousen lignemaintenant.fr/)
477 [https://safe.si/](https://safe.si/)
478 [https://sio.si/tag/varna-raba-interneta/](https://sio.si/tag/varna-raba-interneta/)
479 [https://www.arnes.si/storitve/varnost/most-v/](https://www.arnes.si/storitve/varnost/most-v/)