Facultat de Psicologia, Ciències
de l'Educació i de l'Esport **Blanquerna**
Universitat Ramon Llull

laSalle
UNIVERSITAT RAMON LLULL

FACULTAT DE PSICOLOGIA, CIÈNCIES DE L'EDUCACIÓ I DE L'ESPORT
BLANQUERNA
ENGINYERIA I ARQUITECTURA LA SALLE

UNIVERSITAT RAMON LLULL

Official Master in Training Teachers for Secondary and Sixth-Form Teaching, Vocational Training and Language Teaching

TREBALL FINAL DE MÀSTER
Curs 2021-2022

HOW TO EDUCATE IN CYBER SECURITY?

A TEACHING-LEARNING PROJECT IN THE ENGLISH LANGUAGE

STUDENT: Maria I. Bustamante Rabazo
DIRECTOR: Núria Hernández

DECLARACIÓ D'AUTORIA DEL TREBALL FINAL DE MÀSTER

Data: ***13/06/2022***
Autor(a): ***Maria I. Bustamante Rabazo***
DNI / NIE / Passaport:

Jo, com a signant d'aquest document declaro i faig constar:

1) *Que soc autor/a del treball final de màster que porta per títol:* ***How to educate in cyber security? A teaching-learning project in the English Language.***

2) *Que com a tal autor/a soc el/la responsable intel·lectual de la gènesi i execució del mateix.*

3) *Que el treball és un document de contingut original i que no ha estat prèviament publicat ni total ni parcialment.*

4) *Que he referenciat degudament en el text qualsevol aportació intel·lectual d'altres autors.*

5) *Que per tant no he incorregut en frau i en cas contrari acceptaré les sancions acadèmiques que se'n puguin derivar.*

Signatura

ACKNOWLEDGMENT

A long time ago I discovered that teaching was what I really wanted to do when I grew up. For various reasons, over the years, I drifted away from it. However, in my head, there was always a little voice telling me not to forget, that part of my happiness would not be where I was going, but that I had to fight to go further.

Fate or chance, I met the person who helped me to sit down, think and see what I really wanted. He helped me when I needed it most, without even knowing it myself. Suddenly all my ideas became clear and I decided to go for it. A path that has not been easy or short and that has kept me awake at night more than once. Uncertainty, nerves, fears, desire and passion, all together. But he was always there. So, first of all, I would like to thank him for all his support. Luis, thank you for being who you are, for being with me from the beginning, and for not letting me throw in the towel at any moment. Let's continue to share this path, called life, together.

I would also like to thank the most important part of my life, my family. For always believing in me and supporting me in all my decisions, letting me make my own way and not judging me. Especially to my auntie. You have just left knowing I was reaching my dream and despite I miss you so so much I know that wherever you are, you are very happy for me. I love you very much.

To my friends, above all, to my "master girlss" for being a great discovery and support in this frenetic year full of emotions and work, a lot of work. Thank you.

On the other hand, I would like to thank all the teachers who have accompanied me for years in my academic stage, especially, the team of great professionals who make up this master’s, you are AMAZING. Thank you for giving us so much knowledge and so much passion for this profession which, despite being hard, is also very, very beautiful.

I would also like to thank my internship tutor for teaching me so much and helping me with this project. Without your help, I would not have been able to do it.

And, last but not least, thanks to my tutor Nuria. For helping me from the beginning and guiding me in this project that tries to combine part of my knowledge in the different worlds of cyber security and education. Thank you!

ABSTRACT

This project aims to educate secondary school students in cyber security through a teaching-learning project using the English language. To this end, a study has been carried out on the knowledge and implementation of existing cyber security measures in secondary school classrooms. As part of this study, different instruments were used in a secondary high school in l'Hospitalet de Llobregat. Starting with a student observation phase, questionnaires were carried out with the English department teachers and, finally, surveys were carried out among students in order to design a project that was as appropriate as possible to the needs of the centre. This project, created to be carried out in the English language sessions, has different educational activities with the aim of making teenagers aware that proper use of the Internet and new technologies are of the utmost importance.

Keywords: *teaching-learning project, English language, cyber security, secondary education, educational activities.*

RESUMEN:

El presente trabajo recoge un proyecto de enseñanza-aprendizaje a través de la lengua inglesa para educar a los alumnos de secundaria en ciberseguridad. Para ello, se ha realizado un estudio acerca del conocimiento e implantación de medidas de ciberseguridad existentes en las aulas de los centros de secundaria. Dentro de dicho estudio se han procedido a utilizar diferentes instrumentos en un centro de educación secundaria de l'Hospitalet de Llobregat. A partir de una fase de observación en el alumnado se ha realizado un cuestionario entre los docentes del departamento de inglés y, finalmente, se han pasado encuestas a los alumnos para poder diseñar un proyecto lo más adecuado posible a las necesidades del centro. Este proyecto, creado para ser llevado a cabo en las sesiones de lengua inglesa, cuenta con diferentes actividades educativas con la finalidad de hacer que los adolescentes sean conscientes de que un buen uso de Internet y de las nuevas tecnologías es de vital importancia.

Palabras clave: *proyecto de enseñanza-aprendizaje, lengua inglesa, ciberseguridad, educación secundaria, actividades educativas.*

RESUM:

El present treball recull un projecte d'ensenyament-aprenentatge a través de la llengua anglesa per a educar als alumnes de secundària en ciberseguretat. Per a això, s'ha realitzat un estudi sobre el coneixement i implantació de mesures de ciberseguretat existents a les aules dels centres de secundària. Dins d'aquest estudi s'han procedit a utilitzar diferents instruments d'un centre d'educació secundària de l'Hospitalet de Llobregat. A partir d'una fase d'observació en l'alumnat, s'ha realitzat un qüestionari entre els docents del departament d'anglès i, finalment, s'han passat enquestes als alumnes per a poder dissenyar un projecte el més adequat possible a les necessitats del centre. Aquest projecte, creat per a ser dut a terme en les sessions de llengua anglesa, compta amb diferents activitats educatives amb la finalitat de fer que els adolescents siguin conscients que un bon ús d'Internet i de les noves tecnologies és de vital importància.

Paraules clau: *projecte d'ensenyament-aprenentatge, llengua anglesa, ciberseguretat, educació secundària, activitats educatives.*

TABLE OF CONTENTS

1. INTRODUCTION

It is not a secret to anyone that cyberspace increasingly offers a globally accessible marketplace with a wide range of services for all users, whether natural or legal persons (Kopp, Layton, Sillitoe & Gondal, 2015). To such an extent that we can say that digital has overcome analogue (Gamito, Aristizabal & Vizcarra, 2019).

In January 2022, the annual Global Digital Statistics report estimated that, worldwide, 6 out of 10 people were Internet users. This figure, therefore, indicates that 4.95 billion people are connected to the internet. This data shows us that over the past 10 years Internet users have more than doubled. However, it is also true that the levels of internet adoption are not the same in all parts of the world (Kemp, 2022).

According to the *Ministerio del Interior* (2021), in Spain, 99.8% of young people between the ages of 16 and 24 states that they have accessed the Internet in the last three months. This data should not surprise us because, nowadays and especially after what we have experienced as a result of COVID-19, even educational centres have been forced to adapt to new technologies (García-Collantes & Garrido, 2022). This, therefore, has meant that all students require access to the network.

Moreover, it is worth mentioning that these young people can be considered digital natives as they do not know a world without computers, mobiles, or even the Internet. They have grown up in a world where they have spent long hours surrounded by digital environments and have seen the use of technologies as part of their daily lives (Holt, Bossler & Seigfried-Spellar, 2017). This term was introduced in 2001 by Marc Prensky who established that the digital natives are characterised as the first generation to grow up with new technologies and hence showed quantitative data about the hours they spent in front of them. He also identified a series of differentiating characteristics of those then known as digital immigrants (Vasquez, 2019).

However, technology is not neutral. We can say that the Internet has both lights and shadows (Gamito, Aristizabal & Vizcarra, 2019). These technologies are evolving by leaps and bounds as time goes by and this continuous evolution, in turn, has created in parallel a myriad of opportunities for crime and misuse (Holt, Bossler & Seigfried-Spellar, 2017).

For this reason, cyber security is more and more often becoming a topic of discussion. Mainly because there is an extensive list of possible harmful behaviours that can occur on the internet if the corresponding measures are not taken (García-Collantes &

Garrido 2022), which can seriously affect adolescents. Thus, we can consider that young people conform the most vulnerable group in the digital context (Gamito, Aristizabal & Vizcarra, 2019).

Concerning the educational field, the Law on Education of Catalonia 12/2009, dated the 10th of July, in articles 58 and 59 states that in primary and compulsory secondary education, competencies related to the use of new technologies have to be developed properly to all students (Generalitat de Catalunya, 2015).

Hence, to develop some of these competencies and prevent possible harmful behaviours, this work will try to develop a teaching-learning project to be taught in additional language classes in a secondary school in l'Hospitalet de Llobregat with the aim of educating students in cyber security.

To this end, the purpose of this work is to develop an exploratory work of an interpretative nature to find out what security measures are adopted by secondary school students through the use of different instruments. Subsequently, for the design and possible future implementation of the project, a specific school year will be adjusted according to the centre's needs. Moreover, this project is going to be carried out in AL classes, specifically in English, because this project will work on the first and the eleventh competencies (especially C11) as well as key content six and twenty-six from the "Core competencies in the digital field" document from the *Generalitat de Catalunya* (2015). There it is indicated that these two competencies can be worked in classes which implies the use of ICT (information and communication technology) (C1) and in all subjects (C11). Because of this, that information leads us to the second reason: cyber security is a relevant cross-curricular field where a lot of the terminology used has its origins in the English language, and at the same time is a thematic area that can connect with students' interests and might engage and motivate interesting in-class discussions.

2. OBJECTIVES AND HYPOTHESIS

Nowadays, as far as Spain is concerned, we can observe how the use of new technologies is part of almost everyone's daily life. We can say that they are here to stay in our lives. They make us stay connected and up to date, as well as allow us to adapt more easily to the situations we live in.

Although there are many advantages to surfing the internet, are we aware of the risks we expose ourselves to every time we open the browser, upload a photo or simply" accept" the terms of a new application or extension we download? And, specifically, are teenagers aware?

In recent years, we have seen that this is not an area of little interest, quite the contrary. Different authors have addressed it and have agreed on the need to continue studying it (Vanderhoven, Schellens & Valcke, 2014), as well as the need for young people to know how to establish security measures to prevent fraud and abuse and all the consequences that derive from them (Argente, Vivancos, Alemany & García-Fornés, 2017; Astorga-Aguilar & Schmidt-Fonseca, 2019; Gamito, Aristizabal & Vizcarra, 2019; Venter, Blignaut, Renaud & Anja Venter, 2019). Furthermore, we can see this interest in education (Generalitat de Catalunya, 2015).

Because of this, given the doubt that we are really facing a society that surfs safely on the Internet, and more specifically, the adolescents who have been born in this new era known as digital natives, this work aims to contribute to informing and training young people in this field, that of cyber security.

For this reason, the general objective of the work is to create a teaching-learning project in the English language in which, concretely, secondary school students, can be made aware of the risks they run when using the Internet and its services as well as to establish effective safety measures to prevent possible harm.

This general objective can be broken down into some specific ones:

- First: to know what exactly we mean when talking about cyber security and be aware of the risks and possible consequences we expose ourselves to when using the Internet and its services (such as applications and social networks).

- Second: to establish which protective measures when surfing the Internet are essential to avoid these risks and their consequences, and check and/or establish which ones are used by teenagers.

- Third: find out whether students have received any training in cyber security and check whether it is thorough enough.

- Fourth: from a teacher's perspective, to know which is the appropriate age group to carry out the project.

- Fifth: to be able to propose effective teaching practices for the promotion of cyber security and digital cultures in AL classes, based on evidence.

The hypothesis, therefore, on which this study is based are that:

- H1: Teenagers, on the Internet, do not take the necessary security measures because they do not have the necessary training in cyber security.

- H2: Teenagers think they make appropriate use of the internet but in reality, their use of the net could be improved.

- H3: Teachers, given the need for the use of digital culture through new technologies, are not receiving adequate and up-to-date training.

3. THEORETICAL FRAMEWORK

In this section, we will refer to two main blocks. On the one hand, there is the section on additional languages, which in turn will deal with aspects such as plurilingualism, Content and Language Integrated Learning and Task-Based Language Teaching. On the other hand, there is the digital culture. The second one will try to bring us closer to the concept itself as well as to cyber security, including its risks and protective measures.

3.1. ADDITIONAL LANGUAGES

As Rovira (2008) claims, language has a lot to do with culture and identity "language is intrinsic to the expression of culture. Language is a fundamental aspect of cultural identity. (…) It is through language that we transmit and express our culture and its values". In Spain, particularly in Catalonia, most of students, at least, speak both Spanish and Catalan languages. These languages are the ones taught in the Catalan education system and an additional language (AL) which nowadays is mainly English (Wilson, 2020) but we can find some elective subjects such as French, German, or even Italian.

However, taking into account the level of English at which ESO students finished secondary school in 2007, it was established the *Pla d'Impuls de les terceres llengües*. But some years later, it was changed by the *Pla de Plurilingüisme to extend* the English language further into other curricular subjects (Wilson, 2020).

Besides that, as far as AL is concerned, it should first be considered that, over the years, the terms "foreign", "first" or "second" have been the most commonly used. Nevertheless, these terms have evolved into "additional" or "new" languages. These new terms are more flexible because they imply the reality that, what we find in classrooms, are plurilingual spaces. There is more than only one language in them, and so, connections and identities can be developed (Gonzalez Davies, 2017).

Learners may know more than one language, and what would be a second language for one, might be their third or even fourth for another. We cannot measure languages by numbers. Therefore, the use of these new terms can be better considered when referring to a new language learned by a learner, which is not his or her first language (L1). Furthermore, when using the term "additional" we are avoiding any notion of hierarchy between languages (Gonzalez Davies, 2014, quoted in Wilson, 2020).

3.1.1. PLURILINGUALISM

Over the years, societies have become more and more diverse due to globalisation, mobility, immigration, and the use of new technologies. This fact shows us that nowadays, different languages coexist not only in a society in general but also in education. That's why plurilingualism has become an important framework for language teaching (Piccardo & Galante, 2017).

For the Common European Framework of Reference of Languages (Council of Europe, 2001) the plurilingual approach argues that as individuals, as we learn new languages, our brains do not keep them in separate, unconnected departments, but rather, on the contrary, they build up a communicative competence in which languages interact and interrelate with each other, building our own linguistic repertoire.

Therefore, the contrary happens with multilingualism where there is a coexistence of different languages, at the individual or social level, but these aren't connected (Council of Europe, 2020).

Consequently, authors such as Cenoz & Gorter (2013) state that language policies should move towards plurilingual approaches instead of the traditional monolingual ones when teaching foreign languages, like English (EFL). However, these new policies imply that the educative community should: set realistic goals when teaching English; use plurilingual competence as a tool to progress; create an integrated syllabus between English teachers and other teachers; and, create resources that promote awareness of different types of communicative contexts.

Furthermore, as far as teaching EFL in Spain, as Esteve, Fernández, Martín-Peris & Atienza (2017) mention, there is not a huge debate to promote effectively plurilingualism. Because of this, educational institutions use to impose some approaches on teachers as Content and Language Integrated Learning (best known as CLIL) to promote it.

3.1.2. CONTENT AND LANGUAGE INTEGRATED LEARNING (CLIL)

Content and Language Integrated Learning (known as CLIL) can be defined as "a dual-focused educational approach in which an additional language is used for the learning and teaching of both content and language" (Coyle, Hood & Marsh, 2010).

Following what Coyle, Hood & Marsh (2010) claim, this means that during the process of teaching and learning, the emphasis is on the content given as well as on the language used. That's why it is considered a dual-focused educational approach. However, this can be an experience difficult to accomplish in a language-learning classroom. Some reasons are: the content chosen has to be related to the learning institution context, CLIL has to analyse the effective pedagogic approaches in different contexts, and teachers have to involve and engage cognitively students and make them articulate their learning. Concretely, in Spain, the acronym CLIL was translated as AICLE (Adquisición Integrada de Contenidos y Lengua Extrangera) (Navés & Muñoz, 1999, quoted in Muñoz, 2007).

In order to support the CLIL pedagogy, in 1999, Coyle developed de 4Cs Framework. This framework "focuses on the relationship between content (subject matter), communication (language), cognition (thinking) and culture (awareness of self and 'otherness')" (APAC, 2005).

Following what APAC (2005) mentions, this framework suggests that we have to take into account different factors such as progression in knowledge, engagement, interaction, understanding and so for, to get effective CLIL practices. Herewith these 4Cs must be interconnected and must be considered when planning, conceptualizing, monitoring, and evaluating the teaching and the learning process.

Regarding Catalonia, the first public call for CLIL projects was in 1999 (APAC, 2005). Nevertheless, these calls have been evolving over the years according to the needs of society, and the most recent ones are the ones mentioned before, the *Pla d'Impuls de llengües estrangeres* i el *Pla de Plurilingüisme*. When *Pla d'Impuls* was established, in general terms, it had the aim of improving language teaching, and it also wanted to train non-language teachers to give them the possibility of carrying out their classes via CLIL plans. As results were not as expected, the Catalan Government, initiate the *Pla de Plurilingüisme. It aimed* to ensure the students finish with a B1 level (according to the CEFRL[1]) in one AL language, mainly English, at the end of ESO by 2018. For this, it consisted of imparting in English 15% of ESO's classes and 18% in Baccalaureate. It also required a minimum C1 level for all teachers who wanted to teach through CLIL (Wilson, 2020).

According to the Basic Competence[2] exams and the Aptist texts carried out by the British Council in 2018, the English level in ESO students indicates that it has improved (Wilson, 2020). However, there is still much to do and much room for improvement.

[1] See: https://rm.coe.int/1680459f97

[2] This is a compulsory exam carried out by all students in 4rth ESO in order to know their knowledge in subjects such as English, Catalan, Spanish, Maths, and Science (http://csda.gencat.cat/ca/arees-actuacio/avaluacions-consell/avaluacio-quart-eso/2022/que/)

3.1.3. TASK-BASED LANGUAGE TEACHING (TBLT)

Task-Based Language Teaching (TBLT) is another approach that can be useful in language classes. Richards & Rodgers (2001) define TBLT as "an approach based on the use of tasks as the core of unit of planning and instruction in language teaching". Besides, these authors claim that on TBLT the proposed activities have to follow some principles. These task activities should involve real communication and in them, language has to be used to carry out meaningful tasks because a meaningful language will also support the learning process for the learner.

Therefore, we can observe how the term "task" is the most decisive word in this methodology. That is why some different authors have been discussing it for years. However, Van den Branden (2016) claims that all authors share a common core "a task is a goal-oriented activity that people undertake and that involves the meaningful use of language"

Thus, what this approach aims to do is to get students through the use of language, classroom conditions and other tools, to complete the tasks in order to achieve the goals (Lai & Li, 2011).

3.2. DIGITAL COMPETENCE

The use of the internet and new technologies not only creates a place for socializing but also provides a wide range of learning opportunities. It is for this reason that, both at the European and national levels, recommendations have been drawn up and action plans have been approved to tackle the field of digital competence.

In the European field, we have the *European Framework for the Digital Competence of Educators (DidCompEdu)* created by the Joint Research Centre (Punie & Redecker, 2017) with the aim of presenting a framework on which the European educators could rely on, to promote digital competence in an effective and booster way in their states. Thence, the INTEF (National Institute of Educational Technologies and Teacher Training) elaborated the *Common Digital Competence Framework for Teachers* (CDCFT) in order to adapt the European Framework to the Spanish context (Ministry of Education, 2017).

The CDCFT (Ministry of Education, 2017) counts with five competencies areas where there are twenty-one competencies inside. At the same time, these competencies are defined between the six proficiency levels (A1, A2, B1, B2, C1 y C2) established by the CEFRL. The fourth area is the one of Security and is divided in protecting devices;

protecting personal data and digital identity; protecting health; and, protecting the environment.

However, it is worth mentioning that concerning Catalonia, the Generalitat de Catalunya, in accordance with the art. 97 from LEC (Law 12/2009, July 10, education) has pedagogical autonomy. It is for these reasons that, the Education Department has considered the digital field as one of the different areas to be taken into account within the secondary education syllabus.

Specifically, this field has been structured in four interrelated dimensions, eleven competencies, and twenty-eight key contents that can be developed across all subjects. These aim to provide students with good judgment and encourage appropriate habits of use among the whole educational community in order to preserve their fundamental rights and to achieve their maximum potential in their academic and personal development (Decret 185/2015; Generalitat de Catalunya, 2015).

More concretely, following the *Core competencies in the digital field document (*Generalitat de Catalunya, 2015) the first dimension of *Devices and applications* on its first competency (*Choosing, configuring and programming digital devices depending on the task being performed*) works the security term. Moreover, on the fourth dimension of *Citizenship, habits, civic-mindedness and digital identity* we can find the eleventh competency (*Acting critically and responsibly when using ICT considering factors such as ethics, laws, safety, sustainability, and digital identity)* which tackle this term. At the same time, we have the 26th Key Content which is working the virtual environments safely that includes: safe websites, cybercrime, or visibility of personal data.

Competency 1 could be worked through Language and Literature as well as in ICT subjects and, competency 11 could be worked through any subject. As far as the 26th key content is concerned, this could be worked in the linguistic field through implicit knowledge (Generalitat de Catalunya, 2015).

3.2.1. DIGITAL CULTURE

Traditionally, technology has been defined as the way of doing actions. However, when we refer to new technologies, we are referring to something much more complex. New technologies are more than new tools or methods. Their social implications are causing new social and cultural ways of thinking, to the extent that many relationships are conditioned and contextualized by the new technologies (Riveirón, 2016).

Therefore, we can understand digital culture as the cultural context in which new relationship technologies acquire importance. Oral and written language has historically been the most important markers of culture for being considered as such. In digital culture, these aspects do not lose the importance they had before. They keep it due to their integration in different devices and these configure the production, interaction, and interpretation of language sceneries (Gil, Feliu, River & Gil, 2003).

This new "digital" way of living, can suppose a huge challenge that can be assumed as an opportunity for the development of new educational experiences that take into account the growing complexity of education in this new era (Riveirón, 2016).

3.2.2. INFORMATION MANAGEMENT & COMMUNICATION

Following on from digital competence and digital literacy, we can see how, as the digital field core competences syllabus mentions (Generalitat de Catalunya, 2015), a fundamental aspect to deal with is the management of information that adolescents do on the Internet, as well as communication. More specifically, we are talking about ACTIC (Accreditation of Competences in Information and Communication Technologies). This refers to competences that involve the ability to use digital systems in an autonomous and creative way in line with the provisions of Decree 89/2009 of 9th of June which nowadays has been repealed by the decree 13/2021 of 2nd of March.

It is for this reason that both aspects, information management and communication between others such as authorship, ethics or publication legality are reflected in almost all the competences to be covered in the syllabus (Generalitat de Catalunya, 2015).

As far as competence 11 is concerned, which, through this teaching-learning project, will be dealt with, we can say that it responds to the need to make students aware of the implications they face when using the Internet and other types of technologies. It has a civic content and, among other aspects, it aims to make adolescents aware of the following situations (Generalitat de Catalunya, 2015):

- Evaluate from an ethical point of view the contents they disseminate through the networks. In this way, they will avoid certain risks such as offences.
- Be aware, in the legal sphere, of the licenses and copyrights regarding digital productions (whether their own or those of third parties).

- Take into account aspects related to digital security to prevent attacks, data appropriation, and so on.
- Know what digital identity is and how it is constructed, and therefore know how to effectively manage their visibility, reputation and privacy.
- Bear in mind that the internet provides a false perception of anonymity, but that, in reality, this is not the case.

Therefore, and bearing in mind that most of the terminology they encounter in this field will be in English, it is important that students know how to identify it in its original context and can communicate appropriately. Thus, addressing this competence in an English AL class can be of great value and usefulness.

3.2.3. CYBER SECURITY

We can consider cyber security as the technique of protecting computers, networks, programs data and other devices from unauthorized access or attacks with the aim of exploitation. It is also referred to as information technology security (Mack, 2018).

Over the years, individuals and organizations who desire illegal access to information and data have emerged. These could harm not only other individuals but also institutions or even governments through the use of different methods (Haseski, 2020).

NICE's National Cyber security Workforce Framework (NCWF), a resource from the USA, breaks down the cyber security field into 7 categories and around 33 speciality areas. This resource applies across the private, academic and public sectors. With this Framework, educators can develop some curricular activities, seminars, and projects to implement cyber security among students and young learners (NICCS, 2021).

In June 2021, Spain's government developed the *Plan Integral de Cultura de Seguridad Nacional* with the main objective of increasing social awareness of the indispensability of National Security (Gobierno de España, 2021p.70650). However, despite this plan proposal to foment the inclusion of its content on the primary and secondary education, baccalaureate, and university syllabus this plan will end as a document itself because the government does not count on a sufficient budget (SIC, 2021).

In any case, we can see how cyber security is a very important aspect to take into account, as it will help us to prevent and avoid all possible risks to children and young people (Astorga-Aguilar & Schmidt-Fonseca, 2019). This is why in Catalonia, all educational centres have to work on safety as part of the digital field syllabus in a cross-cutting way. In this case, this is mainly done through competence number 11 (*Act critically and responsibly when using ICT, considering factors such as ethics, laws, safety, sustainability and digital identity)* (Generalitat de Catalunya, 2015).

A) RISKS WHEN USING THE INTERNET & POSSIBLE CONSEQUENCES

As mentioned above, Internet use has increased exponentially in recent years. Especially among children and adolescents who, especially due to the Covid-19 situation, have also needed it to be able to continue their academic development. Thus, we can see how the digital world offers endless opportunities and advantages. However, there are also some risks.

The OECD's 2011 document set out the different types of risks that children face. However, in 2021 they updated it to adapt to the new needs of society. There are four risk categories (content, conduct, contact, and consumer) and there are risks that cut across these four categories like privacy, advanced technology, health, and well-being risks. Furthermore, within each category, inter alia, there are hateful, harmful, illegal, security, or even behavioural risks (OECD, 2021).

Firstly, content risks are defined as the ones where the subject is passively exposed to or receives content that is available to all Internet users. This content can be illegal, age-inappropriate, or harmful such as online scams or pornographic pop-up advertisements. Secondly, conduct risks are the ones where the children participate in peer-to-peer exchange, including when their own behaviour may make them vulnerable, as happens in sexting or cyberbullying. Thirdly, contact risks happen when children participate in the online world. Here we can distinguish: if they are exposed to hateful encounters; if the encounter takes place with harmful intentions; if the encounter is under criminal law and; finally, if the encounter is problematic but does not fit in any of the three previous manifestations. And, fourthly, consumer risks given that children, depending on their maturity, age, and other circumstances, may be more susceptible to fall into fraudulent marketing practices until the extent of being the object of an attack based on the personal data previously collected from them (OECD, 2021).

Hence, it can be seen how there are multiple risks to which teenagers are exposed when using the Internet. If one or more of these risks materialize, the individual can become a cyber-victim.

Montiel (2020) mentions that could be different types of consequences when a subject becomes a cyber-victim. Mainly, there are two types of them: psychological and social consequences. She also mentions that this type of victimization not only affects the direct victim, but also affects the indirect victims (i.e., family, friends, and society). Between the different ways of becoming a cyber-victim, the most common psychological consequences could be anxiety, sadness, embarrassment, low self-esteem, emotional problems or even post-traumatic stress disorder, depression, and suicidal thoughts. On the other hand, there are social consequences, since, when dealing with minors, this can seriously alter their development and socialization process.

B) PROTECTIVE MEASURES

Although today's teenagers are considered digital natives, we should not make the mistake of reckoning they make good use of ICTs and therefore, they do not need any training. In fact, such training is totally necessary (Fernández, 2019).

Concretely, in Spain, the *Observatorio Nacional de Tecnología y Sociedad* (ONTSI), biannually publishes a study related to how citizens protect themselves from cyber risks. The latest was published in December 2021 in relation to the first semester of that year. In it, we can observe that there can be different security measures depending on the gadget (smartphone, computer/laptop, tablets, and so on). However, the most common ones are:

- Firewalls
- Partitioned hard disk
- Antivirus
- Software actualizations
- Back-up copy
- Password manager
- Unlocking system

In general terms, it was found that almost all participants had the firewall enabled on their system (even though they were not aware of it). The same was observed regarding hard disk partitioning. Only 16.2% of the users mentioned that they had it, but the actual data showed that 56.5% of the users had it. On the other hand, concerning the use of antivirus (concretely androids' systems), the use has decreased from previous semesters. The same happened with the use of backup copies. However, the use of password managers has increased (up to 43.1%), as well as the use of an unlocking system such as PINs. Finally, it is worth mentioning that most parts of users think that their gadget is actualized, but in fact, it isn't true. Only around 53.6% have it (ONTSI, 2021).

Besides, concerning the habits when using the internet, the analysis shows that risk behaviours are improving. 62.3% of users state do not intentionally engage in risky behaviour. Nevertheless, there is still 37.7% who do that. Otherwise, it seems that users are raising awareness of the risks they face when using public Wi-Fi, and that's why the study shows a decrease in their use of them. Likewise, concerning the habits when downloading programs, files, and so forth, a decline has been perceived in the use of virus analysis tools to analyse their veracity or reliability. Thus, regarding the social networks' habits, data show that this is still a widely used media. It is therefore recommended to adjust privacy as much as possible, as well as to monitor what is being shared on them (ONTSI, 2021).

With all that information, it can be detected that society is raising awareness in this area, but there is still much to be done. The knowledge and application of appropriate security measures as well as good habits will make us safer and more prepared for possible cyber-attack.

4. METHODOLOGICAL APPROACH

In this section, we will discuss everything related to the methodology used to collect the data. Therefore, contextualisation of the place where it has been carried out, the sample analysed, as well as all the instruments used and their justification will be discussed.

4.1. CONTEXTUALISATION

This study has been carried out in a public high school located in L'Hospitalet de Llobregat (Barcelona) during the end of the second term of the academic year 2021-22.

The students who attend this high school are mainly Spanish-speaking students and of medium-low socioeconomic status. That's why this centre has a lot of diversity in its classrooms and plays an important role in integration.

The high school counts with three lines in 1st, 2nd, 3rd and 1st Baccalaureate. 4th ESO has four lines and 2nd Baccalaureate two.

Moreover, following its Projecte Educatiu de Centre (2022) this centre works and prioritises an integral, inclusive, plural, respectful, innovative, and quality education. For this reason and concerning additional languages, the centre promotes the use of English through different projects in order to engage and motivate students in that matter.

4.2. PARTICIPANTS

This research was implemented on 88 students from the centre. All of them were from different courses and ages. Students were sent a Google Forms survey through their English teachers, and they answered it voluntarily and anonymously. The aim of this questionnaire was to get to know which concepts did the students know about cyber security, risks and protective measures. Furthermore, it wanted to know if they considered they had good habits on the internet and if they wanted to know more about this field.

On the other hand, to contrast that information, I carried out a direct observation with the help of a grid template among students and the way they use ICT in class, I was able to attend so many classes so, I had the opportunity to observe, in total, around three hundred students.

Moreover, another questionnaire was sent to the teachers of the English department to know: if the centre had carried out some training for students or even for them as teachers in cyber security; if there were activated protective measures like firewalls; if they worked digital competence and how; and in which course did they think it was better to implement training in this field.

4.3. INSTRUMENTS

4.3.1 DIRECT OBSERVATION

During my internship in that high school, I realized that ICT is part of our everyday life and we use them as an inherent part of it. Furthermore, as teachers, we are working in front of "digital natives" and even if some of us are also part of this group, as Fernández (2019) mentioned, we cannot affirm they (or we) make good use of this new technologies. That's why adequate training is essential.

Moreover, following what Taylor-Powell and Steele (1996) indicated concerning that observation is useful when, between other conditions, we want to get direct information or there is evidence that can be readily seen. That's the reason why I thought that starting with a structured observation could be convenient. I wanted to "look for" certain aspects of their day-to-day basis in relation to their use of ICT and to standardize the information I got.

In order to follow this, I created a template grid with the different items (see annex 9.1.) I wanted to know more about it, and I also left some spaces in case I wanted to write something. The items I put in the rubric were: books, laptops, Wi-Fi, mobile phone, Internet use, and Moodle. Moreover, with these items, I established some observation parameters to check. These were based on: some of the risks, ICT tools, or devices mentioned throughout the project or connected to it.

- Books: students have "digital" books.
- Laptops: Laptops are needed to follow the class or to do some activities. / Students close the laptop when the class finishes.
- Wi-Fi: Good Wi-Fi connection is needed to develop the class/ Some websites are blocked to prevent their use.
- Mobile phone: Mobile phone is needed in class/ Mobile phone is allowed in class and students bring it.
- Internet use: Students. Accept "cookies" without hesitation/ Students use the Internet only to do what is being asked of them.
- Moodle: Moodle is used and works properly.

These observations were done between December and February 2022 in 1st, 2nd, 3rd, 4th, 1st and 2nd baccalaureate classes. In ESO's courses, all the observations were with different teachers, and regarding baccalaureate, both first and second were with the same teacher. The students knew I was there observing them but they did not know what was I observing. They thought, at all moments, I was looking for the class functioning because I wanted to become a teacher (that in fact, was also true).

The aim of the direct observations was to cross-examine how students behaved in relation to ICT and, at first sight, which protective measures, did they implement. For example: when in class they had to use a tool if they accepted "cookies" without any hesitation; if they share computers with classmates; if they used a mobile phone; if they were connected to the public internet network, and so on.

4.3.2. TEACHERS' QUESTIONNAIRE

Concerning the teachers' questionnaire, firstly, I want to add that at the first moment my idea was to do some interviews. However, due to some circumstances I couldn't and for that reason I designed a survey adapting the questions I wanted to ask.

This survey has been done on the teachers in the English department, concretely four of them, in order to find out how they have noticed, in recent years, the increase of new technologies both in the classroom and among pupils. On the other hand, it also aims to find out whether pupils receive training in cyber security and if so, whether this is also the case for teachers.

However, the most important aspect to be extracted from this survey is to find out whether they consider it necessary for this training to be given in order to work as an extracurricular field in the digital area included in the curriculum of the Generalitat de Catalunya (2015), in which courses and by means, of what methodology. For example, through a TBPL or a CLIL activity or sessions.

4.3.3. STUDENTS' SURVEY

On the other hand, another of the instruments used was student surveys. Between the months of March and April 2022, ESO and Baccalaureate students at the school were asked to answer anonymously a questionnaire related to cyber security.

The aim was to find out what adolescents know about this area, whether they have received training in the past, whether or not they apply security measures and whether they think it would be advisable for them to receive more comprehensive training in this field.

Finally, there were 88 students which answered the survey. Mostly from 1st ESO, 3rd ESO and 1st Baccalaureate.

5. RESULTS & DISCUSSION

At this part, a general division is made between the results obtained and a final discussion. In this discussion, the aim is to interrelate all the results and thus draw a final conclusion as to whether or not it is necessary to develop cyber security training, in which courses and by means of what methodology.

5.1. RESULTS

5.1.1. OBSERVATION PHASE

With regards to the observation phase[3], in the high school, all the students worked with digital books. However, most of them used to have the student's books physically and the Workbook in a digital version. Therefore, if they worked in this way, they do not always need the use of the laptop in class.

It should be added that teachers had both books in digital format which they projected in order to be able to teach the classes. Thus, a good Wi-Fi connection was required to develop properly the session.

In some classes, the teacher asked the students to do something different from the book that implied the use of the laptop. In 1st, 2nd, 3rd and 4th ESO, as the students brought always a laptop because, in some subjects, they did not have physical books, there was no problem. Nevertheless, concerning 1st and 2nd BAC the teacher should notify before the students.

When the students used the laptop and with it the Internet, I could observe how they accepted "cookies" without hesitation. They did not even select only the necessary option. To go faster, they clicked directly on "Accept all" whatever the website was.
Moreover, once they had finished using it, they turned down the screen but they do not close the session properly.

In addition, the centre worked had blocked some websites in order to prevent their use. Nevertheless, these websites were the most common ones such as Facebook, WhatsApp Web, Twitter, Netflix and so forth. There were many others that students used (less known) that were not blocked. So, above all, in ESO's courses and 1st BAC; when they were asked to do something on the laptop, the teacher had to be very attentive to them because if not, they started to do other non-educational things.

[3] See all detailed information in annex 9.2.

On the other hand, concerning the mobile phone, in that centre, it was not forbidden. Students could bring it and use it at playground time but in class, they must have it stored at all times and they must not use it without the teacher's permission. However, some of them did not toe the line. They had it on their desks and check it whenever they wanted. They wait the moment the teacher was not looking at them and used it.

Finally, it is worth mentioning that despite the fact that not all classes required the use of a laptop, the centre had its own Moodle and through it, the students could follow some subjects, do homework, send projects or even do some tests. Furthermore, teachers, above all in 1st and 2nd BAC, used the Classroom app through which they could send the students some tasks.

5.1.2. TEACHERS' QUESTIONNAIRE

Concerning the questionnaire for teachers in the English department, we can observe that of the four teachers who responded, three of them have more than sixteen years of experience and the fourth has between one and five years.

In addition, in the current academic year 2021-2022, one of them is teaching in 2nd ESO, 4th ESO and 1st BAC (T1); another one in 3rd ESO, 1st and 2nd BAC (T2), the other in 3rd of ESO (T3), and finally, the fourth one in 4th ESO (T4) (Figure 1).

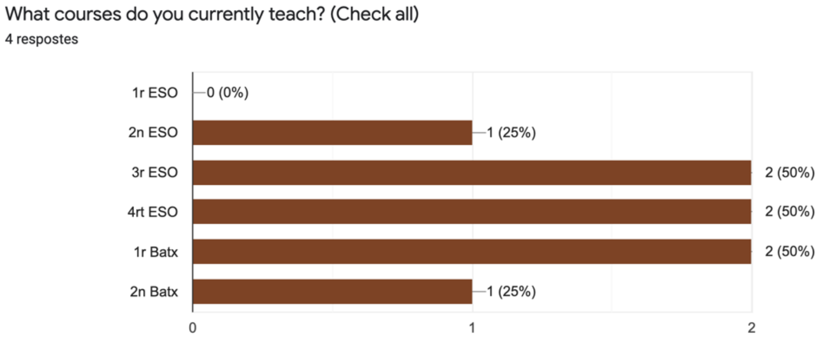


Figure 1: What courses do you currently teach?

Moreover, they all claimed to have noticed that in the course of the last few years, new technologies have been introduced both in classrooms and among students. For example, one of them (T3) explained that:

> *"The use of new technologies has increased in the classroom exhibition (digital book, use of Classroom to communicate, remember or send assignments, use of the digital platform blinklearning - digital workbook-) and in the work of students (digital workbook, digital*

dossier, use of Classroom for delivery of readings or writings, as well as the making of videos)."

Besides that, all of them also considered that students present a significant dependence on electronic devices: *"It responds to both a group and personal need. Often, when the class is over, they take out their cell phone to view received messages or to connect to a game."* (T1) or *"For years, most students have spent any free time in class connecting to a device instead of using books or a notebook."* (T4).

In contrast, three of them stated that students do not are aware of the risks they face when they use the internet. However, one of them (T2), claimed the contrary (Figure 2).

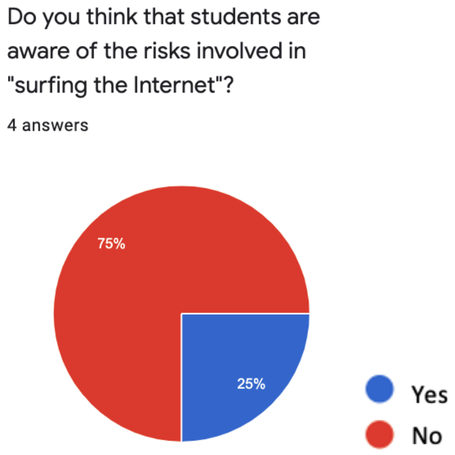


Figure 2: Do you think that students are aware of the risks involved in "surfing the Internet"?

In any case, all of them stated to know what cyber security was and three of them affirmed to know that there are talks, seminars, or training sessions in, at least, 1st and 2nd ESO, to promote "cyber security" among students (Figure 3). Nevertheless, only one of them affirmed to have received training in that field but only from his/her bank and related to data protection, in neither case from the high school entity (Figure 4).

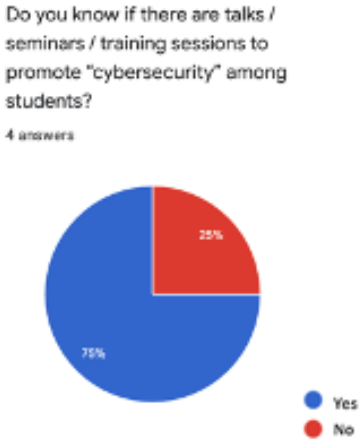


Figure 3: Do you know if there are talks /seminars/ training sessions to promote "cybersecurity" among students?

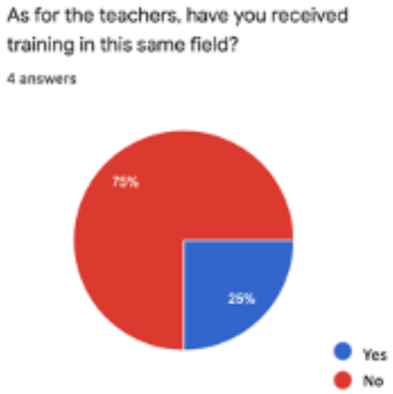


Figure 4: As for the teachers, have you received training in this same field?

On the other hand, concerning the strategies they use to control what students do when working with computers, three of them claimed to have some such as: *"Watch over"* (T2); *"In the Drive, I control the history"* (T1) and *"Check what they are working on, look if they have an open web page that not has been ordered and, also ask for a final product shared with the teacher"* (T3).

Further, also three of them stated to know that the centre is taking certain measures such as firewalls and disabling some web pages or data to prevent the use of websites such as Whatsapp Web or Spotify. However, as teachers, only one of them claimed to use security measures in cyberspace. In that case, T3 affirmed to be careful when receiving any email from unknowns.

Apart from that, all of them considered that it is important for students to receive training and information on how to surf the Internet safely and to know the measures and resources to do so: *"They must know how to defend themselves from any attack on their social networks or when they are playing online. It is also important that they can decipher those suspicious messages"* (T1) . In addition, they had different thoughts concerning when is appropriate to do this training, for example:

- T2: *"4th ESO. In the lower courses, they are too small, they do not pay attention and are not aware of the dangers, the most effective is to take measures to control access. At 4rt they begin to be more aware, responsible, and autonomous. It probably sounds more effective, but I'm not sure."*
- T3: *"1st and 2nd ESO".*
- T4: *"Maybe it would be good every two years, students show tiredness and disconnect."*

Besides that, they also considered that these trainings would also serve them (Figure 5).

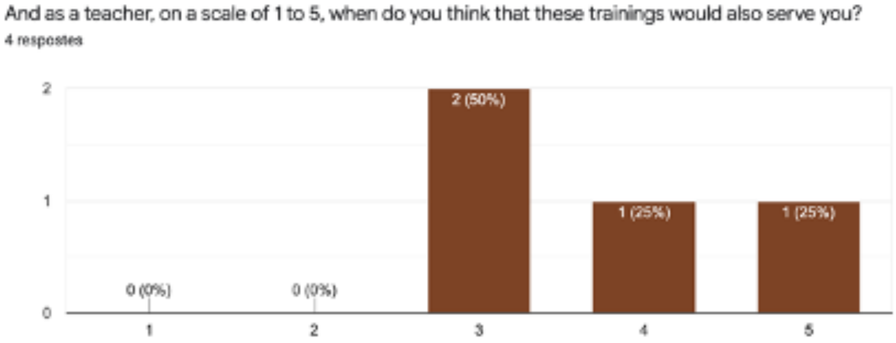


Figure 5: And as a teacher, on a scale of 1 to 5, when do you think that these trainings would also serve you?

Having said that and referring to the digital field and its competences, the teachers stated that there is a centre plan to work on Digital Competence explained in the Educative Centre Project (known as PEC) f.i.: *"Yes, it is in the PEC and in each subject and level a different skill is required, such as making presentations, videos ...".*

Moreover, all of them claimed to work it in the English department:

- T1: *"Oral presentations with any visual support (Powerpowint, Prezi, Canvas, Drive Templates)"*
- T2: *"Presentations with different digital tools, mobile applications, digital workbook, presentation of tasks and correction in digital format, use of the Blinklearning and Classroom platforms for daily work ..."*
- T3: *"Making presentations, videos, podcasts and digital written works."*
- T4: *"Digital workbook, extra material for digital environments (YouTube, Google Forms)".*

Finally, concerning the last question: *"Since in the field of cybersecurity much of the terminology used is in English and can also be a topic of interest to students, how do you think it might be appropriate to educate in this field? (eg through a teaching unit; through 1 or more CLIL (Content and Language Integrated Learning) sessions in technology, computer science or some other subject; through a PBL (Project Based Learning), ...) Why? (More than one methodology can be mentioned)"*, the answers were:

- T4: *"All the methodologies mentioned are suitable for presenting quality information."*
- T2: *"All the methodologies mentioned are suitable and are used in all areas and subjects."*
- T1: *"CLIL as it is the easiest for students, especially if it is done with technology or computer science."*
- T3: *"From technology, it would be necessary to do coordinated work with the tutoring."*

5.1.3. STUDENTS' SURVEY

As we can observe (Figure 6), the survey was answered by a total of 88 students, mainly from 1st and 3rd ESO as well as 1st Baccalaureate. However, some students from 2nd and 4rt ESO also gave an answer.

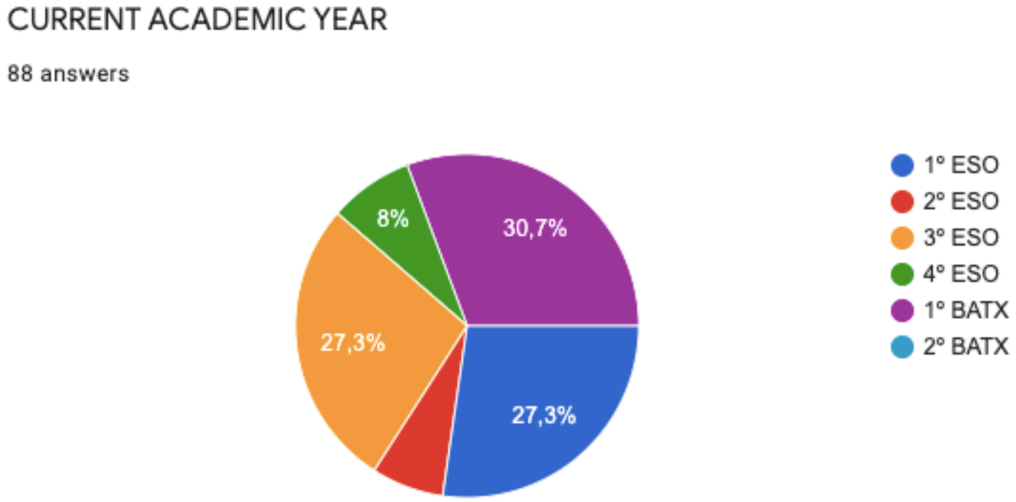
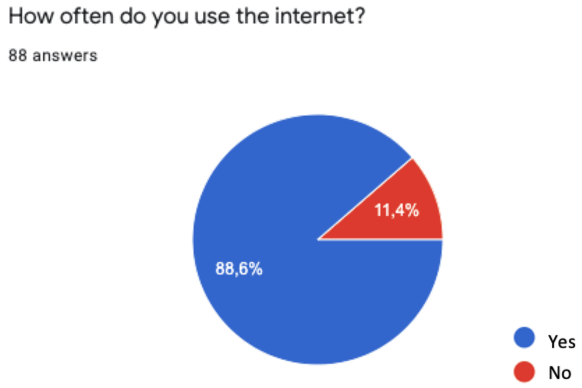


Figure 6: Current academic year

From here on, concerning the reaction to the question: *How often do you use the Internet*? (Figure 7) and *How many hours per day are you connected?* (Figure 8) we can see how all of them use internet diary or almost diary. A 58% of them use it for more than three hours per day, a 31,8% between two and three hours, and a 10,2% between one and two hours. Nobody claimed to used it for less than an hour.



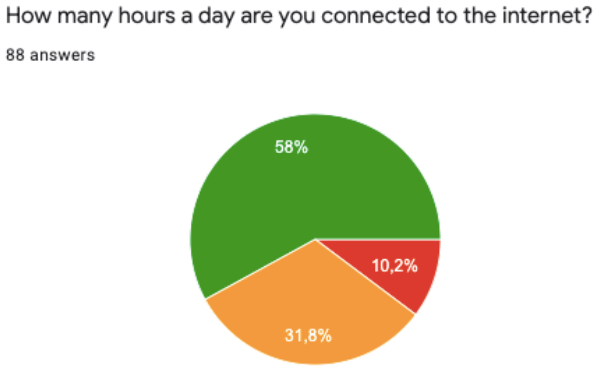


Figure 7: How often do you use the Internet?

Figure 8: How many hours a day are you connected to the internet

Besides, more than 80% of them used it to be on social networks, watch videos, work on school projects and search for information. Near to this, 77,3% used it to talk through Whatsapp, Telegram, etc; 65,9% to send or receive emails; 50% to play online with other people; 42% to watch or download series or films; and, only 28,4% for reading news.

Having said that and concerning cyber security, it is relevant to see how despite using the internet every day or almost every day, only 53,4% knew what cyber security was and was able to give a brief definition: "*Cybersecurity is the security you have on the*

Internet", "I think it's like computer security whose function is to protect the personal data of our devices"; "It's the security that serves to defend devices from being corrupted" and so on.

Besides that, 69,3% claimed to use antivirus and keep it up to date (Figure 9). 53,4% of them affirmed having a password manager in order to remember their passwords (Figure 10). 59,1% also affirmed signing out of a computer if it was used by more users (Figure 11) but, only 55,7% stated to know the risks they faced when connecting to public Wi-FI networks such as the high school one, and mentioned some of them. It is important to see how 44,3% do not know any of them (Figure 12).

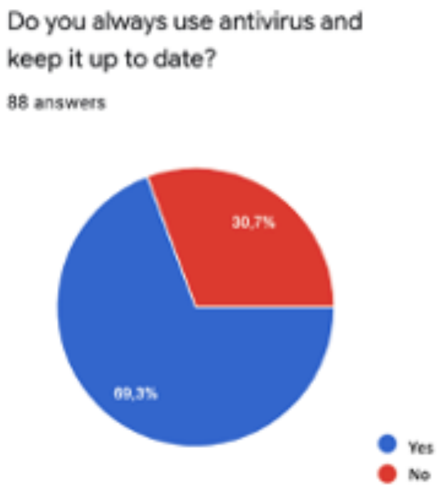


Figure 9: Do you always use antivirus and keep it up to date?

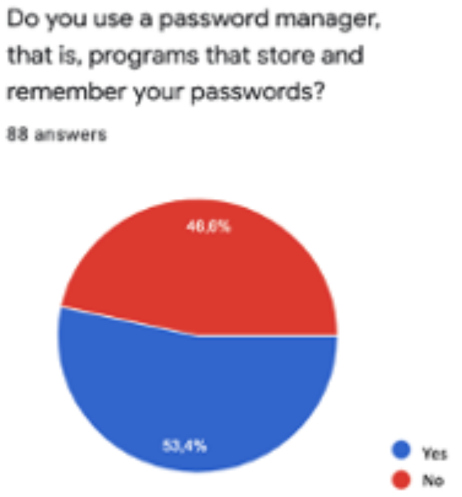


Figure 10: Do you use a password manager, that is, programs that store and remember your passwords?

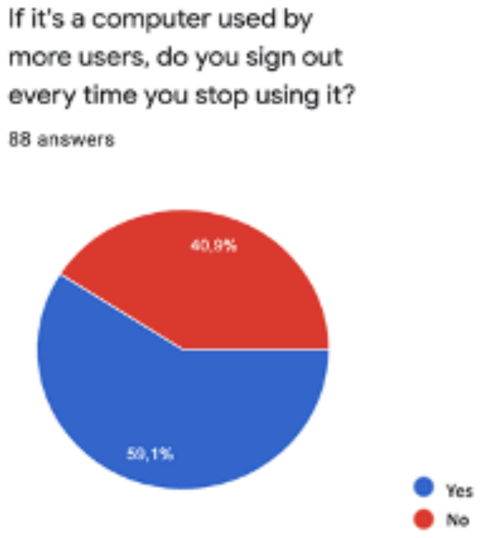


Figure 11: If it's a computer used by more users, do you sign out every time you stop using it?

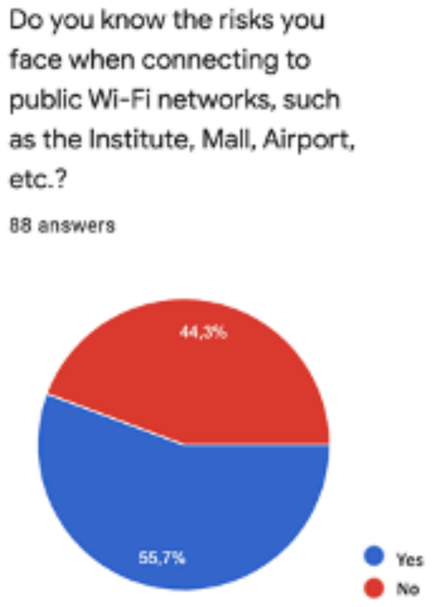


Figure 12: Do you know the risks you face when connecting to public Wi-Fi networks?

Apart from that, it is worth mentioning that one-third of the respondents stated shopping online often, which is quite surprising taking into account that all of them are minors (Figure 13). Moreover, 13,6% affirm have been a direct victim of internet scam or misconduct (Figure 14). They comment that *"80 euros per month"*, *"We were scammed with a television that never arrived"*, *"I bought things on a website and it has been a long time and I haven't received them"*

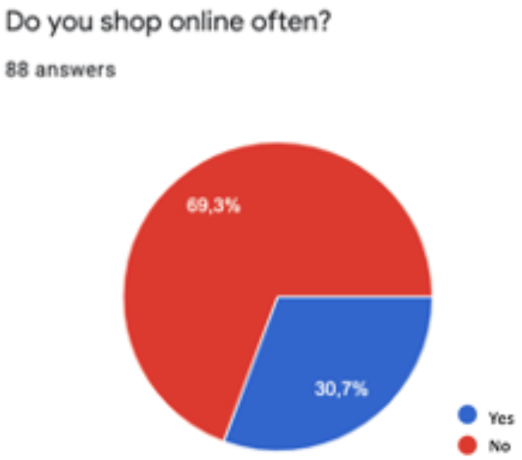


Figure 13: Do you shop online?

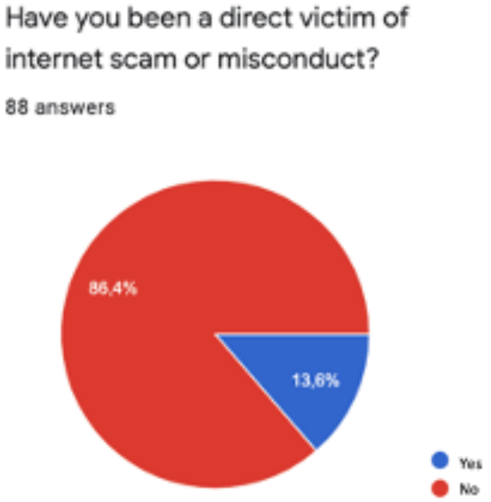


Figure 14: Have you been a direct victim of internet scam or misconduct?

On the other hand, concerning the question: *Have you ever felt uncomfortable on the Internet* (Figure 15), most of them claimed that no (72,7%). However, 27,3% answered "yes" and, between other comments, explained: *"There was a person in an online game who looked like a drug addict, and he told me to smoke and that he was a drug dealer"*, *"To receive unpleasant comments"*, *"A user on Instagram, whom I don't know, sent me nudes"*, *"To redirect me to other websites related to pornography"*, *"A man wrote to me and wanted me to send him some pictures of my private parts"*, *"I made a video in Tik Tok and some people told me I was ugly and fat"*, *"In a social network someone started to talk to me of sex"*.

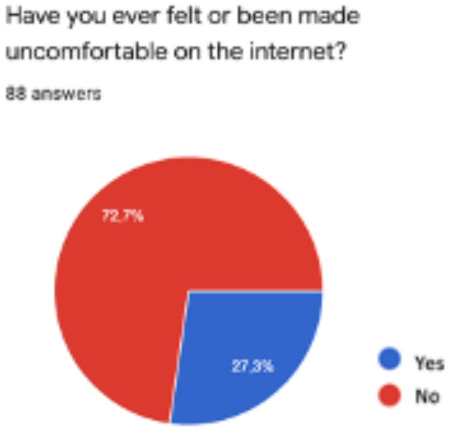


Figure 15: Have you ever felt or been made uncomfortable on the Internet?

Furthermore, following the survey, we can find that 71,6% of teenagers affirm to prove the website when downloading any program, film o music on their computer (Figure 16). Nevertheless, we can observe how about 40% do not know what cookies are used for (Figure 17) and, what it is also relevant, they do not know the meaning of words such: as online grooming, phishing, ransomware or even malware (Figure 18), despite affirming in a 94,3% of having been told about the risks when using the Internet (Figure 19) before mostly at high school and at home (Figure 20).

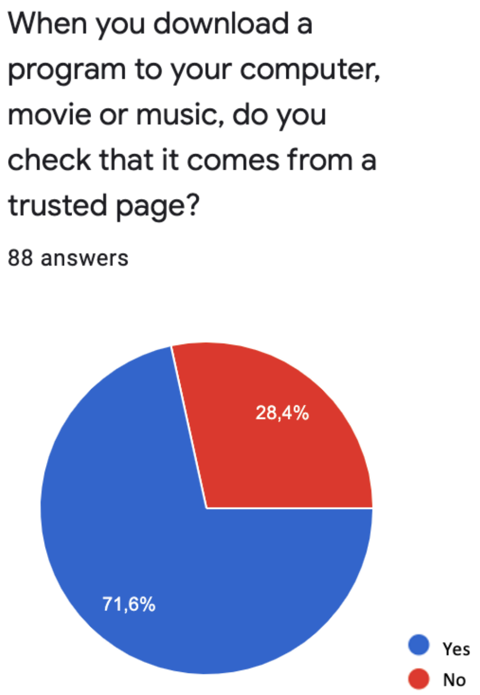


Figure 16: When you download a program to your computer, movie or music, do you check that it comes from a trusted page?

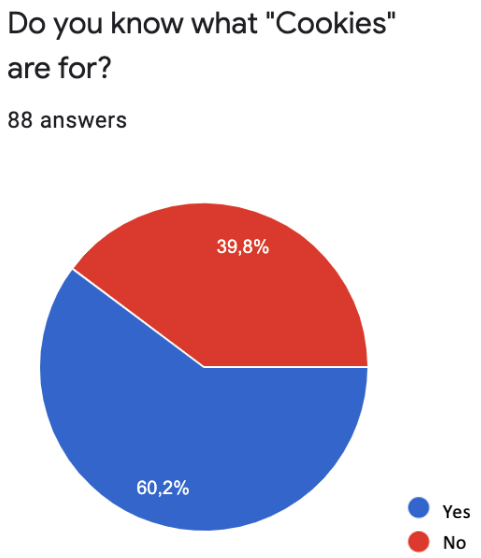


Figure 17: Do you know what "Cookies" are for?

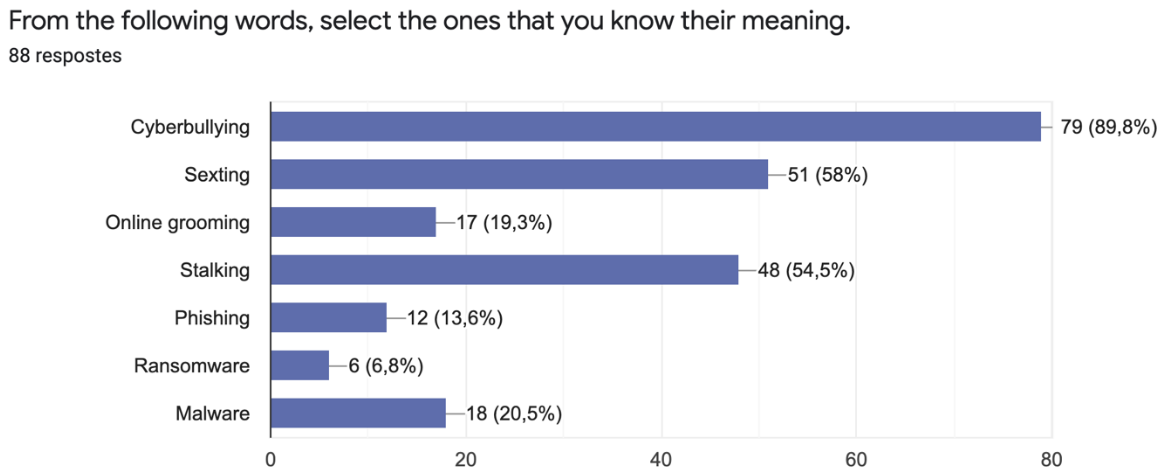


Figure 18: From the following words, select the ones that you know their meaning.

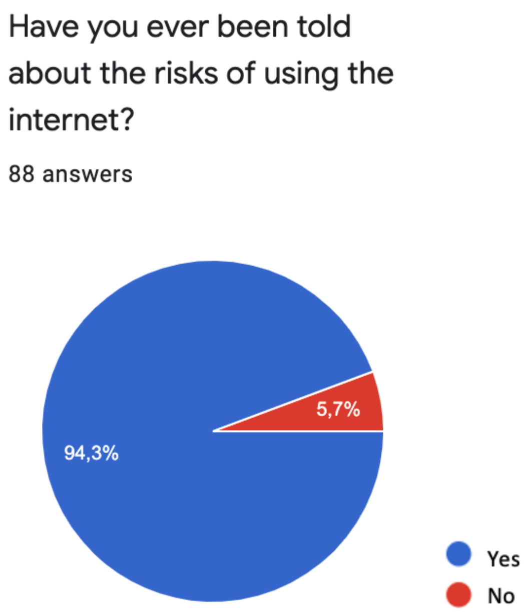


Figure 19: Have you ever been told about the risks of using the Interne?

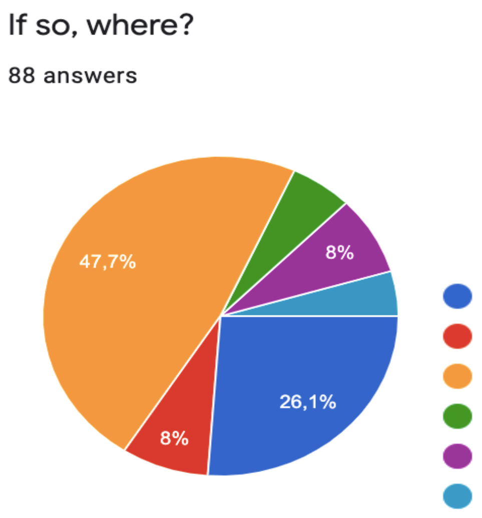


Figure 20: If so, where?

Otherwise, 71,6% of them affirm being a person with good behavioral habits when using the Internet and also taking security measures (Figure 21). They mention that the ones they use or the way they behave are: *"Antivirus and monitor those websites are still reliable"*, *"I do not share my password with anyone and things like that"*, *"To have private accounts"*, *"Having a private account, do not accept requests from strange people, do not share any personal data and, in general, I do not let myself be influenced too much in social networks in order to prevent them from affecting my mental health"*. Nevertheless, we can observe how, only one of them has mentioned something about firewalls, back-up copies, portioned hard disk or software actualizations: *"Good password, three antiviruses, two VPN and one firewall".*

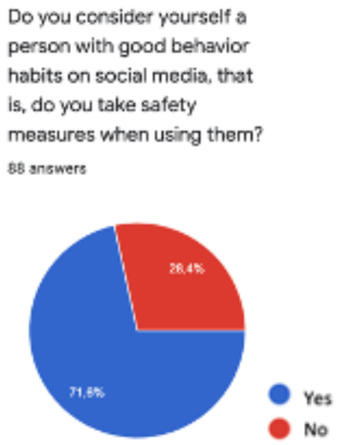


Figure 21: Do you consider yourself a person with good behaviour habits on social media, that is, do you take safety measures when using them?

Finally, concerning the last question which asked if they would have better training and knowledge in cyber security, we can observe how the vast majority have affirmed that "yes" (86,4%) and only a 13,6% said that "no" (Figure 22).

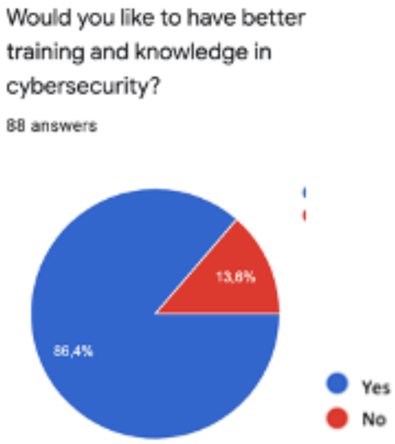


Figure 22: Would you like to have better training and knowledge in cybersecurity?

5.2. DISCUSSION

Once all the data has been analysed, we can clearly see that we are dealing with digital natives who use the internet every day (Holt, Bossler & Seigfried-Spellar, 2017) and, in most cases, for more than 3 hours. Besides, teachers have noticed as well as students how new technologies have been introduced over the years. They are nowadays present in all classes without exceptions. In consequence, teachers consider that students present a significant dependence on them and that they are not aware of the risks they face when using it despite ever having received any training in this matter. So, we can observe how what as Gamito, Aristizabal & Vizcarra (2019) mentioned, is true: technology is not neutral because the Internet has both lights and shadows.

Moreover, these talks or training are always addressed to students, not to teachers and they think it would be interesting to have more information in this field too. On the other hand, although students affirm to have received some information in this field, they strongly state that they would like to have better training concerning cyber security and cyberspace. That's why in accordance with the education law 12/2009, in Catalonia, this training could be done, throughout the first competence of the *Core Competences in the Digital Field* which works the security term or, with the eleventh competence which directly deals with developing a critical and responsible action when using the ICT. More specifically the 26th key content (Generalitat de Catalunya, 2015).

On the other side, referring to which is the more adequate course to do the training there is not a compromise between teachers. Nevertheless, like one of them mentions, 4rth ESO could be interesting because they are still in a compulsory secondary education course and they are older than their 1st, 2nd and 3rd ESO mates so, they might pay more attention and may understand better the content given. Furthermore, they are supposed to be more responsible and autonomous.

Besides, in order to work it as a cross-curricular activity in the digital competence, the training, could be done through some different CLIL sessions held within the timetable assigned for English, but could also involve technology or computer science subjects. In those sessions aspects such as risks when using the Internet or public networks, malware and its different types, password savers and their benefits and drawbacks, privacy, cookies and others would be dealt with. Design CLIL sessions that involve English as a foreign language and computer science, in addition, could be a good choice because, as the eleventh competence points out, this can be worked throughout any subject (Generalitat de Catalunya, 2015)

Finally, this training would imply a final task in which the students should make a presentation, a video, or even a podcast which will allow assessment and evaluation from a rubric of whether significant learning has taken place. In all cases, they could use different digital tools.

5.3. CLIL PROJECT DEVELOPMENT

Before starting to refer and explain to how the CLIL sessions will be developed to address cyber security in 4th ESO students it should be mentioned that as Fernández (2019) stated it is necessary that a clear language and practical examples are used to train young learners. Moreover, it has to be totally personalized; should be implemented by a subject expert in that field; has to be implemented in a practical way (taking into account the material that both the trainer and the trainees have at their disposal); it may include the explanation of real cases; and, this training should be supported by a document.

From this information, therefore, we can say that this CLIL project will consist of 4 sessions of 55 minutes taught in English and that it will also involve the subject of computer science (or, failing that, technology) as the tasks to be carried out will require online knowledge and ICT tools (see detailed all the development of the sessions and its presentation slides in annexes 9.3. & 9.4.)

These sessions will also involve the completion of a final task by the students which will be assessed within the parameters of digital competence.

Moreover, attention to diversity and scaffolding strategies will be taken into account. If there are students with Individual Plans (called PI) the teacher would adapt the activities giving them more time or explaining to them as many times as they need. Also, the teacher will help them to develop the activities. Peers could also do it. Besides, if any student needs it, the teacher will repeat the instructions and solve the doubts at any moment during the session. The teacher also will try to engage all the students in the session at all times. This project also aims to boost students' collaboration and cooperation.

Furthermore, to ensure that the tasks to be performed are interconnected and fit the needs of the learners, Coyle's (1999) 4Cs framework (content, communication, cognition and culture) will also be established (see annex 9.5.).

6. CONCLUSIONS

This exploratory interpretative work has focused on giving visibility and importance to the fact that, within the digital field, cyber security is an aspect that should be dealt with and addressed from an early age in the educational world. There are many risks that we face when using the Internet every day, as well as many security measures that we can easily implement and apply, as long as we are aware of them.

Therefore, we can see how the main objective of the study has been achieved. This has been to centre on investigating the cyber-safety needs of students at the l'Hospitalet de Llobregat high school in order to subsequently develop a teaching-learning project in the English language. In this case, the project consists of four CLIL sessions combining both computer science and English language subjects under the *Core Competencies in the Digital Field* (Generalitat de Catalunya, 2015) as well as the necessary factors to be taken into account for planning, conceptualizing, monitoring and engaging, among others, to develop a CLIL practice (APAC, 2005).

On the other hand, throughout the research, it also has been possible to answer the specific objectives. Firstly, it has been possible to establish what exactly is meant by cyber security, as well as the risks to which we are exposed when using the Internet and its services. Then, a reference to the existing security measures was also made, placing special emphasis on the most essential ones as well as those that are most used by the school's students, such as the use of antivirus, private accounts, VPNs or firewalls. These security measures have been also taken into account during the project development in which the students will carry out different tasks to better understand and apply them.

Thirdly, we have been able to see how students claim to have received training in cyber security but, at the same time, consider that this is not enough and that it would be necessary to receive more training. Fourthly, the teachers did not reach a consensus on the ideal age to carry out this project, but they did reach the conclusion that it is highly recommended to do it during the compulsory secondary school stage, as well as in the last years of secondary school, such as the 4th year of ESO, as the students are older and can better understand the content taught. Finally, based on the evidence gathered through the observation period, the students' survey and the teachers' survey, we have tried to propose in the CLIL project the practices and content in cyber security that best suits the needs of the pupils at the school.

The study also showed that, to a certain extent, the first and the second hypothesis are true, as teenagers, state to apply safety measures and consider that they act safely on the Internet, but when they are asked to explain what they do to keep themselves safe, only a few of them give an optimal answer. Moreover, as it has been mentioned above, they claim to have received training in this area, but they state that it is not enough.

On the other hand, from the surveys carried out among the four teachers in the English department, it was found that they are aware that the use of new technologies has been increasingly implemented in the classroom, especially as a result of Covid-19, but that three of them claim that they have not received any training in this area, and the one who says he has received it, reports that it was through his bank, in neither case from the school. Hence, we can affirm that the third hypothesis formulated above, in that case, also holds true.

However, despite the results achieved and the project designed, there is still much to be done. We must be aware that in the age of the Internet and new technologies, cybercrime has developed overwhelmingly and is increasing over time, so being trained in cyber security must be a fundamental aspect to be addressed. Beginning to tackle the digital sphere in educational syllabuses is a great step forward, but the next step that remains to be taken is to consider cyber security as a curricular aspect, with its own competences and assessment, and thereby give it the weight it deserves.

At the same time, it is true that in terms of cyber security, we can more frequently find studies that refer to the subject. However, there are not so many studies that focus on cyber security as an aspect to be dealt with in educational centres. Quite the contrary. For this reason, we are facing a major methodological limitation, as we cannot compare these results with others and, consequently, cannot contrast them.

Therefore, it should also be noted that we cannot extrapolate on a larger scale the results obtained because they come from a sample that is not significant, these results are specific to the students of the school and the teaching staff of the English department. They are based on what has been observed, questioned and studied about the students and teaching staff of this particular institution. For this, as referred throughout the study, the project design is adapted to the needs of the centre studied, so the data are neither generalizable nor fully to society in general.

For all these reasons, in a society in which technology is becoming increasingly important, we should not take it for granted that we make good use of it. Just as we look after our security and privacy in the offline world, it is of the utmost importance that we also do the same online. What better way to start teaching and training than those who are likely to be among the groups that have the most contact with it: teenagers.

7. BIBLIOGRAPHY

APAC (2005). CLIL in Catalonia : from theory to practice. Barcelona.

Argente, E., Vivancos, E., Alemany, J., & Garcia-Fornes, A. (2017). Educating in privacy in the use of social networks. *Education in the Knowledge Society*, *18*(2), 107-126. Retrieved from: https://pdfs.semanticscholar.org/245d/c09e6b0017060c529e71d6c8c5efb2d40a15.pdf

Cenoz, J., & Gorter, D. (2013). Towards a Plurilingual Approach in English Language Teaching: Softening the Boundaries Between Languages. *TESOL Quarterly*, *47*(3), 591–599. DOI: http://www.jstor.org/stable/43268035

Council of Europe (2001). *Common European Framework of Reference for Languages: Learning, teaching, assessment*, Council of Europe. Retrieved from: https://rm.coe.int/16802fc1bf

Council of Europe (2020). *Common European Framework of Reference for Languages: Learning, teaching, assessment – Companion volume*, Council of Europe Publishing, Strasbourg. Retrieved from: https://rm.coe.int/common-european-framework-of-reference-for-languages-learning-teaching/16809ea0d4

Coyle, Hood, P., & Marsh, D. (2010). *CLIL : content and language integrated learning*. Cambridge University Press.

Esteve, O., Fernández, F., Martín-Peris, E., & Atienza, E. (2017). The Integrated Plurilingual Approach: A didactic model guiding Spanish schools for reconceptualizing the teaching of additional languages. *Language and Sociocultural Theory*, *4*(1), 1-24. DOI: 10.1558/lst.v3i2.32868

Fernández, L. D. (2019). Formación TIC (redes sociales, internet, ciberseguridad, big data, etc.) en casa, en el colegio, en la universidad y en la empresa: características, razón de ser y contenido. *CEF,(12),* 89-110. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=6775564

Gamito, R., Aristizabal, M. P., & Vizcarra Morales, M. T. (2019). Sociedad multipantalla: un reto educativo para familia y escuela. Retrieved from: http://hdl.handle.net/10810/54523

Garrido, M.J. & García - Collantes, Á. (2022). El impacto de las tecnologías de la información y la comunicación en la educación. La importancia de la formación, la información y la sensibilización. *Revista Tecnología, Ciencia y Educación*, (21), 155-182. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=8228576

Generalitat de Catalunya (2015). Core competencies in the digital field. *Ministry of Education.* Retrieved from: https://educacio.gencat.cat/web/.content/home/departament/publicacions/colleccions/competencies-basiques/eso/ambit-digital-angles.pdf

Gil, A.; Feliu, J.; Rivero, I. & Gil, E. (2003). ¿Nuevas tecnologías de la información y la comunicación o nuevas tecnologías de relación? Niños, jóvenes y cultura digital. (En línea). *Barcelona: Universitat oberta de Catalunya.* Retrieved from: https://www.uoc.edu/dt/20347/index.html

Gobierno de España (2021). Plan Integral de Cultura de Seguridad Nacional. (B.O.E. num.138 10-06-2021). Retrieved from: https://www.dsn.gob.es/es/documento/plan-integral-cultura-seguridad-nacional

González Davies, M. (2017). Towards a Plurilingual Development Paradigm. From Spontaneous to Informed Use of Translation in Additional Language Learning. *Universitat Ramon Llull. Barcelona.* Retrieved from: https://recercat.cat//handle/2072/283539

Haseski, H. İ. (2020). Cyber security skills of pre-service teachers as a factor in computer-assisted education. *International Journal of Research in Education and Science (IJRES), 6*(3), 484-500. Retrieved from: https://eric.ed.gov/?id=EJ1258516

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge.

Kemp, S. (2022). Digital 2022: Global Overview Report. *Datareportal*. Retrieved from: https://datareportal.com/reports/digital-2022-global-overview-report

Kopp, C., Layton, R., Sillitoe, J., y Gondal, I. (2015). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. International Journal of Cyber Criminology, 9(2). Retrieved from: http://cybercrimejournal.com/Koppetal2015vol9issue2.pdf

Lai, C., & Li, G. (2011). Technology and task-based language teaching: A critical review. *CALICO journal*, *28*(2), 498-521. Retrieved from: https://www.jstor.org/stable/calicojournal.28.2.498?seq=1&cid=pdf-reference

Mack, M. (2018). *Cyber security*. Scientific e-Resources. Retrieved from: https://books.google.es/books?hl=es&lr=&id=c-PEDwAAQBAJ&oi=fnd&pg=PA338&dq=Mack,+2018+cyber&ots=CEsRs456GW&sig=P1eO-e_gpO-dgtkcwxWYEh16TGI#v=onepage&q=Mack%2C%202018%20cyber&f=false

Ministerio del Interior (2021). Estudio sobre la cibercriminalidad en España. Gobierno de España. Sistema estadístico de criminalidad 2020. Retrieved from: http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3

Ministry of Education (2017). National Institute of Educational Technologies and Teacher Training. Common Digital Competence Framework for Teachers.Science and Sports: Madrid, Spain. Retrieved from: https://aprende.intef.es/sites/default/files/2018-05/2017_1024-Common-Digital-Competence-Framework-For-Teachers.pdf

Montiel, I. (2020). *Consecuencias, prevención e intervención de la cibervictimización.* Master en Ciberdelincuencia. Asignatura: Cibervictimización (UOC). https://materials.campus.uoc.edu/daisy/Materials/PID_00270860/pdf/PID_00270860.pdf

Muñoz, C. (2007). CLIL: Some thoughts on its psycholinguistic principles. *Revista española de lingüística aplicada*, (1), 17-26.

NICCS (20 July 2021). *Workforce Framework for Cybersecurity (NICE Framework). Retrieved from:* https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

Observaciber. https://observaciber.es/

OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers,* No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en.

ONTSI (2021). Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre la percepción y nivel de confianza en España. *Observaciber. Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital.* Edición diciembre 2021. Retrieved from: https://www.observaciber.es/sites/observaciber/files/media/documents/Dossier_Ciberseguridad_RED.pdf

Piccardo, E., & Galante, A. (2017). Plurilingualism and agency in language education: The role of dramatic action-oriented tasks. In *Plurilingualism in Teaching and Learning* (pp. 147-164). Routledge. Retrieved from: https://www.researchgate.net/publication/322603515_PiccardoE_Galante_A_2017_

Plurilingualism_and_agency_in_language_education_The_role_of_dramatic_action-oriented_tasks

Punie, Y. & Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Publications Office of the European Union, Luxembourg. Retrieved from: https://publications.jrc.ec.europa.eu/repository/handle/JRC107466

Richards, J & Rodgers, T. (2001). Approaches and Methods in Language Teaching. *Cambridge University Press. 2n Edition*

Riveirón, G. (2016). La cultura digital en la sociedad moderna. *Revista de Investigación en Tecnologías de la Información: RITI*, *4*(8), 1-6. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=7242782

Rodríguez, G. R. (2016). La cultura digital en la sociedad moderna. *Revista de Investigación en Tecnologías de la Información: RITI*, *4*(8), 1-6.

Rovira, L. (2008). The relationship between language and identity. The use of the home language as a human right of the immigrant. *REMHU-Revista Interdisciplinar da Mobilidade Humana*, *16*(31), 63-81. Retrieved from: https://www.redalyc.org/pdf/4070/407042009004.pdf

SIC (2021). Ciberseguridad, seguridad de la información y privacidad. Revista SIC. Septiembre, núm 146. Retrieved from: https://revistasic.es/sic146/revistasic146.pdf

Taylor-Powell, E. & Steele, S. (1996). Collecting evaluation data: Direct observation. *Program Development and Evaluation. Wiscounsin: University of Wisconsin-Extension*. 1-7. Retrieved from: http://www.pages.drexel.edu/~rosenl/CollectingObservDataProgrEval.pdf

Van den Branden, K. (2016). Task-based language teaching. *The Routledge handbook of English language teaching*, 238-251. Retrieved from: https://books.google.es/books?hl=es&lr=&id=jdUmDAAAQBAJ&oi=fnd&pg=PA238&dq=task+based+language+teaching&ots=XLQhMj7h3P&sig=bUiEpeI8T6qY8sxZPBkKNM61700#v=onepage&q=task%20based%20language%20teaching&f=false

Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Educating teens about the risks on social network sites. An intervention study in secondary education. *Comunicar. Media Education Research Journal*, *22*(2). Retrieved from: https://www.scipedia.com/wd/images/e/ef/Draft_Content_257433227-29652.pdf

Vasquez, D. A. (2019). Nativos Digitales: Aportes para problematizar el concepto/Digital Natives: Contributions to problematize the concept. *Revista de*

Educación, (16), 127-135. Retrieved from: http://fh.mdp.edu.ar/revistas/index.php/r_educ/article/view/2874

Venter, I., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12), e02855. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2405844019365144

Wilson, J. (2020). *Working within the Plurilingual Paradigm. Use of Translation to Enrich Additional Language Learning and Plurilingual Competence in Secondary Education in Catalonia* (Doctoral dissertation, Universitat Ramon Llull). Retrieved from: https://www.tdx.cat/handle/10803/670267 - page=1

8. NORMATIVE FRAMEWORK

Decret 187/2015, de 25 d'agost, d'ordenació dels ensenyaments de l'educació secundària obligatòria. (Annex 10). Retrieved from: https://portaldogc.gencat.cat/utilsEADOP/PDF/6945/1441278.pdf

Ley 12/2009, de 10 de julio, de Educación. (DOGC) (B.O.E. núm 189, 06-08 -2009). Retrieved from: https://www.boe.es/buscar/act.php?id=BOE-A-2009-13038

Deccreto 89/2009, de 9 de junio, por el que se regula la acreditación de competencias en tecnologías de la información y comunicación (ACTIC). (DOGC) (B.O.E. núm 5398, 11-06-2009). (Repealed by Decreto 13/2021). Retrieved from: https://noticias.juridicas.com/base_datos/CCAA/ca-d89-2009.html

Decreto 13/2021, de 2 de marzo, por el que se regula la acreditación de competencias en tecnologías de la información y comunicación (ACTIC). (DOGC) (B.O.E. núm 8356, 04-03-2021). Retrieved from: https://noticias.juridicas.com/base_datos/CCAA/690771-d-13-2021-de-2-mar-ca-cataluna-acreditacion-de-competencias-en-tecnologias.html

9. ANNEXES

9.1. DIRECT OBSERVATION GRID TEMPLATE

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books		
Laptops	Laptops are needed to follow the class or to do some activities		
	Students close the laptop when the class finishes		
Wi-Fi	Good Wi-Fi connection is needed to develop the class		
	Some websites are blocked to prevent their use		
Mobile phone	Mobile phone is needed in class		
	Mobile phone is allowed in class and students bring it		
Internet use	Students accept "cookies" without hesitation		
	Students use the internet only to do what is being asked of them		
Moodle	Moodle is used and works properly		

9.2. DIRECT OBSERVATION RESULTS

1st ESO – 52 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes, but only the Workbook.	In that case, the student's book is used physically. Only some students have both of them in digital version. Moreover, the Workbook is less used in class than the Student's book
Laptops	Laptops are needed to follow the class or to do some activities	Yes, but not always.	Depends on the activity the students have to do.
	Students close the laptop when the class finishes	No	Students turn down the screen but they do not close the laptop properly.
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes	However, depending on some circumstances such as the weather, how many people is using it at the same time, or where is located the class, Wi-Fi does not always work well.
	Some websites are blocked to prevent their use	Yes	However, not all non-educational websites are blocked.
Mobile phone	Mobile phone is needed in class	No	
	Mobile phone is allowed in class and students bring it	Yes	The students keep it in their bags.
Internet use	Students accept "cookies" without hesitation	Yes	
	Students use the internet only to do what is being asked of them	No	They are also in other websites (educational and non-educational).
Moodle	Moodle is used and works properly	Yes	

2nd ESO – 47 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes	They have the Workbook in digital version and some of them also the Student's Book.
Laptops	Laptops are needed to follow the class or to do some activities	Yes	Students are required to use the computer during the class.
	Students close the laptop when the class finishes	No	They turn down the screen without closing it before.
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes	However, it does not work always properly.
	Some websites are blocked to prevent their use	Yes	But only the most known ones such as Netflix or Facebook.
Mobile phone	Mobile phone is needed in class	Yes	In some classes students need it to do some activities such as Kahoots.
	Mobile phone is allowed and students bring it	Yes	The mobile phone should be stored, however, the students have it on the table and in some cases, they are using it to do other things not related to what is asked in class.
Internet use	Students accept "cookies" without hesitation	Yes	
	Students use the internet only to do what is being asked of them	No	Some of them are using Internet for other non-educational purposes.
Moodle	Moodle is used and works properly	Yes	

3rd ESO – 51 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes.	Some of them have both Workbook and Students' book in digital version and others, only have the workbook in digital version.
Laptops	Laptops are needed to follow the class or to do some activities	Yes.	Laptop is required during the class.
	Students close the laptop when the class finishes	No.	They only turn down the screen but they do not close it properly.
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes.	Above all because the teacher uses the Digital Version of the book and when the students are required to do something.
	Some websites are blocked to prevent their use	Yes.	Only the most common and known ones.
Mobile phone	Mobile phone is needed in class	Yes.	But only for specifical things and if they have the laptop it is not even necessary.
	Mobile phone is allowed in class and students bring it	Yes.	Mobile phones are not forbidden in the centre but students must not use it in class. They store it in their bags and only few of them look at it in some moments.
Internet use	Students accept "cookies" without hesitation	Yes.	
	Students use the internet only to do what is being asked of them	No.	If the teacher is not attentive, students start to do non-educational things.
Moodle	Moodle is used and works properly	Yes.	

4th ESO – 47 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes.	Students' have the Workbook in digital version (however, there are some of them that do not have it because they do not pay it). The Students' book mainly is used in a traditional way.
Laptops	Laptops are needed to follow the class or to do some activities	Yes, but not always.	Depend on the activity the students have to do or the way they work (with the use of notebook or not). Nevertheless, in most classes they are required to use it.
	Students close the laptop when the class finishes	No.	They turn down the screen.
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes.	
	Some websites are blocked to prevent their use	Yes.	Only the known ones.
Mobile phone	Mobile phone is needed in class	Yes, but not always.	Only when doing a Kahoot, for example, or when the Wi-Fi connection is slower than their own mobile data.
	Mobile phone is allowed in class and students bring it	Yes*	*To bring the mobile phone in class is not forbidden. However, they must not use it but in some cases they have it on the table and when the teacher does not look at them, they use it.
Internet use	Students accept "cookies" without hesitation	Yes.	They accept them without any hesitation.
	Students use the internet only to do what is being asked of them	No	The teacher should be attentive when he/she ask to do something with the computer because if not, students start to do other things on Internet.
Moodle	Moodle is used and works properly	Yes	It works well and students know how to use it.

1st BAC – 62 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes	They have the Workbook in digital version but the Students' book physically.
Laptops	Laptops are needed to follow the class or to do some activities	No	Usually, they do not need it. They only need it to do some specific activities. When it is required, the teacher ask them to bring it.
	Students close the laptop when the class finishes	No	When they use it and finish, they only turn down the screen.
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes	The teacher needs good Wi-Fi connection because he/she has the book in digital version. Moreover, when the students have to use the laptop, they need a good connection.
	Some websites are blocked to prevent their use	Yes	But only the most known, not all the non-educational ones.
Mobile phone	Mobile phone is needed in class	No	
	Mobile phone is allowed in class and students bring it	Yes	Mobile phone is allowed but students must not use it they have to store it.
Internet use	Students accept "cookies" without hesitation	Yes	
	Students use the internet only to do what is being asked of them	No	When students are required to do something, the teacher have to be attentive because if not, they start to use it for non-educational aims.
Moodle	Moodle is used and works properly	Yes	

2nd BAC – 39 students

Item	Observation parameters	Is the parameter observed?	Additional comments
Books	Students have "digital" books	Yes	Students have the Workbook in digital version; however, they have the students' book physically.
Laptops	Laptops are needed to follow the class or to do some activities	No*	Most classes they do not need it. Only when they have to do a specific activity. In those cases, the teacher tells them to bring it.
	Students close the laptop when the class finishes	No	
Wi-Fi	Good Wi-Fi connection is needed to develop the class	Yes*	Most classes only for the teacher because is he/she who uses the book in digital version. Nevertheless, when they have to do an activity which implies the laptop, it is necessary to have a good Wi-Fi connection.
	Some websites are blocked to prevent their use	Yes	Only some of them such as Netflix or WhatsApp web.
Mobile phone	Mobile phone is needed in class	No	
	Mobile phone is allowed in class and students bring it	Yes	Mobile phones are allowed but they must not use it, they have to keep it stored. However, some of them have it on the table and check the time or use it for non-educational purposes when the teacher is not looking.
Internet use	Students accept "cookies" without hesitation	Yes	
	Students use the Internet only to do what is being asked of them	Yes	When the teacher asks to do something, they use it properly.
Moodle	Moodle is used and works properly	Yes	

9.3. CLIL DEVELOPMENT SESSIONS

Area:	**Class:** *(e.g. 4th of ESO)*	**School Year:** 2021-2022 *(# trimester)*	**Teacher:** *(your name)*	**Timing:** *(# of sessions)*
CLIL – English & Computer Science	4th ESO	2021-2022 (3rd term)	Maria Bustamante Rabazo	55’
Other subjects involved	**Unit (name and justification)**			
Computer Science	**What do you know about cyber security?** (in this unit we are going to talk, mainly, about types of cyber crime, cyber security, privacy, malware and security measures.).			
Dimensions	**Competences**	**Specific Objectives**	**Key Content**	**Evaluation Instruments**
Digital field: - Tools and applications dimension - Citizenship, habits, civics and digital identity dimension. **Linguistic field:** - Oral communicative dimension. - Reading comprehension dimension. - Attitudinal and plurilingual	**Digital field:** C1. Choosing, configuring and programming digital devices depending on the task being performed C11. Acting critically and responsibly when using ICT considering factors such as ethics, laws, safety, sustainability, and digital identity. **Linguistic field:** C2. To plan and produce oral texts of different types appropriate to the	1. To be educated in cyber security and cyberspace. 2. To know the meaning of different words related to cyberspace. 3. To know how to use ICTs to protect themselves on Internet. 4. To be able to conduct simple research practices and to draw conclusions.	**Digital field:** CC26. Virtual environments safely **Linguistic field:** CC1. Oral comprehension CC2. Oral comprehension strategies. CC3. Oral production strategies. CC4. Oral interaction strategies. CC5. Reading out loud. CC9. Search and management information.	- Evaluation criteria grids/rubric: the presentation and the content exposed on it will be assessed throughout a grid. 6. Presentation: 60% 7. Content exposed: 40%

transversal dimension. **Scientific-technological field:** - Technological objects and systems dimension of everyday life	C3. To employ oral interaction strategies according to the communicative situation to start, continue and end a speech. C6. To select and use search tools to access text comprehension and knowledge acquirement. **Scientific-technological field:** C7. Use technological objects of everyday life with basic knowledge of theiroperation, maintenance and actions to be carried out in order to minimise risks in handling and environmental impact.	5. To expose research results orally in front of the class.	CC10. Selection criteria and evaluation of information. CC16. Dictionary use. C20. Pragmatics. CC21. Phonetic and phonology. CC22. Lexis and semantics. CC23. Morphology and syntax. CC24. Verbal and non-verbal strategies to overcome misunderstandings. **Scientific-technological field:** CC17. 17. Technological objects in everyday life.	
Learning and teaching activities				

__Session 1 – Cyberspace__

- **Warm-up:** The teacher will ask the students the following questions related to cyberspace: **What do you know about cyber crime? And cyber security?** Then, the teacher will ask: **Why do you think someone commits a crime?** (‘5)
- Once the discussion is over, the teacher will start explaining the different types of cyber crime according to different classifications and will ask the students to search on the Internet for recent news about one of these types. (20’)
- Once finished, the teacher will ask the students: **Do you know how computers read the information?** And the teacher will explain that computers use a Binary Code. So, with the help of a table that will be projected in the presentation, the students would write their names using this “binary code” and would try to read it out loud. (10’)
- Next to it, the teacher will ask the students: **do you know how networks work?** And will start by explaining what is and IP address, a router, a modem, the Internet Service Provider (ISP) and the Internet. Then, the teacher will ask the students to find their own IP addresses. An article with the steps will help them. (15’)
- Exit ticket: finally, the students in pairs will have to answer some questions and share them with their classmates: (5’)

  Do you have Internet at home? If so, which is your Internet provider?

  Is it the same?

  Does it work properly?

Resources/materials: for this session, we need an Interactive Whiteboard, laptops, projector, Wi-Fi connection and the PowerPoint presentation.

__Session 2 – Digital identity, Privacy & Malware__

- **Warm-up:** The teacher will play a video related to an experiment done to prove how much information we share when connecting to a public Wi-Fi network. (5’)

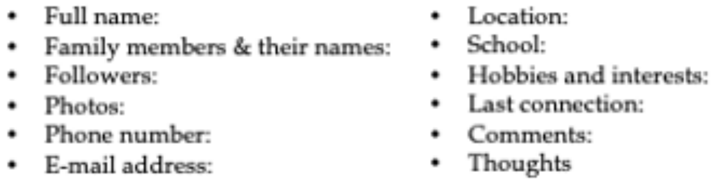
- Then, the teacher will ask some questions and will discuss them with the students (5')

  Do you know what is Digital Identity?

  Do you care about your privacy on the street? And online?

  Did you know/heard about the risks you take when connecting to a public Wi-Fi network?

- Once finished, the students will do a task where they will see what others can know about them. So, in pairs, they will enter into a social network such as Instagram, Facebook and Twitter and will try to find out the following information about his/her classmate: (10')



- Full name:
- Family members & their names:
- Followers:
- Photos:
- Phone number:
- E-mail address:
- Location:
- School:
- Hobbies and interests:
- Last connection:
- Comments:
- Thoughts

- Then, the teacher will ask: **do you know how to create strong passwords?** And will ask the students to follow a link to create the strongest password they could. (10')
- Next, the teacher will ask the students: **Did you know that when we "surf on the Internet" there are a lot of invisible trackers trying to get some information about us?** So, the teacher will show the students some helpful free tools as Privacy Badger and Https Everywhere to help them to avoid it. (10')
- Subsequently, the teacher will explain what is a malware. To do that, the teacher will ask: **are you able to define what a "malware" is? Do you know some of its types and characteristics?** And then the teacher will explain its definition and some different types of malwares with the help of a match game in which the students will take part doing it all together. (10')
- Exit ticket: finally, the students will answer a Mentimeter to give their opinion of the class. (5')

Resources/materials: for this session, we need an Interactive Whiteboard, laptops, projector, Wi-Fi connection and the PowerPoint presentation.

Session 3 – Security measures (a guide of best practices)

- **Warm-up:** the teacher will ask the students: **do you think the Internet makes us worse people?** and they will discuss it in class. (8')
- Then, the teacher will ask the students to watch a brief video about cyber security and security measures. (2')
- Next, the teacher will start talking about them: firewalls, software updates, antivirus, back-up copies, password manager and unlocking the system. And will ask the students to discuss with their partners if they take into account any of them and make a list of all the security measures they both use. (10')
- Once finished, the teacher will start explaining some pieces of advice, that is, the teacher will show a good practice guideline on the screen to help the students be secure. (10')
- Finally, the teacher will explain their final task and the students will start working on it. The teacher will guide the students and solve the problems that may arise. (25')
    - In groups of 3 or 4 choose one of the cyber risks we have talked about.
    - Look for information about:
        - Type of cyber crime
        - Cyber crime definition and characteristics
        - Offender profile
        - Victim profile
        - Security measures to prevent it
    - Prepare a 5 -7 minutes presentation to expose it to all your classmates for the next session.

Resources/materials: for this session, we need an Interactive Whiteboard, laptops, projector, Wi-Fi connection and the PowerPoint presentation.

Session 4 – Final presentations

- Students will start with their presentations. The teacher will assess the presentation (60%) and the content explained (40%) throughout a grid (55').

Resources/materials: computers, a projector, the Whiteboard and the grid.

BIBLIOGRAPHY & WEBGRAPHY

Avast (s/e). *How to Find Your IP Adress on Windows or Mac.* *https://www.avast.com/c-how-to-find-ip-address*

Https Everywhere. https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=ca

Miró, F. (2012). El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *Madrid: Marcial Pons.*

Oficina de Seguridad del Internauta. https://www.osi.es/es

PandaMediaCenter (13th July 2019). *Girls in Tech. 10 Cybersecurity Lessons to teach kids. https://www.pandasecurity.com/en/mediacenter/technology/girls-in-tech/*

Password.es Comprobador de Contraseñas. https://password.es/comprobador/

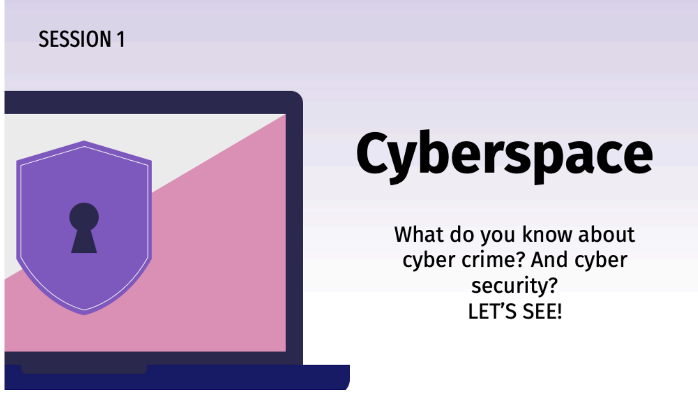
Privacy Badger. https://privacybadger.org/

Stratanetworks (2018, 8 January). *Quick tip. Cybersecurity best practices.* (Video). https://www.youtube.com/watch?v=YuzE-NCP9YE

WithSecure (2014, 29 September). *The Great Wi-Fi Experiment.* (Video). https://www.youtube.com/watch?v=OXzDyL3gaZo

9.4. CLIL SESSIONS PRESENTATIONS

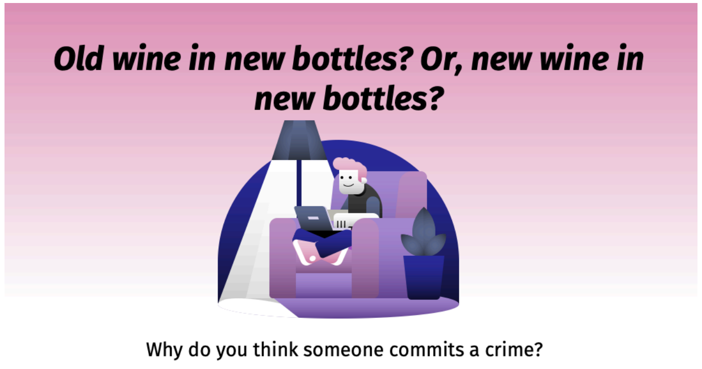
SESSION 1



SESSION 1

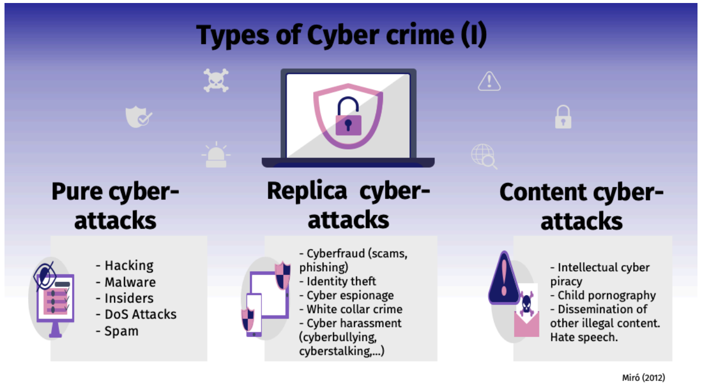
Cyberspace

What do you know about cyber crime? And cyber security?
LET'S SEE!



Old wine in new bottles? Or, new wine in new bottles?

Why do you think someone commits a crime?



Types of Cyber crime (I)

Pure cyber-attacks

- Hacking
- Malware
- Insiders
- DoS Attacks
- Spam

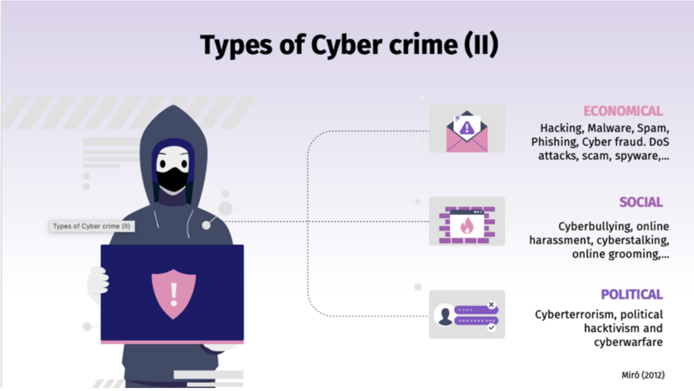
Replica cyber-attacks

- Cyberfraud (scams, phishing)
- Identity theft
- Cyber espionage
- White collar crime
- Cyber harassment (cyberbullying, cyberstalking,...)

Content cyber-attacks

- Intellectual cyber piracy
- Child pornography
- Dissemination of other illegal content. Hate speech.

Miró (2012)



Types of Cyber crime (II)

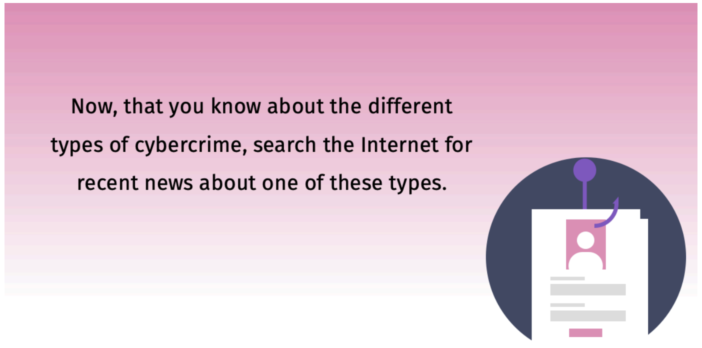
Types of Cyber crime (II)

ECONOMICAL
Hacking, Malware, Spam, Phishing, Cyber fraud. DoS attacks, scam, spyware,...

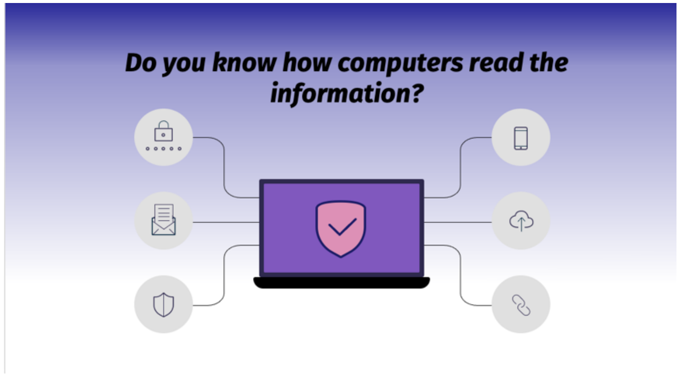
SOCIAL
Cyberbullying, online harassment, cyberstalking, online grooming,...

POLITICAL
Cyberterrorism, political hacktivism and cyberwarfare

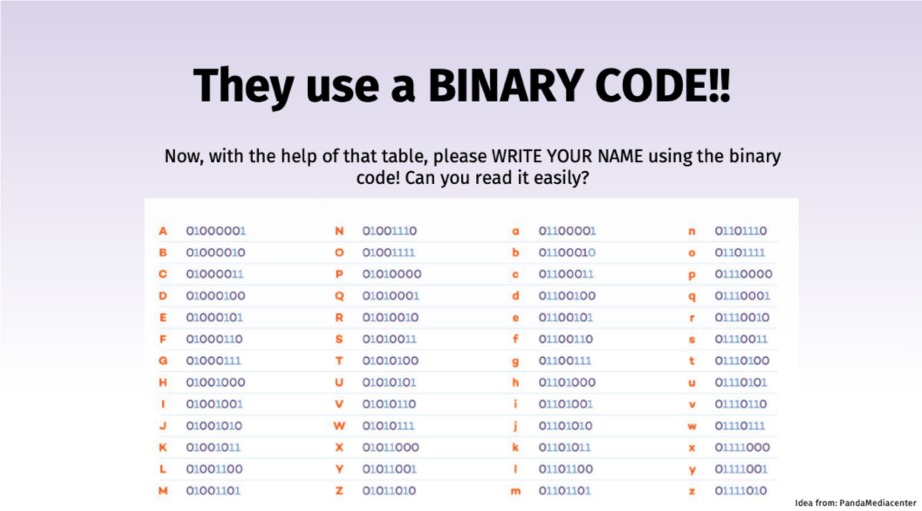
Miró (2012)



Now, that you know about the different types of cybercrime, search the Internet for recent news about one of these types.



Do you know how computers read the information?

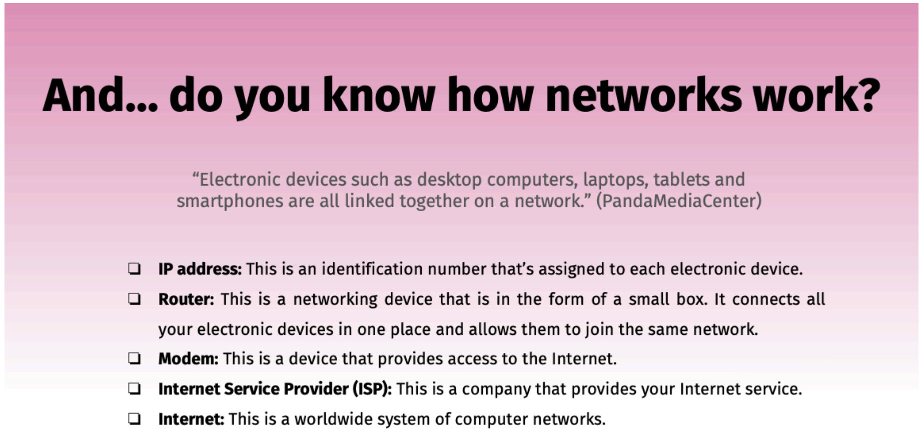


They use a BINARY CODE!!

Now, with the help of that table, please WRITE YOUR NAME using the binary code! Can you read it easily?

A	01000001	N	01001110	a	01100001	n	01101110
B	01000010	O	01001111	b	01100010	o	01101111
C	01000011	P	01010000	c	01100011	p	01110000
D	01000100	Q	01010001	d	01100100	q	01110001
E	01000101	R	01010010	e	01100101	r	01110010
F	01000110	S	01010011	f	01100110	s	01110011
G	01000111	T	01010100	g	01100111	t	01110100
H	01001000	U	01010101	h	01101000	u	01110101
I	01001001	V	01010110	i	01101001	v	01110110
J	01001010	W	01010111	j	01101010	w	01110111
K	01001011	X	01011000	k	01101011	x	01111000
L	01001100	Y	01011001	l	01101100	y	01111001
M	01001101	Z	01011010	m	01101101	z	01111010

Idea from: PandaMediacenter



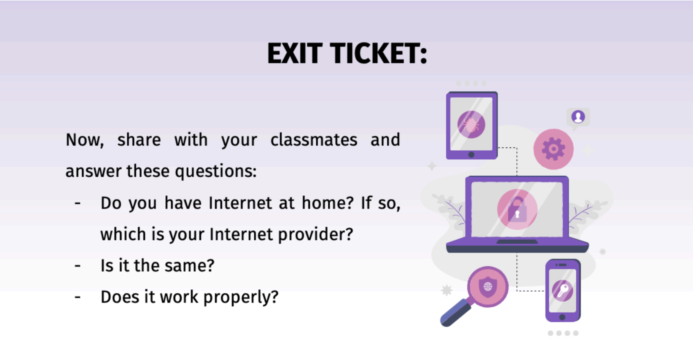
And... do you know how networks work?

"Electronic devices such as desktop computers, laptops, tablets and smartphones are all linked together on a network." (PandaMediaCenter)

- ❑ **IP address:** This is an identification number that's assigned to each electronic device.
- ❑ **Router:** This is a networking device that is in the form of a small box. It connects all your electronic devices in one place and allows them to join the same network.
- ❑ **Modem:** This is a device that provides access to the Internet.
- ❑ **Internet Service Provider (ISP):** This is a company that provides your Internet service.
- ❑ **Internet:** This is a worldwide system of computer networks.

Find your own IP address!

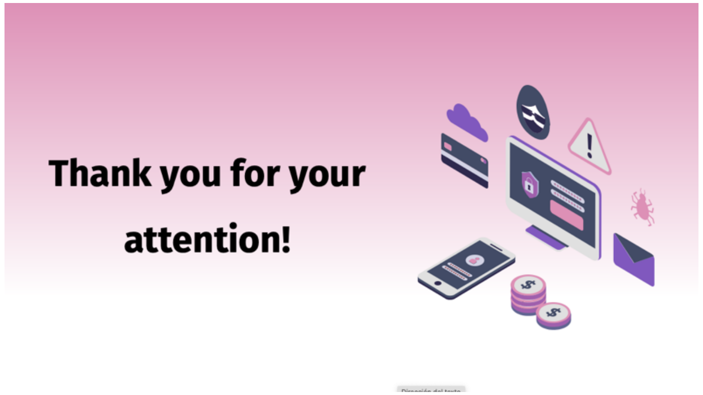
Click here and follow the steps



EXIT TICKET:

Now, share with your classmates and answer these questions:

- Do you have Internet at home? If so, which is your Internet provider?
- Is it the same?
- Does it work properly?

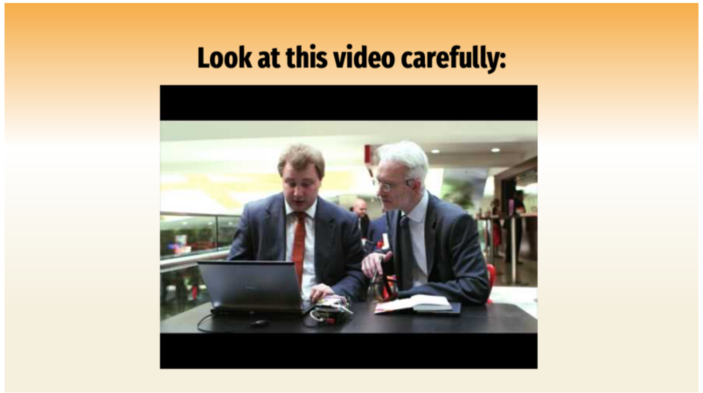


Thank you for your attention!

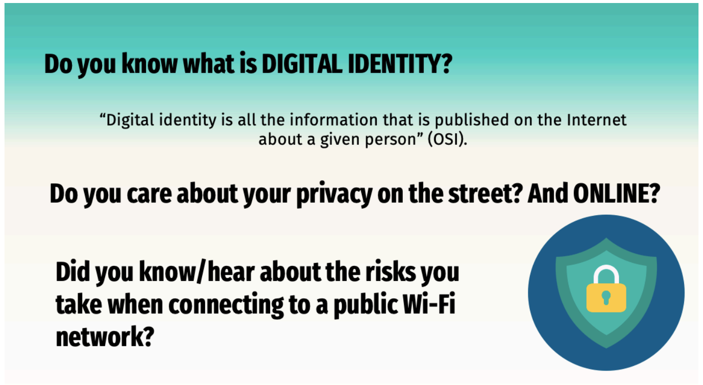
SESSION 2

SESSION 2

Digital identity, Privacy & Malware



Look at this video carefully:

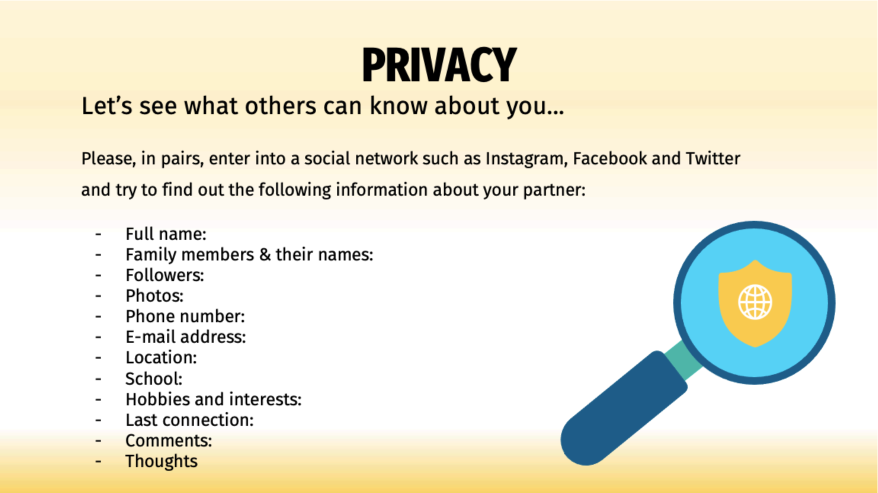


Do you know what is DIGITAL IDENTITY?

"Digital identity is all the information that is published on the Internet about a given person" (OSI).

Do you care about your privacy on the street? And ONLINE?

Did you know/hear about the risks you take when connecting to a public Wi-Fi network?



PRIVACY

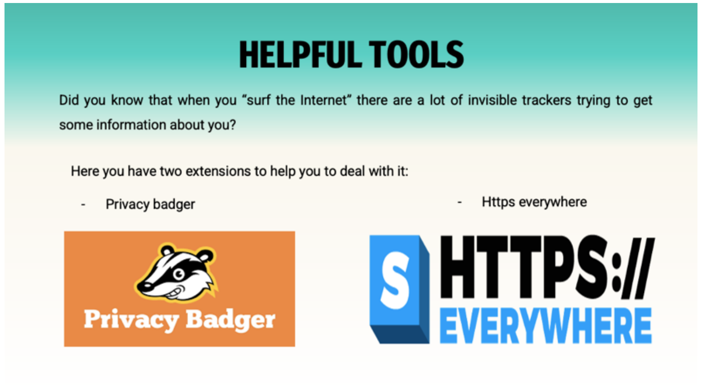
Let's see what others can know about you...

Please, in pairs, enter into a social network such as Instagram, Facebook and Twitter and try to find out the following information about your partner:

- Full name:
- Family members & their names:
- Followers:
- Photos:
- Phone number:
- E-mail address:
- Location:
- School:
- Hobbies and interests:
- Last connection:
- Comments:
- Thoughts

DO YOU KNOW HOW TO CREATE STRONG PASSWORDS?

Follow that link, follow its instructions, and create the strongest password that you can!

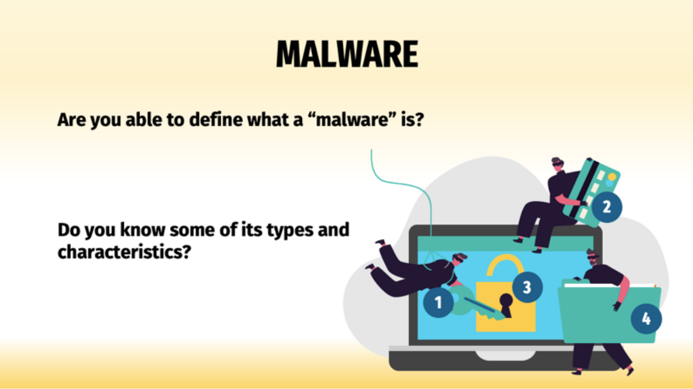


HELPFUL TOOLS

Did you know that when you "surf the Internet" there are a lot of invisible trackers trying to get some information about you?

Here you have two extensions to help you to deal with it:

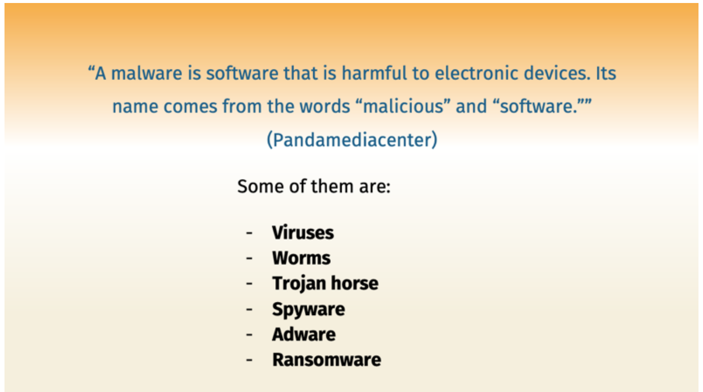
- Privacy badger
- Https everywhere



MALWARE

Are you able to define what a "malware" is?

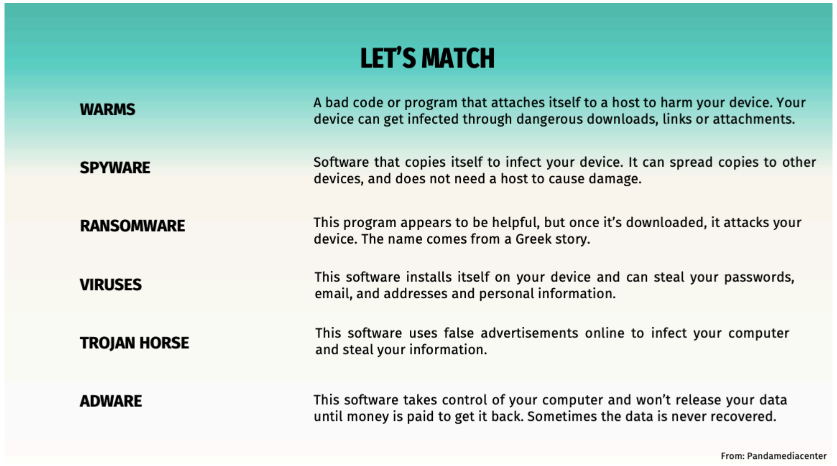
Do you know some of its types and characteristics?



"A malware is software that is harmful to electronic devices. Its name comes from the words "malicious" and "software."" (Pandamediacenter)

Some of them are:

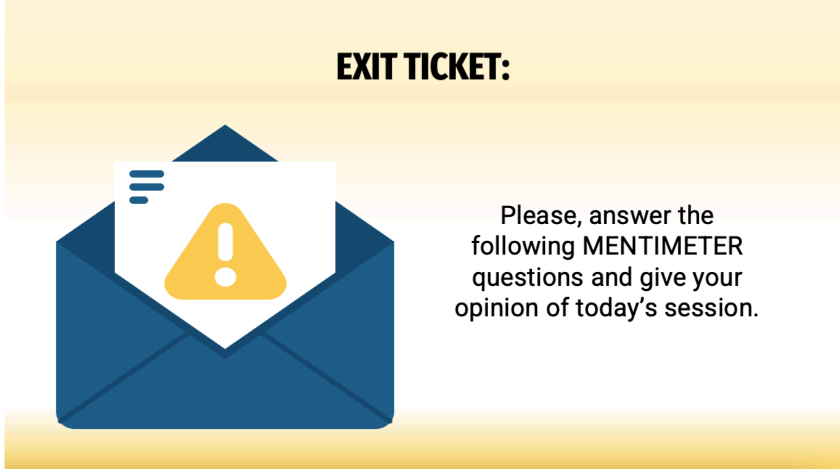
- **Viruses**
- **Worms**
- **Trojan horse**
- **Spyware**
- **Adware**
- **Ransomware**



LET'S MATCH

WARMS	A bad code or program that attaches itself to a host to harm your device. Your device can get infected through dangerous downloads, links or attachments.
SPYWARE	Software that copies itself to infect your device. It can spread copies to other devices, and does not need a host to cause damage.
RANSOMWARE	This program appears to be helpful, but once it's downloaded, it attacks your device. The name comes from a Greek story.
VIRUSES	This software installs itself on your device and can steal your passwords, email, and addresses and personal information.
TROJAN HORSE	This software uses false advertisements online to infect your computer and steal your information.
ADWARE	This software takes control of your computer and won't release your data until money is paid to get it back. Sometimes the data is never recovered.

From: Pandamediacenter



EXIT TICKET:

Please, answer the following MENTIMETER questions and give your opinion of today's session.

SESSION 3

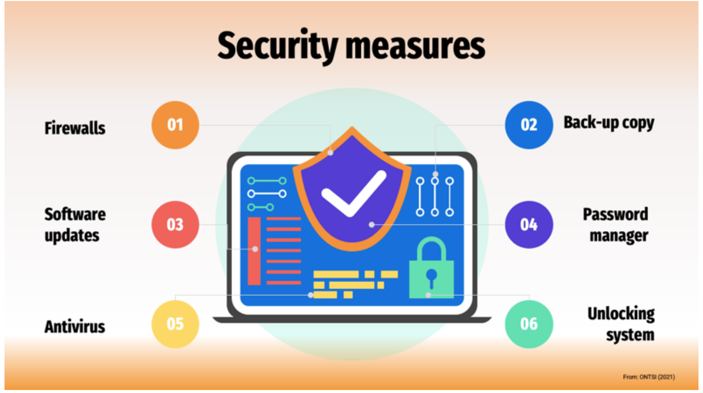
SESSION 3

Security measures

A guide to best practices

Do you think the Internet makes us worse people?

Watch the following video:



Security measures

01 Firewalls

02 Back-up copy

03 Software updates

04 Password manager

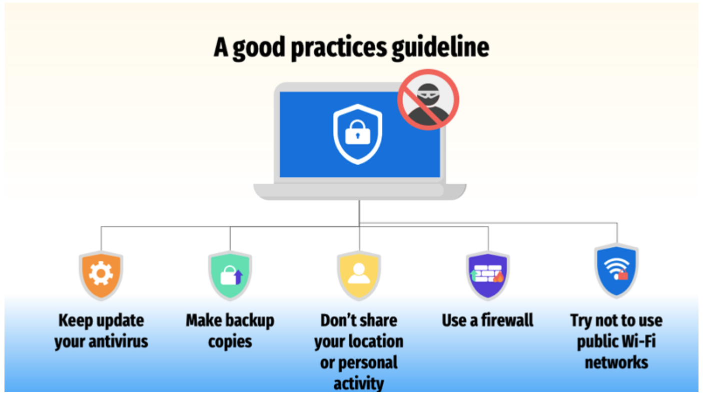
05 Antivirus

06 Unlocking system

From: ONTSI (2021)

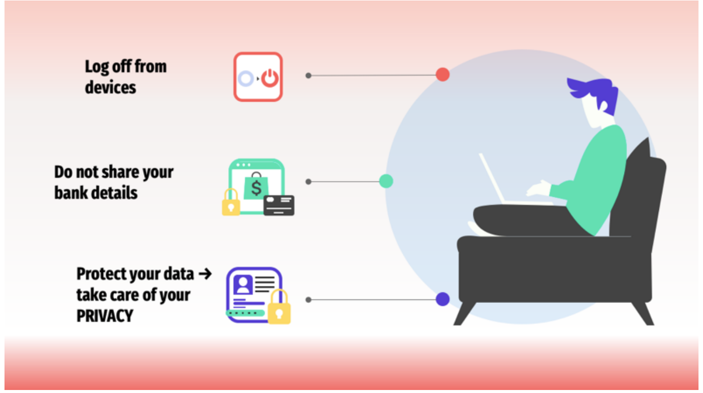
Do you take into account any of them?

Discuss with your partner this question and make a list of all the security measures you both use.



A good practices guideline

- Keep update your antivirus
- Make backup copies
- Don't share your location or personal activity
- Use a firewall
- Try not to use public Wi-Fi networks



Log off from devices

Do not share your bank details

Protect your data → take care of your PRIVACY

Encrypt the important data

Create strong passwords

Don't be tricked

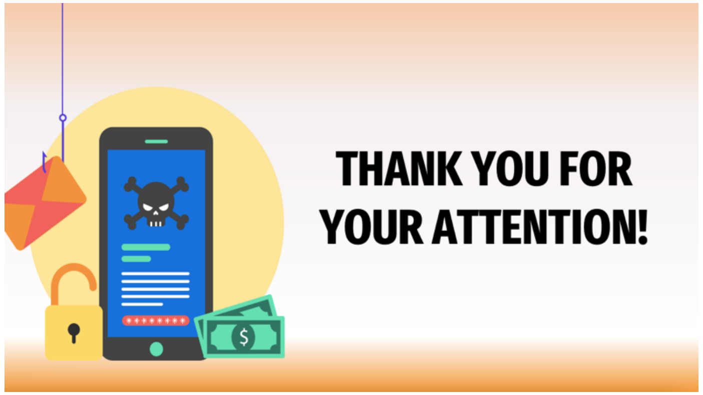
Unlock the system properly

And at last but not least...

Be very careful with the information and photos you share on social media!!

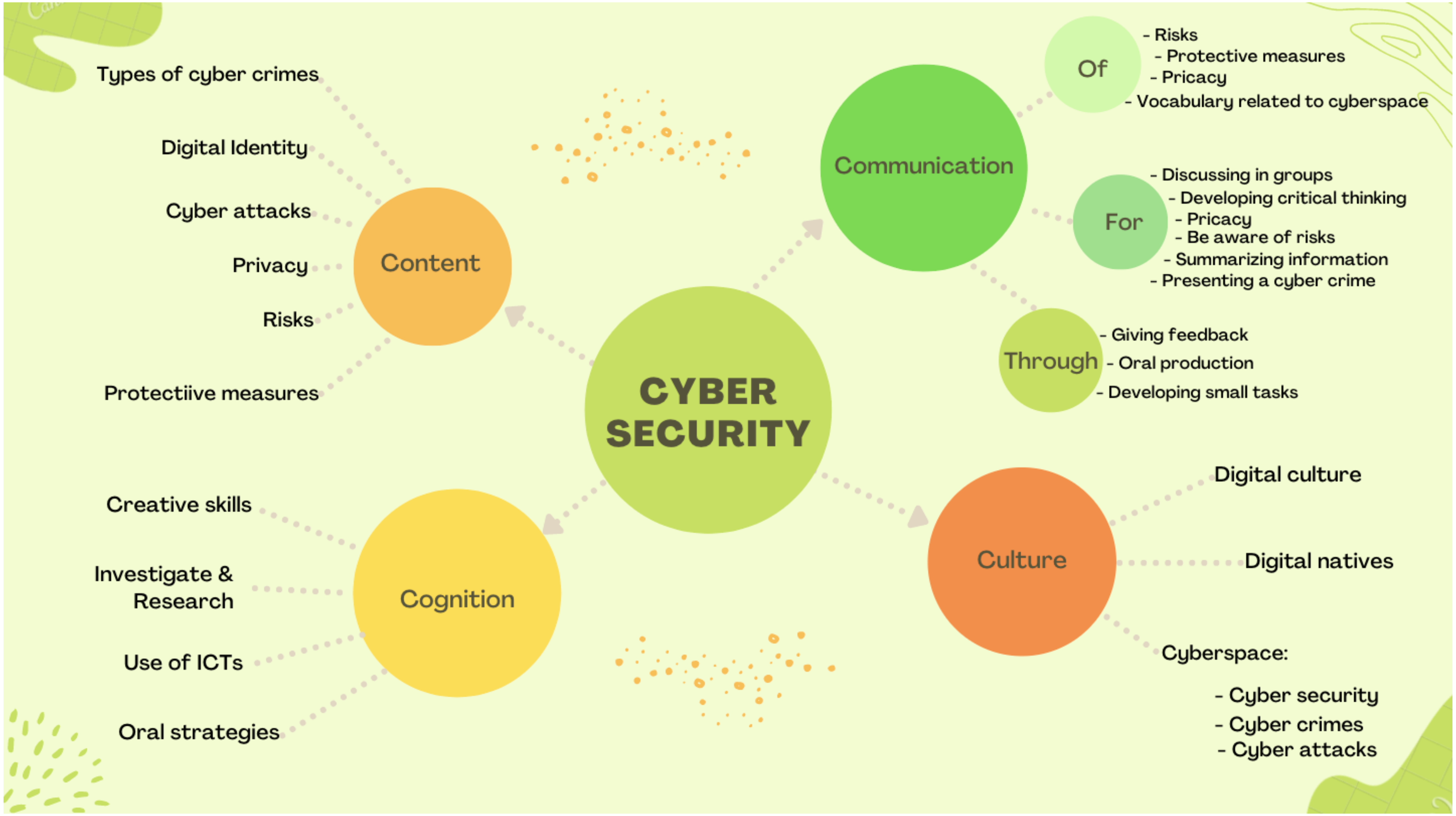
NOW, IT'S TIME TO DO YOUR FINAL TASK....

- In groups of 3 or 4 choose one of the cyber risks we have talked about.
- Look for information about:
  - Type of cyber crime
  - Cyber crime definition and characteristics
  - Offender profile
  - Victim profile
  - Security measures to prevent it
- Prepare a 5 -7 minutes presentation to expose it to all your classmates for the next session.



THANK YOU FOR YOUR ATTENTION!

9.5. 4Cs CLIL FRAMEWORK



CYBER SECURITY

Content

Types of cyber crimes

Digital Identity

Cyber attacks

Privacy

Risks

Protectiive measures

Communication

Of

- Risks
- Protective measures
- Pricacy
- Vocabulary related to cyberspace

For

- Discussing in groups
- Developing critical thinking
- Pricacy
- Be aware of risks
- Summarizing information
- Presenting a cyber crime

Through

- Giving feedback
- Oral production
- Developing small tasks

Cognition

Creative skills

Investigate & Research

Use of ICTs

Oral strategies

Culture

Digital culture

Digital natives

Cyberspace:

- Cyber security
- Cyber crimes
- Cyber attacks