12

cybersafety modules

12

cybersecurity modules

470+

fitted resources

Teaching cybersecurity & cybersafety in high school

The CONCORDIA Methodology and Guidelines in support of teachers

Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cybersecurity cOmpeteNCe fOr Research anD InnovAtion[1]

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

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

[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

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany

CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia
ICENT	Innovation Centre Nikola Tesla	Croatia
Utilis	Utilis d.o.o	Croatia
Polito	Politecnico di Torino	Italy

Table of Contents

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

[2] https://www.eacea.ec.europa.eu/news-events/news/new-publication-eurydice-report-informatics-education-school-europe-2022-09-29_en

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.

[3] https://www.concordia-h2020.eu/wp-content/uploads/2021/12/TEACHING-CYBERSECURITY-IN-HIGH-SCHOOL-survey_report.pdf

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
[5] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC83167/lb-na-26035-enn.pdf
[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

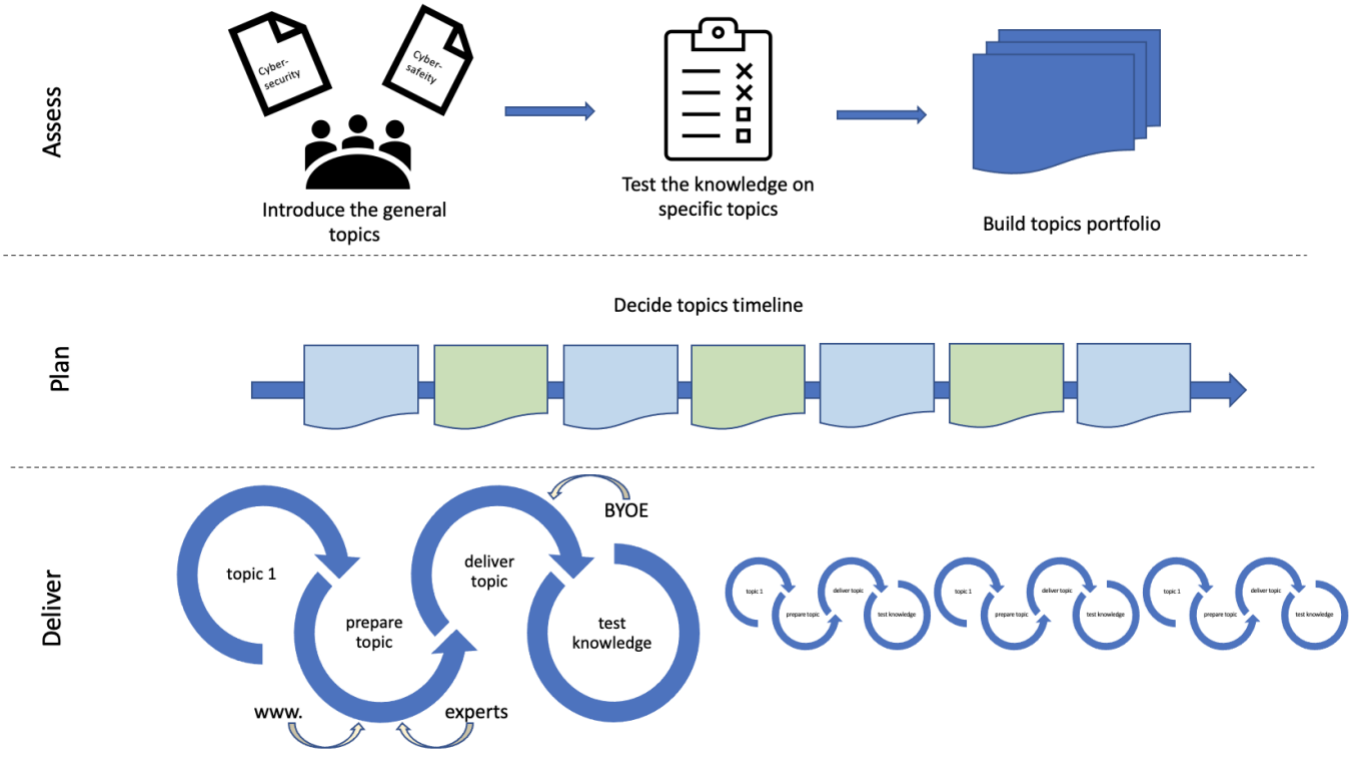
Step 1. Kickstart the discussion on the cybersafety and cybersecurity topics
Step 2. Test the group knowledge level
Step 3. Build the class portfolio

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[9]), 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[10]*

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[11], Women4Cyber Chapters[12], and the Women Know Cyber: The Documentary[13].

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

[9] 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
[10] https://digital-strategy.ec.europa.eu/en/policies/safer-internet-centres
[11] https://www.concordia-h2020.eu/meet-the-women-in-concordia/
[12] https://women4cyber.eu/w4c-chapters
[13] https://www.youtube.com/watch?v=Kpc31WJ6l2M&t=439s

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 Asses - 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
- The main messages to be conveyed - per difficulty level
- Suggestions of questions to be asked during the class
- Suggestion 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.

A. Cybersafety topics			**B. Cybersecurity topics**		
A0. Why discussing cybersafety	A.TEST Testing the group level		B0. Why study cybersecurity	B.TEST Testing the group level	
A1. Personal / Sensitive Data and Privacy	A2. Cyberbullying and Sexual Harassment	A3. Inappropriate Content	B1. OSI Model	B2. Operating systems (OS), Computer Hardware, and how does a computer work	B3. Protection of Data: concerns
A4. Hate speech	A5. Fake profiles, Fraud, and Phishing	A6. The importance of Strong Passwords	B4. Network Standards and Protocols	B5. Cyber security essentials (CIA triad)	B6. Attacks, Threats, Vulnerabilities
A7. Addiction	A8. Keep my online account safe	A9. Stay safe in Online Social Networks	B7. Defense against Cyber threats (Cyber hygiene)	B8. Cryptography	B9. Individual Incident Management
A10. Online Games	A11. Fake News	A12. Transparency of Recommendation Algorithms	B10. Capture the Flag	B11. Penetration testing/ trainings	B12. Roles in Cybersecurity and Top10 certifications

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.

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

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

	PREREQUISITES											
Module	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
A1	x											
A2	x											
A3	x											
A4												
A5	x				x							
A6	x					x						
A7												
A8						x						
A9	x	x	x	x	x	x	x	x				
A10	x	x	x	x	x	x	x					
A11					x					x		
A12	x											x

A0. Why discussing cybersafety	
Level	**Foundation**
Prerequisites	---
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
[15] https://legaljobs.io/blog/privacy-statistics/
[16] https://www.forbes.com/sites/tarahaelle/2017/02/28/online-risks-are-everyday-events-for-teens-but-they-rarely-tell-their-parents/?sh=431bb1f03861
[17] https://www.youtube.com/watch?v=uquRzrcwA18
[18] https://www.youtube.com/watch?v=DiI8Lj0_TGQ
[19] https://www.youtube.com/watch?v=yrln8nyVBLU&ab_channel=watchwellcast
[20] https://www.youtube.com/watch?v=hV1sigh6WKA&ab_channel=TEDxTalks
[21] https://www.youtube.com/watch?v=Czg_9C7gw0o&ab_channel=TEDxTalks
[22] https://www.youtube.com/watch?v=iVTuAS_DE5A
[23] https://www.youtube.com/watch?v=EyQeUwqCDWg
[24] https://www.youtube.com/watch?v=_LElWqXi7Ag&list=PLcetZ6gSk9682A7ZAZq2s9IqB-y8Ng63e
[25] https://www.youtube.com/watch?v=RnHOFlaxQtI
[26] https://www.internetmatters.org/digital-family-toolkit/#explore-further

A1. Personal / Sensitive Data and Privacy	
Level	Foundation **(F)**
Prerequisites	---
Learning objectives **(LO)**	**LO1:** Learn what not to share **LO2:** Discover what are the consequences of sharing sensitive data **LO3:** Lear 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.[27] **P2:** Cyber Safety Lesson Plan[28] **P3:** Movie: The Great Hack[29]
Resources [links]	- How to Protect Your Digital Privacy [30] - What is personal data?[31] - Data protection and online privacy[32] - 5 tips to protect your privacy online[33] - Microsoft shares tips on how to protect your information and privacy against cybersecurity threats[34] - 8 ways to protect your private information online[35] - What is a digital footprint? And how to protect it from hackers[36] - Online safety - it is not about the internet... | Jim Gamble | TEDxStormontWomen[37] - Technology and Control | Bart Preneel | TEDxPatras[38]

[27] https://education.kaspersky.com/en/lesson/16/page/67
[28] https://www.teach-nology.com/teachers/lesson_plans/interdisciplinary/1/index.html
[29] https://www.netflix.com/gr/title/80117542
[30] https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy
[31] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
[32] https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
[33] https://www.youtube.com/watch?v=0cUnFsePZXA&ab_channel=Suncorp
[34] https://www.youtube.com/watch?v=_vrVmkYDrlE&ab_channel=MicrosoftCloud
[35] https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html
[36] https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint
[37] https://www.youtube.com/watch?v=eTTer3-RmFw
[38] https://www.youtube.com/watch?v=lpp8ao0uBik

A1. Personal / Sensitive Data and Privacy	
Level	Intermediate **(I)**
Prerequisites	A1-F
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
[40] https://www.dummies.com/article/technology/internet-basics/defining-and-dealing-with-web-cookies-200521/
[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/x5Gv8aY5y8U
[45] https://www.avast.com/c-web-tracking

A2. Cyberbullying and Sexual Harassment	
Level	Foundation **(F)**
Prerequisites	A1-F
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[46] Online Sexual Abuse Can Happen[47] **P2: Cyberbullying:** Is it Cyberbullying?[48] Heart-Breaking Cyberbullying Statistics for 2022[49] **P3:** Movies: Bully; Audrie and Daisy (16+); Submit the documentary
Resources [links]	- Cyberbullying among young people[50] - Quiz for cyberbullying[51] - Bullying and advice on coping and making it stop[52] - What is Cyberbullying, its bad effects and how to stop it [53] - Peer to peer sexual harassment[54] - Lesson Plans to address sexual harassment[55] - Digital Predators | Full Episode | Dateline[56] - Online Predators[57] - Bad Behavior Online: Bullying, Trolling & Free Speech | Off Book | PBS Digital Studios[58]

[46] https://www.youtube.com/watch?v=GOsgQbmvuUQ&ab_channel=ThinkUKnowAUS
[47] https://www.youtube.com/watch?v=CEivufW2IWs&ab_channel=FightChildAbuse
[48] https://www.youtube.com/watch?v=vtfMzmkYp9E&ab_channel=StopBullyingGov
[49] https://dataprot.net/statistics/cyberbullying-statistics/
[50] https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf
[51] https://www.childnet.com/resources/step-up-speak-up/teaching-toolkit/quiz/
[52] https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/
[53] https://www.iberdrola.com/social-commitment/cyberbullying-definition-effects-and-solutions
[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	
Level	Foundation **(F)**
Prerequisites	A1- F
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[59]) **P3:** TECH - Here's Facebook's once-secret list of content that can get you banned[60]
Resources [links]	- Inappropriate or explicit content | NSPCC[61] - Inappropriate content | Cyber Safety Pasifika[62] - Inappropriate Content - Cyber Safety[63] - Four ways to report inappropriate content online[64] - Find your local child helpline[65] - How to protect children and teens from inappropriate content online[66]

[59] https://www.pandasecurity.com/en/mediacenter/family-safety/is-tiktok-safe-for-kids/
[60] https://www.cnbc.com/2018/04/24/facebook-content-that-gets-you-banned-according-to-community-standards.html
[61] https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/
[62] https://www.cybersafetypasifika.org/stay-safe-online/inappropriate-content
[63] http://cybersafetyed.weebly.com/inappropriate-content.html
[64] https://www.youtube.com/watch?v=iOF7TxX0Kzk&ab_channel=ThamesValleyPolice
[65] https://childhelplineinternational.org/helplines/
[66] https://www.youtube.com/watch?v=aIXhRabFJAc

A4. Hate speech	
Level	Foundation **(F)**
Prerequisites	---
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?[67] **P2:** STARTING POINTS FOR COMBATING HATE SPEECH ONLINE[68] **P3:** The Datafication of Hate: Expectations and Challenges in Automated Hate Speech Monitoring[69]
Resources [links]	What is Freedom of Expression and what is hate speech?[70] How to Recognize Online Hate Speech[71] Teen Voices: Hate Speech Online[72] Hate speech has ability to alter our minds, faiths, convictions and compel us to reject rule of law[73] What Is Hate Speech? We Asked College Students[74] Hate Speech - Survey example 1[75] Hate Speech - Survey example 2[76]

[67] https://www.youtube.com/watch?v=n7p1l2mU-t8&ab_channel=FacingFacts
[68] https://www.researchgate.net/deref/https%3A%2F%2Frm.coe.int%2F1680665ba7
[69] https://www.frontiersin.org/articles/10.3389/fdata.2020.00003/full
[70] https://www.youtube.com/watch?v=BZBP8JZOLSU&ab_channel=CivicsAcademySA
[71] https://www.youtube.com/watch?v=on-_y1yOnn4&ab_channel=SofiaDA
[72] https://www.youtube.com/watch?v=8vUdWpwLv10&ab_channel=CommonSenseEducation
[73] https://www.nationalheraldindia.com/india/hate-speech-has-ability-to-alter-our-minds-faiths-convictions-and-compel-us-to-reject-rule-of-law
[74] https://www.youtube.com/watch?v=skuLK0YpksI
[75] https://www.surveymonkey.com/r/6L3BZWN
[76] https://www.surveymonkey.com/r/QJLTYG8

A5. Fake profiles, Fraud and Phishing	
Level	Foundation **(F)**
Prerequisites	A1-F
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[77] **P2:** Phishing Statistics (Updated 2022) - 50+ Important Phishing Stats - Tessian[78] **P3:** Fake Instagram Account Generator[79] **P4:** Random Person Generator | User Identity, Account and Profile Generator[80]
Resources [links]	- 6 social media scams to avoid in 2022, plus red flags | Norton [81] - 10 Social Media Scams and How to Spot Them - Panda Security Mediacenter[82] - What Is Phishing? Examples and Phishing Quiz - Cisco[83] - Fake Profiles - Student - ISEA[84]

[77] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~phishing-awareness-quiz
[78] https://www.tessian.com/blog/phishing-statistics-2020/
[79] https://generatestatus.com/fake-instagram-account-maker/
[80] https://www.fakepersongenerator.com/
[81] https://us.norton.com/internetsecurity-online-scams-social-media-scams.html
[82] https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/
[83] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
[84] https://infosecawareness.in/concept/student/fake-profiles

A5. Fake profiles, Fraud and Phishing	
Level	Intermediate **(I)**
Prerequisites	A5-F
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	
Level	Foundation **(F)**
Prerequisites	A1-F
Learning objectives **(LO)**	**LO1:** Learn the 'ingredients' to create a strong password **LO2:** Learn the methods mostly used to attack a password **LO3:** Learn managing your passwords safely
Main messages **(M)**	**M1:** Password needs to be long **M2:** Passwords must also contain special characters, and numbers, not only letters **M3:** Password is private data
Example of questions to be asked **(Q)**	**Q1:** How do they create passwords? **Q2:** Do they use the same password in many applications? **Q3:** Who knows their password?
Practical example **(P)**	**P1:** Password Check | Kaspersky[92] **P2:** How to Create a Strong Password[93]
Resources [links]	- Strong Password Tips | Create a strong password in 2022[94] - How to Remember a Unique Password For Everything[95] - Password Guidelines • European University Institute[96] - 6 Types of Password Attacks & How to Stop Them | OneLogin.[97] - RBC Cyber Security - Powerful Passwords[98] - How Do Password Managers Work?[99]

[92] https://password.kaspersky.com/
[93] https://www.youtube.com/watch?v=aEmF3Iylvr4&ab_channel=SafetyinCanada
[94] https://www.youtube.com/watch?v=Cg2Cs_E6f5I&ab_channel=LanguageTechSolutions
[95] https://www.youtube.com/watch?v=HrMHS8EGPC4&ab_channel=ExperimentalJack
[96] https://www.eui.eu/ServicesAndAdmin/ComputingService/ComputingAccounts/PasswordGuidelines
[97] https://www.onelogin.com/learn/6-types-password-attacks#:~:text=Password%20attacks%20are%20one%20of,were%20due%20to%20compromised%20credentials
[98] https://www.youtube.com/watch?v=IhlXtBNNuKs&ab_channel=RBC
[99] https://www.youtube.com/watch?v=DI72oBhMgWs

A6. The importance of Strong Passwords	
Level	Intermediate **(I)**
Prerequisites	A6-F
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=IuAgmkdvwFs&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	
Level	Advanced **(A)**
Prerequisites	A6-I
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[108] **P2:** Password Hashing, Salts, Peppers | Explained![109]
Resources [links]	- How secure is Biometric Authentication Technology and Biometric Data? | Biometric Security[110] - Hash, Salt and Pepper: How cooking a password makes it safer - Gearbrain[111] - Salting, peppering, and hashing passwords[112]

[108] https://www.youtube.com/watch?v=J5n630AMLE8
[109] https://www.youtube.com/watch?v=--tnZMuoK3E&ab_channel=Seytonic
[110] https://www.youtube.com/watch?v=ZPG3XQhZVII
[111] https://www.gearbrain.com/password-security-hashing-salting-peppering-2647766220.html
[112] https://www.youtube.com/watch?v=FvstbO787Qo&ab_channel=mCoding

A7. Addiction	
Level	Foundation **(F)**
Prerequisites	---
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 Addiction[114] - Social Media Addiction | Definition, Signs, Contributing Factors[115] - Addiction to social media: main causes and symptoms[116] - Psychology of Social Networks: What makes us addicted? - Learn UX[117] - 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 Addiction[120] - Video Game Addiction - Treatment, Symptoms, and Causes[121] - Video Game Addiction Symptoms and Treatment[122] - How I Cured My Social Media Addiction (Easiest Way)[123] - How I Cured My Phone Addiction[124] - **Movie:** The Social Dilemma[125]

[113] https://www.psycom.net/internet-addiction-test-quiz
[114] https://www.addictioncenter.com/drugs/social-media-addiction/#:~:text=According%20to%20a%20new%20study,pathways%20affect%20decisions%20and%20sensations
[115] https://socialmediavictims.org/social-media-addiction/
[116] https://www.iberdrola.com/social-commitment/impact-social-media-youth
[117] https://www.keepitusable.com/blog/psychology-of-social-networks-what-makes-us-addicted/
[118] https://www.sciencefocus.com/future-technology/trapped-the-secret-ways-social-media-is-built-to-be-addictive-and-what-you-can-do-to-fight-back/
[119] https://www.hellosocial.com.au/blog/why-is-social-media-addictive
[120] https://www.youtube.com/watch?v=oVK4PAwT9fc&ab_channel=DownwardThrust
[121] https://gamequitters.com/video-game-addiction/
[122] https://americanaddictioncenters.org/video-gaming-addiction
[123] https://www.youtube.com/watch?v=j2MERFltRns
[124] https://www.youtube.com/watch?v=Qk5ftIUMJsM
[125] https://www.netflix.com/gr/title/81254224

A8. Keep my online account safe	
Level	Foundation **(F)**
Prerequisites	A6-F
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 Online[126]
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
[127] https://safety.google/
[128] https://www.internetmatters.org/parental-controls/social-media/tiktok-privacy-and-safety-settings/
[129] https://www.facebook.com/help/238318146535333?helpref=hc_fnav
[130] https://education.kaspersky.com/en/lesson/16/page/71
[131] https://www.facebook.com/help/443357099140264
[132] https://help.instagram.com/811572406418223
[133] https://education.kaspersky.com/en/lesson/16/page/73
[134] https://www.techtarget.com/searchsecurity/definition/one-time-password-OTP#:~:text=A%20one%2Dtime%20password%20(OTP)%20is%20an%20automatically%20generated,or%20reused%20across%20multiple%20accounts
[135] https://support.google.com/accounts/answer/185833?hl=en
[136] https://support.microsoft.com/en-us/account-billing/how-to-help-keep-your-microsoft-account-safe-and-secure-628538c2-7006-33bb-5ef4-c917657362b9
[137] https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/

A9. Stay safe in Online Social Networks	
Level	Foundation **(F)**
Prerequisites	A1-F, A2, A3, A4, A5-I, A6-F, A7, A8
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=vPlWDFtP0T0&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=-QDjx_spkwI&ab_channel=PsychHub
[144] https://www.youtube.com/watch?v=fouSmgZBXsU&ab_channel=TopThink
[145] https://www.euractiv.com/section/digital/news/metaverse-how-to-regulate-a-space-yet-to-be-invented/

A10. Online Games	
Level	Foundation **(F)**
Prerequisites	A1-F, A2, A3, A4, A5-I, A6, A7-F
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
[147] https://www.phishprotection.com/blog/fifa-22-incident-phishing-attacks-gaming-industry/
[148] https://www.independent.co.uk/news/world/asia/playerunknowns-battlegrounds-ban-india-suicide-hyderabad-a8856646.html
[149] https://www.youtube.com/watch?v=QEP7IkMMVjo&ab_channel=Kaspersky
[150] https://education.kaspersky.com/en/lesson/29/page/150
[151] https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/
[152] https://usa.kaspersky.com/resource-center/threats/top-7-online-gaming-dangers-facing-kids
[153] https://cyber.org/find-curricula/cyber-safety-video-online-gaming-safety
[154] https://safety.twitch.tv/s/?language=en_US

A11. Fake News	
Level	Foundation **(F)**
Prerequisites	A5-F
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?[155] **P2:** The Impact Of Fake News On The World As Mistruths Continue To Spread[156] **P3:** How Online Bots Spread Fake News | Young Scot[157] **P4:** Fact Check: How to decipher online news and information: Identifying Fake News[158] **P4:** What Is Fake News and How Can You Spot It?[159] **P6:** EUfactcheck[160]
Resources [links]	- What is fake news and misinformation? | Internet Matters[161] - How Fake News Spreads[162] - How false news can spread - Noah Tavlin[163] - How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting | Center for Information Technology and Society[164] - 10 Examples of Fake News from History - The Social Historian[165] - Fake News: Separating Truth From Fiction[166] - **Game:** Get bad news[167]

[155] https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise
[156] https://www.youtube.com/watch?v=5biqhnWucew&ab_channel=TheProject
[157] https://young.scot/get-informed/national/ysdigiknow-fake-news-bots
[158] https://academicguides.waldenu.edu/library/fakenews/idfakenews
[159] https://www.avg.com/en/signal/what-is-fake-news
[160] https://eufactcheck.eu/
[161] https://www.internetmatters.org/issues/fake-news-and-misinformation-advice-hub/learn-about-fake-news-to-support-children/
[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	
Level	Intermediate **(I)**
Prerequisites	A11-F
Learning objectives **(LO)**	**LO1:** Learn about the main (measurable) characteristics of fake news **LO2:** Understand how social media profiles are related to fake news **LO3:** Learn about available fact-checking tools
Main messages **(M)**	**M1:** Fake news has specific parameters that can be detected **M2:** Some social media profiles are prone to spreading fake news **M3:** Use your critical thinking and fact-checking tools to prevent the spread of fake news
Example of questions to be asked **(Q)**	**Q1:** How do they identify a fake new post? **Q2:** What are the characteristics of social media profiles that are more prone to sharing fake news? **Q3:** Have they ever used/heard someone used a fact-checking tool/website?
Practical example **(P)**	**P1:** How to identify fake news[168] **P2:** Fake vs. Real: Identifying & Evaluating Information Sources - Research Guides at Singapore Management University[169] **P3:** Fact Check Tools[170]
Resources [links]	- How to Spot Fake News - FactCheck.org[171] - Helping Students Identify Fake News with the Five C's of Critical Consuming[172] - Develop Your Fact-Checking Skills: Examples of Fake News[173] - Fact Checking & Investigative Journalism Tools - Public Media Alliance[174] - 13 AI-Powered Tools for Fighting Fake News - The Trusted Web[175] **Quiz and Games:** - Examples - Identify & Challenge Disinformation (aka Fake News) - LibGuides at Portland State University[176] - iReporter - BBC News[177] - Fake or Real? The all-new NewsWise headlines quiz! | | The Guardian[178] - Inoculation Science - Games - Harmony Square[179]

[168] https://www.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news
[169] https://researchguides.smu.edu.sg/c.php?g=732802&p=5240633
[170] https://toolbox.google.com/factcheck/explorer
[171] https://www.youtube.com/watch?v=AkwWcHekMdo&ab_channel=FactCheck
[172] https://www.youtube.com/watch?v=xf8mjbVRqao&ab_channel=JohnSpencer
[173] https://researchguides.ben.edu/c.php?g=608230&p=4220071
[174] https://www.publicmediaalliance.org/tools/fact-checking-investigative-journalism/
[175] https://thetrustedweb.org/ai-powered-tools-for-fighting-fake-news/
[176] https://guides.library.pdx.edu/c.php?g=625347&p=4386301
[177] https://www.bbc.co.uk/news/resources/idt-8760dd58-84f9-4c98-ade2-590562670096
[178] https://www.theguardian.com/newswise/2021/feb/04/fake-or-real-headlines-quiz-newswise-2021
[179] https://inoculation.science/inoculation-games/harmony-square/

A12. Transparency of Recommendation Algorithms	
Level	Foundation **(F)**
Prerequisites	A1-I
Learning objectives (LO)	**LO1:** Understand how a recommendation algorithm works **LO2:** Understand what is a filter bubble **LO3:** Understand the importance of algorithms transparency
Main messages **(M)**	**M1:** There is a logic behind the recommendations delivered to us **M2:** Recommendations are supposed to give the users more content they are interested in **M3:** Platforms should give explanatory information about the recommendations we get
Example of questions to be asked **(Q)**	**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) **Q2**: Why do people require transparency? **Q3:** How do they believe Facebook recommends friends to add?
Practical example **(P)**	**P1:** How Recommender Systems Work (Netflix/Amazon)[180] **P2:** How news feed algorithms supercharge confirmation bias | Eli Pariser | Big Think[181]
Resources [links]	- Presentation - Algorithmic Mediation in Information Access Services[182] - What is a Filter Bubble? - Definition from Techopedia[183] - Recommender system - Wikipedia[184] - Recommender Systems[185] - Algorithmic bias explained[186] - Show me the algorithm: Transparency in recommendation systems — Schwartz Reisman Institute[187]

[180] https://www.youtube.com/watch?v=n3RKsY2H-NE&ab_channel=ArtoftheProblem
[181] https://www.youtube.com/watch?v=prx9bxzns3g&ab_channel=BigThink
[182] http://www.cycat.io/algorithmic-mediation-in-information-access-services/
[183] https://www.techopedia.com/definition/28556/filter-bubble
[184] https://en.wikipedia.org/wiki/Recommender_system
[185] https://www.youtube.com/watch?v=Eeg1DEeWUjA&ab_channel=CS50
[186] https://www.youtube.com/watch?v=bWOUw8omUVg&ab_channel=TRTWorld
[187] https://srinstitute.utoronto.ca/news/recommendation-systems-transparency

A12. Transparency of Recommendation Algorithms	
Level	Intermediate **(I)**
Prerequisites	A12-F
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
[193] https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you
[194] https://transparency.fb.com/features/ranking-and-content/
[195] https://caseguard.com/articles/balancing-online-profiling-and-new-data-privacy-concerns/

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.

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

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

	PREREQUISITES											
Module	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
B1	x											
B2		x										
B3												
B4			x	x								
B5	x	x	x	x	x							
B6	x	x	x	x	x							
B7		x	x		x							
B8	x	x	x	x	x	x	x	x				
B9		x				x	x					
B10	x	x	x	x	x	x	x	x	x	x		
B11	x	x	x	x	x	x	x	x	x	x	x	
B12	x	x	x	x	x	x	x	x	x	x	x	

B0. Why study cybersecurity	
Level	Foundation **(F)**
Prerequisites	**---**
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 cyber security 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-ZhO0
[197] https://cybersecurityonline.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/
[198] https://patchstack.com/articles/website-hacking-statistics/
[199] http://viscog.beckman.illinois.edu/flashmovie/15.php
[200] https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities
[201] https://www.youtube.com/watch?v=inWWhr5tnEA
[202] https://www.youtube.com/watch?v=JIJslcA8Q5g&ab_channel=TEDxTalks
[203] https://www.youtube.com/watch?v=XiU72Vzs5Is&ab_channel=Malwarebytes
[204] https://www.which.co.uk/news/2021/07/how-the-smart-home-could-be-at-risk-from-hackers/
[205] https://www.youtube.com/watch?v=ZLyFt6BdxD4&ab_channel=edureka%21

B1. OSI Model	
Level	Foundation **(F)**
Prerequisites	----
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=LANW3m7UgWs&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
[209] https://www.guru99.com/tcp-vs-udp-understanding-the-difference.html
[210] https://samsclass.info/123/quiz/osi.htm

B1. OSI Model	
Level	Intermediate **(I)**
Prerequisites	B1-F
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[211] - Physical layer in OSI Model | Physical layer Protocols | Physical Layer Tutorial | networking tips[212] - OSI Model - A Real World Example::InetDaemon.Com[213] - OSI Model Explained[214] - Online game: Matching Game: Map OSI and TCP/IP Layers (technology)[215]

[211] https://www.youtube.com/watch?v=LkolbURrtTs&ab_channel=PracticalNetworking
[212] https://www.youtube.com/watch?v=qSk5SLrg7Yg&ab_channel=ISOTrainingInstitute
[213] https://www.inetdaemon.com/tutorials/basic_concepts/network_models/osi_model/real_world_example.shtml
[214] https://www.youtube.com/watch?v=O_rsqVtaloI&ab_channel=DeeRa
[215] https://www.educaplay.com/learning-resources/3212017-map_osi_and_tcp_ip_layers.html

B2. Operating systems (OS), Computer Hardware and how does a computer work	
Level	Foundation **(F)**
Prerequisites	----
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	
Level	Intermediate **(I)**
Prerequisites	B2-F
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[221] and Worksheet 1: Binary Numbers 2 00010 5 3 12 19 8 15[222]
Resources [links]	- 5 main components of computer system and their functions[223] - Components of Computer System[224] - Why Do Computers Use 1s and 0s? Binary and Transistors [225] - ExplGame: tagged "computer parts"[226] - Computer Basics: Understanding Operating Systems[227] Binary Games: - Binary Bonanza! Binary Number game - Fun, Free, Online Way to Learn Binary[228] - Binary Numbers | Classic CS Unplugged[229] - Why Do Computers Use 1s and 0s? Binary and Transistors Explained.[230]

[221] https://corbettmaths.com/wp-content/uploads/2019/04/Binary.pdf
[222] http://csunplugged.mines.edu/Activities/Binary/BinaryWorksheets.pdf
[223] https://sciencerack.com/components-of-computer/
[224] https://www.tutorialspoint.com/computer_concepts/computer_concepts_components_of_computer_system.htm
[225] https://www.youtube.com/watch?v=Xpk67YzOn5w&ab_channel=BasicsExplained%2CH3Vtux
[226] https://matchthememory.com/computer-components1
[227] https://www.youtube.com/watch?v=fkGCLIQx1MI&t=2s&ab_channel=GCFLearnFree.org
[228] https://games.penjee.com/binary-bonanza/
[229] https://classic.csunplugged.org/activities/binary-numbers/
[230] https://www.youtube.com/watch?v=Xpk67YzOn5w&ab_channel=BasicsExplained%2CH3Vtux

B2. Operating systems (OS), Computer Hardware and how does a computer work	
Level	Advanced **(A)**
Prerequisites	B2-F, B2-I
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[231] - Meltdown & Spectre vulnerabilities - Simply Explained[232] - Spectre Explained - The Attack that took the world by surprise in 2018[233] - Different Operating Systems - GeeksforGeeks/[234] - CISCO Learning - Binary Game[235]

[231] https://www.cybok.org/media/downloads/Operating_Systems_Virtualisation_Security_v1.0.1.pdf
[232] https://www.youtube.com/watch?v=bs0xswK0eZk&ab_channel=SimplyExplained
[233] https://www.youtube.com/watch?v=Phmt8UrofDY&ab_channel=HusseinNasser
[234] https://www.geeksforgeeks.org/different-operating-systems/
[235] https://learningnetwork.cisco.com/s/binary-game

B3. Protection of Data: concerns	
Level	Foundation **(F)**
Prerequisites	----
Learning objectives **(LO)**	**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
Main messages **(M)**	**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.
Example of questions to be asked **(Q)**	**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?
Practical example **(P)**	**P1:** Two Scenarios: Your Children Could Open You to Attack | DigiCert.com[236] **P2:** Real example: This is how hackers hack you using simple social engineering[237] **P3:** Real Experiment: Amazing mind reader reveals his 'gift'[238] **P4:** A challenge: Hacking challenge at DEFCON[239]
Resources [links]	- 2022 ForgeRock Consumer Identity Breach Report[240] - Watch Out! 5 Most Common Social Engineering Attacks[241] - Understanding and assessing risk in personal data breaches | ICO[242] - What Is Cyber Warfare? | Fortinet[243] - Social Engineering- The art of hacking humans | Prasad Sawant | - TEDxElproIntlSchool[244]

[236] https://www.digicert.com/blog/children-online-attacks
[237] https://www.youtube.com/watch?v=lc7scxvKQOo&ab_channel=oraclemind
[238] https://www.youtube.com/watch?v=F7pYHN9iC9I&ab_channel=DuvalGuillaume
[239] https://www.youtube.com/watch?v=fHhNWAKw0bY&ab_channel=ConflictInternational
[240] https://www.forgerock.com/resources/2022-consumer-identity-breach-report?adgroupid=119441268234
[241] https://www.youtube.com/watch?v=j5j6c05Btfc&ab_channel=DemakisTechnologies
[242] https://ico.org.uk/for-organisations/sme-web-hub/understanding-and-assessing-risk-in-personal-data-breaches/
[243] https://www.fortinet.com/resources/cyberglossary/cyber-warfare
[244] https://www.youtube.com/watch?v=lEK84lV6dxs&ab_channel=TEDxTalks

B4. Network Standards & Protocols	
Level	Foundation **(F)**
Prerequisites	---
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 - Tablets of Stone—Network Communication Protocols[245]
Resources [links]	- Game : Map OSI and TCP/IP Layers - Print Matching Game[246] - Physical Layer | Layer 1 | The OSI-Model[247] - Computer network Facts for Kids[248] - How The Internet Works? | What Is Internet? | Dr Binocs Show | Kids Learning Video | Peekaboo Kidz[249] - Network Protocol | TechTerms[250]

[245] https://classic.csunplugged.org/documents/activities/network-protocols/unplugged-en-network_protocols-v3.1.pdf
[246] https://www.educaplay.com/printablegame/3212017-map_osi_and_tcp_ip_layers.html
[247] https://osi-model.com/physical-layer/
[248] https://kids.kiddle.co/Computer_network
[249] https://www.youtube.com/watch?v=UXsomnDkntI&ab_channel=PeekabooKidz
[250] https://www.youtube.com/watch?v=BnWn18qUYyA&ab_channel=TechTerms

B4. Network Standards & Protocols	
Level	Intermediate (I)
Prerequisites	B3, B4-F
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 - 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[251]
Resources [links]	- OSI Model Layers and Protocols in Computer Network[252] - tcp vs udp compared and explained in simple terms | CCNA 200-301[253] - What is an IP Address? Everything You Need to Know[254] - Understanding Routing! | ICT#8[255]

[251] https://classic.csunplugged.org/documents/activities/routing-and-deadlock/unplugged-10-routing_and_deadlock.pdf
[252] https://www.guru99.com/layers-of-osi-model.html
[253] https://www.youtube.com/watch?v=bDjP6bQLy3M&ab_channel=NETWORKINGWITHH
[254] https://www.youtube.com/watch?v=BY8zN46smz4&ab_channel=ElegantThemes
[255] https://www.youtube.com/watch?v=gQtgtKtvRdo&ab_channel=Lesics

B4. Network Standards & Protocols	
Level	Advanced **(A)**
Prerequisites	B3, B4-F, B4-I
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 of 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_tTiNw&ab_channel=WidyaLestari
[259] https://www.tutorialspoint.com/data_communication_computer_network/application_protocols.htm

B5. Essentials in Cyber security	
Level	Foundation **(F)**
Prerequisites	B1, B2, B3
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[260] at 9:24 min (Confidentiality), at 9:50 min (Integrity), at 10:15 minute (Availability) - 3 Steps to Protect Your Reputation Online[261] - CIA in Cyber Security: Definition, Examples, Importance[262] - What is the C.I.A. Triad?[263] - What is the CIA Triad? Confidentiality, Integrity, Availability[264] - Ways to Ensure Data Integrity | Google Data Analytics Certificate[265] - Quiz: Code-HS Flashcards | Quizlet[266] - Cyber Security Full Course for Beginner[267] - Introduction to Cybersecurity Essentials[268]

[260] https://www.youtube.com/watch?v=agnDpN961xU&ab_channel=InvensisLearning
[261] https://www.youtube.com/watch?v=rwigKjEsdTc&ab_channel=ProjectAres
[262] https://www.knowledgehut.com/blog/security/cia-in-cyber-security
[263] https://www.youtube.com/watch?v=BrjqLE4fiSc&ab_channel=IntellectualPoint
[264] https://www.youtube.com/watch?v=11_Hp5Dvx5E
[265] https://www.youtube.com/watch?v=9qCfJv-zoyE
[266] https://quizlet.com/627578434/code-hs-flash-cards/
[267] https://www.youtube.com/watch?v=U_P23SqJaDc
[268] https://www.coursera.org/learn/introduction-to-cybersecurity-essentials

B5. Essentials in Cyber security	
Level	Intermediate **(I)**
Prerequisites	B1, B2, B3, B4
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?[269] - Andress, Jason Basics of Information Security, Second Edition[270] - The CIA Triad: Confidentiality, Integrity, Availability - Panmore Institute[271] - TOP 10 biggest data breaches in history[272] - 5 of the biggest data breaches ever[273] - The 66 Biggest Data Breaches (Updated August 2022) | UpGuard[274]

[269] https://www.brookings.edu/opinions/what-do-we-mean-by-security-anyway/
[270] https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition
[271] https://panmore.com/the-cia-triad-confidentiality-integrity-availability
[272] https://www.youtube.com/watch?v=lhOY5j8oPOc&ab_channel=SurfsharkAcademy
[273] https://www.youtube.com/watch?v=fIR-RbA-R4s&ab_channel=CNNBusiness
[274] https://www.upguard.com/blog/biggest-data-breaches

B5. Essentials in Cyber security	
Level	Advanced **(A)**
Prerequisites	B1, B2, B3, B4
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[275]
Resources [links]	- Cybersecurity Tutorial for Beginners | Introduction to Cybersecurity | Invensis Learning[276] at 11:30 min - CIA Triad[277] - Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data[278] - What Is a Firewall? - Cisco[279] - What is Network Security?[280] - What Is A Firewall? | Firewall Explained | Firewall Tutorial[281]

[275] https://www.liveworksheets.com/qa2928338ag
[276] https://www.youtube.com/watch?v=agnDpN961xU&ab_channel=InvensisLearning
[277] https://www.youtube.com/watch?v=gx0vlRpdFnc&ab_channel=NesoAcademy
[278] https://www.usenix.org/system/files/conference/soups2018/soups2018-karunakaran.pdf
[279] https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
[280] https://www.paloaltonetworks.com/cyberpedia/what-is-network-security#:~:text=What%20Are%20the%20Essential%20Components,essential%20components%20of%20network%20security.
[281] https://www.youtube.com/watch?v=9GZlVOafYTg&ab_channel=Simplilearn

B6. Attacks, threats, vulnerabilities	
Level	Foundation **(F)**
Prerequisites	B1, B2, B5
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 threat?
Practical example **(P)**	**P1**: Use haveibeenpwned[282] to check passwords **P2**: Games with animation: -ikeepsafe[283] -Cyber-Five Internet Safety • ABCya![284] -thinkuknow[285] - BREACH a data loss prevention game[286] **P4**: Activity CyberSprinters Wordsearch[287]
Resources [links]	-Threats, Vulnerabilities, and Attacks[288] -Videos | NOVA Labs | PBS[289] -Detailed resource: Teaching Security |[290] -Attackers and Type of attackers[291] -Types of Cyber Attacks[292] -15 Types Of Cyber Attacks To Look Out For[293] -What is Malware?[294]

[282] https://haveibeenpwned.com/
[283] https://ikeepsafe.org/faux-paw-the-techno-cat/
[284] https://www.abcya.com/games/cyber_five_internet_safety
[285] https://www.thinkuknow.co.uk/8_10/
[286] https://www.educationarcade.co.nz/breach
[287] https://www.ncsc.gov.uk/files/CyberSprinters-Wordsearch.pdf
[288] https://www.uobabylon.edu.iq/eprints/publication_3_25852_324.pdf
[289] https://www.pbs.org/wgbh/nova/labs/videos/#cybersecurity
[290] https://teachingsecurity.org/
[291] https://www.youtube.com/watch?v=4xY7NHxMco8&ab_channel=ShahzadaKhurram
[292] https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks
[293] https://www.youtube.com/watch?v=NDcEOW8r0xc
[294] https://www.youtube.com/watch?v=QozdEbyMK5E

B6. Attacks, threats, vulnerabilities	
Level	Intermediate **(I)**
Prerequisites	B1,B2,B4, B5, B6-F
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[295] **P2**: An Online experiment Have you taken phishing IQ test?[296]
Resources [links]	-Cybersecurity Tutorial for Beginners[297] from 13:14 min -10 Types of Cyber Attacks You Should Be Aware in [2022][298] -SQL Injection | OWASP Foundation[299] -Threats to Information Security - GeeksforGeeks[300] -defending your organisation from email phishing attacks[301] - Active games: Free Cyber Security Games | Education Arcade[302] -Phishing attacks: defending your organisation - NCSC.GOV.UK[303] -What is Ransomware Attack? Types, Protection and Removal[304]

[295] https://www.sciencebuddies.org/science-fair-projects/project-ideas/Cyber_p005/cybersecurity/crack-caesar-cipher
[296] https://www.sonicwall.com/phishing-iq-test/
[297] https://www.youtube.com/watch?v=agnDpN961xU&ab_channel=InvensisLearning
[298] https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks#:~:text=What%20are%20the%20four%20types,attack%2C%20and%20SQL%20injection%20attack.
[299] https://owasp.org/www-community/attacks/SQL_Injection
[300] https://www.geeksforgeeks.org/threats-to-information-security/
[301] https://youtu.be/gGoPNrRVQUQ
[302] https://www.educationarcade.co.nz/game-time
[303] https://www.ncsc.gov.uk/guidance/phishing
[304] https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ransomware-attack

B6. Attacks, threats, vulnerabilities	
Level	Advanced **(A)**
Prerequisites	B1, B2, B3, B4, B5, B6-F, B-I
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?[305] MIM real example[306] **P2**: Discuss the different kind of attacks at the application layer
Resources [links]	-Cyber security in schools: Practical tips[307] -Threats, Attacks, and Vulnerabilities | Cyber.org[308] -internet-traffic-light[309] -Man in the Middle Attack: Tutorial & Examples | Veracode[310] -Malware+projects :Course materials for Malware Analysis by RPISEC[311]

[305] https://www.youtube.com/watch?v=DgqID9k83oQ&ab_channel=Hacksplaining
[306] https://resources.infosecinstitute.com/topic/man-in-the-middle-demystified/
[307] https://www.ncsc.gov.uk/files/NCSC_NEN%20cards_PRINT-2.pdf
[308] https://cyber.org/cybersecurity/threats-attacks-and-vulnerabilities
[309] https://www.commonsense.org/education/digital-citizenship/lesson/internet-traffic-light
[310] https://www.veracode.com/security/man-middle-attack
[311] https://github.com/RPISEC/Malware

B7. Defense against Cyber threats (Cyber Hygiene)	
Level	Foundation **(F)**
Prerequisites	B2, B3, B5
Learning objectives **(LO)**	**LO1**: Be aware of cyber hygiene practices and their importance. **LO2**: Know what password hygiene is. **LO3:** Define what is a Digital Identity.
Main messages **(M)**	**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.
Example of questions to be asked **(Q)**	**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 ?
Practical example **(P)**	**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
Resources [links]	-School of Cyberthreats: 3 Attacks Impacting Today's Schools[312] -QUIZ: What does your digital footprint say about you?[313] -What Do Your Digital Footprints Say About You?[314] -How To Crack Passwords [315] -Back-to-School Cybersecurity Tips | Information Security Office[316] -How To Recognize and Avoid Phishing Scams | Consumer Advice[317] - **Online Games** Cybersecurity | NOVA Labs | PBS[318] band runner[319] - Top Tips for Cyber Hygiene[320]

[312] https://www.mcafee.com/blogs/consumer/mobile-and-iot-security/cybercriminals-target-educational-institutions/
[313] https://www.mariecurie.org.uk/talkabout/articles/what-does-your-digital-footprint-say-about-you/259870#:~:text=Your%20digital%20footprint%20%E2%80%93%20ie%20the,health%20concerns%20or%20unusual%20hobbies.
[314] https://www.youtube.com/watch?v=RVX8ZSAR4OY&ab_channel=TEDxTalks
[315] https://www.simplilearn.com/tutorials/cyber-security-tutorial/how-to-crack-passwords
[316] https://security.berkeley.edu/education-awareness/back-school-cybersecurity-tips
[317] https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
[318] https://www.pbs.org/wgbh/nova/labs/lab/cyber/
[319] https://www.thinkuknow.co.uk/8_10/
[320] https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

B8. Cryptography	
Level	Foundation **(F)**
Prerequisites	B1, B2, B3, B5, B6
Learning objectives **(LO)**	**LO1:** Know the storyline of Cryptography and its importance. **LO2:** Understand simple cryptography. **LO3**: Identify the elements needed to encrypt/decrypt.
Main messages **(M)**	**M1**: Cryptography is the art and science of concealing meaning. **M2**.: Encryption is the process of encoding a message. **M3**: Decryption is the process of converting the encoded message. **M4**. The Encryption key is necessary for encryption and decryption. **M5**: Caesar Cipher is an encryption algorithm that shifts the alphabet.
Example of questions to be asked **(Q)**	**Q1**. What is the aim of encryption? **Q2**. Why do we use a key for encryption/decryption? **Q3**. What is a Caesar cipher?
Practical example **(P)**	**P1**: Explain how the enigma worked using The Imitation Game [321]movie. **P2**: Propose this sentence on the board: "serr cvmmn va gur pnsrgrevn" Give students about 3-5 minutes to work on cracking the message. Answer: "free pizza in the cafeteria" - the A-Z alphabet is shifted to 13 characters. **P3**. Discuss that this encryption technique took a few minutes to decode a small message. Imagine with a computer how much it would take Resource[322]
Resources [links]	-Cryptographic Protocols | Classic CS Unplugged[323] -Activities Interactive: Caesar Cipher - Interactivate[324] Caesar Cipher II - Interactivate[325] Caesar Cipher III - Interactivate[326] -Cryptography: Crash Course Computer Science #33[327] -Instructions : Paper Enigma Machine[328] -Sheets: Paper Enigma Machine[329] Basic Crypto Systems[330] Basic Crypto Systems II[331] -How to Explain Modern Security Concepts to your Children[332]

[321] https://www.imdb.com/title/tt2084970/
[322] https://curriculum.code.org/csp-18/unit4/7/
[323] https://classic.csunplugged.org/activities/cryptographic-protocols/
[324] http://www.shodor.org/interactivate/activities/CaesarCipher/
[325] http://www.shodor.org/interactivate/activities/CaesarCipherTwo/
[326] http://www.shodor.org/interactivate/activities/CaesarCipherThree/
[327] https://www.youtube.com/watch?v=jhXCTbFnK8o
[328] https://www.slideshare.net/mckoss/paper-enigma-machine
[329] https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/paperEnigma.pdf
[330] http://archive.dimacs.rutgers.edu/drei/1997/classroom/lessons/basic.html
[331] http://archive.dimacs.rutgers.edu/drei/1997/classroom/lessons/basic2.html
[332] https://hal.archives-ouvertes.fr/hal-01397035/document

B8. Cryptography	
Level	Intermediate **(I)**
Prerequisites	B1, B2, B3, B4, B5, B6, B8-F
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[333] **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[334] -Sheets: Kid krypto—Public-key encryption[335] -Presentation 6: Privacy and Encryption - Children and Technology [336] -UNIT 16 Modern Encryption Teacher Resource Material[337] -The Public Key[338] -Public Key Cryptography - Computerphile[339] -Digital Signatures[340] -Games:Solve the Cryptoquote [341] RSA Encryption and Decryption[342] -Difference between Symmetric and Asymmetric encryption[343]

[333] https://docs.google.com/document/d/1l0KDF33-gWIssZGqfuHgD0QpF50Pdyqras46FeuNLgc/edit
[334] https://www.youtube.com/watch?v=ZghMPWGXexs&ab_channel=Code.org
[335] https://classic.csunplugged.org/documents/activities/public-key-encryption/unplugged-18-public_key_encryption_0.pdf
[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_lvRv4&ab_channel=Computerphile
[340] https://www.youtube.com/watch?v=704dudhA7UI
[341] https://demonstrations.wolfram.com/SolveTheCryptoquote/
[342] https://demonstrations.wolfram.com/RSAEncryptionAndDecryption/
[343] https://www.youtube.com/watch?v=gRec1hWXFo0&ab_channel=KnowledgePowerhouse

B8. Cryptography	
Level	Advanced **(A)**
Prerequisites	B1, B2, B3, B4, B5, B6, B7, B8-F, B8-I
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[344] **P2**: A worksheet Worksheet - Keys and Passwords **P3**: Worksheet on the enigma: Lesson Three Code makers and breakers[345]
Resources [links]	-ENCRYPTED TRAFFIC ANALYSIS[346] -A complete lesson with activity for:Public Key Cryptography[347] -Advanced sheet: Public Key Cryptography[348] -The Knapsack Problem and Public Key Cryptography[349] -Course: Code-Based Cryptography - Course - FUN MOOC[350] -Book:(PDF) Understanding Cryptography: A Textbook for Students[351] -Worksheets:Substitution Ciphers [352] Encryption And Decryption[353] Challenge[354] -Secret Code Breaker[355] -Advanced course:NIH Information Security Awareness Course[356]

[344] https://www.security.org/how-secure-is-my-password/
[345] https://cnduk.org/wp-content/uploads/2018/03/Lesson-3-Codemakers-and-Breakers.pdf
[346] https://www.enisa.europa.eu/publications/encrypted-traffic-analysis/at_download/fullReport
[347] https://curriculum.code.org/csp-18/unit4/9/
[348] https://nrich.maths.org/2200
[349] https://nrich.maths.org/2199
[350] https://www.fun-mooc.fr/en/courses/code-based-cryptography/
[351] https://www.academia.edu/18966194/Understanding_Cryptography_A_Textbook_for_Students_and_Practitioners
[352] https://www.cimt.org.uk/resources/codes/codes_u1_tr.pdf
[353] http://archive.dimacs.rutgers.edu/drei/1997/classroom/lessons/matrices.html
[354] http://archive.dimacs.rutgers.edu/drei/1997/classroom/lessons/challenge.html
[355] http://www.secretcodebreaker.com/
[356] https://irtsectraining.nih.gov/publicUser.aspx

B9. Individual Incidents Responses	
Level	Foundation **(F)**
Prerequisites	B2, B6, B8-F
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?[357] **P2:** You can practice with them how to activate Two Factor Authentication
Resources [links]	-What is incident response in cyber security [358] -3 Benefits of an Incident Response Plan - Cybriant[359] -A list of very useful videos about privacy and data breach:Guidance[360] -Good Practice Guide for Incident Management (ENISA)[361] -Student Guide for CyberSecurity Awareness[362] -A College Students Guide[363] -Cyber Security Threats: How Students Can Protect Their Data[364] -The 7 things you need to do if you get hacked[365] -Online games: Cybersecurity Games[366] NCSC - Cyber Sprinter[367]

[357] https://www.shsu.edu/dept/it@sam/newsletter/july-2016/security-tip.html
[358] https://www.youtube.com/watch?v=NL1ShMo4Gm4
[359] https://cybriant.com/incident-response-plan/
[360] https://studentprivacy.ed.gov/content/guidance-videos
[361] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport
[362] https://www.cdse.edu/Portals/124/Documents/student-guides/CS130-guide.pdf?ver=00gYkCPZlAzxAVjUFdDQ5Q%3D%3D
[363] https://www.security.org/resources/college-guide-data-cyber-protection/
[364] 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
[366] https://it.tamu.edu/security/cybersecurity-games/index.php
[367] https://www.ncsc.gov.uk/training/ncsc-cyber-security-for-young-people-english-scorm-v2/index.html

B10. Capture the Flag	
Level	Foundation **(F)**
Prerequisites	B1, B2, B4, B6
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[368] **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[369] -Capture-The-Flag Competitions: all you ever wanted to know![370] -Full course: Capture the Flag - Cyber Security Base 2022[371] -Challenges: Easy challenges[372] -Platform: HackTheBox[373] -Hacking-Lab[374] -Online CTF events: CTFTime[375] -Capture the Flag - Cyber Security Base 2022[376]

[368] https://ctflearn.com/
[369] https://gdsc.community.dev/events/details/developer-student-clubs-guru-tegh-bahadur-institute-of-technology-delhi-presents-introduction-to-ctf/
[370] https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know
[371] https://cybersecuritybase.mooc.fi/module-6.1/index
[372] https://csb-capture-the-flag.cs.helsinki.fi/ctf/
[373] https://www.hackthebox.com/
[374] https://www.hacking-lab.com/events/
[375] https://ctftime.org/
[376] https://cybersecuritybase.mooc.fi/module-6.1/index

B10. Capture the Flag	
Level	Intermediate **(I)**
Prerequisites	B1, B2, B4, B6, B7, B10-F
Learning objectives **(LO)**	**LO1:** Know some tools and platforms for CTF. **LO2**: Develop Team spirit and learn cooperative work
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.
Example of questions to be asked **(Q)**	**Q1**: What is a flag? **Q2**: Why do we submit a flag?
Practical example **(P)**	**P1**: Prepare a VM with different challenges. **P2**: Practical examples: Challenges » CyberTalents[378]
Resources [links]	-Website for security training:tryhackme.com[379] -Good resource with videos: Introduction · CTF Field Guide[380] -Full course: Capture the Flag - Cyber Security Base 2022[381] -Challenges: Easy challenges[382] CTF Challenges [383] Vulnhub-CTF-Writeups[384] -List of WriteUps and resources: CTFWriteups[385] CTF-Writeups[386] resources[387] -**CTF Platforms:** RootTheBox[388] Facebook: facebookarchive[389] ctfd[390]picoctf[391] OWASP[392] Mellivora[393] HackTheArch[394]

[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://csb-capture-the-flag.cs.helsinki.fi/ctf/
[383] https://github.com/Ignitetechnologies/CTF-Difficulty#easy
[384] https://github.com/Ignitetechnologies/Vulnhub-CTF-Writeups
[385] https://github.com/Ignitetechnologies/TryHackMe-CTF-Writeups
[386] https://github.com/Ignitetechnologies/HackTheBox-CTF-Writeups
[387] https://github.com/enaqx/awesome-pentest#ctf-tools
[388] https://github.com/moloch--/RootTheBox
[389] https://github.com/facebookarchive/fbctf
[390] https://ctfd.io
[391] https://picoctf.com/
[392] https://github.com/OWASP/SecurityShepherd
[393] https://github.com/Nakiami/mellivora
[394] https://github.com/mcpa-stlouis/hack-the-arch

B10. Capture the Flag	
Level	Advanced **(A)**
Prerequisites	B1, B2, B3, B4, B5, B6, B7, B8, B10-F, B10-I
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[395] **P2**: Practical examples: Challenges » CyberTalents[396] **P3**: Mitre exercises MITRE Cyber Academy · GitHub[397]
Resources [links]	-Full course: Capture the Flag - Cyber Security Base 2022[398] -List of challenges: Easy challenges[399] CryptOMG CTF[400] Vulnhub-CTF[401] -HackTheBox-CTF-Writeups[402] -Online hacking competition designed to educate high schoolers in computer HSCTF[403] - GitHub - Aksheet10/Cyber-Security-Resources[404] -A famous CTF: Google CTF[405]

[395] https://overthewire.org/wargames/
[396] https://cybertalents.com/challenges
[397] https://github.com/mitre-cyber-academy
[398] https://cybersecuritybase.mooc.fi/module-6.1/index
[399] https://csb-capture-the-flag.cs.helsinki.fi/ctf/
[400] https://github.com/SpiderLabs/CryptOMG
[401] https://github.com/Ignitetechnologies/Vulnhub-CTF-Writeups
[402] https://github.com/Ignitetechnologies/HackTheBox-CTF-Writeups
[403] http://hsctf.com/
[404] https://github.com/Aksheet10/Cyber-security-resources
[405] https://capturetheflag.withgoogle.com/

B11. Penetration testing	
Level	Advanced **(A)**
Prerequisites	B1→B10
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] ; OWASP | Hacker101[420] - Create the red team and blue team at home: hausec[421] - Vulnerable Web (DSVW) : DSVW[422] - Vulnerable machine: Metasploitable3[423] - Events of hacking/training: Hacking-Lab[424]

[406] https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
[407] https://drive.google.com/file/d/1thItoYnfgNuAhY7rOxiaKBvUQWHyqNO_/view
[408] https://drive.google.com/file/d/1cMHo91JKeubcvvgOW9bWLSNpdexkLL_U/view
[409] https://www.youtube.com/watch?v=vAe1gq0H2q8&ab_channel=TypicallyEthical
[410] https://www.hackerhighschool.org/lessons/HHS_en12_Defensive_Hacking.v2.pdf
[411] https://www.hackerhighschool.org/lessons/HHS_en11_Hacking_Passwords.v2.pdf
[412] https://www.hackerhighschool.org/lessons.html
[413] https://portswigger.net/web-security
[414] https://www.root-me.org/
[415] https://www.hackingarticles.in/devguru-1-vulnhub-walkthrough/
[416] https://www.hackingarticles.in/pwned-1-vulnhub-walkthorugh/
[417] https://www.hackingarticles.in/cybox-1-vulnhub-walkthrough/
[418] razrsec
[419] https://www.hacker10Complete Guide to Cryptography Certifications for 20221.com/playlists/pentesting_series
[420] https://www.hacker101.com/sessions/pentest_owasp
[421] https://hausec.com/2021/03/04/creating-a-red-blue-team-home-lab/
[422] https://github.com/stamparm/DSVW
[423] https://github.com/rapid7/metasploitable3
[424] https://www.hacking-lab.com/events/

B12. Roles in Cyber security and Top Certifications	
Level	Advanced **(A)**
Prerequisites	B1→ B11
Learning objectives **(LO)**	**LO1** Realize that there is an increasing demand for people in Cyber security. **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[425]. **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[426] 10 Certifications[427] -European Cybersecurity Skills Framework Role Profiles[428] -Cyber Security Career [429] -Will Smith's Cybersecurity Career Map - Xmind[430] -Cybersecurity Domain Map ver 3.0[431] -Cybersecurity education and workforce needs in Europe[432] - Cybersecurity HR Recruitment [433] -How can I develop a career in Cybersecurity?[434]

[425] https://www.idc.com/getdoc.jsp?containerId=prEUR149609822
[426] https://cybersecurityguide.org/programs/cybersecurity-certifications/cryptography/
[427] https://www.coursera.org/articles/popular-cybersecurity-certifications
[428] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
[429] https://www.youtube.com/watch?v=BlsW9jp9NJM&ab_channel=Simplilearn
[430] https://xmind.app/m/97mJ/
[431] https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/
[432] https://ecs-org.eu/newsroom/unlocking-our-potential-cybersecurity-education-and-workforce-needs-in-europe
[433] https://www.ecs-org.eu/documents/publications/6202804a65a70.pdf
[434] https://digital-skills-jobs.europa.eu/en/community/online-discussions/how-can-i-develop-career-cybersecurity

Annex – Education related initiatives in Europe

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

[435] https://digital-strategy.ec.europa.eu/en/policies/safer-internet-centres
[436] https://www.betterinternetforkids.eu. Educational resources avaiable at https://www.betterinternetforkids.eu/resources
[437] https://inhope.org/
[438] https://hsin.hr/
[439] https://sini.hr/
[440] https://www.klicksafe.de/
[441] https://www.saferinternet.de/

Cyberstart[442]	Cyber security training (fee-paying) brought to life through real-world hacking challenges and puzzles.	EN	Youth, young adults	Cybersecurity
Microsoft Learn[443]	Free curriculum, training, and tools for teaching.	EN	Not defined	Diverse cyber security topics
Internet Segura Kids[444]	EU funded initiative in Spain on internet safety. Different information and material[445] provided for children, youth, parents and teachers.	ES	Children and youth	Mostly cybersafety
Tonis Escape dem Hacker auf der Spur[446]	Online game for youth that can be used as part of lectures[447]. Part of the German national initiative[448] funded by the BMBF where security topics are covered.	DE	Age 12-15	Cybersecurity, security in smart homes, authentication and security of AI.
CyberSchool[449]	Program run by Foundation cyber school that organizes workshops for cyber safety and awareness in schools with the involvement of teachers.	NL	Children and youth	Cybersafety and cybersecurity awareness
DataDetox[450]	Offers an 8-day program and game about data awareness, that is suitable for explanations and use during the lectures.	NL	Children and youth	Data privacy

[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/

DataDetoxKit[451]	Guide through everyday steps one can take to control digital privacy, security, and wellbeing.	Multilingual	Not defined	GDPR, Data privacy
De baas op internet[452]	The programme "The boss on the internet" about internet safety offering also material for teachers[453].	NL	Children but also youth at age of 14	Internet safety
It's up to you[454]	Interactive video about cyberbullying that can be used in class.	NL	Youth	Cyberbullying
CyberEDU[455]	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.	EN	Youth, young adults	cybersecurity
UNbreakable Romania[456]	Romanian national contest for high-school students and university students	RO	Youth, young adults	Cybersecurity
My Data done right[457]	Help in access, remove, correct, move your data from specific platforms	Multilingual	Not defined	GDPR
Cybersafety[458]	National platform gathering different initiatives and bringing closer cyber safety topics to children.	EL	Mostly children	cybersafety
Education game "The Witch's Secret"[459]	Interative game teaching basics of cryptography methods.	EN	Youth, young adults	Cryptography

[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/

	Published as part of a student project at the University Zagreb Faculty of electrical engineering and computing (FER), Croatia.			
E-LearningScape game[460]	Educational game developed by Sorbonne University	FR	youth	Cybersecurity
Cybermalveillance[461]	Official govermental site with relevant information and guidelines.	FR	Children and youth	Cybersecurity and cybersafety
E-Enfance[462]	Governmental supported initiative on spreading information targeted to different age groups.	FR	Children and youth	cybersafety
Internet licence for children[463]	Educational information and material	FR	Children	cybersafety
EDUSCOL[464]	Governmental official material and guidelines for teachers	FR	Children and youth	Cybersecurity and cybersafety
Fables la fontaine cyberse[465]	4 fables of La Fontaine diverted to raise awareness of cyber security	FR	Children and youth	Cybersecurity and cyber safety

[460] https://webia.lip6.fr/~muratetm/elearningscape/?fbclid=IwAR3F8VUV7K3CCvMpLWIAGmuylvbVELjqFxbYgaUV0vChqAaq_SWhntJMKLA
[461] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-accompagnement-sensibilisation-des-jeunes
[462] https://e-enfance.org/
[463] https://permisinternet.com/
[464] https://eduscol.education.fr/
[465] https://creapills.com/fables-la-fontaine-cybersecurite-cybermalveillance-20220602

Cybersecurity: The 4 Hack Academy films CIGREF[466]	Cybersecurity campaign films	FR	youth	Cybersecurity
Guide Des Bonnes Pratiques De L'informatique[467]	CPME ANSSI / 12 rules for security	FR	Youth and adults	Cybersecurity and cyber safety
Game "1,2,3 Cyber"[468]	Online free available material for the game developed by Centre de la Cybersécurité pour les Jeunes[469] and company Wavestone.	FR	11-14 years	Cybersecurity
Capitaine Cyber[470]	5 videos made for security hygiene	FR / by Belgium	Youth	Cybersecurity
Cyber security games for school[471]	Worksheet and examples for students	FR	Youth	Cybersecurity
gca toolkit by Global Cyber Alliance[472]	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[473] CNIL	5 cyber Modules with activities and attestation at the end.	FR	Youth	Cyber security
L'essentiel de la securite numerique[474]	A full guide for cyber security, written by the greatest minds in the Academia and Industry	FR	Professionals	Cyber security

[466] https://www.cigref.fr/archives/entreprise2020/cybersecurite-les-4-films-de-la-hack-academy-cigref/
[467] https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
[468] https://github.com/wavestone-cdt/1-2-3-Cyber
[469] https://www.cyberccj.com/
[470] https://www.youtube.com/channel/UCqtX3lM4BBXPDcxnsw6qXgw/featured
[471] https://www.ssi.gouv.fr/actualite/au-college-et-au-lycee-former-a-la-cybersecurite-par-le-jeu/
[472] https://gcatoolkit.org/fr/petites-entreprises/
[473] https://atelier-rgpd.cnil.fr/login/index.php
[474] https://www.nxtbook.fr/newpress/CEIDIG/l_essentiel-de-la-securite-numerique-pour-les-dirigeants-et-les-dirigeantes-2eme-edition/index.php?xtor=cigref#/p/Couverture

Guide Cybersecurite [475] by Cyber Malveillance	A good guide with practical examples.	FR	Managers of small and medium sized companies	Cyber security
Tous en ligne maintenant[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	FR	Youth	Cyber security
Project SAFE.SI[477]	Inform, advise and assist children, parents, teachers and carers on digital questions and fights against online child sexual abuse. Offers (8not regularly) courses and seminars, especially for teachers. Co-funded by the European Commission and as national awareness centre	SI	Children and youth	Cybersafety, cyberbullying, grooming and data privacy
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.	SI	Youth (from secondary and primary school)	Basic knowledge about internet and safty
Slovenian education and research network education initiative[479]	Regular educational platform providing webinars for school students and teachers about safe internet use.	SI	Mostly youth	Safe internet use

[475] https://www.cybermalveillance.gouv.fr/medias/2021/05/Guide-de-cybers%C3%A9curit%C3%A9-%C3%A0-destination-des-dirigeants-de-TPE-PME-et-ETI.pdf
[476] https://tousenlignemaintenant.fr/
[477] https://safe.si/
[478] https://sio.si/tag/varna-raba-interneta/
[479] https://www.arnes.si/storitve/varnost/most-v/