European Commission

JRC TECHNICAL REPORTS

Attitudes towards cyber risks
Implicit and self-report measures

The Happy Onlife edutainment experience of secondary school children

Di Gioia, R. (JRC)
Di Pomponio, I. (UTIU)
Gemo, M. (JRC)
Chaudron, S. (JRC)

2019

EUR 28401 EN

Contact information
Name: Rosanna Di Gioia
Address: Joint Research Centre, Via E. Fermi, 2749, I-21027 Ispra (Varese) – Italy
Email : rosanna.di-gioia@ec.europa.eu
Tel: 0332.785826

JRC Science Hub
https://ec.europa.eu/jrc

JRC104984

EUR 28401 EN

PDF	ISBN 978-92-79-64955-4	ISSN 1831-9424	doi:10.2760/752186
Print	ISBN 978-92-79-64954-7	ISSN 1018-5593	doi:10.2760/974597

Luxembourg: Publications Office of the European Union, 2019

How to cite this report:
DI GIOIA R., DI POMPONIO I., GEMO M., CHAUDRON S. (2019) *Attitudes towards cyber risks. Implicit and self-report measures. The Happy Onlife edutainment experience of secondary school children*, EUR 28401 EN, JRC104984, ISBN 978-92-79-64955-4 doi:10.2760/752186

Attitudes towards cyber risks
Implicit and self-report measures

The Happy Onlife edutainment experience of secondary school children

Di Gioia, R. (JRC)
Di Pomponio, I. (UTIU)
Gemo, M. (JRC)
Chaudron, S. (JRC)

2019

Joint Research Centre

EUR 28401 EN

Table of Contents

Acknowledgements

This work is indebted to the numerous students, parents and teachers who have placed trust and confidence in this research.

We would like to express our sincere gratitude to all of them.

Finally, we are grateful to everyone who contributed to the entire Happy Onlife project development and inspiration.

Authors

Rosanna Di Gioia, European Commission, Joint Research Centre

Rosanna Di Gioia is a researcher in the JRC Cyber and Digital Citizens' Security Unit. Her background is in Social Psychology and she has earned a master degree in Cognitive Processes and Technology from UTIU - International Telematics University Uninettuno with a focus on Media Education, Social Cognition and Cyber Risk Propensity Assessment. In the past five years she has been involved in projects on cyber-security, cyber-bullying and empowering citizens' rights in emerging ICT. Her research interests include privacy and data protection practices together with digital play. She is currently coordinating the development and dissemination of an edutainment in the format of a storytelling game introducing data protection rights to (young) citizens. Previously, she contributed to development of the Happy Onlife toolkit raising awareness on internet risks and opportunities. Currently she is involved in projects exploring the digital transformation impact of the Internet of Toys. She is also contributing to Prevention Policies Fighting Child Sexual Abuse.

Ileana Di Pomponio - International Telematic University Uninettuno

Ileana Di Pomponio, PhD is professor at International Telematic University Uninettuno (Italy) - Department of Psychology and at University of Rome Tor Vergata. She is Psychologist, Researcher, Data Analyst and Social Media Marketing Specialist with full expertise in Explicit and Implicit Measure of children's attitudes towards risky behaviours.

Monica Gemo, European Commission, Joint Research Centre

Monica Gemo is a scientific officer in the JRC Cyber & Digital Citizens' Security Unit, where she is investigating participatory mobile edutainment tools. She holds an MSc degree from Politecnico di Milano, Italy. From 2002 to 2007, she worked at the Catholic University of Louvain, Belgium, specializing in multimodal applications.

Stéphane Chaudron, European Commission, Joint Research Centre

Stéphane Chaudron works on research projects dedicated to (Young) Digital Citizens' Security and Safety at the Joint Research Centre of the European Commission. Her background is in Social Geography and Science Pedagogy. She has been for years in charge of the coordination of large European Research Networks dedicated to e-Safety, new media education, standardization and science teaching education (Imperial College London, UCLouvain, European Schoolnet). She has been in charge of the coordination of EC's research project 'Young Children (0-8) and Digital Technology' since 2014. She contributed to the development of the Happy Onlife toolkit raising awareness on internet risks and opportunities and of Cyber Chronix, an edutainment on Digital rights. Recently she undertook research focusing on security and safety of the Internet of Toys and explores the effect of the digital transformation on the concept of Identity, on the way users manage (or not) their personal data.

Abstract

The Happy Onlife experience has contributed to children's right to be heard in matters affecting them in their digital interactions and lives. Happy Onlife has been considered as effective awareness raising and learning tool regarding cyber security issues by its end-users, namely students, teachers, parents and educators. By playing with Happy Onlife game, children could naturally self-disclose and express their emotions, needs, understanding and sometimes worries and doubts. Indeed, self-reporting provides valuable insights for a wide range of research, policy and educational questions, however it can be susceptible to self-presentation and socially desirable responding. To overcome these limitations, implicit measures were considered to complement experimental research about children's attitude towards cyber risks.

The work described in this document aims at evaluating the effect of the Happy Onlife tool on attitudes towards cyber risk of children aged 10-12, from Time T1 to Time T2, before and after using Happy Onlife edutainment. The first research aim is to test the Happy Onlife edutainment reliability as a learning tool for enhancing digital competences with a focus on cyber security, data protection, privacy, online communication, netiquette and digital identity management. Moreover, a second purpose is the contribution to the development and validation of a new implicit measure of cyber risk propensity for children (10-12 years old). A third aim is to investigate the relationship between implicit risk attitudes and explicit risk-taking behaviour.

In this pilot research all explicit and implicit measures showed adequate reliability. There was a significant effect pre and post Happy Onlife gaming experience. Current results suggest that the *Cyber Security Implicit Association Test (IAT)* is a reliable and valid method and may be a useful tool to be added to self-report batteries for cyber risk propensity assessment in children. The *Cyber Security Implicit Association Test* could be considered for future and wider research on risk-taking behaviour by citizens of all ages. The experiment protocol can be improved, however this contribution could be taken into consideration for the study and implementation of European cyber security strategies and policies to limit online threats and risks.

1 Introduction

In recent years, researchers and policymakers, worldwide, have taken into consideration empirical research findings to better understand online behaviours and consequences of decision-making processes.

This research is part of a larger project to raise awareness of online risks and opportunities for children and adults, which has encouraged the development of the Happy Onlife edutainment toolkit ([1]). The Happy Onlife resources were firstly developed and validated following a qualitative approach based on observations, focus groups and self-report measures by children, teachers and parents. With this work we would like both to consider quantitative assessment measures and to study children's attitudes and behaviours towards cyber security threats and risks.

The work described in this document aims at confronting the previous research results (Di Gioia, Gemo, & Chaudron, 2015), thus testing the validity of Happy Onlife resources as a learning tool for digital competences. Moreover, a second purpose of the present research is the development and validation of new implicit measures of risk propensity for children (10-12 years old). A third aim is to investigate the relationship between implicit risk attitudes and objective risk-taking behaviour. A final aim is to examine the role of personality factors, sensation seeking and emotion regulation on the implicit risk propensity. The experiment was conducted with 106 secondary school students in the northern part of Italy. Participants had to respond to a questionnaire, to take an Implicit Association Test (Harward University, 2016), to participate in the Happy Onlife edutainment experience, to respond to a second questionnaire - Brief Sensation-Seeking Scale (BSSS) for children - and to take a second round of the Implicit Association Test (IAT).

Results are as follows:

- the cyber security IAT shows good reliability (the split-half method) and good convergent validity, demonstrated by positive correlations with the sensation-seeking scale;
- Time 2 (T2) scores will be higher than in Time 1 (T1);
- there is a positive correlation between explicit and implicit measures of cyber security.

This empirical research has to be considered as a pilot that could be improved and then exploited across other European Union Member States. These results could be explored in a larger project at European Union level as other academics have shown interest in such research projects, thus they could be useful to policymakers interested in online behaviours and potential cyber security threats and risks.

The theoretical framework is presented in the first chapter and the second defines the social cognition framework, attitudes and implicit measures. The methodology is treated in the third chapter, while the fourth provides results with discussion and limits. Finally, further research developments are explored and conclusions are provided.

([1]) Edutainment is a neologism to express the process of entertainment and education at the same time.

2 Theoretical framework

This research was conceived under a theoretical framework, which includes notions of cyber security and risks, privacy and data protection, digital competences and social cognition.

2.1 Cyber security and risks

The explosion of mobile and globally interconnected new technologies alters the cyber threat landscape and underlines the need to develop a cyber security culture amongst internet users independently of their age, race or social and economical status.

In its report, *Status of privacy and Network Information System directive (NIS) course curricula in the Member States* (Anderson, De Paoli, & Câtâlui, 2015), the European Union Agency for Network and Information Security states that cyber security is a key competence for Information and Communication Technology (ICT) users. In addition, Massive Open Online Courses (MOOCs) and serious games are considered to be a path to transfer knowledge, to support learning, to raise awareness, to offer professional training and to unveil controversial issues and practices surrounding privacy and data protection in a practical way.

First of all, the term cyber security needs to be defined, since no standard or universally accepted definition exists to date.

The Internet Society refers to the term as 'a catchword, cyber security is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges and solutions ranging from the technical to the legislative' (InternetSociety, 2012).

The International Telecommunication Union defines cyber security as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, action, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets' (InternationalCommunicationTelecommunication, 2015).

Weber and Studer (Weber & Studer, 2016) assume that to start a discussion about cyber security it is necessary to identify the threats that challenge it. They distinguish threats by (i) threats agents, (ii) threats tools, and (iii) threats types.

Threats agents can include profit-driven cyber criminals, criminal organisations, hackers, hacktivists, extremists and nation states. This list cannot be considered as exhaustive and these categories are not mutually exclusive.

Threat tools encompass breach tools as malware and its variants (virus, worms, Trojan, etc.), and botnets.

Threat types to cyber security involve threats related to information, modification or misuse, information destruction, unauthorised access, data breaches, data theft and denial of service.

At the European Union level, the European Agenda on Security 2015-2020 (COM(2015) 185) adopted in April 2015 and the digital single market communication of 6 May 2015 (COM(2015) 192 final pp.13-20, 2015) underline the need for a common approach to address cyber threats across Europe, building on the existing cyber security strategy of the European Union launched in February 2013 (EEAS, 2013). Proposed measures in these documents outline the need for an inclusive definition for the concept of cyber security, covering five policy dimensions:

1. achieving cyber resilience in Europe;
2. fighting cyber crime;
3. developing the industrial and technological resources for cyber security;
4. developing a cyber defense policy and capabilities related to the common security and defense's policy;

5. establishing a coherent international cyber space policy for the EU and promoting EU core values.

The two major policy pillars of the current cyber security policy landscape are the NIS (European Parliament and Council (NIS), 2015) and the General Data Protection Regulation (Regulation (EU)679, 2016).

These policy actions and strategies prove that the cyber security risk is a topic of much interest nowadays. As such, it deserves the attention and to be investigated from both technological and societal points of view. The 'human factor' dimension of cyber security is considered to be the 'weakest link' in the whole security process. More research should probably be necessary on the cognitive and psychological behaviours of internet users. Risk-taking behavioural measures of citizens of all ages can contribute to the study and implementation of cyber security strategies to limit online threats and risks.

2.2 Privacy and data protection

How do children see and manage their own privacy online? Do they know their rights about data protection?

The concept of privacy dates back more than a century. The first privacy theorists addressed the definition from a legal or regulatory perspective, referring to the individuals' 'right to privacy' (Warren & Brandeis, 1890). However, more modern social sciences approaches have conceptualised privacy as a dynamic process of social boundary management.

Privacy has been described as a fuzzy concept (Vasalou A., 2014). Designers, policymakers and users have different views in defining privacy as a concept itself and sometimes might be missing nuances that lead to a rich definition.

Burgoon (Burgoon, J. K., 1982). identified four different dimensions of privacy relating to different facets of the self as well as to different forms of social interaction.

1. *Informational privacy* describes the level of control over the amount, content and recipients of information released about the self. This facet of privacy is most closely related to classical definitions of privacy in terms of limited access to (information about) the self.

2. *Social privacy* refers to the aspects of privacy that are related to communication and describes an individual's 'ability to withdraw from social intercourse' (Burgoon J.K., 1982). It thus refers to a person's level of control over social relationships, interactions and encounters.

3. *Psychological privacy* is defined as 'one's ability to control affective and cognitive inputs and outputs' (Burgoon, J. K., 1982). Psychological privacy is high when individuals are protected from unsolicited external psychological influences such as persuasive communication (inputs) and can freely choose the degree to which they will self-disclose their thoughts and feelings (outputs).

4. *Physical privacy* addresses 'the degree to which one is physically inaccessible to others' (Burgoon, J. K., 1982). It thus describes a person's level of control over spatial intrusions, the physical presence of others and the physical accessibility of the self.

The cyber side of individuals' daily life implies certain challenges to manage their own privacy. On the one hand, most net users report being aware about these challenges and sometimes also about being worried about their privacy. On the other hand, they do not so much behave in a way to protect and defend their private life as they are generally willing to disclose information and sometimes sensitive data (Trepte & Reinecke, 2013). This dissonance is now known as the privacy paradox (Barnes, 2006) and it is commonly experienced both by young and adult users.

Why do attitudes and behaviours not seem to match with regard to privacy?

Previous research has shown that gratifications are considered as the major motivation to behave in contrast to one's own attitudes (Taddei & Contena, 2013). Intrinsic gratifications are related to gains in social capital, social support and identity and material gratifications such as content/information retrieval and shopping (Trepte & Reinecke, 2013).

To date, the majority of research on adolescent and children risk-taking behaviours has relied on self-report methods (See EU Kids Online), and more recently on behavioural measures such as computer-based simulation of real-world risk-taking behaviour (Gullone & Moore, 2000) (Morrongiello & Lasenby, 2006). More novel, and to our knowledge unexplored, implicit cognition approaches and IATs could be considered a valuable tool to overcome the limit of previously used assessment tools and, thus, the understanding between privacy intentions and behaviours.

2.3 Digital Competences

Digital competences are essential in the era we are living in. In particular, safe attitudes towards privacy, data protection and responsible, respectful uses of ICT need to be developed by adults and children alike. The Happy Onlife edutainment pack has been designed as a tool to prompt the development of such competences. The underlining theoretical framework refers to the work carried out by the JRC–IPTS, which has recently developed and published a detailed DigComp (Ferrari, Punie, & N., 2013), identifying and describing 21 specific competences that citizens should acquire to participate in our digital society and economy. The 21 competences are structured along five main areas: information, communication, content creation, safety and problem solving (See Figure 1).

The DigComp is a general reference model for all EU Member States with the aim to create a common language on the development of digital competences. It is currently being used by more than 10 Member States for several purposes: digital skills strategies, review of education curricula, teacher digital competence development and employability. At the European level, it is used for the measurement and monitoring of digital skills as part of the digital economy and society index (DESI, 2016) and is incorporated into the Europass CV as a self-assessment module (Europass, 2016).

The DigComp was first published in 2013 and it is now followed by the 2.0 version (Vuorikari, Punie, Carretero, & Van den Brande, 2016), which constitutes the phase 1 of the conceptual reference model update, a revision of the vocabulary and more streamlined descriptors. Citizens of all ages need digital competences to be part of society and to benefit from the opportunities of its digitalisation, in different areas such as employment, education, social inclusion, health and many others. Being digitally literate also means being able to mitigate the possible risks that can be encountered in the digital world.

The domains investigated by the present research have been highlighted in bold in the table summarising the DigComp, and specifically safety and communication areas.

Digital competences

Competence areas	Detailed competences
Information and data processing	• Browsing, searching and filtering information • Evaluating information and data • Storing and retrieving information and data
Communication	• Interacting through digital technologies • Sharing information and content through digital technologies • Engaging in citizenship through digital technologies • Collaborating through digital technologies • **Netiquette** • **Managing digital identity**
Content creation	• Developing content • Integrating and re-elaborating content • Copyright and licenses • Programming
Safety	• **Protecting devices** • **Protecting personal data and privacy** • **Protecting health and well-being** • **Protecting the environment**
Problem solving	• Solving technical problems • Identifying needs and technological responses • Creatively using digital technology • Identifying digital competences gaps

Table 1. The DigComp framework on digital competences

2.4 Social Cognition

Social cognition has been studying social behaviours, attitudes, prejudices and stereotypes by way of explicit measures through questionnaires, scales (Likert, Guttman, Thurstone, etc.), semantic differential and other auto-evaluative tools. Social behaviours are ordinarily considered as being under conscious and thoughtful control (Greenwald A. B., 1995). However, considerable evidence now supports the view that people may not say what is on their mind either because they are unwilling or because they are unable to do so. Social behaviour often operates in an implicit or unconscious fashion.

2.4.1 The implicit social cognition

The development of 'implicit social cognition' and of 'implicit measures' enables the insight into both conscious and unconscious thoughts, which in turn facilitates the measurement of implicit attitudes and beliefs that people are either unwilling or unable to report. The implicit social cognition in children provides techniques for accessing children's attitudes that require no oral response possibly reducing the difficulty with poor comprehension of task requirements and/or immature verbal expression. Indeed, this subject should be more extensively treated and discussed but it will not be tackled at this stage for question of brevity.

The identifying feature of implicit cognition is that past experience influences judgment in a fashion not introspectively known by the actor.

One of the most important contributions in social cognition research within the last decade was the development of techniques to measure implicit attitudes, stereotypes, self-esteem and self-concepts; a number of paradigms have been developed in recent years. Nevertheless, the most reliable procedure to measure implicit attitudes has been the Implicit Association Test (IAT) (Greenwald, McGhee, & Schwartz, 1998).

The IAT provides a measure of strengths of automatic associations. This measure is computed from performance speeds at two classification tasks in which association strengths influence performances. The validity of the IAT derives from its combination of apparent resistance to self-presentation artefacts, its lack of dependence on introspective access to the association strengths being measured, and its ease of adaptation to assess a broad variety of socially significant associations (Greenwald, Nosek, & Banaji, 2003).

2.4.2 Risk-taking behaviours

Together with risk concept, risk-taking behaviour themes count vast analysis and study in different scientific domains and policy debates. Some researchers have argued that risk taking should be studied because of its relevance to three important issues in the field of psychology: the adaptiveness of human behaviour (Byrnes J. , 1998), the rationality of human thought (Baron, 1994) and the relative importance of genes versus the environment in determining the phenotypic expression of traits (Wilson & Daly, 1985) (Zuckerman, Psychobiology of personality, 1991).

Fishoff argues that the decision to undertake these types of activities depends on different dimensions of human development: cognitive, affective and social (Fishoff, 1992).

These are a few examples of existing differences between several approaches about risk taking, which need to be considered in the assessment validity of risk-taking measures. Moreover, risk perception as a powerful predictor of demand for risk mitigation (Sjoberg, 1999) also has to be considered.

2.4.3 Risk taking behaviours by children

And what about children's risk-taking behaviours?

There are several possible variables associated with children's risk-taking behaviours: age, gender, social experiences (Livingstone, Developing social media literacy: how children learn to interpret

risky opportunities on social network sites, 2014), parenting and schooling influences (Livingstone, Haddon, Görzig, & Ólafsson, 2011)temperament, sensation seeking and optimistic bias.

The extended literature about children's risk-taking behaviours is dominated by an injury-prevention approach of risk taking. In particular, there has been minimal recognition of the role of risk-taking behaviours as a contributory factor in children's development (Little, 2006) (Mascheroni & Haddon, Children, risks and the mobile internet, 2015).

2.4.4 Attitudes and implicit attitudes

Regarding attitudes, several studies (Bargh, Chaiken, & Pratto, 1992) (Fazio, Sanbonmatus, Powell, & Kardes, 1986) have established that attitudes are activated outside of conscious attention, by showing that activation occurs more rapidly than it can be mediated by conscious activity as well as that activation is initiated by (subliminal) stimuli, the presence of which is unreportable. Greenwald and Banaji extended the work on automatic activation to explain how the attitude activated by one object can be (mis)attributed to another (Greenwald & Banaji, 1995). They defined attitudes as 'favourable or unfavourable dispositions toward social objects, such as people, places and policies' (p. 7). Many researches have established that attitudes have predictive validity in situations in which they are strongly activated and/or when the actor clearly perceives a link between attitude and behaviour (Ajzen & Fishbein, 1980) (Fazio R. , 1986) (Fazio & Zanna, 1981) (Fishbein & Ajzen, 1974) (Zanna & Fazio, 1982). In this sense, Greenwald and Banaji tried to demonstrate that 'attitudes of which the actor is not conscious at the moment of action (implicit attitudes) are also strongly predictive of behaviours (Greenwald & Banaji, 1995). To do this, they firstly addressed the lack of mention of consciousness in most conceptual definitions of attitude, which have been influential in guiding scholarly and empirical treatments of attitudes. This lack reflects a long scholarly tradition of having no concern with the distinction between the conscious and the unconscious operation of attitudes but, at the same time, nothing in this scholarly tradition actively opposes either the possibility or the importance of the unconscious operation of attitudes. Some of these definitions that they mentioned are the following.

'Attitude is the affect ([2]) for or against a psychological object.' (Thurnstone, 1931, p. 261).

'An attitude is a mental and neural state of readiness, organised through experience, exerting a directive or dynamic influence upon the individual's response to all objects and situations with which it is related.' (Allport, 1935, p. 810).

'Attitude is an implicit, drive-producing response considered socially significant in the individual's society.' (Doob, 1947, p. 136).

'[Attitudes] are predispositions to respond, but are distinguished from other such states of readiness in that they predispose toward an evaluative response.' (Osgood, Suci, & Tannenbaum, 1957).

'[An attitude is] a disposition to react favourably or unfavourably to a class of objects' (Sarnoff, 1960, p. 261).

The authors showed how Doob's definition is the only one that could suggest an unconscious operation, labelling 'attitude' as an 'implicit, drive-producing response'. However, in spite of Doob's association with a behaviourist theory (Hull, 1943) that had no use for conceptions of either

([2]) Affect is the emotion or desire as influencing behaviour.

conscious or unconscious cognition, Doob did conceive 'attitude' as operating unconsciously (May & Doob, 1937, p. 13).

Evidence concerning the strength of attitude–behaviour relations has generally been regarded as the primary evidence bearing on predictive validity of the attitude construct. To justify the concept of implicit attitude, Greenwald and Banaji described a series of empirical findings that demonstrated that some strong effects of attitude can and do occur when the actor is not attentionally focused on the attitude and as a consequence merits an 'implicit designation' (Greenwald & Banaji, 1995).

The first effect that can be addressed as an 'implicit attitude effect' is the 'halo effect'. Thorndike named the halo effect after noticing that personality ratings showed a tendency for positive characteristics to be associated with other positive characteristics more than they should be if experience is the only guide (Thorndike, 1920). Subsequently, the halo effect came to be regarded as the tendency for judgment of a novel attribute (A) of a person to be influenced by the value of an already known, but objectively irrelevant, attribute (B). In this case, the explicit measure of evaluation of A implicitly expresses the attitude toward B. The attitude toward B is implicit, in present terms, when the subject does not identify the attitude toward B as the source of the evaluation of A. In much halo effect research, physical attractiveness plays the role of the objectively irrelevant attribute that influences evaluative judgement on various other dimensions (Dion, Berscheid, & Walster, 1972) (Downs & Lyons, 1991) (Landy & Sigall, 1974).

The physical attractiveness-based halo effect has been replicated in subject populations of Black Americans (Cash & Duncan, 1984) and Japanese (Onodera & Miura, 1990), as well as across the life span (Adams & Crane, 1980) (Eagly, Ashmore, Makhijani, & Longo, 1991). As a general interpretation of halo effects, it can be supposed that the subject's learning that an unfamiliar target person possesses attribute B tends to produce a diffuse positive or negative attitude (depending on the affective value of B) toward the target person; that attitude is then likely to generalise to any specific attribute (A) that the subject is asked to judge. Greenwald and Banaji (1995) affirmed how 'the attitude toward B is said to operate implicitly when the subject does not notice that B is influencing the judgment of A'.

3 Method

This research is part of a larger project to raise awareness of online risks and opportunities for children and adults, which has encouraged the development of the Happy Onlife edutainment toolkit ([3]). The Happy Onlife resources were firstly developed and validated following a qualitative approach based on observations, focus groups and self-report measures by children, teachers and parents. With this work we would like both to consider quantitative assessment measures and to study children's attitudes and behaviours towards cyber security threats and risks.

To our knowledge, the present research is the first study investigating implicit cyber risk attitudes in secondary school children. To date, the majority of research on children's risk-taking behaviours has relied on other or self-report methods, and more recently on behavioural measures such as computer-based simulation of real-world risk-taking behaviours (Gullone & Moore, 2000) (Morrongiello & Lasenby, 2006)

3.1 Objectives

The main purpose of the present research is to investigate the change in 10-12 years old children's attitudes towards cyber risk related to privacy, data protection and security. Particularly, we tested the effect of the Happy Onlife tool on attitudes towards cyber risk of users from T1 to T2, before and after using Happy Onlife edutainment.

The objectives are as follows:

1. testing the validity of Happy Onlife resources as a learning tool for digital competences with a focus on cyber security, data protection, privacy, cyberbullying, netiquette and digital identity management;

2. contributing to the development and validation of a new implicit measure about cyber risk propensity for children (10-12 years old);

3. investigating the relationship between implicit risk attitudes and explicit risk-taking behaviour.

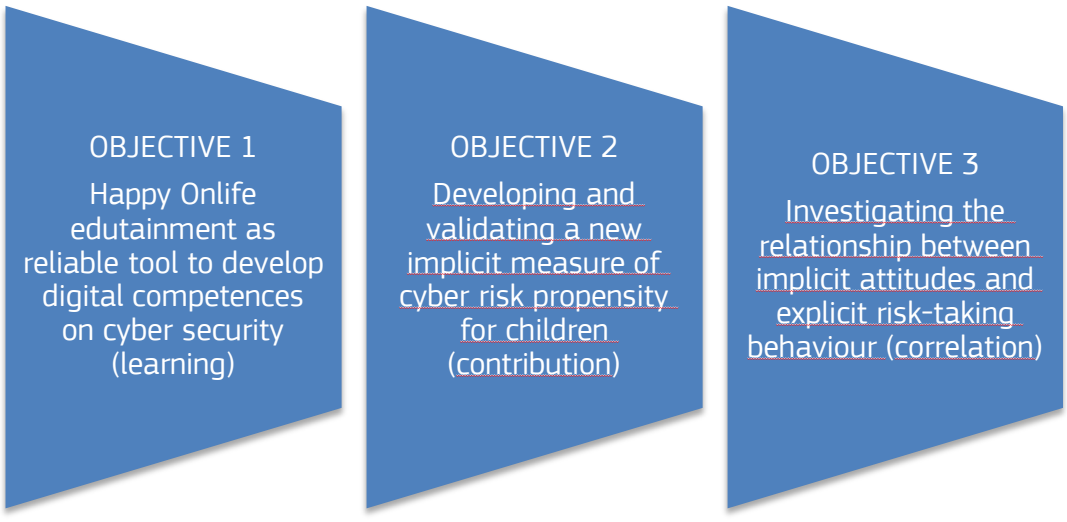


Figure 1. Objectives of the research

([3]) Edutainment is a neologism to express the process of entertainment and education at the same time.

3.2 Hypotheses

The hypotheses are as follows:

1. the Happy Onlife edutainment learning experience will produce an increase of knowledge on cyber security and scoring will be higher from Time 1 (T1) and Time 2 (T2);

2. the cyber security IAT will show good reliability (Cronbach's alpha and split-half method) and good convergent validity, demonstrated by positive correlations with the explicit cyber security measures;

3. high score of implicit risk propensity will predict high score of explicit risk attitude;

4. males will have higher implicit risk propensity than females (Byrnes J. M., 1999).

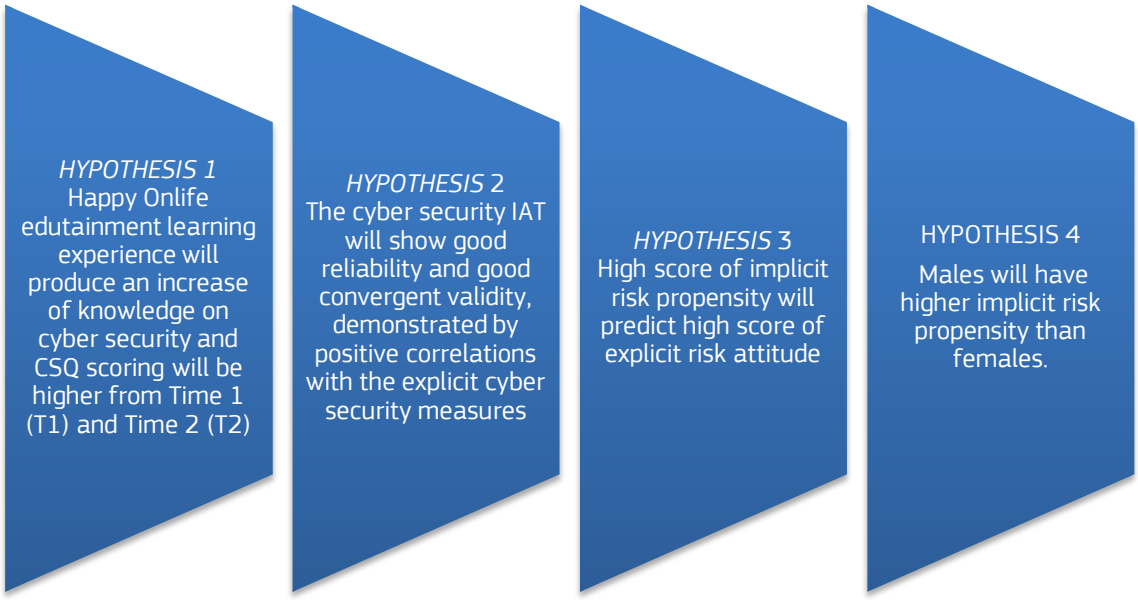


Figure 2. Research Hypotheses

3.3 Participants

The data presented in this report were collected in a four-waves testing over the course of 2 months, in October and November 2016. Four events were arranged during this period, chronologically on 24 October 2016 (day 1), 11 November 2016 (day 2), 22 November 2016 (day 3), and the last one on 25 November 2016 (day 4). Participants were recruited via previous contacts with the school interested in awareness-raising activities about online risks and coding activities. The secondary school is based in the northern part of Italy and more specifically in Varese. Students were attending the first class of the secondary cycle of the compulsory national education system.

A total of 106 participants took part in the research:

24 students were present during day 1 and 23 completed the test;

27 students were present during day 2 and 25 students completed the test;

28 students were present during day 3 and 26 students completed the test;

27 students were present during day 4 and 13 students completed the test.

Only participants whose complete data could be registered from the pre-activity and post-activity were included in the analysis (N = 87).

Final participants were 87 children, 48 males and 39 females, aged 10-12, (males: mean age = 10.88, S.D. = .334; females: mean age = 10.97, S.D. = .362).

To ensure participants' anonymity, no personally identifiable information was saved with participants' responses. A detailed letter with full research purposes and methods was drafted and addressed to the school headmaster. According to the European Data Protection Regulation (EC) No 45/2001, parental informed consent (See Annex 2) was sent to pupils' parents and signed consents were collected and obtained by school hierarchy for all participants in the research. The school headmaster provided the researchers with a letter confirming the collection of signed parental informed consent forms for the four arranged data collections (See Annex 4). JRC processing of personal data collected in the Happy Onlife IAT study, namely the school headmaster's contact data, consists in contact list management and is compliant with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The full text of the specific privacy statement for the empowering citizens' rights in emerging information and communications technology (E-CIT) project contact lists is detailed in Annex 3.

To match participants' data over the course of all measuring points of the study, research instruments were saved on dedicated USB keys for each student involved in the research. Each USB key was labelled with a number.

Figure 3. USB keys with labels and numbers

3.4 Measures

In this section, the main research tools are extensively described and chronologically analysed. Different types of measures were collected: explicit and implicit measures. Explicit measures, developed and administered to collect self-report measures., are: the Cyber security Questionnaire (CSQ), a 29 item self-report questionnaire, with a 4 points Likert scale focused on cyber risk assessment and the Brief Sensation Seeking Scale (BSSS). For the implicit measures an Implicit Association Test (IAT) (Greenwald, McGhee, & Schwartz, 1998) has been developed and administered.

In brief, they can be summarised as follows:

1. pre-activity 'CSQ' questionnaire;
2. pre-activity 'Cyber security IAT';
3. Happy Onlife serious-gaming activity;
4. Post-activity 'CSQ' questionnaire with BSSS;

5. post-activity ‘Cyber security IAT’;

Figure 4. Summary of the research procedure

3.4.1 Pre-activity questionnaire

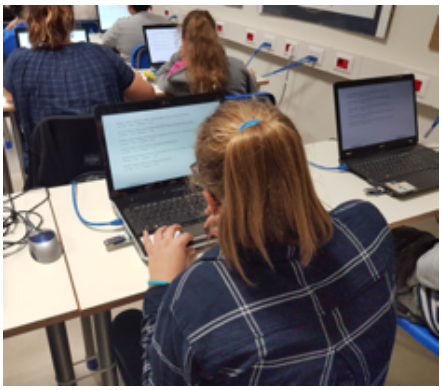


Figure 5. Pre-activity 'CSQ' questionnaire filled in by a student

The pre-activity questionnaire was developed to investigate the presence of pre-existing digital competences and an awareness on risks related to privacy, data protection, security/safety, cyberbullying, netiquette and digital identity management. Initial questions were dedicated to statistics, demographic data, preferred devices and online activities: the following ones were built according to the topics treated in the Happy Onlife edutainment game and categorised in four areas:

1. ‘Let’s chat!’ area;
2. ‘Stop online bullying!’ area;
3. ‘Play safely!’ area;
4. ‘Watch out!’ area.

As the empirical work was carried out in an Italian school, the submitted questionnaire was in Italian (see Annex 4 for the Italian version). For consistency with the rest of the text, the English version of questions is herewith proposed.

3.4.1.1 CSQ Questionnaire

General Data

1. How old are you?

□8 □9 □10 □11 □12

2. You are a

□ Boy □ Girl

3. Which are your preferred online activities?

□ Play and game □ Communication (E-mail, Skype, WhatsApp, …)

□ Social Network (FB, Instagram, …) □ Information (Searching, Reading, Youtube, …)

4. What are the devices you use to go online?

□ Smartphone □ Tablet □ PC □ Smart TV

5. How many hours a day do you normally spend online?

□ 1 □ 2 □ 3 □ 4 □ 5

6. How old were you when you started using internet?

□I do not know □3 □4 □5 □6 □7 □8 □9 □10 □11 □12

The 'Let's chat!' area leads to questions and tips for safety and security issues.

7. In your opinion, how much do you think people risk when they publish their own data online?
8. In your opinion, how much do you think people risk when they publish their own pictures online?
9. In your opinion, how much do you think people risk when they publish other persons' data online?
10. In your opinion, how much do you think people risk when they publish pictures of other persons online?
11. In your opinion, how much do you think people risk when they copy and paste information?

The 'Stop online bullying!' area regards questions and tips on how to protect ourselves and others from risky behaviours, such as (cyber) bullying and stalking and how to prevent them.

12. In your opinion, how risky is it to annoy/provoke someone online?
13. In your opinion, how risky is it to hurt someone online?
14. In your opinion, how risky is it to be a witness of online bullying?
15. In your opinion, how risky is it to be accused of online bullying?
16. In your opinion, how risky is it not to report unpleasant messages received online?
17. In your opinion, how risky is it to pretend to be someone else online (false identity)?

In this specific area a multiple-choice question on cyberbullying was addressed.

18. Do you know what cyberbullying is? Please indicate the most appropriate sentence.

Options:

- I do not know
- A new app that allows you to develop animations on a virtual reality environment
- Intentional, planned and repetitive behaviours aiming at damaging either physically or emotionally one or more persons that might be in a vulnerable position and/or fragility
- Two boys/girls fighting and sometimes boxing
- It is an offence/crime that only the cyber police can punish.

The 'Play safely!' area is about questions and tips on safe and healthy gaming practice and content creation.

19. In your opinion, how risky is it to use your real name when video gaming online?
20. In your opinion, how risky is it to use your real name and family name when video gaming online?
21. In your opinion, how risky is it to use geo-localisation when video gaming online?
22. In your opinion, how risky is it to download music and films for free?
23. In your opinion, how risky is it to use video gaming for several hours without any break?

The 'Watch out!' area concerns questions and tips on the secure and safe search of information and the safe and respectful communication and online collaboration.

24. In your opinion, how risky is it to organise a date with someone that you have only met online?
25. In your opinion, how risky is it to open pop-up and add-on messages?
26. In your opinion, how risky is it to not check the privacy settings of online applications?
27. In your opinion, how risky is it to not install an anti-virus for our own devices?
28. In your opinion, how risky is it to register on a social network (Facebook, WhatsApp) before the age suggested by the national legislation?
29. In your opinion, how risky is it to tell our own password to someone else?

A four-level Likert item scale was used to answer the questionnaire. The format used is described as follows.

 Not at all Too little About right Too Much

3.4.2 Pre-implicit association test

Figure 6. Pre-Cyber security IAT test carried out by a student

Figure 7. General view of pre-Cyber security IAT session

To verify the research hypothesis, the IAT has been used. The test was named the *'Cyber security Implicit Association Test'*. In its abbreviation the *'Cyber security IAT'*.

In general, an IAT can measure the strength of associations between concepts (e.g., black people, gay people, old people, etc.) and evaluations (e.g., good, bad) or stereotypes (e.g., athletic, clumsy). The main idea is that making a response is easier when closely related items share the same response key.

When instructions oblige highly associated categories (e.g., chocolate + pleasant) to share a response key (e.g. key/button *'e'* of your keyboard), performance is faster than when less associated categories (e.g., lemon + pleasant) share a key/button. This performance difference implicitly measures differential association of the 2 concepts with the attribute.

When doing an IAT you are asked to quickly sort words into semantic categories that are on the left and right hand side of the computer screen by pressing a designated button of the keyboard. The IAT has five main parts.

In the first session/block of the IAT you sort words relating to the concepts (e.g., old people, young people) into categories. So if the category '*Old People'* was on the left, and a picture of an old person appeared on the screen, you would press the correspondent button of the keyboard.

In the second session/block of the IAT you sort words relating to the evaluation (e.g., good, bad), pressing the correspondent key either to the left or right side of the screen.

In the third session/block of the IAT the categories are combined and you are asked to sort both concept and evaluation words. So the categories on the left hand side would be *'Old People/Good'* and the categories on the right hand side would be '*Young People/Bad'*. It is important to note that the order in which the blocks are presented varies across participants, so some people will do the

'Old People/Good', 'Young People/Bad' part first and other people will do the *'Old People/Bad', 'Young People/Good'* part first.

In the fourth session/block of the IAT the placement of the concepts switches. If the category *'Old People'* was previously on the left, now it would be on the right. Importantly, the number of trials in this part of the IAT is increased in order to minimize the effects of practice.

In the final session/block of the IAT the categories are combined in a way that is opposite what they were before. If the category on the left was previously *'Old People/Good'*, it would now be *'Old People/Bad'*.

The IAT score is based on how long it takes a person, on average, to sort the words in the third part of the IAT versus the fifth part of the IAT. We would say that one has an implicit preference for young people relative to old people if they are faster to categorise words when *'Young People'* and *'Good'* share a response key and *'Old People'* and *'Bad'* share a response key, relative to the reverse. (Harward University, 2016)

In the '*Cyber security IAT'* presented in this research the target bipolar concepts were:

'SAFE navigation' versus *'UNSAFE navigation'* (*SICURO/NON SICURO*).

The evaluations are made using: *'SMILING emoticons'* versus *'SAD emoticons'* ('adjectives' evaluation – target). The *'SMILING emoticons'* replaced *'Good/pleasant'* and the *'SAD emoticons'* the adjective *'Bad/unpleasant'*. There were five sessions/blocks[4] where the subjects were asked to perform a semantic classifications of the displayed stimuli after receiving instructions to respond as quickly as possible. In the first block we presented terms indicating either elements or procedures increasing *'SAFE navigation'* and terms indicating either elements or procedures increasing *'UNSAFE navigation'*.

Safe navigation:	**Unsafe navigation:**
Privacy	HACKER
Password	CYBERBULLYING
Antivirus	VIRUS
Nickname	PUBLISH PERSONAL DATA
Protection	ILLEGAL WEB SITES
Security	CONTINUOUSLY CONNECTED

Table 2. IAT Stimuli

The choice of stimuli to be used in the IAT blocks has been conceived with reference to the four macro areas, which have been designed to raise awareness about online risks and digital skills enhancement in the Happy Onlife edutainment game: 'Let's chat!'; 'Watch out!';'Stop online bullying!';'Play safely!'.

[4] The word block is here used to refer to a set of stimuli presented in the IAT session.

	Safe navigation:	Unsafe navigation:
'Let's chat!'	Think before posting/Web reputation Netiquette (respectful social behaviour)	Pictures, data, video, sharing Hate speech, cyber-bulling, stalking
'Watch out!'	Protecting devices (passwords, anti-virus/malware, …) Protecting personal data and privacy (nickname, privacy settings, …)	Indicating your name, address and telephone can be unsafe/Cookies, profiling, geo-localisation Meeting someone offline whom you have only met online can be dangerous
'Stop online bullying!'	Managing digital identity Netiquette (respectful social behaviour)	Insulting, stalking, self-disclosure, sexting, etc.
'Play safely!'	Regulate timing Adapt age/game choice	Addiction, gambling Violent content

Table 3. Detailed concepts underling safe/unsafe navigation in the 4 HOL areas

3.4.2.1 Cyber security IAT procedure

A first 'learning' session was proposed to participants with the following block.

Children were introduced to the IAT test as a 'computer game' in which they would see 'words' displayed on the computer screen and have to sort them in two categories on the left- and right-hand side of the screen. The sorting had to be done by pressing buttons in response to each prompting. To attribute words to the 'Non Sicuro' (Unsafe) block they had to press the 'C' button and to attribute words to the 'Sicuro' (Safe) block they had to press the 'N' button. Proposed stimuli were words listed in Table 2. Five 'safe' stimuli and five 'unsafe' stimuli were presented.

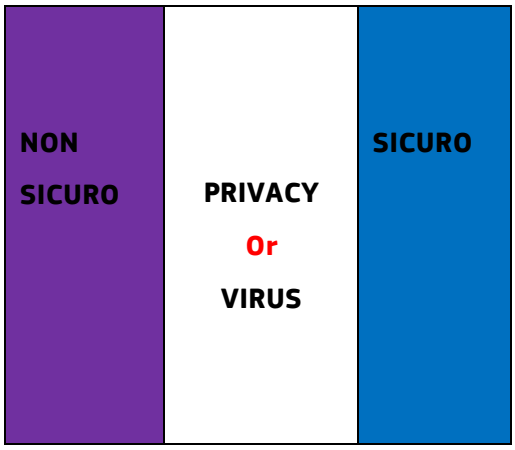


Figure 8. Block with stimulus of first IAT session

A second 'learning' session was proposed to participants with the following block.

Children had 'happy and sad emoticons' displayed and had to press a button in response to each prompting. To attribute an emoticon to the *'Sad emoticon'* block they had to press the *'C'* button and to attribute 'emoticon' to the *'Smiling emoticon'* block, they had to press button *'N'*. Proposed stimuli proposed were both *'Smiling and Sad emoticons'*.

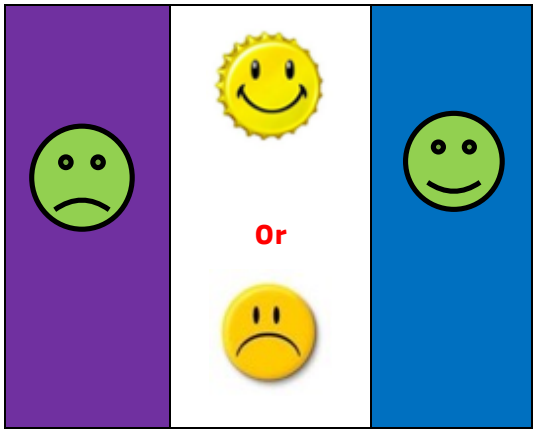


Figure 9. Block with stimulus of second IAT session

For the third IAT session, stimuli categories were combined and children were asked to sort both concept and evaluation words. A *'Sad emoticon'* was associated to *'Unsafe'* block and *'Smiling emoticon'* to *'Safe block'*. Children were asked to follow the choice instructions.

In this case stimuli proposed were words listed in table 2. Five *'Safe stimuli'* and five *'Unsafe stimuli'* in addition to *'Smiling and Sad emoticons'*. By pressing *'C'* they had to attribute *'emoticon/word'* to the *'Sad emoticon'* left block + *'Unsafe'*. By pressing button *'N'* they had to attribute *'emoticon/word'* to the *'Smiling emoticon'* + *'Safe'* right block.

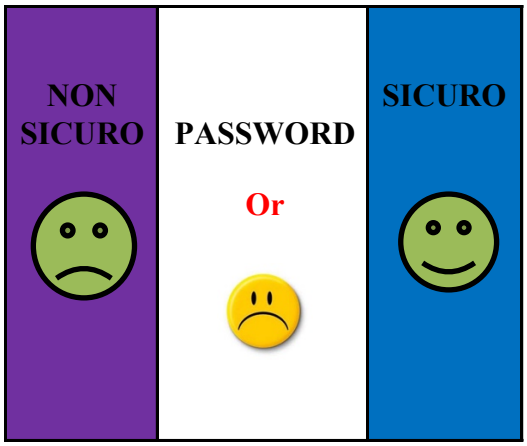


Figure 10. Block with stimulus of third IAT session

Also in this forth session, the instructions were in accordance with the previous ones and stimuli proposed were words listed in Table 2. Five *'Safe stimuli'* and five *'Unsafe stimuli'*. The placement of the concepts was switched from left to right on the computer screen. The number of trials/prompts in this session was increased in order to minimise the effects of practice.

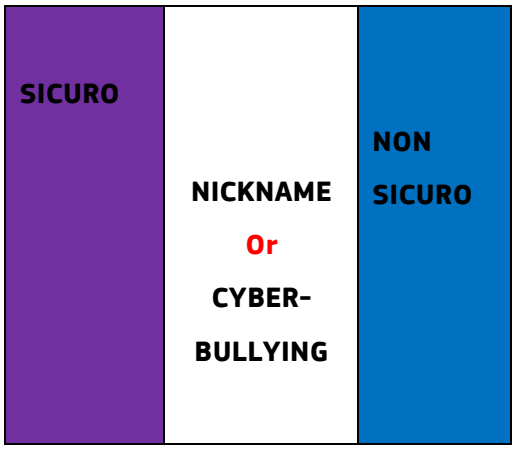


Figure 11. Block with stimulus of fourth IAT session

At this stage, *'Safe'* was paired with *'Sad emoticon'* and *'Unsafe'* was paired with *'Smiling emoticon'*. Categories were combined in such a way as to be switched with regards to how they were before. In this case stimuli proposed were words listed in Table 2. Five *'Safe stimuli'* and five *'Unsafe stimuli'* in addition to *'Smiling and Sad emoticons'*.

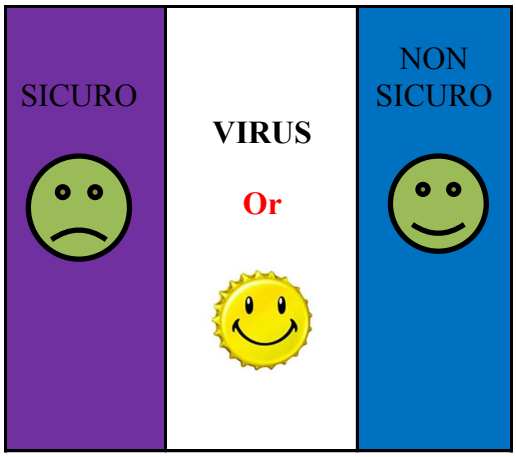


Figure 12. Block with stimulus of fifth IAT session

The IAT score was based on how long it takes a person, on average, to sort the words in the third part of the IAT versus the fifth part of the IAT.

The following table summarizes the *'Cyber security IAT'* procedure with blocks and stimuli proposed in the five sessions of the experiment:

Block Number

	1	2	3	4	5
Aim	**Learning**	**Learning**	**Measuring**	**Learning**	**Measuring**
Stimuli	Words	Emoticons	Words/ Emoticons	Words	Words/ Emoticons
Press right key 'C' for	Safe	Sad	Unsafe/ Sad	Safe	Safe/ Sad
Press left 'N' key for	Unsafe	Smiling	Safe/ Smiling	Unsafe	Unsafe/ Smiling

Table 4. Summary of 'Cyber security IAT' procedure with blocks and stimuli

After the first session a dedicated page with a 'Stop' instruction was introduced. The English translation is: 'Well done! You have completed the first part of the survey. Now wait for our instructions'.

Figure 13. Stop sign

Figure 14. Student ending the first session

3.4.3 Happy Onlife serious-gaming activity

Figure 15. Happy Onlife digital game — Screenshot

Figure 16. Happy Onlife gaming session — General view

The Happy Onlife edutainment game has been developed to empower teachers and parents in actively guiding children to become smarter, responsible and respectful when using media and to help them understand the ethical consequences behind the decisions they make online.

The enhancement of digital skills development, together with the change in attitudes, is supported by the serious-gaming activity. In Annex 5 the Happy Onlife leaflet describes in detail the resources proposed.

For this specific survey the digital version of the Happy Onlife game was used and run on a wall display.

During each test sitting, the class (counting an average of 26/27 students) was split in two teams and a spokesperson was appointed among students of each team.

The gaming session lasted from a minimum 40 min till a maximum 1 hour during the third session arranged on 22 November 2016.

Students played and enjoyed the gaming activity. Moreover, they had the opportunity to open the discussion among peers, teachers and researchers on treated themes (cyber security, privacy, data protection, gaming, cyberbullying, netiquette, safe communication, etc.).

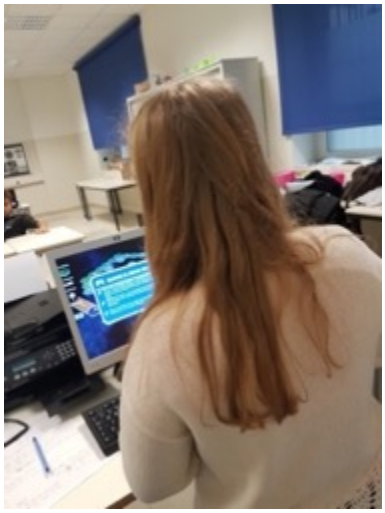


Figure 17. Child reading a 'Power card' during HOL session

An itinerary appears on the screen and rules are very close to the Snake and Ladder game (in Italy *'Gioco dell'oca'*) with quiz questions on the squares marked with symbol of *'Challenge cards': 'Let's chat!', 'Stop online Bullying', 'Watch out!'* and *'Play safely!'*

Figure 18. Example of HOL question

To better understand the game dynamics, herewith some quiz questions are proposed:

Figure 19. Happy Onlife quiz game cards

The playful aim of the game is to be the first to arrive at the *'Finish'* square, whereas the educational aim of the game is to enhance digital competences on cyber security, data protection, privacy, etc. and to foster mediation and intergenerational dialogue if played among children and adults.

3.4.4 Post-activity questionnaire & Children's brief sensation-seeking scale

The post-activity questionnaire '*CSQ'* included questions presented in the pre-activity questionnaire plus nineteen (19) items where children were asked to respond with *'True'* (*'Vero'*) or *'False'* (*'Falso'*).

The sensation-seeking scale is one of the most common psychological instruments for measuring sensation-seeking behaviours/attitudes. An important aspect of any investigation of children's risk-taking behaviour is an examination of the behavioural and psychological factors that underlie children's decision-making in risky situations. Sensation seeking is one such personality trait that has been related to the propensity in risk-taking behaviours.

Marvin Zuckerman and his colleagues have identified four factors that are involved in sensation seeking (Zuckerman, Kolin, Price, & Zoob, 1964):

1. thrill and adventure seeking: the desire to engage in sports or activities involving speed and danger;
2. disinhibition: the desire for social and sexual disinhibition;
3. experience seeking: the desire for experience through the mind and senses, travel and a non-conforming lifestyle;
4. boredom susceptibility: aversion to repetition, routine and dull people.

For the present research a BSSS (Holey, Palmgreen, Pugzels Lorch, & Donohew, 2002) (Morrongiello & Lasenby, 2006)for children has been adopted with a reduced number of questions, and still carries reasonable reliability and validity.

The English translation of the Italian version of the questionnaire is herewith reported.

1. I like to do new and exciting experiences even if they are a bit scary.
2. I like to do things just for the thrill.
3. Sometimes I do crazy things just to have fun.
4. Sometimes I like to do things that are a bit scary.
5. I have fun when I am involved in new situations that you do not know how they will end.
6. I think any experience should be tested at least once.
7. I prefer friends who are excitingly unpredictable.
8. I like 'wild' uninhibited parties.
9. I would like a lifestyle with a lot of travelling, opportunities and fun.
10. I am an impulsive person.
11. I like to explore a foreign city or suburb by myself, even it means getting lost.
12. I would like to set off on a trip with no pre-planned or definite routes or timetable.
13. Before beginning a difficult job, I make careful planning.
14. I often spend a lot of time on details and on planning things.
15. I tend to begin a new job without planning too far ahead what I will have to do.
16. I often think of what I am about to do before doing so.
17. I often do things impulsively.
18. Often I am so caught up with new things and exciting ideas that I never think about the possible complications.
19. I tend to change many interests.

3.4.5 Post-implicit association test

A post-IAT on cyber security was conducted following the same pattern as the pre-IAT.

The post-IAT was meant to observe effectiveness of the Happy Onlife edutainment game in promoting cyber security digital competences.

4 Results

In this section we present the research results as follows:

1. Reliability of measures;
2. Descriptive statistics and gender differences;
3. Explicit and implicit measures.

4.1 Reliability of measures

Reliability of *'Cyber security IAT'* was estimated, as suggested by Greenwald et al.(2003) (Greenwald, Nosek, & Banaji, Understanding and Using the Implicit Association Test: I. An Improved Scoring Algorithm, 2003), through a Spearman-Brown corrected correlation between the test halves, while reliability for self-report measures of Cronbach's alphas (Cronbach L. , 1951) were computed (cfr. Table 5).

Reliability of measures

Measures	**A**	**No. of items**
IAT	**0.94**	**60 trials**
Brief Sensation-seeking total score	**0.68**	**19**
CSQ Questionnaire		
Cyber security total score	**0.94**	**22**
Let's chat!	*0.74*	*5*
Stop online bullying!	*0.89*	*5*
Play safely!	*0.80*	*9*
Watch out!	*0.86*	*6*

Table 5. Reliability of measures

In this research IAT showed excellent reliability measure (α = .94 for 60 trials). The Implicit Association Test has been run through the Inquisit software[5] that includes dedicated features to the detection of answers to the IAT either given in a very short reaction times or long reaction time. The first might be the fruit of hazard replies and the second might be the result of conscious thoughts, which can be influenced by judgment, stereotypes and prejudices. Therefore, those results are not considered as meaningful for the assessment of unconscious implicit attitudes and beliefs. The cyber security IAT shows good reliability and good convergent validity, demonstrated by a positive correlation with the sensation-seeking scale (Pearson's r = -0,40, p < .05).

We used also a Brief Sensation Seeking Scale (BSSS) that showed questionable reliability (0.68). This questionable result can be explained by the limited number of items (19 items against 40

[5] http://www.millisecond.com/download/

items of the original Sensation Seeking Scale). We choose this adaptation from 40 to 19 items given the age of the participants to the study.

All others explicit measures showed adequate reliability, with alpha ranging from .74 to .94. Those results are considered acceptable to excellent.

Box 1. Comments on Reliability of measures.

Spearman brown prophecy formula is used to measure split half reliability. One way to test the reliability of a test is to repeat the test. This is not always possible. Another approach, which is applicable to questionnaires is to divide the test into two halves and compare the results. In split half method, two scores are obtained for each person by dividing the test into equivalent halves.

Cronbach's α (alpha) (Cronbach L. J., 1947) is a measure used to estimate the reliability of a psychometric test. It has been proposed that α (alpha) is a coefficient of reliability/internal consistency and it can be viewed as the expected correlation of two tests that measure the same construct. By using this definition, it is implicitly assumed that the average correlation of a set of items is an accurate estimation of the average correlation of all items that pertain to a certain construct.

Cronbach's alpha	**Internal consistency**
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

4.2 Descriptive statistics and gender differences

Participants were asked which were their preferred online activities among Playing, Social Network, Communication (E-mail, Skype, WhatsApp) or Information (Searching, Reading, YouTube). Following this question. Only one option was possible.

3. Which are your preferred online activities?

- *Play and game*
- *Communication (E-mail, Skype, WhatsApp, …)*
- *Social Network (FB, Instagram, …)*
- *Information (Searching, Reading, Youtube, …)*

Figure 20 and 21 show the distribution of this variable in the entire sample and by gender. Most of participants reported that their preferred online activity was playing games (46%), followed by searching for information (32%). Interestingly none of them declared to prefer to go online for communication (E-mail, Skype, WhatsApp).

Despite of a slight difference between males and female results, chi square test showed no differences between gender ($x^2_{(1)}$ = 3.590, p = 0.309).

Box 2. Comments on Chi-squared test results.

A chi-squared test, also written as x2 test, is used to determine if there is a significant relationship between two nominal (categorical) variables (e.g. males/females).

The chi-square test of independence was used to examine the relationship between gender (male vs. female) and preferred online activities (high vs. low).

Hypothesis

Null hypothesis: Assumes that there is no association between the two variables.

Alternative hypothesis: Assumes that there is an association between the two variables.

Null hypothesis was accepted in this case as the Chi-squared test showed no relationship between gender and preferred online activities.

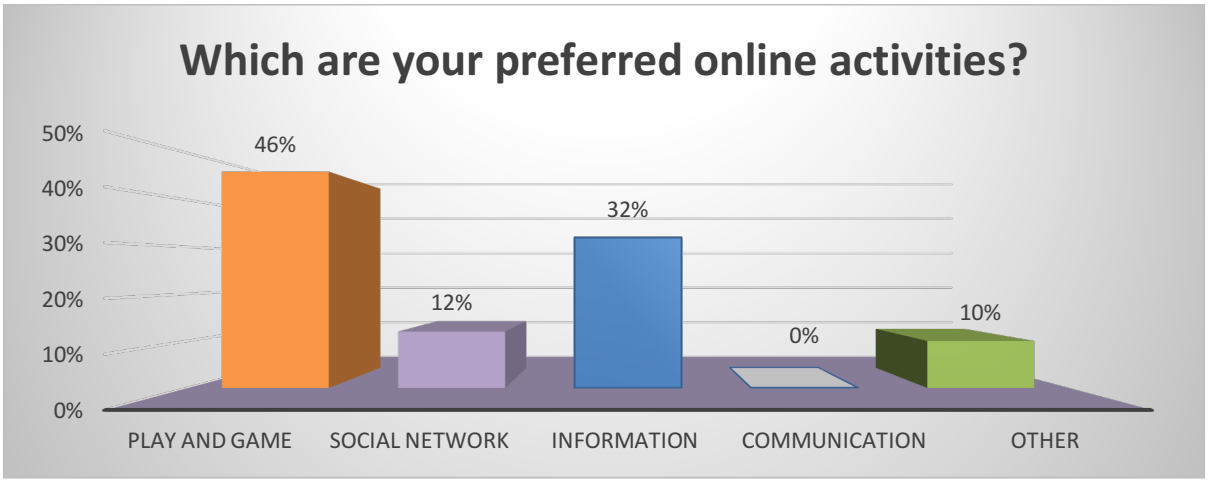


Figure 20. Preferred online activities

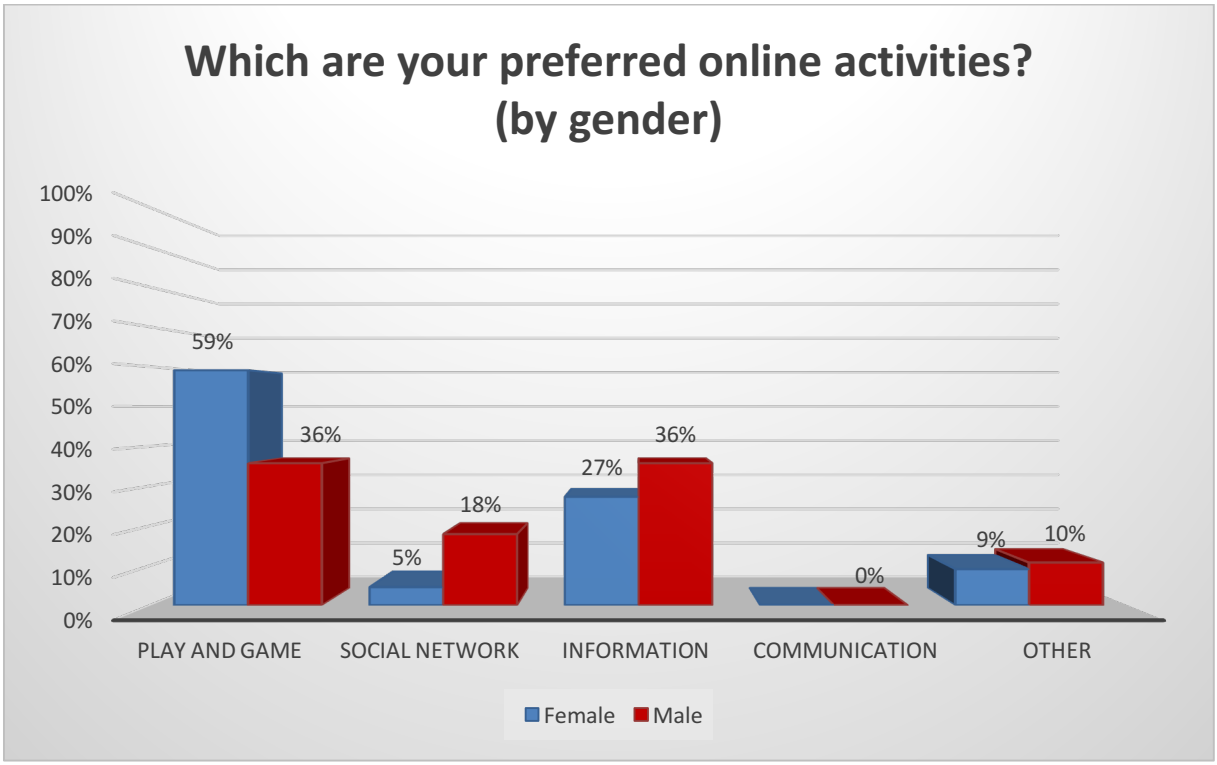


Figure 21.Preferred online activities by gender

By way of the *'CSQ'* questionnaire we also asked how many hours a day participants usually spend online. Males reported that in average they spend more than 2 hours a day online (mean=2.31), while females reported that they spend in average less than 2 hours (mean=1.56). 10 and 11 years old children involved in the research reported that they spend less than 2 hours.

The age sample of this pilot research presented was heterogeneous. Its main part was composed by children of 11 years old, plus 9 children aged 10 years old and only 2 aged 12 years old.

We are aware of the limit that there are only 2 subjects aged 12 old, however we have reported them for completeness reasons and because of interesting differences related to the number of hours reported by children (8 hours/day by 12 years old against +/- 2 hours/by 10-11 years old),

although not to be taken as significant. Nonetheless, other researches report an increase of the time children spent online when they enter in teenager age (12-13) (Mascheroni & Ólafsson, 2013).

Number of hours per day online - Mean, Standard deviation, F and p values

	N	Mean	SD	F	Sig.	Partial Eta Squared
Gender						
Male	*39*	***2.31***	*1.89*	*0.61*	*0.437*	*0.007*
Female	*48*	***1.56***	*1.27*			

Table 6. Number of hours online - Mean, Standard deviation, F and p values

We also asked at what age children of the sample started using internet. The most part of participants reported that they started to use internet at 6 (Mean=6.11). This result raises further research questions as the age of six is the age that most European member states require children to be enrolled at school. At the same time children engage in new practices and Information and Communication Technology (ICT) uses also either accordingly to digital skill development school programs or ownership of devices. ANOVA for gender showed no significant effect of gender on the reported starting age for using internet (cfr. Table 7).

Starting age using internet - Mean, Standard deviation, F and p values for the effect of gender

	N	Mean	SD	F	Sig.	Partial Eta Squared
Gender						
Mean 6,11						
Male	39	**5.82**	3.41	0.001	0.982	0.000
Female	48	**6.35**	3.64			

Table 7. Starting age using internet - Mean, Standard deviation, F and p values for the effect of gender

4.2.1 Cyber security: explicit and implicit measures

To evaluate gender and group age differences, a 2 X 2 (gender X age) and a MANOVA was conducted on all dependent variables. Results showed no main effect of gender (Wilks' Lambda = .946, $F_{(2;85)}$ = 0.469, p = .891), no main effect of age (Wilks' Lambda = .813, $F_{(3;84)}$ = 1.867, p = 071) and no interaction effect (Wilks' Lambda = .935, $F_{(5;74)}$ = .566, p = .820). Table 8 and 9 report, for gender and age groups, the descriptive statistics, univariate F, p value and partial eta squared for all

measures. For gender and age groups, Tables 6 and 7 report the descriptive statistics, univariate F, p value and partial eta squared for all measures.

Mean, standard deviation, F and p values for the effect of gender

	Mean		**Std. deviation**		**Std. error mean**		**$F_{(2;85)}$**	**Sig.**	**Partial Eta Squared**
	F	***M***	***F***	***M***	***F***	***M***			
LetsChat_pre	*2.31*	*2.33*	*0.62*	*0.50*	*0.10*	*0.07*	*0.71*	*0.40*	*0.01*
LetsChat_post	*2.47*	*2.60*	*0.69*	*0.37*	*0.11*	*0.05*	*0.41*	*0.53*	*0.01*
StopOnLineBullying_pre	*2.41*	*2.61*	*0.60*	*0.38*	*0.10*	*0.05*	*0.21*	*0.65*	*0.00*
StopOnLineBullying_post	*2.44*	*2.75*	*0.80*	*0.30*	*0.13*	*0.04*	*0.00*	*0.96*	*0.00*
PlaySafely_pre	*2.18*	*2.29*	*0.72*	*0.56*	*0.12*	*0.08*	*0.64*	*0.43*	*0.01*
PlaySafely_post	*2.39*	*2.64*	*0.85*	*0.48*	*0.14*	*0.07*	*0.39*	*0.53*	*0.01*
WatchOut_pre	*2.15*	*2.19*	*0.64*	*0.50*	*0.10*	*0.07*	*1.12*	*0.29*	*0.01*
WatchOut_post	*2.04*	*2.25*	*0.89*	*0.72*	*0.14*	*0.10*	*0.29*	*0.59*	*0.00*
Cyber security_total_pre	**2.27**	**2.36**	**0.59**	**0.39**	**0.09**	**0.06**	**0.96**	**0.33**	**0.01**
Cyber security_total_post	**2.34**	**2.56**	**0.71**	**0.37**	**0.11**	**0.05**	**0.30**	**0.58**	**0.00**
SSS_total	**0.45**	**0.48**	**0.24**	**0.18**	**0.04**	**0.03**	**1.78**	**0.19**	**0.02**
IAT D_asis	**0.10**	**0.15**	**1.02**	**0.98**	**0.05**	**0.04**	**1.89**	**0.23**	**0.01**

Table 8. Mean, standard deviation, F and p values for the effect of gender

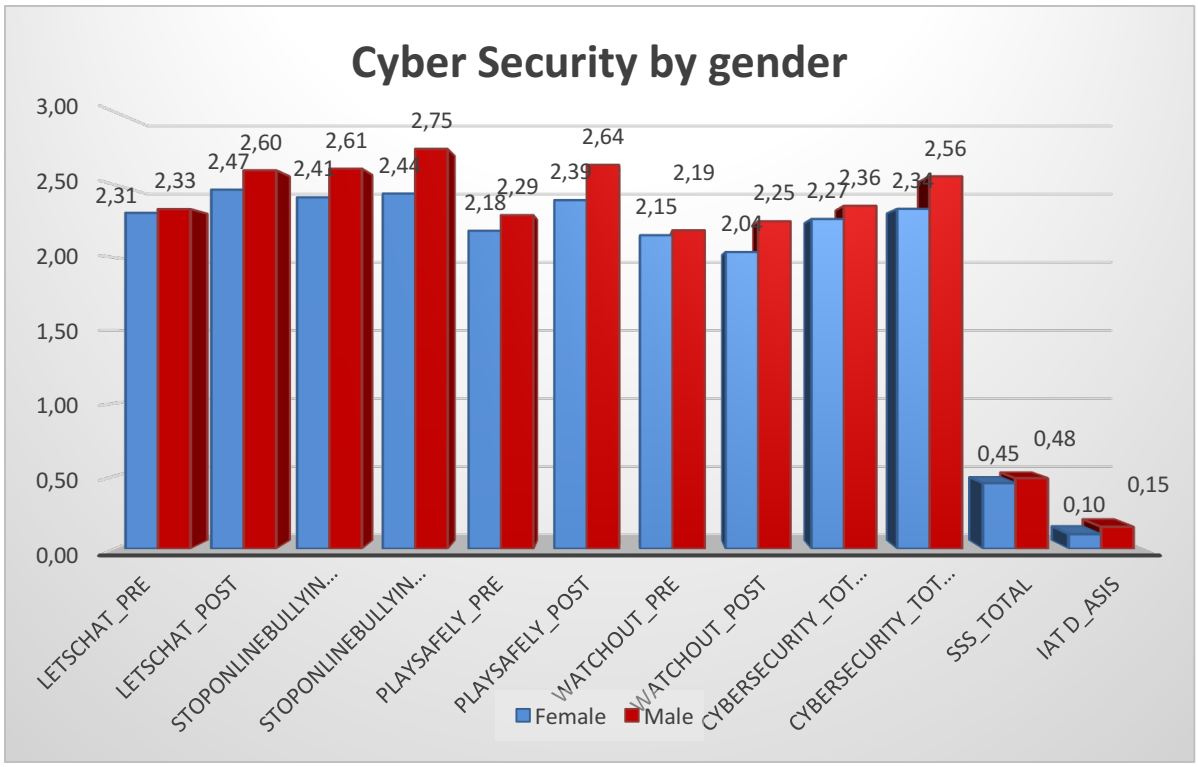


Figure 22. Cyber security by gender

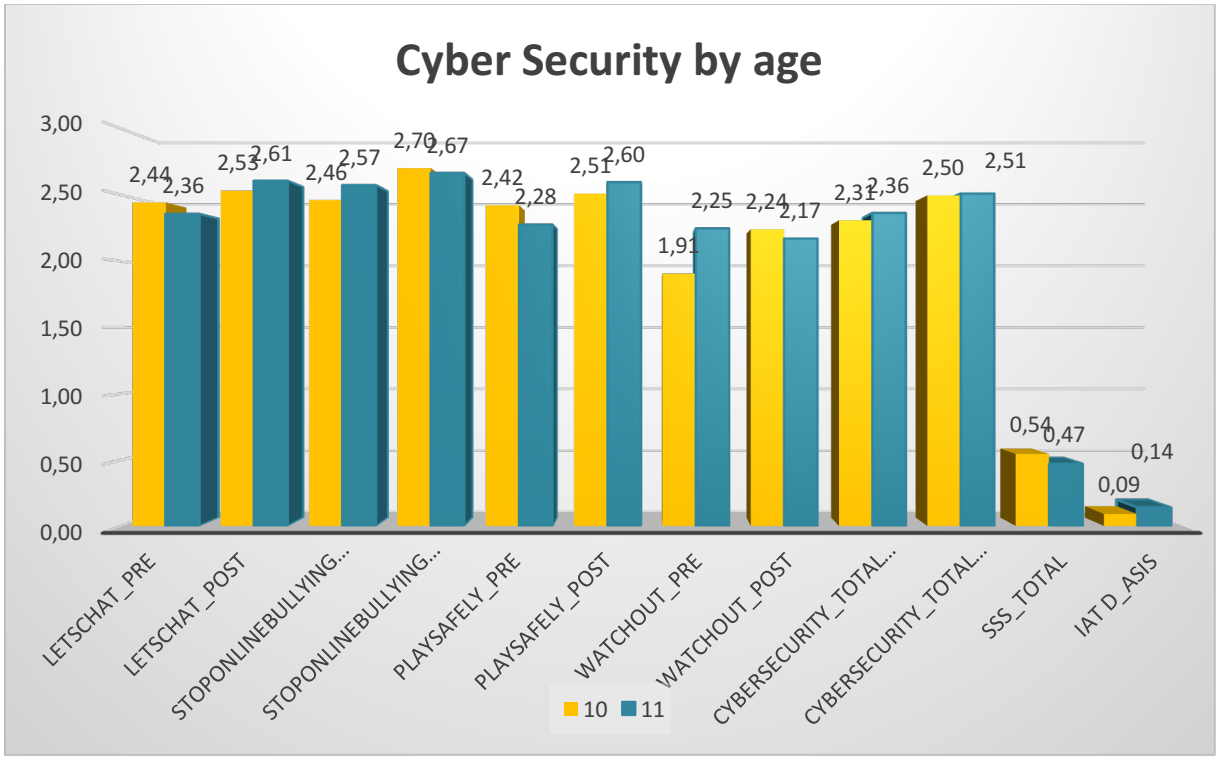


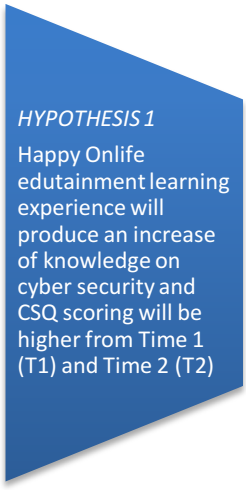
Figure 23. Cyber security by age

Mean, standard deviation, F and p values for the effect of age

	Mean		**Std. deviation**		**Std. error mean**		**F**	**Sig.**	**Partial Eta Squared**
Age	**10**	**11**	**10**	**11**	**10**	**11**			
LetsChat_pre	*2.44*	*2.36*	*0.38*	*0.48*	*0.13*	*0.06*	*0.48*	*0.49*	*0.01*
LetsChat_post	*2.53*	*2.61*	*0.45*	*0.36*	*0.15*	*0.04*	*0.08*	*0.77*	*0.00*
StopOnLineBullying pre	*2.46*	*2.57*	*0.45*	*0.40*	*0.15*	*0.05*	*0.12*	*0.73*	*0.00*
StopOnLineBullying _post	*2.70*	*2.67*	*0.35*	*0.46*	*0.12*	*0.05*	*0.24*	*0.63*	*0.00*
PlaySafely_pre	*2.42*	*2.28*	*0.42*	*0.57*	*0.14*	*0.07*	*0.99*	*0.32*	*0.01*
PlaySafely_post	*2.51*	*2.60*	*0.70*	*0.54*	*0.23*	*0.06*	*0.00*	*0.98*	*0.00*
WatchOut_pre	*1.91*	*2.25*	*0.60*	*0.49*	*0.20*	*0.06*	*2.20*	*0.14*	*0.03*
WatchOut_post	*2.24*	*2.17*	*0.84*	*0.79*	*0.28*	*0.09*	*0.35*	*0.56*	*0.00*
Cyber security_total_pre	**2.31**	**2.36**	**0.42**	**0.40**	**0.14**	**0.05**	**0.00**	**1.00**	**0.00**
Cyber security_total_post	**2.50**	**2.51**	**0.53**	**0.44**	**0.18**	**0.05**	**0.10**	**0.75**	**0.00**
SSS_total	**0.54**	**0.47**	**0.23**	**0.20**	**0.08**	**0.02**	**2.35**	**0.13**	**0.03**
IAT D_asis	**0.09**	**0.14**	**1.00**	**0.97**	**0.05**	**0.04**	**1.87**	**0.22**	**0.01**

Table 9. Mean, standard deviation, F and p values for the effect of age

4.3 Differences between pre-activity and post-activity



To evaluate the effect of Happy Onlife serious gaming session on cyber security attitudes of the participants, a repeated measures MANOVA was conducted. Results showed a significant effect within groups (pre- vs post-activity: Wilks' Lambda = .633, $F_{(4;83)}$ = 12.014, p = .367). Particularly, there was a significant effect of pre-and post-activity on: 'Let's chat!', 'Stop online bullying!' and 'Play safely!' scales, but no effect was found on the 'Watch out!' scale. The cyber security score is higher from T1 and T2 (cfr Table 10).

Moreover, there was a significant effect of pre- and post-activity on IAT measures.

A post-activity level of implicit cyber security increased from T1 to T2 (cfr. Table 10), indicating that Happy Onlife serious gaming session had a positive effect on the participants' implicit attitudes towards cyber security.

Significant effects (Sig.)* are reported by scores that are from 0,05 and below. 'Let's chat!', 'Stop online bullying!' and 'Play safely!' scored respectively 0,000; 0,050; 0,000; showing significant effect between pre and post serious gaming HOL activity. In contrast, the 'WatchOut' area scored 0,83 showing non significant effect between pre and post activity.

We can interpret these results in different ways:

(i) there is no effect of Happy Onlife serious gaming activity as concerns 'WatchOut' area;

(ii) as in the serious gaming activity the HOL questions come up randomly, there can be gaming matches where one or more categories are not treated. This fact could explain the non significant effect between pre and post activity. To overcome these doubts, in future researches, we will consider to design a research-dedicated Happy Onlife gaming session where all 4 areas are considered equally by raising the same number of questions;

(iii) children had already developed digital skills and awareness in the 'WatchOut' area, thus the effect between pre and post activity is not present for this specific area;

(iv) in contrast with point (iii), children might not have neither knowledge, nor digital competences for the 'WatchOut' area and, as a consequence, they might not understand the content proposed by the HOL serious gaming activity for the 'WatchOut' area. This incomprehension could impact on the learning process of children. According to Ausubel (Ausubel), a meaningful learning is installed on a progressive's cognitive structure. In Ausubel's view, to learn meaningfully, students must relate new knowledge (concepts and propositions) to what they already know. He proposed the notion of an advanced organizer as a way to help students link their ideas with new material or concepts. Ausubel's theory of learning claims that new concepts to be learned can be incorporated into more inclusive concepts or ideas. In any case, the advance organizer is designed to provide, what cognitive psychologists call, the mental scaffolding to learn new information.

Mean, standard deviation, F and p values for pre- and post-activity

	Possible range		Observed range		Mean		Std. Deviation		F	Sig.	Partial Eta Squared
	Pre	Post	Pre	Post	Pre	Post	**Pre**	**Post**			
Let'sChat	0-3	0-3	1.66-2.70	2.24-2.72	2.32	2.54	0.55	0.53	30.63	**0.000***	0.26
StopOnLine Bullying	0-3	0-3	2.24-2.75	2.40-2.79	2.52	2.61	0.50	0.60	3.96	**0.050***	0.04
PlaySafely	0-3	0-3	1.86-2.48	2.48-2.57	2.24	2.53	0.64	0.67	31.85	**0.000***	0.27
WatchOut	0-3	0-3	1.52-2.62	1.67-2.62	2.17	2.16	0.56	0.80	0.05	0.830	0.00
IAT D_asis					-0.19	0.98	0.16	1.04	3.96	**0.020***	0.06

Table 10. Mean, standard deviation, F and p values for pre-activity and post-activity

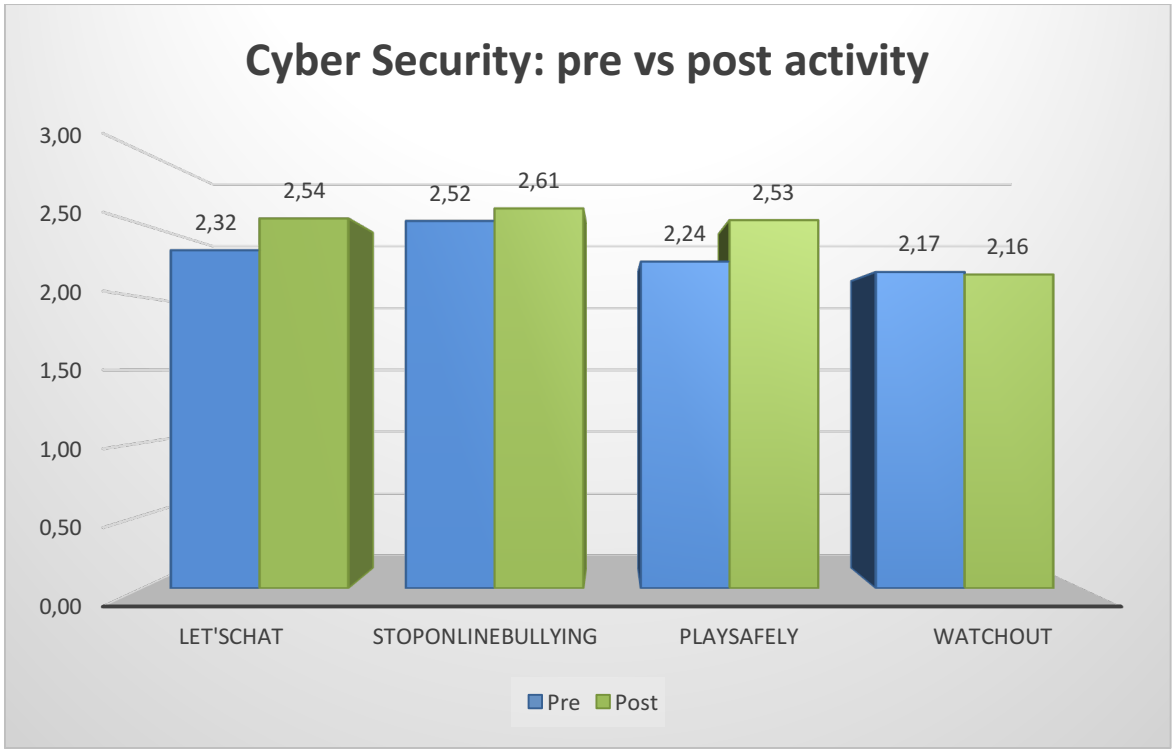


Figure 24. Cyber security pre-activity versus post-activity

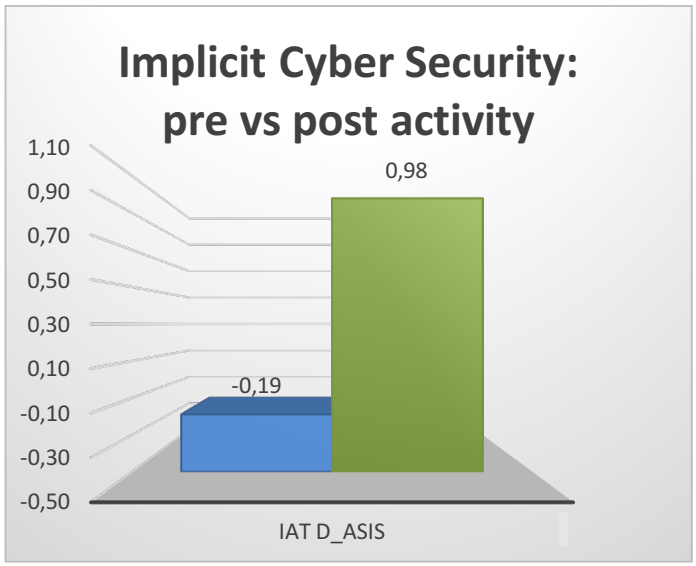


Figure 25. Implicit cyber security: pre-activity versus post-activity

Moreover, we tested a mixed model to explore if there is an effect of gender and age on on *Cyber security score* from T1 and T2. Results showed a significant interaction effect pre and post for gender (Wilks' Lambda = .950, $F_{(1;85)}$ =4.433, p < .05), no interaction effect for age.

Scores in T1 were very close (2.36 for male and 2,27 for female).

Cyber security score is higher from time 1 (T1) and time 2 (T2), and this change is higher in males group (cfr. Figure 26). This result can be explained as follows:

(i) Males could have been more cautious in comparison to female;

(ii) Male could have more notions of data literacy;

(iii) Other psychological variable related to gender could play a role in this change.

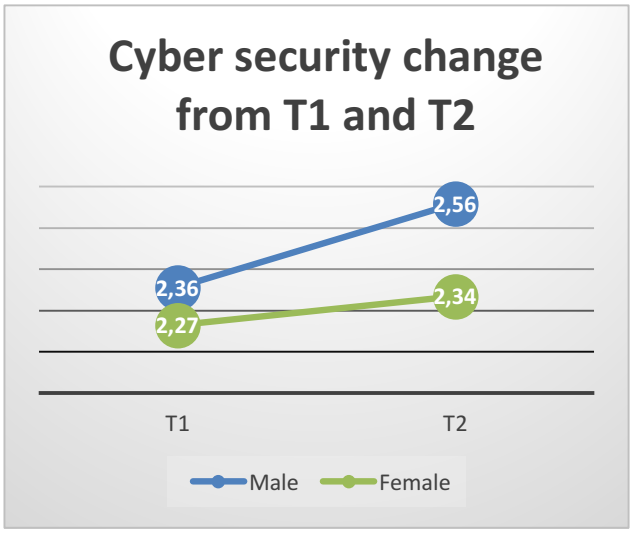


Figure 26. Cyber security: pre-activity versus post-activity by gender

Additionally, to deepen the effect of Happy Onlife training on each items, a repeated measures MANOVA was conducted on all items. Results showed a significant effect *within* groups (pre vs post activity: Wilks' Lambda = .291, $F_{(4;83)}$ =6,793, p < 0.05).

Herewith we comment the four areas:

Let'sChat

In this area there was a significant effect of pre and post activity in two items: "To publish own pictures online" (Mean pre = 2.20, Mean post = 2.57) and "To copy & paste information" (Mean pre = 1.66, Mean post = 2.24).

We assume that pictures are considered as sensitive data by participants, thus participants are more inclined to take care of their own pictures in comparison with other general personal online information. The term data deserves particular attention and it should be explained more accurately as during discussion with children it emerged that pictures are not considered as data by several participants. This reinforces the idea that Data literacy should be promoted among students.

Participants seemed to be familiar with "copy and paste" actions.

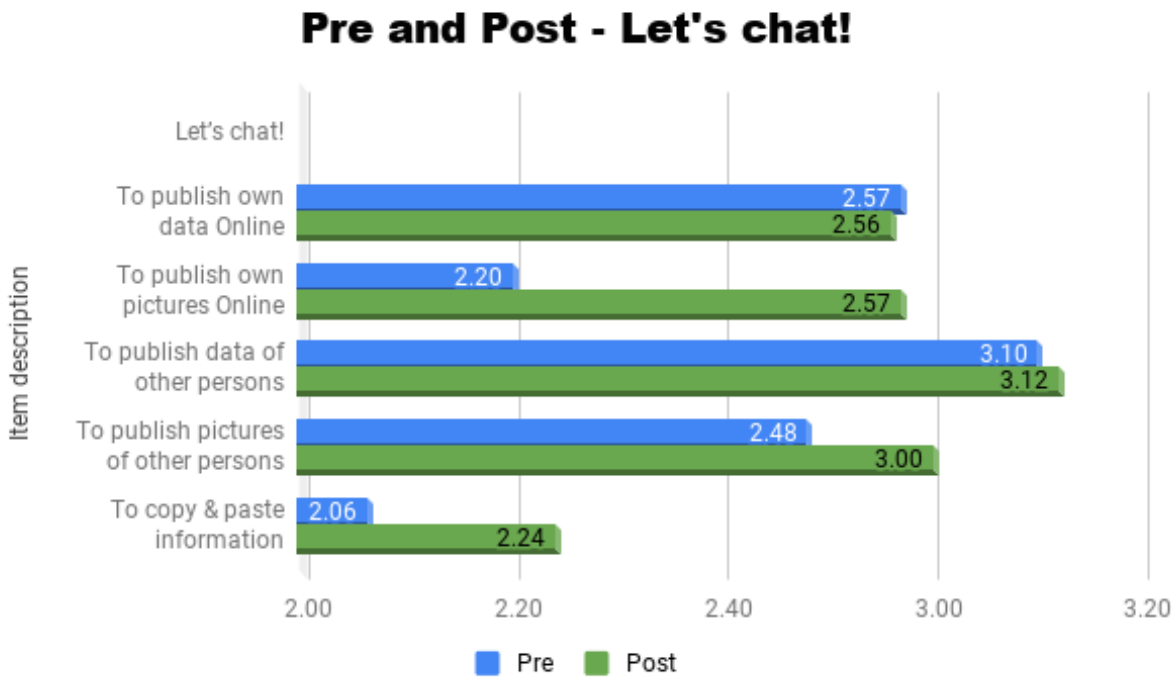


Figure 27. Let's chat! -: pre-activity versus post-activity

StopOnLineBullying

In this area there was a significant effect of pre and post activity only in one item: "To provoke someone online" (Mean pre = 2.56, Mean post = 2.79).

StopOnLineBullying scores range from 2.24 to 2.75 and from 2.40 to 2.79 (respectively pre and post activity).

In this area the mean pre and post score is higher than in other areas. This score might be the effect of previous knowledge on cyberbullying phenomenon. This knowledge might be the consequence of school and awareness raising campaigns on the theme. The term provoking is not full understood. Maybe it should be replaced by a different term such as hurting that can be considered more meaningful at this age.

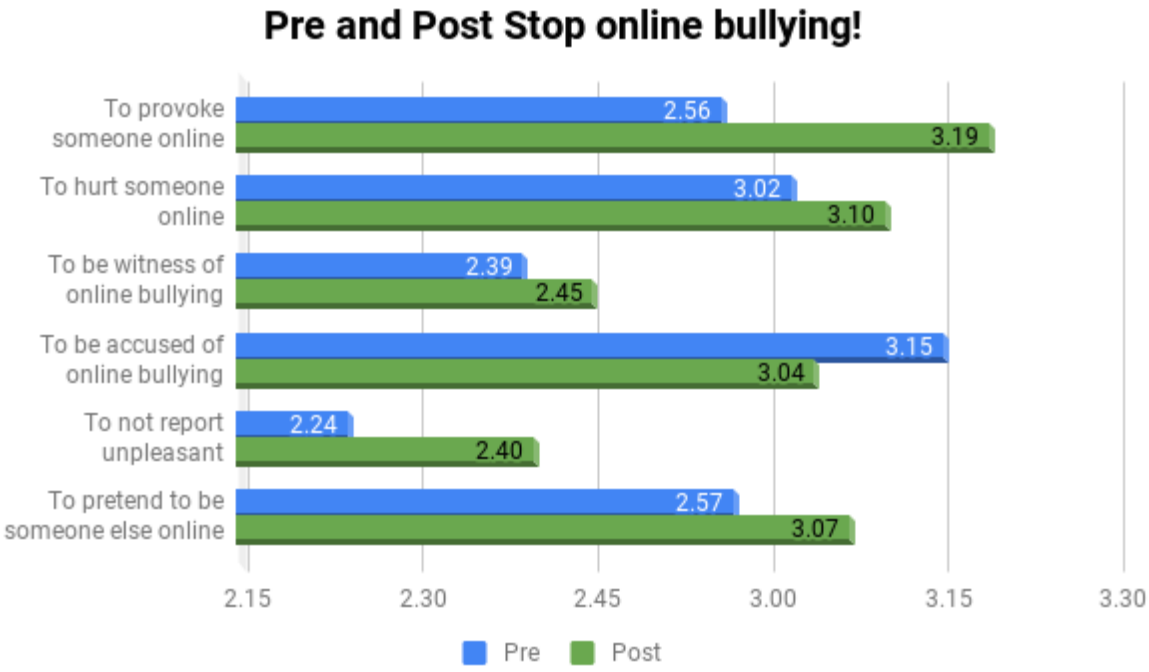


Figure 28. Stop online bullying! -: pre-activity versus post-activity

PlaySafely

In PlaySafely area there was a significant effect of pre and post activity in three items:

- To use a real name and family name when video gaming online (Mean pre = 1.86, Mean post = 2.48)
- To download music and film for free (Mean pre = 2.25, Mean post = 2.52)
- To use video gaming for several hours without any breaks (Mean pre = 2.26, Mean post = 2.57)

PlaySafely scores vary from 1.86 to 2.48 in pre-activity and from 2.48 to 2.57 in post-activity. This can be explained by familiarity and knowledge developed in this specific area.

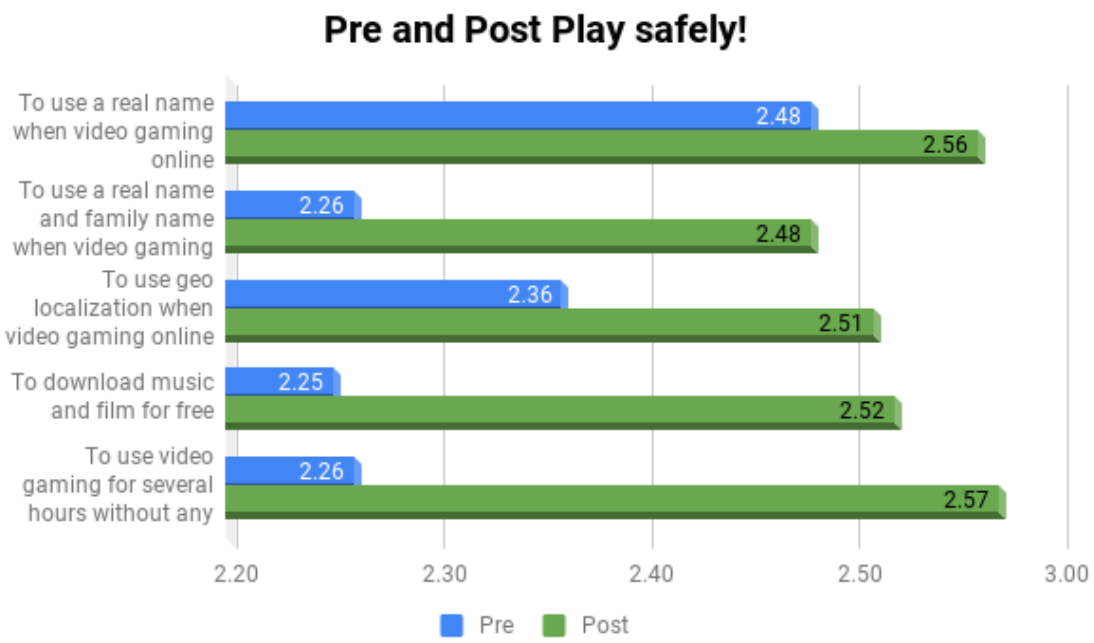


Figure 29. Play safely! -: pre-activity versus post-activity

WatchOut

In this area there was a significant effect of pre and post activity in three items:

- To open pop-up and add- messages (Mean pre = 2.02, Mean post = 2.62)
- To not check the privacy setting of online applications (Mean pre = 2.38, Mean post = 2.05)
- To tell our own password to someone else (Mean pre =2.62, Mean post = 2.14)

WatchOut scores vary from 1.52 to 2.62 in pre-activity and from 1.67 to 2.62 in post-activity.

We observe that scores in this area are the lowest ones. We assume that participants are not familiar neither with the actions listed in the are nor with the vocabulary of the area.

In particular item 21 “To register to a Social Network…” is the lowest one and scores in the pre and post are 1.52→ 1.67.

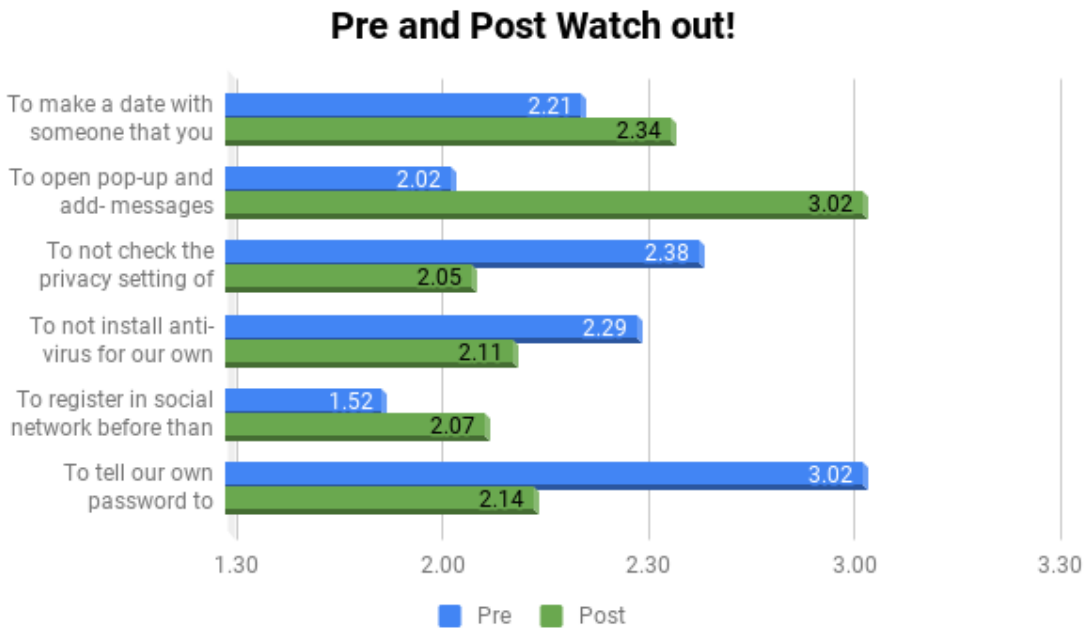


Figure 30. Watch out! -: pre-activity versus post-activity

In general, it is interesting to observe how results showed a significant effect on those items where pre-scores were low.

To improve understanding of these results, it would recommendable to understand which are the activities that children are doing in their daily life (e.g. searching for information, downloading, communicating, etc.). In some cases, they might not be aware of the activities proposed in the items or they might identify them with different wording.

Box 4. Repeated measures MANOVA (Multivariate analysis of variance) is Multivariate analysis of variance (*MANOVA*) is an ANOVA with several dependent variables. ANOVA is a collection of statistical models and their associated estimation procedures (such as the "variation" among and between groups) used to analyse the differences among group means in a sample. The MANOVA extends this analysis by taking into account multiple continuous dependent variables, and will compare whether or not the newly created combination differs by the different groups, or levels, of the independent variable. In this way, the MANOVA essentially tests whether or not the independent grouping variable simultaneously explains a statistically significant amount of variance in the dependent variable.

Mean, Standard deviation, F and p values for pre and post activity of all items

		Mean		SD				
Nr.	**Item description**	**Pre**	**Post**	**Pre**	**Post**	**F**	**Sig.**	**Partial Eta Squared**
	Let's chat!							
1	To publish own data Online	2.57	2.56	0.676	0.872	0.017	0.897	0.000
2	To publish own pictures Online	**2.20**	**2.57**	0.833	0.676	31.218	**0.000***	0.266
3	To publish data of other persons Online	2.70	2.72	0.573	0.623	0.124	0.726	0.001
4	To publish pictures of other persons Online	2.48	2.60	0.729	0.673	2.204	0.141	0.025
5	To copy & paste information	**1.66**	**2.24**	1.055	0.889	27.035	**0.000***	0.239
	Stop online bullying!							
6	To provoke someone online	**2.56**	**2.79**	0.71	0.631	8.004	**0.006***	0.085
7	To hurt someone online	2.62	2.70	0.686	0.684	1.090	0.299	0.013
8	To be witness of online bullying	2.39	2.45	0.783	0.846	0.314	0.577	0.004
9	To be accused of online bullying	2.75	2.64	0.511	0.731	1.998	0.161	0.023
10	To not report unpleasant messages received online	2.24	2.40	0.849	0.882	3.138	0.080	0.035
11	To pretend to be someone else online (false identity)	2.57	2.67	0.676	0.71	1.398	0.240	0.016
	Play safely!							
12	To use a real name when video gaming online	2.48	2.56	0.951	0.788	0.729	0.396	0.008
13	To use a real name and family name when video gaming online	**1.86**	**2.48**	0.865	0.833	54.922	**0.000***	0.390
14	To use geo localization when video gaming online	2.36	2.51	0.862	0.861	2.649	0.107	0.030
15	To download music and film for free	**2.25**	**2.52**	0.943	0.819	8.875	**0.004***	0.094
16	To use video gaming for several hours without any breaks	**2.26**	**2.57**	0.814	0.725	16.908	**0.000***	0.164
	Watch out!							
17	To make a date with someone that you have met online only	2.21	2.34	1.047	0.775	2.083	0.153	0.024
18	To open pop-up and add- messages	**2.02**	**2.62**	0.915	0.719	32.235	**0.000***	0.273
19	To not check the privacy setting of online applications	2.38	2.05	0.703	1.247	5.643	0.020	0.062
20	To not install anti-virus for our own devices	2.29	2.11	0.848	1.146	1.630	0.205	0.019
21	To register in social network before than the age suggested by the national legislation	1.52	1.67	0.9	1.128	1.427	0.236	0.016
22	To tell our own password to someone else	**2.62**	**2.14**	0.669	1.143	15.607	**0.000***	0.154

Table 11.Mean, Standard Deviation, F and p values for pre-activity and post activity of all items

Finally, there was a significant effect of pre and post on IAT measure. Post activity level of implicit Cyber security was higher (cfr. Figure 29), indicating that *Happy Onlife* had a positive effect on children as learning tool about Cyber security.

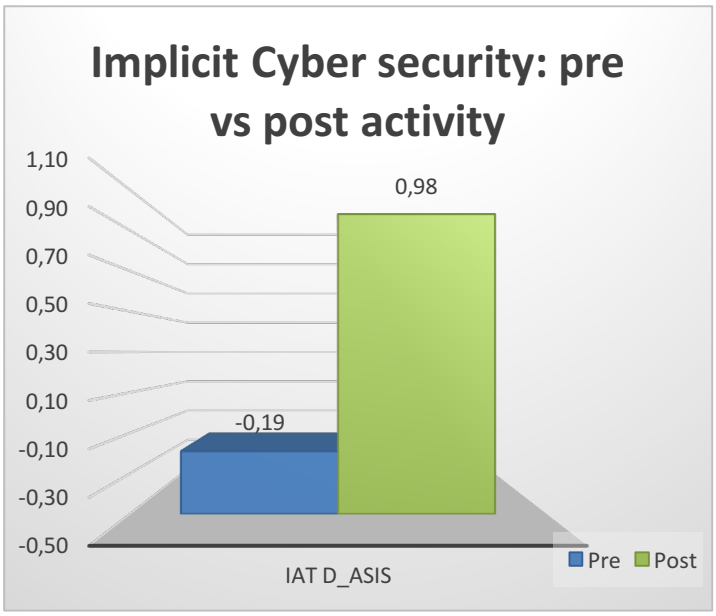
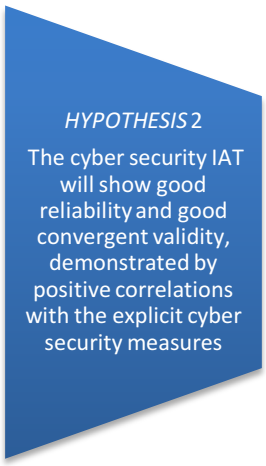


Figure 31. Implicit Cyber security: pre-activity versus post-activity

4.3.1 Correlations



Pearson correlations among pre- and post-activity measures and implicit measures were computed (See Table 12). All sign correlations were significant and positive ($p < .05$).

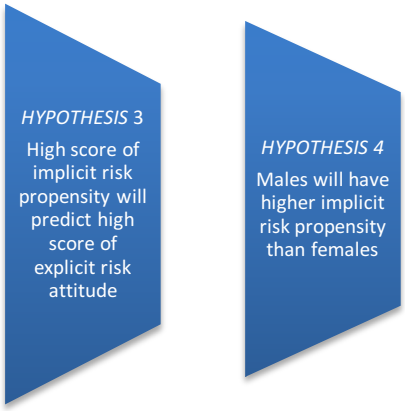
The IAT measure had a moderate and positive correlation with all measures, particularly as the highest correlation was with the 'Stop online bullying!' and 'Play safely!' scales. Moreover, post-activity measure correlations were higher than pre-activity ones.

Pearson Correlations

	IAT D_ASIS
LetsChat_pre	.396(**)
LetsChat_post	.391(**)
StopOnlineBullying_pre	.388(**)
StopOnlineBullying_post	.490(**)
PlaySafely_pre	.440(**)
PlaySafely_post	.494(**)
WatchOut_pre	.377(**)
WatchOut_post	.405(**)
Cyber security_total_pre	.464(**)
Cyber security_total_post	.521(**)
**** Correlation is significant at the 0.05 level (2-tailed).**	

Table 12. Correlation among pre- and post-activity measures and implicit measures

4.3.2 Regression analyses: the predictive role of implicit measure on explicit cyber security



The pattern of correlations revealed the presence of significant relations between explicit and implicit (IAT) measures of Cyber security. Hence several linear regression analyses were performed to verify the predictive power of implicit Cyber security. We conducted separate regressions on the two dependent variables: Cyber security explicit total score pre-activity and post-activity, with IAT as independent variable (the predictor variable). Moreover, we tested the predictive power in males, females and age groups.

In the first regression series (group by gender), results showed no significant effect of predictor on Cyber security pre-activity in males but significant effects of predictor in males post-activity and in females (cfr. Table 13 and Figure 30). However, the most significant model was the prediction of post-activity Cyber security score in females, with the 39%f explained variance ($R2 = 0.387$, $p < 0.05$).

Regression analyses in males and females

Dependent variable	Group	Stand.Coeff. (Beta)	t	Sig.	R square
Cyber security total score pre	Males	0.280	1.981	0.054	0.079
	Females	0.572	4.241	**0.000***	0.327
Cyber security total score post	Males	0.322	2.310	0.025	0.104
	Females	0,622	4,828	**0,000***	0,387

Table 13.Regression analyses in males and females

4.3.3 Factor Analysis

To explore the construct validity of the Cyber security questionnaire, exploratory factor analysis was performed. Exploratory factor analysis detects the constructs - i.e. factors - that underlie a dataset based on the correlations between variables (in this case, questionnaire items). (Bornstedt, 1977; Field, 2009; Tabachnik & Fidell, 2001; Ratray & Jones, 2007; Rietveld & Van Hout, 1993). In contrast to the commonly used principal component analysis, factor analysis does not have the presumption that all variance within a dataset is shared (Costello & Osborne, 2005; Field, 2009; Tabachnik & Fidell, 2001; Rietveld & Van Hout, 1993).

The prerequisites for factor analysis were satisfied (cfr. Table 14):

- the Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) was good (KMO = 0.847). The KMO *'represents the ratio of the squared correlation between variables to the squared partial correlation between variables'* and it can signal in advance whether the sample size is large enough to reliably extract factors (Field, 2009). When the KMO is near 1, a factor or factors can probably be extracted, since the opposite pattern is visible. Therefore, KMO *'values between 0.5 and 0.7 are mediocre, values between 0.7 and 0.8 are good, values between 0.8 and 0.9 are great and values above 0.9 are superb.'* (Field, 2009. p. 647).
- the Barlett's test is significant ($x^2_{(231)}$ = 884.042, $p < 0.05$). If the Barlett's test gives a significant result, we can assume that the items correlate anyhow, like in this data set. Since the Barlett's test gives a significant result and the items correlate at most with a third of the items too lowly, items were not excluded before the factor analysis was conducted.

KMO and Bartlett's Test – Factor Analysis prerequisites

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.847
Bartlett's Test of Sphericity	Approx. Chi-Square	884.042
	Df	231
	Sig.	0.000

Table 14. KMO and Barlett's Test - Factor Analysis prerequisites

A reliable and rather easy method to determine how many factors to retain is to look at the scree plot, as the graph in Figure 29 (Costello, 2005).
The factors with values above the point at which the curve flattens out should be retained. The factors with values at the break point or below should be eliminated. Thus, looking at Figure 29, two factors should be retained.

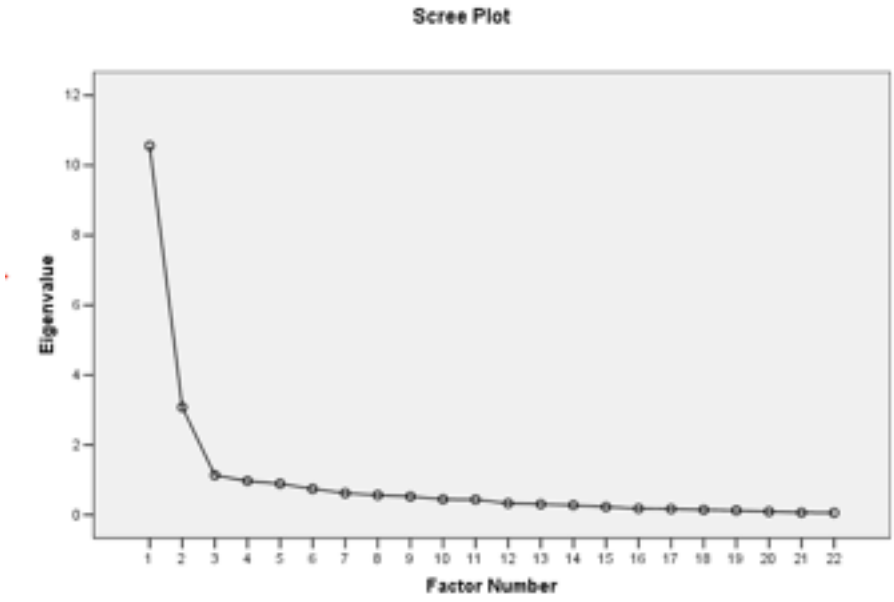


Figure 32. Scree Plot

The 'oblique rotation' was used. This type of rotation is used when the factors are assumed to correlate. Since it was assumed that all 23 items in this questionnaire measured the same construct, such as *Cyber security*, we may expect that an oblique rotation is appropriate. This can be checked after having conducted the factor analysis, since statistical packages always give a correlation matrix of the factors when you opt an oblique rotation method (oblimin or promax). Therefore, it is highly recommended to always do a factor analysis with oblique rotation first, even if you are quite sure that the factors are independent. The Pattern Matrix is showed in Table 16. The two factors explained a total percentage of variance of about 62%, with the first factors explaining the 48% and the second one the 14%. Variables with loadings lower than 0.3 are considered to have a no significant impact on a factor, and need therefore to be ignored (Field, 2009). Ignoring the variables that load lower than 0.3 on a factor, we can conclude based on the output of the factor analysis with two extracted factors (see Table 16) that there are two main factors:

- a main factor, that includes the three scales: *'Let's chat!'*, *'Stop online Bullying!'* and *'Play safely!'*;
- a second factor including items belonging to the *'Watch out!'* scale.

All the factor loadings were pure, with the exception of item 1: '*To publish own data online*', that was complex, having a high loading on both factors (r = 0. 414 and 0.499, respectively).
The two factors correlated positively with each other (r = 0.30).

Box 1. Exploratory Factor Analysis

Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization. Rotation converged in 5 iterations. Only loadings higher than 0.3 are displayed.

Exploratory Factor Analysis with Oblimin Rotation – Pattern Matrix				
			Factor	
Nr.	**Scale**	Item description	1	2
6	**StopOnlineBullying**	To provoke someone online	0.849	
7	**StopOnlineBullying**	To hurt someone online	0.824	
17	**PlaySafely**	To use video gaming for several hours without any breaks	0.778	
13	**PlaySafely**	To use a real name when video gaming online	0.761	
3	**Let'sChat**	To publish data of other persons online	0.756	
14	**PlaySafely**	To use a family name when video gaming online	0.730	
16	**PlaySafely**	To download music and film for free	0.728	
12	**StopOnlineBullying**	To pretend to be someone else online (false identity)	0.724	
15	**PlaySafely**	To use geo localisation when video gaming online	0.721	
8	**StopOnlineBullying**	To be witness of online bullying	0.719	
2	**Let'sChat**	To publish own pictures online	0.718	
10	**StopOnlineBullying**	To be accused of online bullying	0.709	
4	**Let'sChat**	To publish pictures of other persons online	0.655	
19	**WatchOut**	To open pop-up and add- messages	0.595	
18	**WatchOut**	To make a date with someone that you have met online only	0.579	
11	**StopOnlineBullying**	To not report unpleasant messages received online	0.568	
5	**Let'sChat**	To copy & paste information	0.408	
23	**WatchOut**	To tell our own password to someone else		0.967
20	**WatchOut**	To not check the privacy setting of online applications		0.909
21	**WatchOut**	To not install anti-virus for our own devices		0.883
22	**WatchOut**	To register in social network before than the age suggested		0.757
1	**Let'sChat**	To publish own data online	*0.414*	*0.499*

Table 15. Exploratory Factor Analysis with Oblimin Rotation - Pattern Matrix

5 Future developments

The Happy Onlife digital game is now available under the European Union Public License, open-source software. Since its release on August 2015, more than 1500 paper kits in Italian were distributed in 16 Italian regions and more than 3100 worldwide installations were downloaded from the mobile stores in 79 countries. Around 1000 Happy Onlife boxes in English were distributed during the Universal Exposition Expo 2015 in Milan, the Researchers Night in Bratislava held in September 2017 for the "JRC 60 years of science for society" and to schools visiting the JRC Ispra site, Italy, both during Open days and dedicated visits at the Visitors Centre. If we count that for every kit distributed, at least 6 players have played with Happy Onlife, we can say that 15.000 citizens have benefited from this resource. However, we know that the kit has reached more people as it is used as an off-the-shelve tool in schools and libraries. To these numbers, web version users and app users need to be added.

JRC E3 Unit keeps receiving daily requests for toolkit dissemination and educational support from schools and informal educators, to which it is quite difficult for the JRC to respond. Non-commercial/societal entities showed interest in valorising current JRC Happy Onlife products for maturation and dissemination, as well as wider community building and expanding the success of Happy Onlife at the European level.

Future objectives are to perform the transfer and maturation of the current JRC product to:

- perform a deeper analysis to investigate peers and adults' influences and components (in home and school contexts) on cyber risk attitudes and cyber risk taking behaviours;
- deploy and promote validated participatory services[6] on 'Do-it-together' Happy Onlife game-based learning towards educational entities in European countries, in support of EU policies in cyber security, privacy, data protection and children's rights domains;
- investigate, together with educational experts, the assessment of validated innovative participatory services for wider community building and for nourishing shared content (e.g. the co-construction of shared collective memories on actual uses, attitudes and experiences in ICT);
- create synergies and promote novel pedagogy, didactics and digital literacy aids in data protection and cyber security harmonised with digital competences and critical and creative thinking while sharing best practices at the European level.

Further research is planned and the toolkit has been translated in Romanian, Portuguese, and Greek. Georgian translation is ongoing and the Information and Data Protection Authority in Albania is now arranging Media Literacy classes in English with Happy Onlife toolkit and considering the translation in Albanian. Many other initiatives are ongoing, nevertheless for reason of brevity they cannot be listed all. The analysis reported in this document has already drawn the attention of researchers interested in the *Happy Onlife* edutainment toolkit adoption and dissemination. The explicit and implicit research methods and tools reported in this document have been considered at European level in the frame of a JRC Proof of Concept Project 'Do-It-Together with Happy Onlife' awarded to JRC Unit Cyber and Digital citizens' security. The research has some limitations and the experiment protocol can be improved. For instance, a control group could be considered to make comparison with the experimental group results and a dedicated experimental session of Happy Onlife game should be developed to avoid that HOL questions come up randomly. The duration of the test should be considered. Repeating similar tests before and after playing Happy Onlife can be perceived as time-consuming and boring for children and this can have a negative impact on the quality of the data collected. Pre-test and advanced arrangement of all resources (usb keys, informatic classroom availability) is strongly recommended.

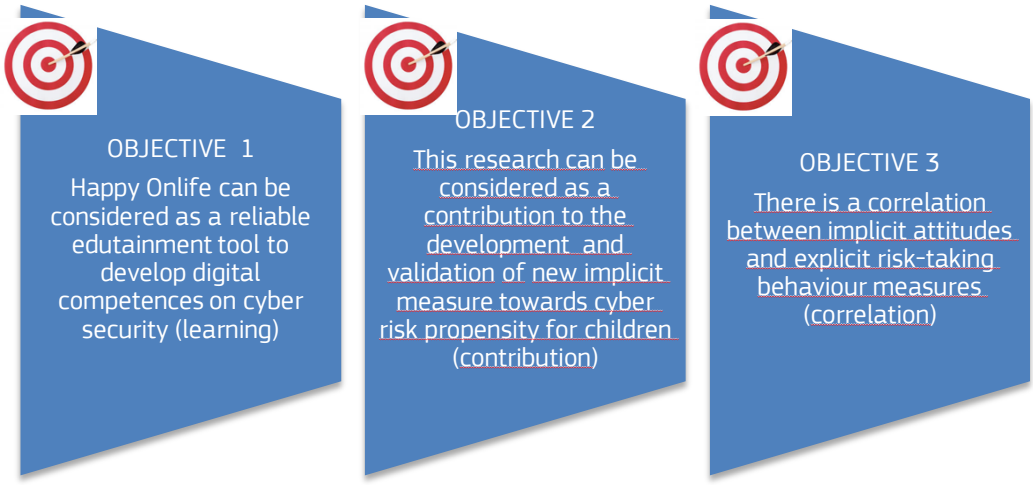
[6] https://web.jrc.ec.europa.eu/happyonlife/participate.html

6 Conclusions

The Happy Onlife experience has contributed to children's right to be heard in matters affecting them in their digital interactions and lives. By playing with Happy Onlife game children could naturally self-disclose and express their emotions, needs, understanding and sometimes worries and doubts.

Indeed, self-reporting provides valuable insights for a wide range of research, policy and educational questions, however it can be susceptible to self-presentation and socially desirable responding. Moreover, self-report measures, as those gathered within the presented survey, are not well suited to capture thoughts and feelings that are outside of conscious awareness (Greenwald & Banaji, 1995). To overcome these limitations, implicit measures were considered to complement this experimental research about children's attitude towards cyber risks. To our knowledge, the present research is the first study to investigate implicit attitudes towards cyber risk-taking behaviours in secondary school children.

This work seeks to contribute to prior research by addressing innovative method as the Implicit Test Association (Harward University, 2016) that may explain the relation between (implicit) attitudes and cyber risk-taking behaviours by youngsters. Furthermore, we argued that by way of *Happy Onlife gamification experience and training on cyber security*, subjects may change their attitudes towards cyber risks, thus develop their digital competences on themes as cyber security, privacy and data protection.



1. Data showed that instruments had satisfactory reliability:
   - IAT showed good reliability (α =.94);
   - all the explicit measures showed adequate reliability, with ranging alpha from .68 to .94;
   - the cyber security IAT showed good reliability (split-half method) and good convergent validity, demonstrated by a negative correlation with a sensation-seeking scale (Pearson's r = — 0.40, p < .05).
2. To evaluate the effect of *Happy Onlife gamification experience and training on cyber security*, a repeated measures MANOVA was conducted:
   - the *CSQ* cyber security score was higher from T1 and T2;
   - there was a significant effect of pre- and post-IAT measure;
   - post-activity level of implicit cyber security was higher, indicating that Happy Onlife had a positive effect on children in training about cyber security.
3. All sign correlations were significant and positive (p < .05).

- the IAT measure had a moderate positive correlation with all measures, particularly the highest correlation, which was with the *'Stop online bullying!'* scale and *'Play safely!*'.

To deepen the effect of *Happy Onlife gamification experience and training on cyber security*, we analysed each items separately with a further repeated measures MANOVA. Results showed that 8 items scored significantly higher after the *Happy Onlife gamification experience and training on cyber security*. Particularly, after the training, children learnt better the risk of copying and pasting information, of provoking someone online (cyberbullying), of using a real name and family name when video gaming online, of downloading music and film for free, of using videogames for several hours without any breaks, of opening pop-up and add-message, of not checking the privacy setting of online applications and of revealing their own password to someone else.

4. There was also a significant change of pre and post IAT measure:
    - post activity level of implicit cyber security was higher, indicating that *Happy Onlife gamification experience and training on cyber security* had a positive effect on children as learning tool to enhance the development of digital skills on cyber security;
    - the mixed model activity (pre vs post) X gender (males vs females) showed a significant interaction effect, indicating that females were more affected by *Happy Onlife gamification experience and training on cyber security* then males.
    - the pattern of correlations between implicit and explicit measures was positive, all correlations were positive and moderate. The IAT measure had moderate positive correlation with all measures, particularly the highest correlation was with *'Stop online bullying!'* scale and *'Play safely!'***.**
    - in addition, post activity measure correlations were higher than pre activity ones.
5. Regression analyses showed that IAT measure was a significant predictor of Cyber security explicit attitude, most of all in females, with the 39% of explained variance.

The research has some limitations and the experiment protocol can be improved. Overall, current results suggest that the '*Cyber security-Implicit Association Test'* can be considered as a reliable and valid method and may be a useful additional tool to self-report batteries for assessment of cyber risk propensity in children. The *'Cyber security-Implicit Association Test'* offers some suggestions and reflections about risk-taking behaviour about cyber world and it can be considered as tool for future and wider research about risk-taking behaviour by citizens and young citizens.

Further studies, at European Union level, may compare results of several implicit assessments, or may investigate the predictive power of internet users' risk-taking behaviours on attitude towards risks.

This contribution could be taken into consideration in future research, that would enhance understanding risk-taking behaviours on the daily lives of internet users and, last but not the least, it would support implementation of cyber security European strategies and policies to limit online threats and risks.

Bibliography

Adams, G., & Crane, P. (1980). An assessment of parents' and teachers' expectations of preschool children's social preferences for attract live or unattractive children and adults. *Child Development , 51*, 224-231.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. *Englewood Cliffs, NJ* .

Allport, G. (1935). Attitudes. *A handbook of social psychology* , 798-844.

Anderson, P., De Paoli, S., & Câtâlui, D. (2015). *Status of privacy and NIS course curricula in Member States.* European Union Agency For Network And Information Security. Athens: ENISA.

Ausubel, D. *The acquisition and retention of knowledge: a cognitive view. .* Kluwer Academic Publishers.

Bargh, J., Chaiken, S. G., & Pratto, F. (1992). The generality of the automatic activation effect. *Journal of Personality and Social Psychology , 62*, 893-912.

Barnes, S. B. (2006, September). *A privacy paradox: Social Networking in the United States*. Retrieved from http://journals.uic.edu /ojs/index.php/fm/article/view/1394/1312 boyd

Baron, J. (1994). Thinking and deciding (2nd ed.). *Cambridge University Press* .

Burgoon J.K. (1982). Privacy and Communication. In *Communication Yearbook 6* (pp. 206-249). Beverly Hillsm , CA: Sage.

Byrnes, J. M. (1999). Gender Differences in Risk Taking: A Meta-Analysis. *Psychological Bulletin* (125), 367-383.

Byrnes, J. (1998). The nature and development of decision-making: A self-regulation mode. *NJ: Erlbaum* .

Cash, T., & Duncan, N. (1984). Physical attractiveness stereotyping among Black American college students. *The Journal of Social Psychology , 122*, 71-77.

COM(2015) 185, E. C. (2015, April 28). *http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.* Retrieved from http://ec.europa.eu: http://ec.europa.eu

COM(2015) 192 final pp.13-20. (2015, May 6). *eur-lex.europa.eu.* Retrieved from eur-lex.europa.eu: eur-lex.europa.eu

Costello, A. B. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. . *Practical Assessment, Research, & Evaluation* (10), 1-9.

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika , 16*, 297–334.

Cronbach, L. J. (1947). Test “reliability”: its meaning and determination. In *Psychometrika* (Vol. 12, pp. 1-16).

DESI. (2016). *The Digital Economy & Society Index (DESI),*. Retrieved from Europa, Digital Single Market, Desi: https://ec.europa.eu/digital-single-market/desi

Di Gioia, R., Gemo, M., & Chaudron, S. (2015). *Empowering children and adults for a safe and responsible use of ICT, EUR 27702.* Joint Research Centre, Ispra, European Commission,. Luxembourg: Publications Office.

Dion, K., Berscheid, E., & Walster, E. (1972). What is beautiful is good. *Journal of Personality and Social Psychology , 24*, 207-213.

Doob, L. (1947). The behaviour of attitudes. *Psychological Review* , 135-156.

Downs, A., & Lyons, P. (1991). Natural Observations of the links between attractiveness and initial legal judgments. *Personality and Social Psychology Bulletin , 17*, 541-547.

Eagly, A., Ashmore, R., Makhijani, M., & Longo, L. (1991). What is beautiful is good, but ...: A meta-analytic review of research on the physical attractiveness stereotype. *Psychological Bulletin* , 109-128.

EEAS. (2013, February 28). *https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.* Retrieved from https://eeas.europa.eu: https://eeas.europa.eu

Europass. (2016). *Resources Digital Competences*. Retrieved from Europass Cedefop Europa: http://europass.cedefop.europa.eu/resources/digital-competences

European Parliament and Council (NIS). (2015, December 15). *https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation.* Retrieved from https://ec.europa.eu: https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation

Fazio, R. H., Sanbonmatus, D., Powell, M., & Kardes, F. (1986). On the automatic activation of attitudes. *Journal of Personality and Social Psychology , 50*, 229-238.

Fazio, R. (1986). How do attitudes guide behaviour? (R. S. (Eds.), Ed.) *Handbook of motivation and cognition: Foundation of social behaviour* , 204-243.

Fazio, R., & Zanna, M. (1981). Direct experience and attitude bahaviour consistency. *Advances in experimental social psychology , 14*, 161-202.

Ferrari, A., Punie, Y., & N., B. (2013). *DIGComp: A Framework for Developing and Understanding Digital Competences in Europe.* Joint Research Centre - European Commission, IPTS. Seville: Publications Office.

Fishbein, M., & Ajzen, I. (1974). Attitude toward objects as predictros of single and multiple behaviour criteria. *Psychological Review , 81*, 59-74.

Fishoff, B. (1992). Risk taking: A developmental perspective. *J.F. Yates Risk taking behavior* , pp. 132-162.

Greenwald, A. B. (1995). Implicit social cognition: Attitudes, self-esteem, and stereotypes. In P. Keith J. Holyoak, *Psychological Review* (Vol. 102 (1), pp. 4-27).

Greenwald, A., & Banaji, M. (1995). Implicit social cognition: attitudes, self esteem, and stereotypes. *Psychological Review* , 4-27.

Greenwald, A., McGhee, D. E., & Schwartz, J. (1998). Measuring individual differences in implicit cognition: The Implicit Association Test. *Journal of Personality and Social Psichology , 74*, 1464-1480.

Greenwald, A., Nosek, B., & Banaji, M. R. (2003). Understanding and Using the Implicit Association Test: I. An Improved Scoring Algorithm. *Attitudes and Social Cognition* .

Gullone, E., & Moore, S. (2000). Adolescent risk taking and the five factor model of personality. *Journal of Adolescence , 23*, 393-407.

Harward University. (2016). *https://implicit.harvard.edu/implicit/takeatest.html.* (H. U. Edu, Producer) Retrieved December 19, 2016, from https://implicit.harvard.edu/implicit/takeatest.html: https://implicit.harvard.edu/implicit/takeatest.html

Holey, R. S., Palmgreen, P., Pugzels Lorch, E., & Donohew, R. (2002). Reliability and validity of a brief measure of sensation seeking. *Personality and Individual Differences , 32*, 401-414.

Hull, C. (1943). Principle of behaviour. *Appleton-Century-Crofs* .

InternationalCommunicationTelecommunication. (2015). Retrieved from ITU: www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

InternetSociety. (2012). *Some Perspectives on Cybersecurity: 2012*. Retrieved from Internet Society: www.internetsociety.org/doc/some-perspectives-cybersecurity-2012.

Landy, D., & Sigall, H. (1974). Beauty is talent: Task evaluation as a function of the performer's physical attractiveness. *Journal of Personality and Social Psychology , 29*, 299-304.

Little, H. (2006). Children's risk taking behaviour: implications for early childhood policy and practice. *International Journal of Early Years Education* , 141-154.

Livingstone, S. (2014). Developing social media literacy: how children learn to interpret risky opportunities on social network sites. *LSE Research Online , 39* (3), 283-303.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the Internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries.* Deliverable 4, LSE Research Online, London School of Economics and Political Science, London.

Mascheroni, G., & Ólafsson, K. (2013). Mobile internet access and use among European children. Initial findings of the Net Children Go Mobile project. Milano: Educatt. *Initial findings of the Net Children Go Mobile project* .

Mascheroni, G., & Haddon, L. (2015). Children, risks and the mobile internet. (Y. Z. (Ed.), Ed.) *Encyclopedia of Mobile Phone Behavior* , pp. 1409-1418.

May, M., & Doob, L. (1937). Competition and cooperation. *Social Science Research Council* .

Morrongiello, B., & Lasenby, J. (2006). Finding the daredevils: Development of a sensation seeking scale for children that is relevant to physical risk taking. *Accident Analysis and Prevention , 38* (6), 1101-1110.

Onodera, T., & Miura, M. (1990). Physical attractiveness and its halo effects on a parner: 'Rating beauty' in Japan also? *Japanes Psychological Research , 32*, 148-153.

Osgood, C., Suci, G., & Tannenbaum, P. (1957). The measurement of meaning. *University of Illinois Press* , 189.

Regulation (EU)679. (2016, April 27). *eur-lex.europa.eu/.* Retrieved from eur-lex.europa.eu: eur-lex.europa.eu

Sarnoff, I. (1960). Psychoanalytic theory and social attitudes. *Public Opinion Quarterly , 24*, 251-279.

Sjoberg, L. (1999). The psychometric paradigm revisited. *Royal Stat. Society Conference.* Warwick: July, 12-15.

Taddei, S., & Contena, B. (2013). Privacy, Trust and Control: Which Relationships With Online Self-Disclosure? . *Computers in Human Behavior* , 821-826.

Thorndike, E. (1920). A constant error in psychological ratings. *Journal of applied Psychology , 4*, 25-29.

Thurnstone, L. (1931). The measurement of attitudes. *Journal of Abnormal and Social Psychology , 26*, 249-269.

Trepte, S., & Reinecke, L. (2013). The Reciprocal Effects of Social Network Site Use and the Disposition for Self-Disclosure: A Longitudinal Study. *Computers in Human Behaviours , 29* (3), 1102-1112.

Vasalou A., J. A. (2014, July). Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the American Society for Information Science and Technology* , p. 23.

Vuorikari, R., Punie, Y., Carretero, S., & Van den Brande, L. (2016). *DigComp 2.0: The Digital Competence Framework for Citizens.* Publications Office of the European Union.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review* , 193-220.

Weber, R., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review , 32*, 715 - 728.

Wilson, M., & Daly, M. (1985). Competitiveness, risk-taking, and violence: the young male syndrome. *Ethnology and Sociobiology , 6*, 59-73.

Zanna, M., & Fazio, R. (1982). The attitude-behaviour relation: Moving toward a third generation of research. (E. H. M.P. Zanna, Ed.) *Consistency in social behaviour: The Ontario Symposium , 2*, 283-301.

Zuckerman, M. (1991). Psychobiology of personality. *Cambridge University Press* .

Zuckerman, M., Kolin, E., Price, L., & Zoob, I. (1964). Development of a sensation-seeking scale. *Journal of Consulting Psychology , 28* (6), 477-482.

List of abbreviations and definitions

BSSS	Brief Sensation Seeking Scale
CSQ	Cyber security Questionnaire
DESI	Digital Economy and Society Index
DigComp	Digital Competence Framework
E-CIT	Empowering Citizens' rights in emerging Information and Communications Technology
EU	European Union
GDPR	General Data Protection Regulation
HOL	Happy Onlife
IAT	Implicit Association Test
ICT	Information and Communication Technology
IPTS	Institute for Prospective Technological Studies
JRC	Joint Research Centre
MOOCs	Massive Open Online Courses
NIS	Network Information Systems directive
UCD	User Centred Design
USB	Universal Serial Bus
UTIU	Uninettuno Telematics International University
ZOPED	Zone of Proximal Development

List of figures

List of tables

Annexes

Annex 1. Letter to the school headmaster

Alla cortese attenzione del
Dirigente Scolastico
della Scuola Manfredini
Via Dalmazia 55, 21100 Varese
(VA)

Gentile Dirigente,
stiamo effettuando una ricerca sulla propensione ai rischi connessi alla sicurezza digitale in ragazzi delle scuole elementari e medie, che prevede la somministrazione di alcuni semplici questionari e divertenti test al computer, oltre ad attività con il gioco ludo-educativo Happy Onlife.
La somministrazione verrà effettuata dalle ricercatrici del 'Joint Research Centre of the European Commission' Rosanna Di Gioia, Monica Gemo, supervisionate dalla Prof.ssa Ileana Di Pomponio, cattedra di 'Analisi dei Dati' presso l'Università Telematica Internazionale Uninettuno.
La somministrazione avverrà in un luogo tranquillo, durante l'orario scolastico e durerà indicativamente 60 minuti. La presentazione e l'esperienza di gioco con Happy Onlife richiederà ulteriori 60 minuti.
La raccolta dei dati è anonima, i dati raccolti saranno trattati in modo aggregato per fini di ricerca scientifica.
Pur trattandosi di una raccolta dati anonimi, sarà rispettata rigorosamente la privacy dei soggetti e i dati saranno trattati ai sensi del d.lgs. 30 giugno 2003 n.196 'Codice in materia di protezione dei dati personali' e alle norme vigenti per le istituzioni europee (Regolamento Europeo 45/2001/EC).
In ogni caso siamo disponibili ad esporre la ricerca e i suoi risultati.
Le chiediamo a tale scopo di farsi carico della raccolta del consenso parentale degli alunni della scuola che dirige e di provvedere alla conservazione delle autorizzazioni firmate dai genitori.

Autorizzo la realizzazione della ricerca nelle Scuola Manfredini. La ricerca si svolgerà dietro la supervisione della Prof. Ileana Di Pomponio.

Firma _____ Data_____

La ringraziamo della preziosa collaborazione.

Ispra, xx/xx/2016

Rosanna Di Gioia e Monica Gemo

rosanna.di-gioia@jrc.ec.europa.eu, monica.gemo@jrc.ec.europa.eu

European Commission — Joint Research Centre (JRC)
Cyber and Digital Citizens' Security Unit
Via Fermi 2749
I-21027 Ispra

Il docente responsabile della ricerca

Dott.ssa Ileana Di Pomponio, PhD

UTIU Università Telematica Internazionale Uninettuno
Facoltà di Psicologia — Corso Psicometria ed Analisi dei dati
Facoltà di Psicologia — Corso Teorie e Strumenti della Valutazione Psicosociale
Facoltà di Psicologia — Corso Analisi dei dati

i.dipomponio@uninettunouniversity.it

Annex 2. Parental informed consent authorising child's participation in the research

Gentile Genitore,

Per conto del 'Cyber and Digital Citizens' Security Unit of the Joint Research Centre of the European Commission' e del Dipartimento di Psicologia dell'Università Telematica Internazionale 'Uninettuno' stiamo conducendo una ricerca sui bambini delle scuole elementari e medie; vorremmo indagare il modo in cui i bambini riescono a percepire i rischi connessi alla sicurezza digitale e quanto influisce la propensione individuale nello studio degli atteggiamenti dei ragazzi di 10-12 anni verso i rischi connessi alla sicurezza digitale.

La nostra indagine prevede che ciascun bambino partecipi ad un incontro in cui gli viene chiesto di rispondere a delle semplici domande e di partecipare attivamente ad una sessione di gioco con lo strumento ludo-educativo Happy Onlife. in cui si approfondiscono gli usi dei nuovi media, insieme alla consapevolezza sui rischi in materia di privacy, sicurezza e anti cyber-bullismo.

La prova si svolgerà all'interno della scuola, con la collaborazione di un'insegnante, e non sarà impegnativa per il bambino. La sua durata sarà di circa un'ora per ciascun bambino. L'attività ludo-educativa Happy Onlife avrà una durata di un'ora circa.

Le chiediamo, cortesemente, la sua fiducia e il consenso per la partecipazione di suo/a figlio/a all'attività.

Teniamo a farle presente che l'interesse della nostra ricerca è puramente conoscitivo: speriamo di ottenere informazioni utili anche a livello educativo. I risultati che saranno ottenuti, non saranno utilizzati se non per scopi di valutazione strettamente pertinenti l'attività di ricerca, e quindi non saranno mirati ad ottenere informazioni personali. In ogni caso, sarà garantito l'anonimato dei bambini.

La raccolta dati è anonima, i dati raccolti saranno trattati in modo aggregato nel rispetto della legge sulla privacy.

Lei, Suo figlio o Sua figlia potrete decidere id abbandonare lo studio in ogni momento comunicando la richiesta al preside insieme ai codici identificativi della raccolta dati (numeri di id e di gruppo). Firmando il modulo di autorizzazione non rinuncia ad alcun diritto legale che può avere un partecipante in questo studio.

AUTORIZZAZIONE

Nome del Bambino _____

Autorizzo mio/a figlio/a a partecipare alla ricerca coordinata dal 'Cyber and Digital Citizens' Security Unit of the Joint Research Centre of the European Commission' e dal Dipartimento di Psicologia dell'Università Telematica Internazionale Uninettuno.
La ricerca si svolgerà dietro la supervisione della Prof. Ileana Di Pomponio.

Si
No

Firma_____ Data_____

La ringraziamo della preziosa collaborazione.

Rosanna Di Gioia e Monica Gemo

rosanna.di-gioia@jrc.ec.europa.eu, monica.gemo@jrc.ec.europa.eu
European Commission — Joint Research Centre (JRC)
Cyber and Digital Citizens' Security Unit
Via Fermi 2749, 21027 Ispra

Il docente responsabile della ricerca

Dott.ssa Ileana Di Pomponio, PhD
UTIU Università Telematica Internazionale Uninettuno
Facoltà di Psicologia — Corso Psicometria ed Analisi dei dati
Facoltà di Psicologia — Corso Teorie e Strumenti della Valutazione Psicosociale

i.dipomponio@uninettunouniversity.it

Annex 3. JRC privacy statement for processing Happy Onlife contact lists

Specific privacy statement
E-CIT project contact lists and network partners database at the JRC/IPSC

1. Description
The processing of personal data concerns:
— the description of a contact list holding postal and/or telematics address details of individuals or organisation-related persons;
— the description of an information database about stakeholders and partners cooperating in scientific research networks.
This processing is managed at the Joint Research Centre (JRC) by the Institute for the Protection and Security of the Citizen (JRC/IPSC) in relation with the JRC research project E-CIT for the purpose mentioned under point 2.

As this processing collects and further processes personal data, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data is applicable.
The head of unit of customer and stakeholders relations acts as a controller of the processing of personal data covered by the generic notification 'Contact lists and network partners databases at the JRC' (DPO-1924).
The coordinator (e.g. head of unit) of the JRC/IPSC manages the processing itself under the responsibility of their director who acts as a processor.

2. What personal information do we collect, for what purpose and through which technical means?

Identification data

Data contained in contact lists such as:
— for postal address details: name/surname, title, company name, private/professional address, etc.;
— for telematics address details: name/surname, title, phone/fax/email/website, etc.
Data contained in contact information databases such as:
— name/surname, place/date of birth, nationality, company name, office/mobile phone numbers;
— fields of interest, preferred/default language, information distribution format desired (for publications), etc.

Purpose

Personal data are collected and processed in order to communicate with the data subjects about the JRC research activities related to the E-CIT.

Technical information

Personal data are normally collected through classical databases or Excel forms and stored on JRC servers.

3. Who has access to your information and to whom is it disclosed?

Access to the personal data is allowed to authorised officials and other staff of the JRC. No personal data is transmitted to parties outside the recipients and the legal framework mentioned.

4. How do we protect and safeguard your information?

The collected personal data are stored on the servers of JRC and are processed complying with Commission Decision C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission defining IT security measures in force. Annex I defines the security requirements of the European Commission's information systems. Annex II defines the different actors and their responsibilities. Annex III defines the rules applicable by users.

5. How can you verify, modify or delete your information?

The data subject can send a message to the controller or to the address mentioned under 'Contact information' by explicitly specifying their request to have their personal data modified or deleted. Special attention is drawn to the consequences of a delete request, in which case any trace to be able to contact the data subject will be lost.

6. How long do we keep your data?

All personal data will be deleted at the end of the E-CIT, which is scheduled for the end of 2017.

7. Contact information

In case you have questions related to this processing or concerning any information processed in this context, or on your rights, feel free to contact:

— the JRC controller or the JRC processor using the address mentioned on the announcement page, questionnaire form or web page;

— the JRC Data Protection Coordinator: jrc-data-protection-coordinator@ec.europa.eu;

— the Commission's Data Protection Officer: data-protection-officer@ec.europa.eu.

8. Recourse

Complaints, in case of conflict, can be addressed to the European Data Protection Supervisor: edps@edps.europa.eu.

Annex 4. Happy Onlife questionnaire

QUESTIONARIO per la VALUTAZIONE della PERCEZIONE DEL RISCHIO di bambini (10-12 anni) verso una NAVIGAZIONE ON-LINE SICURA/INSICURA
L'ESPERIENZA Happy Onlife

Ciao e grazie per aver accettato di partecipare a questa ricerca!
In questo modo ci aiuterai a capire gli atteggiamenti di bambini e ragazzi nei confronti dei rischi che si possono incontrare online.
Il tuo contributo è veramente importante. Ti chiediamo di rispondere in maniera onesta.

DATI ANAGRAFICI

1. Quanti anni hai?
8 9 10 11 12

2. Sei un/a
Maschio Femmina

3. Quali attività svolgi online?

□ Gioco □ Comunicazione (E-mail, Skype, WhatsApp, ...)
□ Social Network (FB, Instagram, ...) □ Informazione (Ricerca, Lettura, Youtube, ...)
□ Altro

4. Quali dispositivi utilizzi online?
□ Smartphone □ Tablet □ PC □ Smart TV □ Smartwatch
□ Game console (Wii, PS, Nintendo, ...) □ Altro

5. Quante ore al giorno utilizzi per connetterti online?

□ 1 □ 2 □ 3 □ 4 □ 5 6 □ 7 □ 8 □ 9 □ 10 □

6. A quanti anni hai iniziato a usare internet?
□ Non lo uso 0□ 1□ 2□ 3□ 4□ 5 □ 6□ 7□ 8□ 9□ 10□ 11□ 12□

MACRO AREA 'RESTA CONNESSO!'

7. Secondo te quanto è rischioso pubblicare i propri dati personali (nome, cognome, indirizzo, ...) online?
□ Per nulla □ Poco □ Abbastanza □ Molto

1 2 3 4

8. Secondo te quanto è rischioso pubblicare le proprie fotografie online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

9. Secondo te quanto è rischioso pubblicare online i dati personali di altre persone?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

10. Secondo te quanto è rischioso pubblicare online le immagini di altre persone?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

11. Secondo te quanto è rischioso copiare e incollare informazioni trovate in internet?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

MACRO AREA 'FERMA IL BULLO ON LINE!'

12. Secondo te quanto è rischioso provocare qualcuno online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

13. Secondo te quanto è rischioso insultare qualcuno online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

14. Secondo te quanto è rischioso essere testimone di provocazioni e o insulti online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

15. Sai cos'è il cyber-bullismo? Indica la frase che ti sembra più corretta.

□ una nuova app. che permette di realizzare animazioni in ambienti di realtà virtuale
□ insieme di comportamenti intenzionali, mirati e ripetuti a scopo di danneggiare fisicamente e/o emotivamente una o più persone, che si trovano a volte in posizioni di debolezza e/o fragilità
□ sono due ragazzi/e che litigano, a volte facendo anche a botte
□ è un reato punibile solo dalla polizia cyber

16. Secondo te quanto è rischioso essere accusato di cyber-bullismo?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

17. Secondo te quanto è rischioso non segnalare chi ti manda messaggi spiacevoli online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

18. Secondo te quanto è rischioso fingere di essere un'altra persona online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

MACRO AREA ‘GIOCA SICURO!’

19. Secondo te quanto è rischioso scaricare dei giochi dai siti illegali presenti online?
□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

20. Secondo te quanto è rischioso usare il proprio nome o cognome mentre giochi online?
□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

21. Secondo te quanto è rischioso usare la geo-localizzazione mentre giochi online?
□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

22. Secondo te quanto è rischioso scaricare da internet (siti illegali) musica e film gratuitamente?
□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

23. Secondo te quanto è rischioso video-giocare per diverse ore senza interruzioni?
□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

MACRO AREA ‘IN GUARDIA!’

24. Secondo te quanto è rischioso incontrare realmente qualcuno che hai conosciuto solo online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

25. Secondo te quanto è rischioso aprire messaggi pubblicitari e pop-up online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

26. Secondo te quanto è rischioso non curarsi delle impostazioni di privacy (privacy settings) delle applicazioni usate online?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

27. Secondo te quanto è rischioso non usare anti-virus per i propri dispositivi?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

28. Secondo te quanto è rischioso iscriversi o aprire profili in social network (FB, Whatsup, ecc)?

□ Per nulla □ Poco □ Abbastanza □ Molto
1 2 3 4

29. Secondo te quanto è rischioso dire la propria password ad altri?

□ Per nulla □ Poco □ Abbastanza □ Molto

1 2 3 4

Annex 5. Happy Onlife leaflet

HAPPY ONLIFE

Together in the digital world!

Happy Onlife is an edutainment toolkit conceived by the **Joint Research Centre** of the European Commission promoting a safe and responsible use of Internet among children and adults. It is also used to raise awareness on online safety risks for privacy, cyber security and cyberbullying.

It is available as paper version (EN, IT) and digital application for mobile and web platforms (EN, FR, IT, NL, ES).

Download Happy Onlife from Apple iTunes, Google Play and Windows Phone stores.

Happy Onlife on JRC Science Hub:
http://europa.eu/!pD47hy

Privacy and online safety

Improving privacy, safety awareness and skills

Happy Onlife is the product of research supporting EU policy and awareness raising strategies on online opportunities and risks.

The game and toolkit are proposed as work in progress to be extended with the contributions of all stakeholders (adults and children). It applies innovative research methods for formal, informal and participatory education in the use of digital technologies with children aged between **8 and 12 years**.

Playful empowerment

Empowering children and adults for a safe and responsible use of ICT

Playful sharing of digital life experiences to open up the **intergenerational dialogue.**

Edutainment tools developed under user-centred, participatory and multi stakeholder approaches with **active mediation among actors**: young citizens, parents, school and childhood professionals, civil society and institutions.

Digital skills

Enhancing digital skills individually and collectively

Through active and creative appropriation, community engagement, active mediation of **adults to children** and reverse mediation of **children to adults** enhancing **digital skills** on:

- Information and data processing
- Communication
- Content creation
- Safety
- Problem solving

HAPPY ONLIFE

The toolkit

The toolkit is designed to prompt discussion and to drive the actors towards a responsible and safe way of using digital media.

Happy Onlife promotes positive engagement, mediation, dialogue enhancing digital competences especially in **privacy**, **online safety**, **netiquette** and **digital identity** management.

The digital toolkit is under release with open-source EUPL licence (European Union Public Licence).

Happy Onlife JRC report:
http://europa.eu/!FD84FK

The Happy Onlife toolkit is a paper '**toolbox**' with a number of **resources**:

- a game with 40 challenge cards, 10 'Stop Online bullying!' cards, 10 'Let's Chat' cards, 10 'Watch-Out!' cards and 10 'Play Safely' cards;
- four 'Powercards' summarising the golden rules for a responsible and safe use of Internet;
- a set of 17 'Extra Activities' cards collecting ideas for home or school projects. These are also referenced in the project booklet promoting digital competences and shared experiences of the digital world among teachers, parents and children between 8-12 years old;
- stickers and emoticons commonly used in the digital world.

The toolkit also includes a digital version of the Happy Onlife game and complementary resources.
It is available on **mobile** platforms (**iOS**, **Android** and **Windows Phone**) and on desktop computer or smartboard through the web.

Schools can either request a free copy of the box in English and Italian (limited to available stock) at this e-mail address:

jrc-e3-secretariat@ec.europa.eu

or download, print and cut out a Do-It-Yourself copy in English and Italian at:

http://europa.eu/!pD47hy

Link to the web application:

http://web.jrc.ec.europa.eu/happyonlife

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

KJ-NA-28401-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/752186
ISBN 978-92-79-64955-4