TEENAGERS and **CYBERSECURITY:**
A Practical Guide for Teachers and Parents

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

CONTENTS

Project number: 2018-1-ES01-KA201-050461

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

INTRODUCTION

For a considerable amount of European citizens, cybersecurity remains an unknown term. According to recent data, many European citizens have not yet recognised the importance of following the most basic cybersecurity measures (Erixon & Lamprecht, 2018; Pupillo, 2018). For instance, it is estimated that 50% of professionals have no passwords, PIN or biometric security protecting their devices, and 66.6% reported lack of data encrypting (Reischuk, 2019). In this context, it is understandable that in the last decade the European Union (EU) decided to develop a strong approach to enhance cybersecurity at very different levels.

Cybersecurity could be defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen, Diakun-Thibault & Purse, 2014). More concretely, according to the International Telecommunications Union (ITU), cybersecurity entails the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (Von Solms & Van Niekerk, 2013).

According to the European Agency for Cybersecurity (ENISA, 2020), cyberattacks are becoming more sophisticated, targeted, widespread and undetected. According to this agency, phishing, identity theft and ransomware have increased, particularly in the COVID-19 environment, which has served as a breeding ground to promote attacks

> The organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Craigen, Diakun-Thibault & Purse, 2014).

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

on homes, businesses, governments and critical infrastructure (Kohler, 2020; Sterlini, Massacci, Kadenko, Fiebig & van Eeten, 2019; Štitilis, Rotomskis, Laurinaitis, Nadvynychnyy & Khorunzhak, 2020). As a result, the economic losses related to cyberattacks are overwhelming for governments, agencies and institutions, businesses and individuals, who are vulnerable to increased cyber threats (Carrapico & Barrinha, 2018; Lis & Mendel, 2019). It is estimated that cybercrime costs the global economy up to $575 billion annually (Sobers, 2019). The increase of disruptive technologies such as the Internet of Things, which connects more than 50 billion devices nowadays, has increased the potential risk of cyberattack hugely (Lis & Mendel, 2019).

In this context, it seems reasonable to consider a significant investment of economic and human resources that are capable of dealing with this threat. However, little is done to deal with the lack of available resources and human capital that could address such threat. It is estimated that, by 2021, there will be 3.5 million unfilled cybersecurity positions (Ventures, 2017). Therefore, organizations will need to face the challenge of recruiting cybersecurity professionals and experts in a labour market where there is a shortage of professionals with the appropriate skills and training to meet the demands of the market (Crumpler & Lewis, 2019).

In addition, the low proportion of qualified women working in the cybersecurity sector could exacerbate the problem. According to recent data, the proportion of women employed in this sector is estimated at 7% in Europe, which is far from the gender equity demanded by the current market needs (Poster, 2018). Gender stereotypes, discrimination and a highly masculinised working environment could be behind the gender gap in cybersecurity (Bagchi-Sen, Rao, Upadhyaya & Chai, 2010; Poster, 2018). The existing literature indicates that women face many barriers to enter and progress in the sector; social, institutional, and personal challenges (Bagchi-Sen, et al., 2010). The male-oriented culture plays an important role in women's choices to engage in higher education computer science (Heaton & McWhinney, 1999). In this context, female students have limited guidance and mentoring opportunities, and such opportunities play a crucial role in encouraging their entrance in the IT job market (Ahuja, 2002; Parasuraman, Purohit, Godshalk & Beutell, 1996). Educational background, interest and abilities, and IT identify may collapse with different aspects of the feminine role identity, negatively influencing woman's belief in her ability to succeed in the sector (Trauth, Quesenberry & Morgan, 2004). In addition, the difficulty of balancing professional and family responsibilities have been found to be a considerable barrier in

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

their career advancement (Armstrong, Riemenschneider, Allen & Reid, 2007). Taking into account that cybersecurity's future depends on its ability to attract and retain women, promoting their presence in cybersecurity should be understood as a priority nowadays (Poster, 2018). Minimizing early career barriers, assuring equal opportunities in accessing IT careers, promoting women's careers advancement in IT as well as technical and analytical skills among women could increase their presence in the IT sector. These aspects could, in turn, contribute to a higher presence of female models that guide and inspire young women to get involve in the field (Bagchi-Sen, et al., 2010).

For all of these reasons, Be@CyberPro is an EU project dedicated to bridging the skills and gender gaps in the cybersecurity sector by training, inspiring students, empowering teachers, and involving parents. Be@CyberPro's goal is to address the gender gap by collaborating with private sector companies and academic institutions and working with middle, high schools and vocational schools to promote cybersecurity careers. The primary target group of the project are secondary school and formal vocational training students in general, and girls in particular. Secondly, teachers and families will be impacted. Making information about cybersecurity careers more available to students, teachers and parents could positively affect more young people in choosing this path. In addition having access to information about positive female role models may help to motivate young girls to follow through with their passion.

This is precisely the aim of this book: to disseminate some of the most outstanding outputs of this project amongst teachers and families.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

MOODLE E-LEARNING FRAMEWORK

An online course has been developed on Moodle with the basic contents of computer security for teachers, so that they have the appropriate knowledge to teach computer security to their students and knowledge of the profession to be able to guide students.

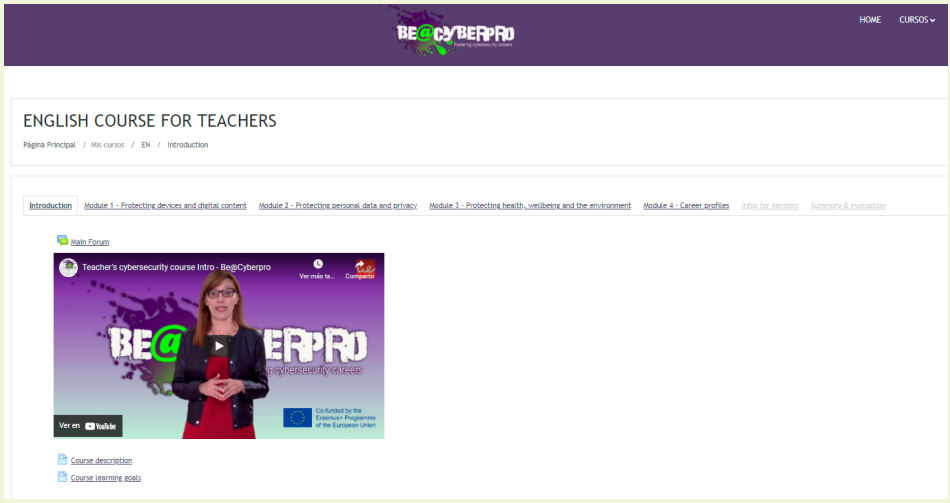


Figure 1. Screenshot of the Cybersecurity course for Teachers on Moodle platform.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Moodle is a Course Management System (CMS), also known as a Learning Management System (LMS) or a Virtual Learning Environment (VLE). It is a free web application that educators can use to create effective online learning sites. It has become very popular among educators around the world as a tool for creating online dynamic web sites for their students. To work, it needs to be installed on a web server somewhere, either on one of your own computers or one at a web hosting company.

- The focus of the Moodle project is always on giving educators the best tools to manage and promote learning, but there are many ways to use Moodle: Moodle has features that allow it to scale to very large deployments and hundreds of thousands of students, yet it can also be used for a primary school or an education hobbyist. Many institutions use it as their platform to conduct fully online courses, while some use it simply to augment face-to-face courses (known as blended learning).

- Many of our users love to use the activity modules (such as forums, databases and wikis) to build richly collaborative communities of learning around their subject matter (in the social constructionist tradition), while others prefer to use Moodle as a way to deliver content to students (such as standard SCORM packages) and assess learning using assignments or quizzes.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

DIDACTIC PROGRAMMING: Cybersecurity for teachers

INDEX

SCANNING...

Project number: 2018-1-ES01-KA201-050461

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

PRESENTATION

The didactic material prepared by Be@CyberPro can be used in your classes to work with your students. The aim is to improve their digital competence and above all to generate responsible and informed behaviour in accordance with the basic principles of cybersecurity.

This program offers a proposal to work with students based on these materials. You can work on all of the content or. select individual modules.

The recommended timing in this programming is 8 one-hour sessions. 1 to 3 work sessions for each of the modules or blocks of content.

For ESO and baccalaureate students, group tutoring sessions can be a perfect space to implement these didactic proposals in case you do not teach subjects specifically focused on digital technologies, although you can also use this program in other subjects.

SOME PRACTICAL TIPS BEFORE GETTING STARTED

- Introduce each topic to be discussed through a dialogue with the students. Ask open-ended questions that allow them to share experiences and concerns with each other.
- You can use some other resources to introduce a topic such as:
    - Current news.
    - Excerpts from movies.
    - Excerpts from a series that is focused on your age group.
    - Works from real case studies that are close to the students' needs and interests. Don't do it all yourself. Invite cybersecurity experts so students can learn about other realities.
- Speak honestly, without minimising or softening the risks but without exaggerating. Prevention begins with knowing the truth
- Encourage their critical thinking by contrasting information or conducting activities in which they can share their ideas and opinions.
- Use a variety of material. Apart from the ones we havesuggested, you can find more material in online educational spaces such as https://www.betterinternetforkids.eu/. There is also a network of Safer Internet Centres (SICs) across Europe – typically comprising an awareness centre, helpline, hotline and youth panel.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

MODULE 1. PROTECTION OF DIGITAL DEVICES AND CONTENTS

LEARNING GOALS

- Be able to differentiate a wide variety of risks and threats in digital environments: fake news, ransomware, phishing, spam, grooming, sexting, copyright infringement, etc.
- Know how to apply security and protection measures and guide others (peers and students) to apply them.
- To know about safety and security measures and to have a due regard to reliability and privacy.

COMPETENCIES BASED ON DigComp FRAMEWORK

4.1. Devices and digital content protection

Knowledge:

- K1. Advanced risks and threats in digital environments.
- K2. Advanced protection measures for digital devices: use of antivirus, antimalware, antispam filters, passwords, software updates.
- K3. Personal information. Levels of protection according to the nature of the data.

Skills:

- To protect devices and digital content, and to understand risks and threats in digital environments.

Contents[1]:

1.1. Protection of digital devices.

1.2. Risks and threats in digital environments.

1.3. Protection of digital content.

1.4. Responsible use of technology.

SESSION 1

Introduction. Previous knowledge

- Initial dialogue "The advantages and risks we already know about when using a smartphone".
- Questionnaire to identify device usage habits.
- Brainstorming about a glossary of terms: fake news, ransomware, phishing, spam, grooming, sexting, copyright infringement, industrial espionage, etc.

[1] All contents are available on the project website: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Identification of problem situations in cooperative groups What kind of problem is it? How do you think it can be solved?
- Resolution with the whole class of the problematic situations.
    - o You access the school/IES website and get a message asking you to install an update to the teacher communication app. It is malware.
    - o You have been talking to a person on Instagram for two months, they are very nice and are asking you to meet them in person, but when you arrive at the meeting place they don't seem to be who they said they were.
    - o You just got an sms asking you to access your school account /IES and include the password, but this message has not been sent from the institute.

SESSION 2

Sextorsión[2]

- **"Pencils in the Centre" or round Robin** is a very useful way to build knowledge where students interact with each other to review content they have learned. In teams of 4, they take turns to read some questions and answer them orally. When it's time to listen and speak, they put their pencils or devices in the middle of the table. They can't write or use their devices when it is time to listen and speak. Once they have finished talking and everyone knows what they have to do, it's time to pick up their pencils or devices and start writing. When it's time to write they cannot talk to their classmates.
- For "Pencils to the centre" Groups of 4 people are formed and 4 questions or exercises are posed about content of thethe previous session.
- To start the work, all the students must leave their pencils/computers in the center of the table; this indicates to students that it is time to have a conversation with their classmates. First, the person responsible for activity number 1is in charge of reading the question/exercise to the their group.. Together, they discuss and decide the best way to solve the activity. Once they have reached an agreement, all of the students take their respective pencils/devices, (signaling that they now remain silent) and individually write down the solution they have reached as a group. Once everyone has finished writing the answers individually,they put their pencils/devices back in the center. Then the person in charge of the second activity reads it repeating the same process, until all the exercises are finished.

[2] This topic may not be considered as adequate for the curricula of all countries. Please, confer with the school board or a sex educator before addressing it.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Viewing of a fragment of the series *Skam* (sextortion case).
- Search for news in the press about sextortion cases.
- Complete the Decision Tree[3] based on a situation of possible sexting: "If an unknown person is trying to flirt with you on social networks...". "A tree diagram which is used for making decisions in business or computer programming and in which the branches represent choices with associated risks, costs, results, or probabilities" (Merriam-Webster).

SESSION 3

Fakenews

- Initial dialogue: What do we know about fake news? We share some that we know. We have prepared some of the most current examples.
- Guidelines to identify a fake news.
- Group activity: "The guardians of the truth". Several news items are provided, students must identify the truth and the lie in each one of them by contrasting the information. The dynamics of the cooperative activity "Pencils to the center" can be followed.

[3] "A tree diagram which is used for making decisions in business or computer programming and in which the branches represent choices with associated risks, costs, results, or probabilities" (Merriam-Webster).

MODULE 2. PROTECTING PERSONAL DATA AND PRIVACY

LEARNING GOALS

- Apply different strategies to prevent physical and psychological risks derived from the use of digital technologies and guide others (peers and students) to apply them.
- Be able to differentiate a wide variety of undesireable effects on the environment derived from the use of digital technologies and reflect on how to minimize this impact.
- Guide others (peers and students) in the use of technological resources, useful for the development of inclusion and/or well-being.

COMPETENCIES BASED ON DigComp FRAMEWORK

Digital identity management

Skills:

- S1. Critical use of different digital identities, selecting the most appropriate in each context or situation.
- S2. I select and manage my digital identity in documents and data produced by me.
- S3. I use different ways to protect my digital identity and verify that they work correctly.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

4.2. Personal data and privacy protection in digital environments

Knowledge:

- K1. Risks derived from an incorrect protection of personal data or information.
- K2. Simple tools and methods for the protection of personal data and information.
- K3. Basic aspects and facts of privacy policies.
- K4. Tools and strategies of personal data and content protection (intermediate level).
- K5. Technological resources for data protection.

Contents[4]:

Lesson 2.1. The importance of data protection and personal information.

Lesson 2.2. Tools and methods to protect personal information and data online.

Lesson 2.3. Tools and methods for protecting personal information and data offline

Lesson 2.4. Privacy policies and digital fair play

Skills:

- To protect personal data and privacy in digital environments.
- To understand how to use and share personally identifiable information while being able to protect oneself and others from damages.
- To understand that digital services use a "Privacy policy" to inform how personal data is used.

SESSION 1

Introduction. Previous knowledge

- Initial dialogue: Do we know what personal data cannot be shared without permission? How can we protect our personal information?

[4] All contents are available on the project website: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- We solve some problematic situations in cooperative groups. You can follow the dynamics of the cooperative activity "Pencils in the middle".
    - Someone takes a picture of you falling in the street and your friends want to upload it to Tik Tok.
    - A friend has posted pictures from the summer at the beach on Instagram and you are in a bikini.
    - A person has started following you on Instagram and makes comments on your photos, they say they know you but you don't know who they are.
- We review together the privacy policy of the social networks we all use: How is it set up? What would be the safest way? What does this involve?

SESSION 2

My data and me

- Group activity "Numbered heads together" to remember review work from the previous session.
    1. Groups of four members are formed and numbered.
    2. The teacher asks a question and the students will individually think of an answer: How do you prevent your friends from sharing information that you do not want to share?
    3. A group discussion is held in each of the groups "putting heads together" in the form of a circle. (Hence the name of this activity).
    4. After a few minutes, the teacher chooses a number from 1 to 4 and the corresponding student answers the question on behalf of his or her team.
- Here are some tools and methods for protecting information online and offline:
    - #1 Cortafuegos.
    - #2 Software antivirus.
    - #3 Create strong passwords.
    - #4 Don't overshare on social media.
- Complete the Decision Tree "Reflect on what you publish".

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

MODULE 3. PROTECTING HEALTH, WELLBEING AND THE ENVIRONMENT

LEARNING GOALS

- Respect copyrights, licenses and usage restrictions on the resources I share and promote among students respect for the copyright rules of digital resources embedded in virtual learning environments.
- Take measures to protect sensitive data and information in digitally shared items and encourage students to do the same with their assignments.

COMPETENCIES BASED ON DigComp FRAMEWORK

4.3.1. Protecting health and well-being

Knowledge:

- Knows the effect of prolonged use of technologies.
- Knows about the addictive aspects of technologies.
- Understands the environmental impact of computers and electronic devices and how s/he can make them last longer by recycling parts of it.
- Can determine if appropriate and safe digital means are available, that are efficient and cost-effective in comparison with other means.

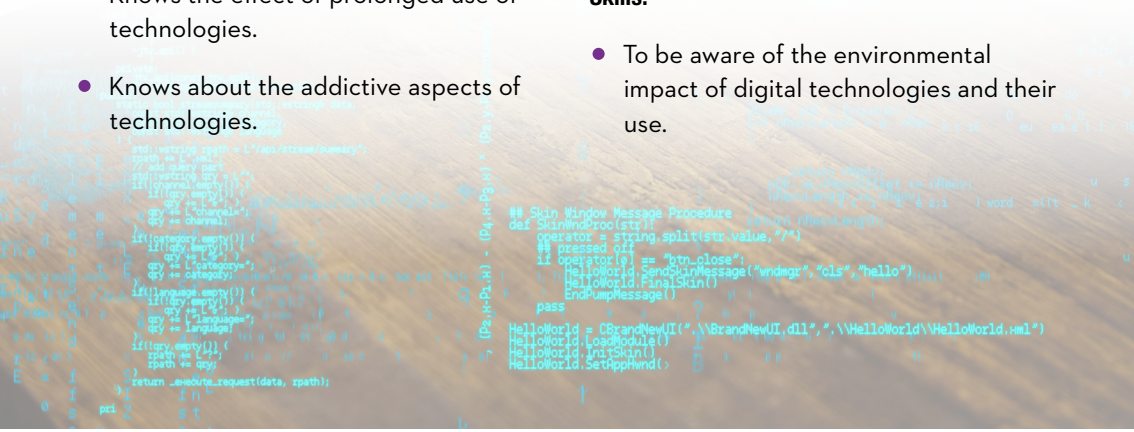
Skills:

- To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies.
- To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying).
- To be aware of digital technologies for social well-being and social inclusion.

4.4. Protect the environment

Skills:

- To be aware of the environmental impact of digital technologies and their use.



Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Contents[5]:

Lesson 3.1. Positive and negative effects of computer and digital technology use.

Lesson 3.2. Protecting physical health during the use of technology.

Lesson 3.3. Protecting psychological well-being in the digital environment.

Lesson 3.4. Digital technologies for social well-being and social inclusion.

Lesson 3.5. Protecting the environment.

SESSION 1

- **Initial conversation:** Technology and health: Does the use of technological devices affect your physical and mental health? Previous knowledge is identified and tips are provided.
- Survey about their habits regarding the use of technology and health.
- Team dramatisation exercise to reflect on behaviours that do or do not enhance physical health and/or psychological well-being using technology (poor ergonomics, bad lighting, ignoring someone, etc.).
- Group activity "Rotating Folio" to summarize what was learned in the session.
- The teacher asks the teams to do an activity (summarise, write an essay, make a list, etc.). One student from each team is in charge of writing a part on a sheet of paper that will rotate among all the teammates. When one student writes, the others must pay attention to what he/she writes, they must help them, advise them and motivate them. Once they have made their contribution, they passs the sheet of paper to the next teammate and the same operation is repeated. until the paper has passed through all the team members.

[5] All contents are available on the project website: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

MODULE 4. PROFESSIONAL PROFILES

LEARNING GOALS

- Communicate to students a positive attitude towards digital technologies, making them aware of the possible risks and limits, but also generating confidence that they will be able to manage them to reap the benefits of these technologies and encouraging them to use them in a creative way and review.
- Develop pedagogical strategies to prevent, identify and respond to the unsafe use of digital devices and publication of digital contents by students.
- Develop strategies to promote that students protect their personal data and digital identity in digital environments.
- Develop strategies to prevent, identify and respond to the behaviours of my students that negatively affect their health and well-being using digital technologies.

Contents[6]:

Lesson 4.1. Professional profiles.

SESSION 1

- **Initial conversation:** "Do you know anyone working in the cybersecurity sector?"
- Presentation of the ebook of interviews with professionals.
- Conversation about the book presented: What surprised you?
- Individual activity "If I worked in cybersecurity I would like to do..." and what would you ask someone who works in cybersecurity?

SESSION 2

- Visiting cybersecurity women experts (face-to-face or synchronous online). They tell us about their experience
- We initiate a debate based on the questions from the individual activity of the previous session and others that arose during the presentation of the guests.
- We generate a collaborative prezi presentation to draw the conclusions of this module.

[6] All contents are available on the project website: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

CYBERSECURITY FOR PARENTS
Best practice guide

INDEX

Project number: 2018-1-ES01-KA201-050461

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

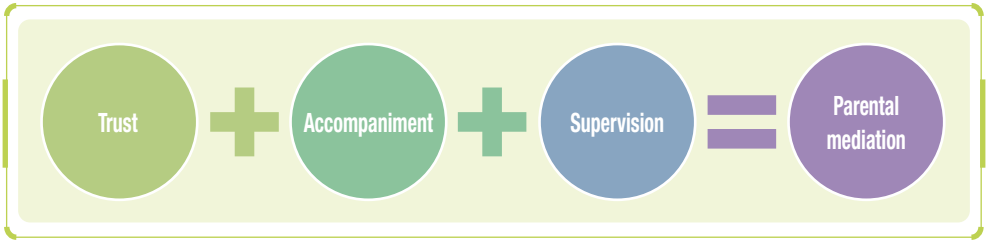
PRESENTATION

The purpose of this guide is to help parents ensure their children understand the basic principles of cybersecurity to ensure their safety online, as well as nurturing responsible informed online behavior.

Together you can:

- Enjoy the Net
- Prevent risks
- Detect and deal with problems

We will give you some practical tips to parental mediation toensure the safety of your children on the Net.



SOME PRACTICAL TIPS BEFORE YOU BEGIN

- Maintain an open and non-judgmental dialogue with your children. Ask open-ended questions that allow them to share experiences and concerns. It won't always be easy and they won't always be receptive. Find the time to let the conversation flow.
- You can use some other resources to start a conversation such as:
  - Current news.
  - Movie clips.
  - Excerpts from a tv show or series focused on their age group.
- Don't do it all yourself. If you think your child may have a problem, talk to the tutor at the school, so that you can act in a coordinated way.
- Speak honestly, without minimising or softening the risks but without exaggerating. Prevention begins with knowing the truth.
- Encourage their critical thinking by contrasting information or carrying out activities in which they can share their ideas and opinions.
- Adapt to your child's level of autonomy and maturity.

Here are some tips on how to work on different cybersecurity issues at home.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

1. PROTECTION OF DEVICES AND DIGITAL CONTENT

OBJETIVES

- Createa positive attitude towards digital technologies raising awareness of the possible risks and limits, while also generating the confidence to handle them to take advantage of the benefits of technologies and encouraging creative use in a safe and responsible way.
- Be able to differentiate a wide variety of risks and threats in digital environments, for example: fake news, grooming, sexting, sharenting, etc. (see Glossary at the end of the guide) and how to protect against them.
- Know how to apply security and protection measures and guide children to apply them.

WHAT CAN YOU DO?

TRUST

- Be careful how you react if children tell you they are having a problem. It is not a time to blame, but to solve together.

ACCOMPANIMENT

- Guide your children in the appropriate use of technology. You can agree on some guidelines for responsible use or even sign a pact that is visible at home.
- Be a role model.
- Share online activities together. It's not a matter of invading the online space and "liking" everything they post, but you can spend time together online looking for information.

SUPERVISION

- Keep up to date with their online presence. The apps they use the most, the social networks they have profiles on.
- You can make use of parental control resources to limit access to unsafe sites. (Qustodio, Secure Kids or Parental Click are some examples).
- Keep an eye out for inappropriate content (content that encourages risky or negative behaviours or content that is not appropriate for their developmental level).

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

2. PROTECTING PERSONAL DATA AND PRIVACY

OBJETIVES

- Apply different strategies to prevent physical and psychological risks derived from the use of digital technologies and guide children to apply them.
- Be able to differentiate a wide variety of unwanted effects in the environment derived from the use of digital technologies and reflect on how to minimize this impact.
- Guide in the use of technological resources useful for the development of inclusion and/or well-being.

WHAT CAN YOU DO?

TRUST

- Generate a climate of trust, so that you can talk about your presence on the Web, the information you receive and the information you share.

SUPPORT

- Create strong passwords together to protect your devices.
- Review the configuration options of the devices and services on the network together and be aware of what information that is being shared.
- Be a role model

SUPERVISION

- The PEGI code of conduct classifies apps by age, review the apps children have access to in order to avoid use of inappropriate ones.
- If t app has a limited user (go to advanced settings > users or accounts and follow the steps), restrict the apps or files they have access to by applying parental controls if necessary.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

3. PROTECTING HEALTH, WELL-BEING AND THE ENVIRONMENT

OBJETIVES

- Develop strategies to prevent, identify and respond to children's behaviours that negatively affect their health and well-being using digital technologies.

WHAT CAN YOU DO?

TRUST

- Talk openly about the harmful effects of inappropriate use of technology on health, well-being or the environment in order to establish agreements for correct use at home and away from home. These agreements should make clear the times and places for connecting to the Net. Excessive use can affect sleep, social relations or study.
- Trust them to comply with these agreements without becoming a constant supervisor.

SUPPORT

- Be a role model.
- If your child has had a problem and there are other minors involved, contact their parents or guardians to clarify the situation and resolve it in a coordinated manner.

SUPERVISION

- Observe your child's behaviour and make sure that agreements about the appropriate use of technology are followed without invadingtheir privacy.
- Establish clear boundaries to prevent them from suffering or exercising abuse through technologies. For example, the agreement makes it clear that it is not permissible to make fun of someone who has been videotaped without their consent and that they must protect their privacy.

GLOSSARY

Cyberbullying: A form of bullying or harassment using digital technologies.

Fake news: News stories that are false: the story itself is fabricated, with no verifiable facts, sources or quotes.

Online Grooming: Is where someone befriends a child online and builds up their trust with the intention of exploiting them and causing them harm. Sexting: A minor shares content with sexual connotations.

Sharenting: Overuse of social media.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

DIDACTIC PROGRAMMING ABOUT Be@cyberpro Video Game

Project number: 2018-1-ES01-KA201-050461

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

WHAT IS Be@CyberPro?

Be@CyberPro is a project dedicated to bridging the skills and gender gaps in the cybersecurity sector training, by inspiring students, empowering teachers, and involving parents. Be@CyberPro is an immersive multi-language experience game used to explore various cybersecurity professional profiles and challenges. It is an interactive browser-enabled digital game, to enable students from various contexts and with different equipment to be able to play.

> **Gametime:** The gameplay – incorporating all levels – is designed to span between 40 minutes and 1 hour – the duration of a regular school class.
>
> **Game Narrative:** The game follows a role-playing game style, where players assume the roles of characters in a fictional setting. The main protagonist, a girl attending high school or secondary school, has to solve a variety of cybersecurity-related challenges, associated with different cybersecurity career profiles, to help out her friends and schoolmates.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

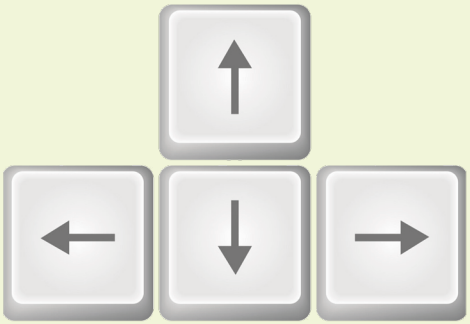
How to play the game:

- To begin, click on New Game with your mouse or trackpad.
- When the screen loads, click anywhere using the mouse/ trackpad to begin conversations between the characters.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Use the arrows on the keyboard, or click an area to make the character move around.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union



- Approach characters within the game to engage in conversations.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Click anywhere on the screen to continue conversations.
- Click on pop-up buttons using the mouse or press the enter key to choose your response.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Approach doors to move to different rooms.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Press Esc at any time to view the Options Menu.

Project number: 2018-1-ES01-KA201-050461

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

- Follow instructions from the characters in the game to complete tasks and learn about cyber security.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Game Link: The game can be accessed online from all devices at:
http://telprojectgames.com/CyberPro/Test/index.html

Appendix: Be@CyberPro Storyboard:
https://drive.google.com/file/d/18HWpPqragp9Pstp7hgEsAmtg97Af2W8i/view?usp=sharing

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

BEFORE INTRODUCING THE GAME TO YOUR CLASSROOM

Here are some suggestions about how you might use the game in your classroom:

1. Play the Game yourself, make yourself familiar with the controls, narrative and learning content surrounding the game.

2. Consider involving parents and guardians. One suggested way to open the door to parent or guardian participation would be sending a letter home with students, or communicating through other means your game-based learning plan and its benefits to parents and guardians. Doing so might also help avoid confusion if students come home and talk about playing games in class.

3. Dedicate time to consistent in-class play. To ensure your students enjoy enough "play time" with the Be@CyberPro game to reap its benefits, try to:

    - Include game time as a designated activity in your lesson plan.
    - Use a game as an entry or exit ticket to learning. By using the game as an entry point to learning about cyber security, it allows students to draw their own conclusions about the importance of cyber security before the concept is explained in detail and reinforced by the knowledge expert.
    - Create a series of learning stations, one of which is playing the game.

INTRODUCING LEARNING STATIONS TO STUDENTS

Learning stations are physical locations in the classroom where students are asked to solve a problem and answer some questions using the materials provided.

A learning station can be used to allow students to play the game individually, in pairs or small groups during class.

Take time to very explicitly introduce the new learning stations to the class and discuss rules associated with using the learning stations.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Before you begin, clearly explain expected behaviour while using the learning stations and the consequences of not meeting these expectations. Then, introduce the nEw learning station to your students by modeling the following steps:

- *If applicable,* use a timer that students can see and hear to keep track of time spent in the learning stations.
- Teach the students how you will get their attention while they are in the learning station (e.g. raise hand).
- Explain in detail the purpose of the selected activity they will be working on —

"This is what you should learn at this learning station."

Show only enough that students understand and feel comfortable working on activities. Demonstrate how to clean up the area and rotate to the next student when the timer goes off.

USING THE GAME IN YOUR CLASSROOM

1. Introduce the topic briefly and explain the aims and narrative of the game to the students prior to playing the game.
2. Set a quick baseline of knowledge prior to gameplay. Ask by a show of hands or similar, if anyone knows anything about cybersecurity or if they have ever had an issue with cybersecurity before.
3. Let the students play the first level and ask them to pause the game when they have finished.
4. Once everyone has finished the first level, have a debriefing session and discuss with them what they have learned so far. Some suggested discussion points are:
    - What students have learned from this level.
    - What they think about what they have learned so far.
    - If anyone has had any similar experiences.
    - If anyone had any difficulties understanding the material.
    - If students are motivated to continue with the game.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

5. Ask the students to continue playing the game following this same structure (play level, then discussion points).

6. When students have completed the game, distribute game evaluation tools (i.e., the online questionnaire) to the students.

7. Use data collected from discussions and feedback to create lessons using your findings. For example, focus on a common trouble spot.

SUPPORTED LEARNING

Using game-based learning whic incorporates goals, rules, challenges and interactions can help to engage students and increase learning outcomes. Game based learning can also:

- Build an emotional connection to learning and subject matter.
- Provide opportunity for feedback and practice.
- Can be customised to individualised teaching.

As part of the educational use of information communication technology, digital games can be used as learning tools, motivators and generators of curiosity and, as a result, games in the classroom have been widely agreed as an effective means of optimising student learning and performance in daily educational practice. The positive relationship between a students' engagement and their intake of information while using digital games has been confirmed by various independent studies over recent years (Cojocariua, Boghiana, 2014; Papadakis, 2018).

> "Using game-based learning whic incorporates goals, rules, challenges and interactions can help to engage students and increase learning outcomes."

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

ONLINE GAME LINK

The game can be accessed online from all devices at:

http://telprojectgames.com/CyberPro/Test/index.html

PROJECT WEBSITE

https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461

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

REFERENCES

Ahuja, M. K. (2002). Women in the information technology profession: A literature review, synthesis and research agenda. *European Journal of Information Systems*, *11*(1), 20-34.

Armstrong, D. J., Riemenschneider, C. K., Allen, M. W., & Reid, M. F. (2007). Advancement, voluntary turnover and women in IT: A cognitive study of work-family conflict. *Information & Management*, *44*(2), 142-153.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, *12*(1), 24-31.

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight profi-ciency levels and examples of use*, EUR 28558 EN, doi:10.2760/38842

Cojocariu, V. M., & Boghian, I. (2014). Teaching the relevance of game-based learning to preschool and primary teachers. *Procedia-Social and Behavioral Sciences*, *142*, 640-646.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

Carretero, S., Vuorikari, R., & Punie, Y. (2016). *DigComp: Marco Europeo de Competencias Digitales para la ciudadanía*.

ENISA (The European Union Agency for Cybersecurity) (2020). *ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Erixon, F., & Lamprecht, P. (2018). The next steps for the digital single market: From where do we start. *ECIPE Policy Brief*, *2*, 2018.

Heaton, C. A. N., & McWhinney, G. (1999). Women in management: the case of MBA graduates. *Women in Management Review*.

Kohler, K. (2020). Estonia's National Cybersecurity & Cyberdefense Posture.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2).

Papadakis, S. (2018). Evaluating pre-service teachers' acceptance of mobile devices with regards to their age and gender: a case study in Greece. *International Journal of Mobile Learning and Organisation*, *12*(4), 336-352.

Parasuraman, S., Purohit, Y. S., Godshalk, V. M., & Beutell, N. J. (1996). Work and family variables, entrepreneurial career success, and psychological well-being. *Journal of vocational behavior*, *48*(3), 275-300.

Poster, W. R. (2018). Cybersecurity needs women.

Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, (2018/06).

Reischuk, R. (2019). *Let's Encrypt: Cybersecurity disruptieren*.

Sobers, R. (2019). must-know cybersecurity statistics for 2019. *Varonis*.

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Security & Privacy*, *18*(1), 46-54.

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National Cyber Security Strategies: Management, Unification and Assessment.

Trauth, E. M., Quesenberry, J. L., & Morgan, A. J. (2004, April). Understanding the under representation of women in IT: Toward a theory of individual differences. In *Proceedings of the 2004 SIGMIS conference on Computer personnel research: Careers, culture, and ethics in a networked environment* (pp. 114-119). Ventures, 2017

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Project number: 2018-1-ES01-KA201-050461

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

PARTNERS

Universidad Europea de Madrid (Spain)

- Eva Jiménez García
- Gonzalo Mariscal Vivas
- Javier Fernández Collantes
- Luis Antonio López Fraile
- Sara Esteban Gonzalo
- Sonia Martínez Requejo

Colegio JOYFE (Spain)

Munster Technological University (Ireland)

European Software Institute – Center Eastern Europe (Bulgaria)

- Christina Todorova
- Pavel Varbanov

Project number: 2018-1-ES01-KA201-050461

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

PARTNERS

The Irish Computer Society
(Ireland)

- Liz Mc Carthy

PROMPT-H LTD
(Hungary)

- Annamaria Kacsur

SZÁMALK-Szalézi Vocational and Technical School
(Hungary)

- Ildikó dr Sediviné Balassa
- Gabriella Kőhegyi

University of Alcala
(Spain)

- Maite Villalba Benito
- Luis Fernández Sanz
- Ana Castillo
- Inés López Baldominos
- Vera Pospelova

125th High School «Boyan Penev»
(Bulgaria)

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

 ERASMUS+ Project 2018-1-ES01-KA201-050461

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Edited by McGraw Hill, Madrid, Spain
c/ Basauri, 17
28023 Aravaca (Madrid)
Editor: Cristina Sánchez Sainz-Trápaga
General Manager (South Europe): Álvaro García Tejeda
Development team: Diseño y Control Gráfico

ISBN (digital): 978-84-486-2696-9
ISBN (print on demand): 978-84-486-2697-6
MHID: 978-000-85-0304-8

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union