Horizon 2020 Programme

H2020-SU-TDS-02-2018
Trusted digital solutions and Cybersecurity in Health and Care

ProTego

DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND CARE CENTERS

Project Nº 826284

ProTego

D3.2 Initial description of educational framework: Protocols and methodologies for health staff and patients

Responsible:	MS (Salvador Garcia)
Contributors:	MS, OSR, Gfi, IBM, KUL
Document Reference:	D3.2
Dissemination Level:	Public
Version:	1.0
Date:	29/06/2020

Executive summary

This document contains the initial description of the Educational framework developed as part of the ProTego project. It offers an overview of what should be the process of implementation of cybersecurity in a healthcare organization. Among the different aspects and phases, it focalizes in those referred to user awareness, explaining in detail a user awareness training program created as part of ProTego and that will be deployed in MS and OSR. This awareness training program has been designed in alignment to the conclusions of the Deliverable 3.1 within this project and is intended to improve situational awareness and increase the good behaviours in terms of cybersecurity. It is based on the people centric security paradigm and aims to achieve that users apply cybersecurity principles in any situation even outside the work environment.

ProTego includes the development of a technical toolkit that will reduce cybersecurity risks. Regarding that toolkit this educational framework will describe how this toolkit is aligned with the cybersecurity standards: based on the NIST CSF the items that the ProTego toolkit helps to accomplish have been identified.

The final version of the educational framework will also include the protocols for a correct use of this toolkit in two different scenarios, one first developed by OSR as a model of a typical on premise installation of the toolkit, and a second one developed in MS as a model of the use of the toolkit in a hybrid cloud. The educational framework will not only be limited to the ProTego toolkit but will include relevant elements on each use case as well, offering replicable models that can be easily adapted to almost any other healthcare organization.

Contributors Table

DOCUMENT SECTION	AUTHOR(S)	REVIEWER(S)
¡Error! No se encuentra el origen de la referencia.	Pietro Vismara (OSR) Salvador Garcia (MS)	Antonio Jesús Gamito González (GFI), Ubaldo Hidalgo Arriaga (GFI), Luis Carrascal Crespo (GFI), María Pérez Ortega (GFI), Kostas Kouvaris (IT Innov)
II	Antonio Jesús Gamito (GFI), Dave Singelee (KUL), Eliot Salant (IBM), Salvador Garcia (MS)	Antonio Jesús Gamito González (GFI), Ubaldo Hidalgo Arriaga (GFI), Luis Carrascal Crespo (GFI), María Pérez Ortega (GFI), Kostas Kouvaris (IT Innov)
III	Vicent Moncho (MS) Salvador Garcia (MS)	Antonio Jesús Gamito González (GFI), Ubaldo Hidalgo Arriaga (GFI), Pietro Vismara (OSR), Luis Carrascal Crespo (GFI), María Pérez Ortega (GFI), Kostas Kouvaris (IT Innov)
IV, V, VI, VII	Salvador Garcia (MS)	Antonio Jesús Gamito González (GFI), Ubaldo Hidalgo Arriaga (GFI), Luis Carrascal Crespo (GFI), María Pérez Ortega (GFI), Kostas Kouvaris (IT Innov)

Table of Contents

Table of Figures

List of tables

Table of Acronyms and Definitions

Acronym / Definition	Explanation
BYOD	Bring Your Own Device
CDSS	Clinical Decision Support System
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer

COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations
EMAR	Electronic Medical Administration Record
EMR	Electronic Medical Record
EMRAM	Electronic Medical Record Adoption Model
ENISA	European Union Agency for Network and Information Security
ENS	Spanish National Security Framework
FDPA	French Data Protection Act
GDPR	General Data Protection Regulation
ICT	Information and Communications Technologies
IO(M)T	Internet Of Medical Things
IS	Information Security
ISMS	Information Security Management System
MS	Marina Salud
NIS	EU Network and Information Security directive
NIST CSF	NIST Cyber Security Framework
NIST	National Institute of Standards and Technology
OSR	Ospedale San Raffaele
PCS	People-Centric Security
USC	User Support Centre

I. Overview of ProTego Educational Framework

I.1. Background

The ProTego project will provide a toolkit for health care organizations to better assess and reduce cybersecurity risks related to remote devices access to Electronic Health Record data, including risks assessment and risks mitigation tools as well as methodologies and protocols for prevention and reaction. In addition, the toolkit will provide tools to raise awareness and educate stakeholders in how they can reduce or prevent risks.

This stakeholder education is crucial, especially if we consider non IT personnel, mostly clinical but also administrative. After all, it has been demonstrated that people are the weakest link of an organization's security and they are the most exploited vulnerability by attackers.

Although it is feasible to compose and distribute protocols and work instructions explaining the correct use of the tools and systems from the cybersecurity perspective, the reality is that all those protocols are perceived by health staff as technical material treating technical issues that are, hence, responsibility of the IT department. Furthermore, any protocol or work instructions set cannot cover all existing risks in a changing environment that offers new functionalities every day, such as BYOD, IO(M)T, telemedicine and remote patient care through cloud services. And all under the mandatory requirement of interoperability that on the one hand allows the existence of a unified EMR whose benefits are out of the scope of this document, but on the other hand offers attack vectors to reach many interconnected systems.

Therefore, the educational framework defined in ProTego has as fundamentals the following objectives for each target audience:

- healthcare industry: to describe the adherence to the cybersecurity standards of the ProTego toolkit. Choosing the NIST CSF [7] as reference the document elicits which items are facilitated by the toolkit (Section II).

- healthcare staff and patients: to improve situational awareness of healthcare staff and patients, increasing correct behaviours regarding cybersecurity and making them more receptive to future recommendations or protocols (Section IV and V).

- healthcare IT and external providers: to create recommendations and good practices regarding cybersecurity in the implementation of novel and trendy mechanisms that allow to broaden patients care and surveillance of population’s health (Section V; the recommendations for external providers to create ProTego compliant tools will be included in Section VI).

These recipients are described in more detail in section I.2.

I.2. Stakeholders

The stakeholders of the educational framework must correspond to the stakeholders of the ProTego toolkit. This is the ProTego toolkit stakeholder map resulted from the analysis performed in Deliverable 2.2:

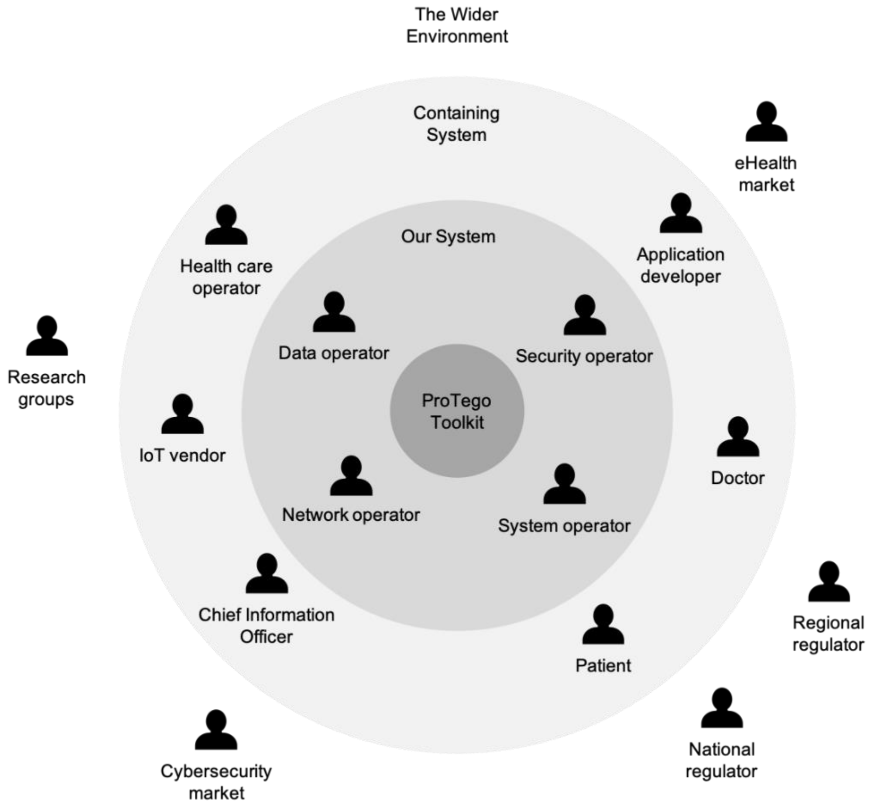


Figure 1: Stakeholder map of the ProTego toolkit

Attending to the interests, objectives and therefore type of educational material developed, this stakeholder map has been classified in five groups that conform the final stakeholder map of the educational framework.

ProTego toolkit stakeholders	Educational framework stakeholders	Description
Research groups	Health staff	Physicians, researchers, nurses, ancillary clinical personnel.
Doctors		
Patients	Patients	Patients
App developers	IT staff	Technical staff with responsibilities in the management (design, development, deployment, configuration, monitoring) of corporate applications
Healthcare operators		
CIO		
Network operators		
System operators		
Security operators		
Data operators		
eHealth market	External HW/SW providers	External HW/SW providers that need to know how to develop ProTego compliant products
IoT vendors		
Cybersecurity market	Regulators	External stakeholders interested in the compliance of ProTego toolkit with the information security standards
National Regulators		
Regional regulators		

Table 1: Educational framework stakeholders

This classification makes the list more general because although the segregation of duties and functions is a common recommendation in Information security standards, for example in control A.6.1.2 from ISO 27001:2013 [1], it is not widely applied, usually depending on the size of the organization.

I.3. Scope

The general scope of the educational framework is to provide tools to each stakeholder that contribute to reduce risks and to improve the overall security. It is necessary to define the main objectives to reach for each component of the stakeholder's map.

Health staff

Description: This group includes the most of the final users of the corporate applications and devices. They treat systematically sensitive data of patients from interconnected systems. They make use of BYOD strategies introducing risks to the working environment that were caused by behaviours in the private sphere. They don't know all the types of attacks in which they are potential victims.

Objectives: Let them know the consequences of incorrect behaviours, even from private context and with their own devices. Increase a collaborative environment with cybersecurity operators, promoting the notification of incidences and risky situations.

Patients

Description: Final users of applications offered from healthcare organizations. Lower impact in the overall security due to restricting permissions, but very low level of cybersecurity awareness. Difficult to make training reach them.

Objectives: Increase situational awareness by reaching them with concrete messages through the limited communication channels.

IT staff

Description: Technical staff with responsibilities in the management of corporate applications and the design of the technological infrastructure.

Objectives: Describe good practices regarding cybersecurity in elements that are characteristic of healthcare organizations.

Describe the management of the ProTego toolkit in two different environments from a technological point of view, represented by the FoodCoach and Pocket EHR scenarios respectively.

Describe good practices in cybersecurity regarding technological elements externals to ProTego toolkit but required to make the toolkit work in each scenario, as well.

External providers

Description: External hardware and software providers of healthcare applications and IO(M)T devices that have historically focused on clinical functionality but less in information security.

Objectives: Describe the requirements for those hw/sw elements to be ProTego compliant, that is, to be able to integrate with ProTego taking advantage of the functionalities that the toolkit offers in fields as authentication, authorization, encryption or real time monitoring.

Regulators

Description: Regulators that may have interest or responsibility derived of the fact that the healthcare organizations accomplish with international cybersecurity standards.

Objectives: Explain to what extent the toolkit is compliant with the standards, helping to perform the controls that those standards recommend.

I.4. Structure

The following figure illustrates the structure of the educational framework:

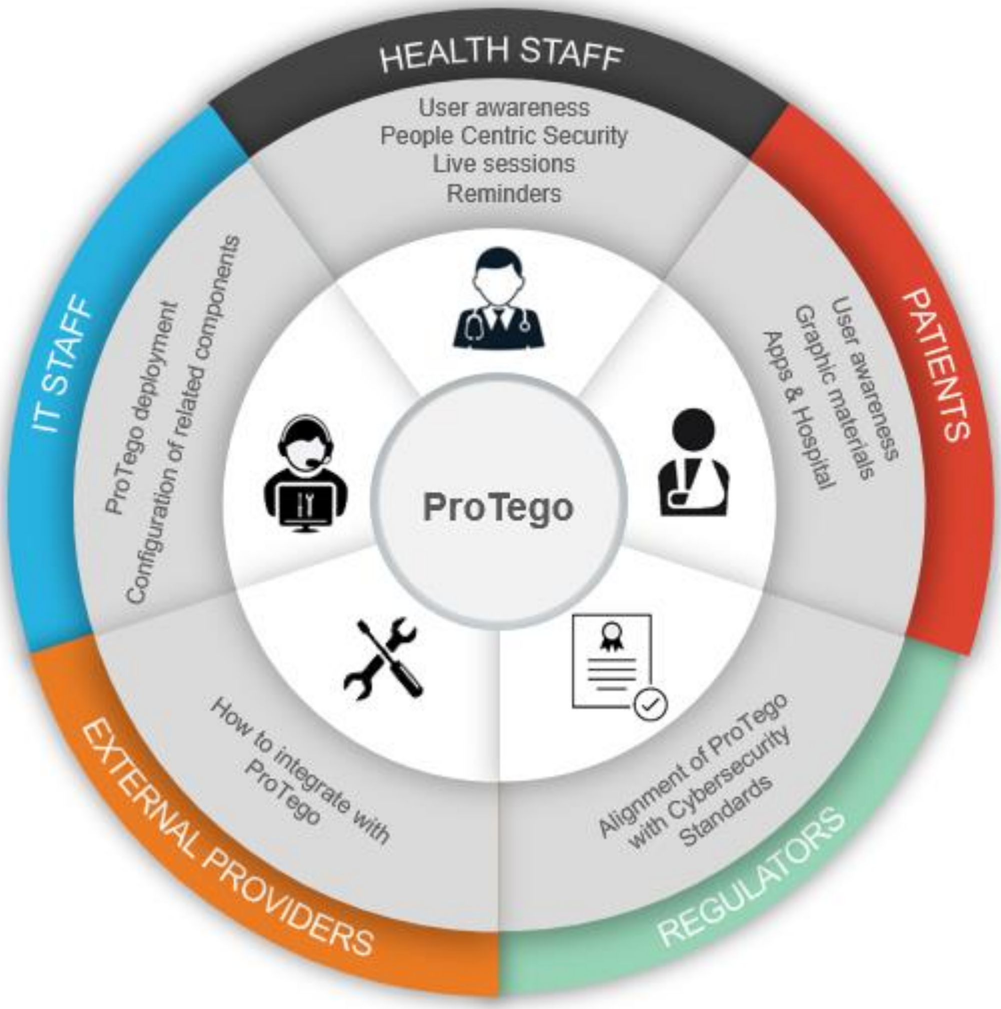


Figure 2: Structure of educational framework

The table below shows in which section of the document is included the content for each stakeholder:

STAKEHOLDER	SECTION OF THE DOCUMENT
REGULATORS	II.- Adherence to standards and regulations
HEALTH STAFF	IV-Educational material for health staff
PATIENTS	V-Educational material for patients

IT STAFF	VI-Educational material for IT staff
EXTERNAL PROVIDERS	VII-Educational material for external providers

Table 2: Stakeholders and document sections

I.5. Relation to the survey in D3.1

In Deliverable 3.1 of ProTego, a survey based on the Health Belief Model was executed to extract conclusions regarding the factors that lead users to adopt correct cybersecurity behaviours. Those conclusions have been observed for the design of the educational framework presented in this document.

The conclusions of the survey are summarised by the table below showing the hypothesis tested and the result in a binary categorical format of "SUPPORTED" / "NOT SUPPORTED":

ID	HYPHOTESIS	CONCLUSION
H1	Perceived Susceptibility (SUS) would be positively related to Cybersecurity Behaviour	NOT SUPPORTED
H2	Perceived Severity (SEV) would be positively related to Cybersecurity Behaviour	SUPPORTED
H3	Perceived Benefits (BEN) would be positively related to Cybersecurity Behaviour	NOT SUPPORTED
H4	Perceived Barriers (BAR) would be negatively related to Cybersecurity Behaviour	SUPPORTED
H5	Self-Efficacy (SEF) would be positively related to Cybersecurity Behaviour	SUPPORTED
H6	Cues to Action (CUES) would be positively related to Cybersecurity Behaviour	SUPPORTED

Table 3: Conclusions of the Health Belief Model survey in D3.1

Those conclusions have been used to focus on that factors that have been demonstrated to elicit better results in terms of good cyber security behaviours. The fact, for example, that H1 have not been supported does not mean that we don't need users to feel identified as potential victims of cyberattacks. It means that, once covered that basic objective, the more effort wasted on that subject will not be rewarded as increased levels of good behaviours.

That said, this is how each of the previous factors have been covered by the educational framework:

H1 - Perceived Susceptibility (SUS): Especially for the awareness program designed for health staff, daily situations are presented and it is explained the risk they can represent. It is mandatory that users understand that they can be used as attack vector just by performing normal behaviours.

H2 – Perceived Severity (SEV): The first block of the awareness training includes an explanation of the three main components (dimensions) of information security and which kind of impact may have a potential breach in each of them. By this, it is reinforced the concept of *perceived severity*: health staff can exactly map the potential consequences of unappropriated cybersecurity behaviours over the patient's safety. The goal behind that is to keep user's attention from the first beginning by letting them map impacts over patient's safety.

H3 – Perceived benefits (BEN): No special reference to this factor has been made. The benefits will be derived from avoiding risks.

H4 – Perceived Barriers (BAR): Mainly when speaking of non IT users (health staff) it has been an objective that the good behaviours to perform don't be perceived as complex technical matters. Almost all the recommendations are about paying attention and perform actions in feasible ways that avoid risks, so the perceived barriers have been set very low.

H5 – Self-Efficacy (SEF): Linked to the BAR factor, the objective has been that users understand how to perform correct behaviours by themselves even in their private scope.

H6 – Cues to Action (CUES): The Health Belief Model on which the survey was based posits that a cue, or trigger, is necessary for prompting engagement in health-promoting behaviours. In this framework "Reminders" have been designed to reinforce training and to improve correct behaviours among the Health Staff. These reminders come in the shape of graphic material in both paper and digital format, placed in strategic locations where can be consumed while performing other tasks and with short messages that will make the training concepts persistent in time.

In D3.1 it was also presented the *Risk Awareness Profile*, a tool that allows benchmarking of the cybersecurity awareness between different organizations or the same organization in different times. It will be used to measure in an objective way the result of the awareness training over the health staff by a second execution of the survey after the training session will be performed.

The results will be explained in D3.3 with the analysis of the main concerns covered by the Risk Awareness profile:

- Number of users that decided to voluntary participate
- Level of adherence to good cyber security behaviours
- Ability to identify potential risks
- Risk and cybersecurity awareness
- Adherence to corporate protocols
- Self-perceived IT maturity

II. ADHERENCE TO STANDARDS AND REGULATIONS

As explained further in this section the normative and regulation that healthcare organizations must follow in terms of cybersecurity is different among countries in the EU, but all those regulations have a shared aim and, thus, share concrete items and controls as well.

In addition, GDPR's recital 81 states: "*The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller*" [2], and those approved codes of conduct and certification mechanisms include international recognized standards as ISO/IEC 27000 family, NIST ST-800, COBIT, etc.

From this point of view, it is relevant to know how the ProTego toolkit is aligned with the standards and facilitates to perform the controls included.

II.1. ISMS: Incorporating information security

Every organization is a target for cyber attackers, and that's particularly true in healthcare because healthcare manages the most sensitive data and with the higher value (and price) in black market. That high value is due to its business potential as healthcare services are expensive and being able to identify potential customers would be a high valued item for companies. In addition, any other information about individuals has or may have caducity: credit card numbers, addresses, even names or passport numbers can be changed. But biometrical and medical information is stored as part of the citizen personality and accompany them forever.

In addition, healthcare information has the higher potential to cause detriments or even physically harm individuals if its security is compromised in any of its dimensions:

- **confidentiality**: the unauthorized access or diffusion of healthcare information may cause social detriments as denegation of insurances, barriers to access jobs or social discriminations.

- **availability**: the unavailability of healthcare information may preclude the adequate provision of healthcare services. This risk is higher as the organization is more IT dependent, what use to come with the process integration and efficiency. It may make impossible the provision of services or obligate to take decisions without all the required information which may lead to errors.

- **integrity**: most of the clinical decisions are taken based on antecedents and the falsification of that information may lead to wrong decision as inadequate drug prescription, wrong diagnosis, etc. That risk is getting higher with the inclusion of automated or semi-automated CDSS.

This reality explains why the cyber security is a mandatory concern in healthcare industry. But robust cyber security requires an ISMS built on three pillars: people, processes and technology.

An ISMS can be defined as "*a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. An ISMS typically addresses employee behaviour and processes as well as data and technology. It can be implemented in a comprehensive way that becomes part of the company's culture.*"[3]

By implementing an ISMS, organizations can secure information, increase resilience to cyber-attacks, and reduce the costs associated with information security

An ISMS brings these benefits to an organization:

- Secure information in all its forms: An ISMS helps protect all forms of information, whether digital, paper-based or in the Cloud.

- Increase organization's attack resilience: Implementing and maintaining an ISMS will significantly increase organization's resilience to cyber-attacks.

- Manage all information in one place: An ISMS provides a central framework for keeping organization's information safe and managing it all in one place.

- Respond to evolving security threats: Constantly adapting to changes both in the environment and inside the organization, an ISMS reduces the threat of continually evolving risks.

- Reduce costs associated with information security: Thanks to the risk assessment and analysis approach of an ISMS, organizations can reduce costs spent on indiscriminately adding layers of defensive technology that might not work.

To implement an ISMS, each organization has to choose a standard specification that serves as guide, and the most spread is the ISO 27001. Neither the concept of ISMS nor the ISO27001 are healthcare exclusives, but it is an accepted evidence that healthcare sector needs special consideration due to its particularities regarding criticism and risk level.

To address these peculiarities, specific branches of the standards are being created specific to this sector. That's the case of ISO that has branched ISO 27002 (Best practices in cyber security) into ISO 27799 (Best practices in cyber security in healthcare).

But healthcare has another significant difference: in the EU it is a business sector that in most cases is considered a public service and as consequence it is directly dependent on the public administration of each state. That has impact on the cyber security as well because in some countries the government states the standards and regulations they must follow. Those specific regulations are aligned with the International standards but have different structure and content. In other words, they are not contradictory to the standards.

As an example, in Spain any public administration, including healthcare organizations, is required to accomplish the ENS (Spanish National Security Framework). In France any chosen regulation needs to be aligned with the FDPA (French Data Protection Act). While, in other countries there is no need to follow additional regulations added to the selected standard framework, but there is still to choose one framework among all the possibilities: ISO / IEC 27001, COBIT, COSO guidelines, or NIST SP 800-53, just to name a few.

Resuming, although all the regulations are aligned and share objectives, recommendations and controls, there is not any standard that can serve as unique reference to implement an ISMS in all the EU healthcare organizations.

When an Information Security Officer plans the strategy for managing the risks associated with the information assets of his organization, he is faced with a decisive question that will define the course of protection actions in the future: What framework of reference should be used to ensure the coordinated management of security controls in an optimal, scalable and integrable way?

However, if one wanted to take advantage of the best of each of these frameworks, the best practices and methodologies in the industry and the experience of hundreds of volunteers in order to establish a consistent and practical line of work to address the risks of current cybersecurity, most likely the choice would be the NIST Cybersecurity Framework (hereinafter CSF).

II.2. NIST CSF

II.2.1. Background

As a result of the increasing number of computer attacks on critical infrastructure systems and the impact that such attacks could have in the context of United States national security, on February 12, 2013 President Barack Obama drafted the Executive Order (EO) of Critical Infrastructure Cybersecurity Improvement [4] where the NIST was delegated the development of a framework for the reduction of risks associated with this type of environments, with the support of the Government, industry and users.

The result of this work - after the publication of multiple preliminary versions and receipt of contributions from volunteers through the Request for Information (RFI) model - was the first version of the document "Framework for Improving Critical Infrastructure Cybersecurity", known as "NIST Cybersecurity Framework" which was released on February 12, 2014.

At the same time (2013) in the European Commission, ENISA first introduced the Network and Information Security (NIS) Directive [5] but it required to align 28 different sets of national cybersecurity agendas, and of securing a common view from a European Parliament that has somewhere between four and six major party groups, took considerably longer than the gestation of the Framework.

That's because the NIS directive started the implementation phase in 2017, and as of April 2020 it is still not possible to find any concrete content that can serves as a guide to implement any ISMS in an organization. The European directive entered in force in August 2016 and it has been transposed into each's EU member, but those transpositions are enumerations and brief descriptions of lines of action at high country levels, that are more oriented to national cyber security as global than to offer resources that a single company or organization can use. Some examples can be found following the links in the above table [6]:

EU MEMBER	LINK TO NIS TRANSPOSITION
Spain	https://www.dsn.gob.es/es/file/932/download?token=9-T_SSTE
Italy	https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
France	https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Table 4: Examples of EU NIS transpositions

Meanwhile, the NIST CSF was undergoing its first major revision in 5 years based on changes in threat and experiences of global adopters.

In this situation, NIST CSF is the chosen framework to base the adherence to standards of the ProTego project.

II.2.2. Structure and implementation

The bases of the NIST CSF were established as the following:

1. Identify security standards and guidelines applicable across the board to all critical infrastructure sectors
2. Establish a common language to manage cybersecurity risks
3. Provide a prioritized, flexible, repeatable, neutral, performance-based and cost-effective approach based on business needs
4. Help managers and operators of critical infrastructure to identify, inventory and manage computer risks
5. Establish criteria for defining metrics to monitor performance in implementation
6. Establish controls to protect intellectual property, the privacy of individuals and civil liberties when cybersecurity activities are carried out
7. Identify areas for improvement that can be managed through future collaborations with particular sectors and organizations oriented to the development of standards

8. Do not introduce new standards when there are already developed initiatives that cover the objectives of the executive order.

And is the 8th point which promotes the link between other standards, as the subcategories (lower level elements) point to controls to be performed, that can be conducted with the preferred standard (ISO, COBIT, NIST 800). Therefore, an organization does not need to adhere fully and only to one standard using all its defined controls, but it is allowed to choose the most suitable standard to perform each control, among the following:

- Control Objectives for Information and Related Technology (COBIT)
- Council on Cyber Security (CCS) Top 20 Critical Security Controls (CSC)
- ANSI / ISA-62443-2-1 (99.02.01) -2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI / ISA-62443-3-3 (99.03.03) -2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- ISO / IEC 27001: 2013, Information technology --Security techniques --Information security management systems --Requirements
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

To better understand how it works:

Framework Core

It is a set of cybersecurity activities, expected results and applicable references that are common to critical infrastructure sectors, in terms of industry standards, guidelines and practices that allow the communication of cybersecurity activities and their results throughout the organization, from the executive level to the implementation / operation level.

To do this, it uses five fundamental functions:

Identify: Identify the organization's systems, assets, data and competencies, its business context, the resources that support critical functions and cybersecurity risks that affect this environment.

Protect: Protects and implements the necessary countermeasures and safeguards to limit or contain the impact of a potential cybersecurity event.

Detect: Allows to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event through continuous monitoring.

Respond: Allows the definition and deployment of activities to react to an identified cybersecurity event and mitigate its impact.

Recover: Allows the deployment of activities for resilience management and the return to normal operation after an incident.

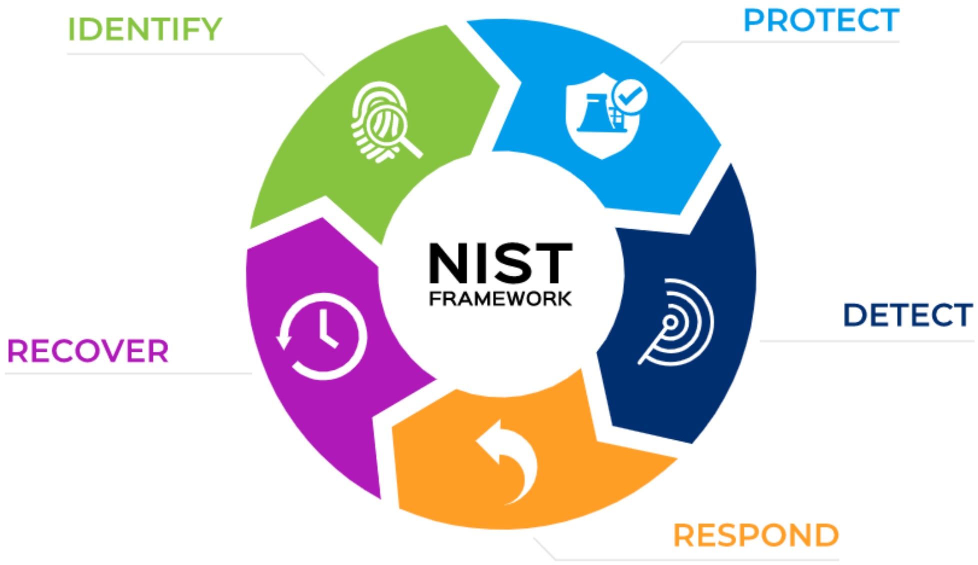
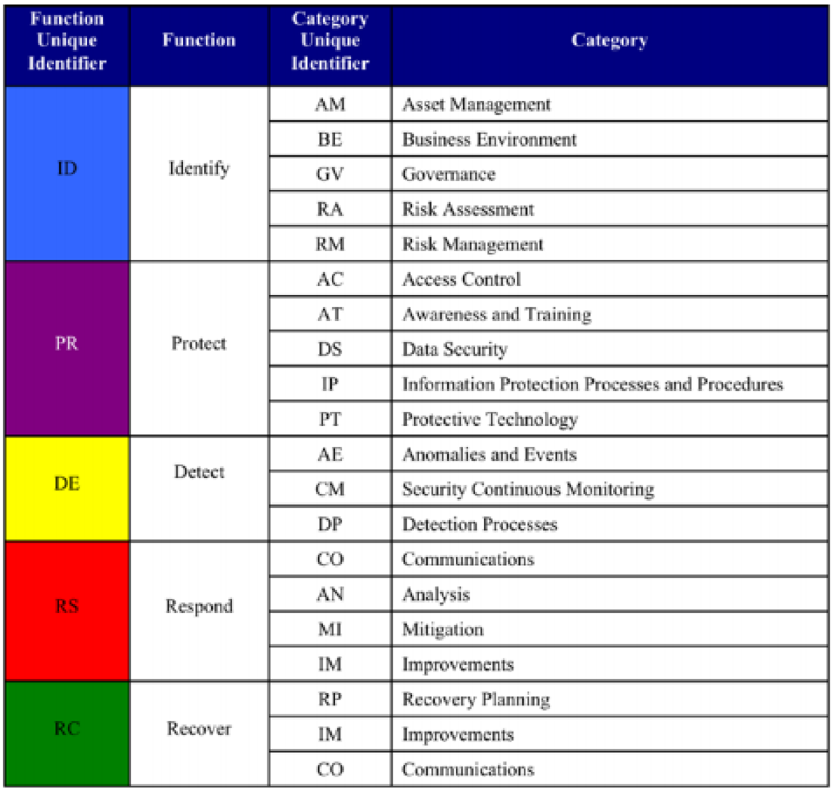


Figure 3: NIST CSF Functions

In turn, each of these functions is divided into categories as shown in the above figure:

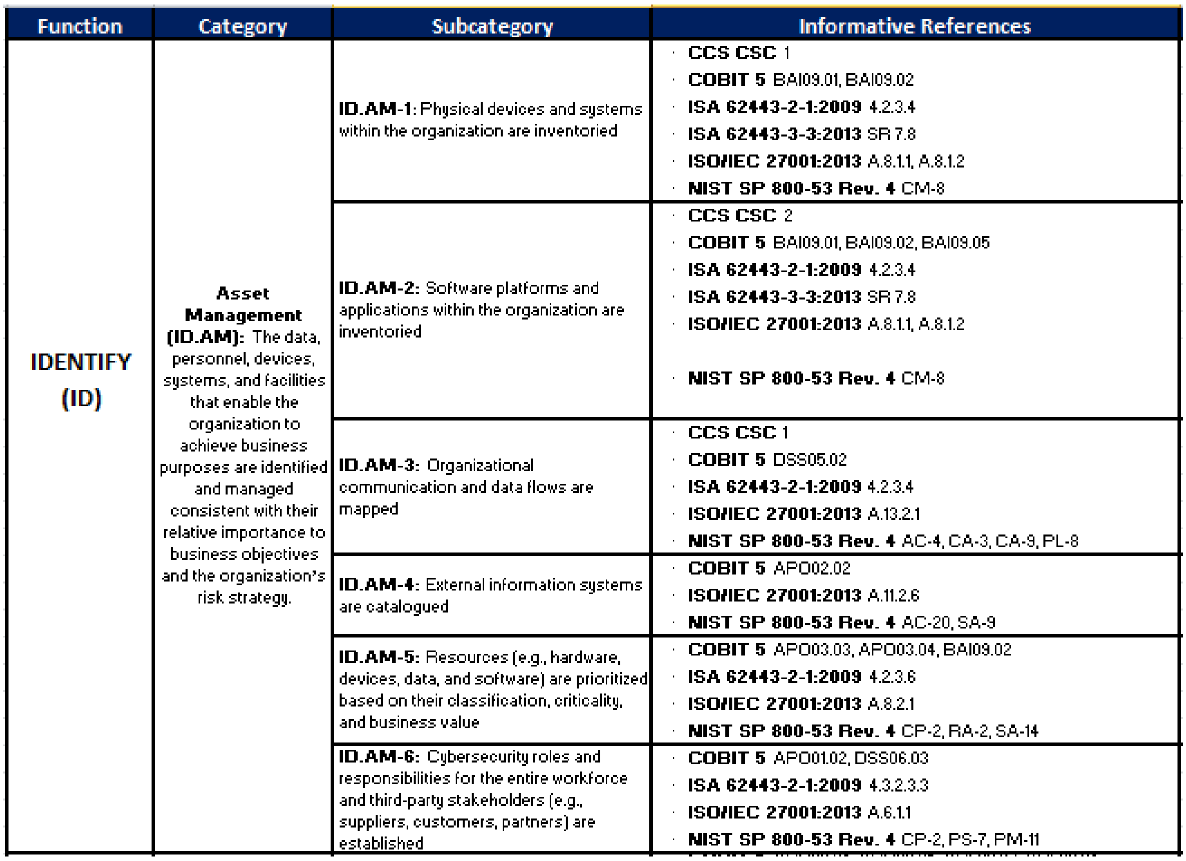


Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Figure 4: NIST CSF Categories

And these categories divide themselves in subcategories that finally guide to the implementation of controls referred in international standards.

As NIST is a guideline it can be tailored to each organization, this is, organization is free to select those items (subcategories and referenced controls in the selected standard) that best fits its objectives.



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Figure 5: NIST CSF Subcategories and informative references

Framework Implementation Tiers

Implementation tiers enable the organization to rank at a predefined threshold based on current risk management practices, the threat environment, legal and regulatory requirements, business objectives and mission, and the constraints of the company itself.

The ranges of the implementation levels are as follows:

- **Level 1 – Partial**: At this level, cybersecurity risk management practices are not formalized (ad-hoc) and generally act reactively. The prioritization of activities is not aligned with the organizational risk objectives, the threat environment or with business requirements. There is minimal external participation in terms of collaboration and information sharing.
- **Level 2 - Risk Informed**: At this level, risk management practices are approved by Management, but may not be established as a global policy. There are defined and implemented procedures and processes and qualified personnel. External participation is done informally.
- **Level 3 - Repeatable**: At this level, formal risk management practices are regularly updated as part of the application of analysis of changes in business requirements, threats or technologies. A formal collaboration framework with third parties has been established.
- **Level 4 - Adaptive**: Cybersecurity practices are based on lessons learned and predictive indicators derived from previous and current cybersecurity activities, through a process of continuous improvement to adapt to changes. These tasks are part of the organizational culture. It collaborates actively with third parties, sharing information on cybersecurity events.

Framework Profiles

Profiles are used to describe the current status and current profile of certain cybersecurity activities. The differential analysis between profiles allows the identification of gaps that should be managed to meet the risk management objectives.

For this, the definition of an action plan is required that includes a prioritization of activities depending on the business needs and risk management processes of the organization. This risk-based approach allows the organization to estimate the resources necessary (for example, personnel and funding) to achieve the established cybersecurity goals in a prioritized and cost-effective manner.

According to the previous descriptions, the global architecture of the cybersecurity framework would be as follows:

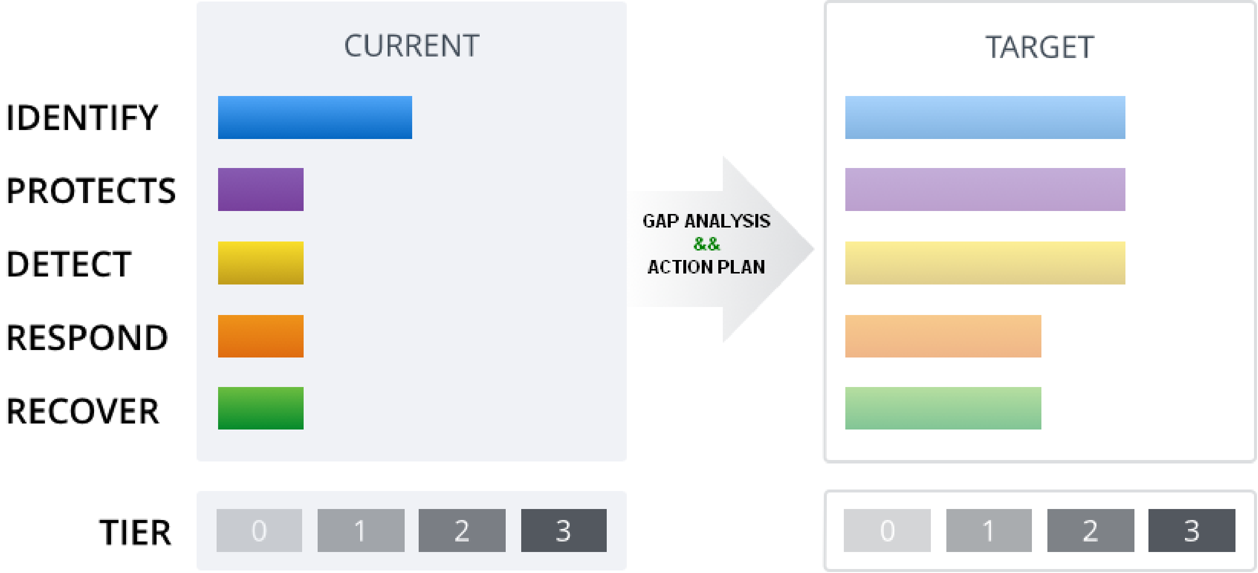


Figure 6: NIST CSF Profiles

How is CSF implemented?

The implementation of a CSF-based cybersecurity program consists of the following iterative steps:

Step 1 - Prioritization and scope definition: By identifying the business objectives and mission and high-level priorities in organizational terms, the control applicability environment is strategically decided. This environment can be the entire organization, a particular line of business or a process, bearing in mind that each of these elements may have different levels of risk tolerance.

Step 2 - Orientation: The systems, assets, regulatory requirements, threats and vulnerabilities related to the defined applicability environment are identified.

Step 3 - Create a current profile: Through the functions of the basic framework and using the categories and subcategories, the results of implementing controls in the environment are obtained.

Step 4 - Run a risk analysis: A risk analysis is carried out to determine the probability and impact of cybersecurity events in the analysed environment.

Step 5 - Create an objective profile: The objectives that the organization intends to cover in terms of cybersecurity are established.

Step 6 - Determine, analyse and prioritize the detected gaps: Through the differential analysis between the current profile and the objective profile, an action plan prioritized in terms of cost / benefit is defined, which allows the determination of resources and improvement actions.

Step 7 - Implement the action plan: Proceed with the alignment of controls and deployment of improvements gradually and monitored.

All these actions must be implemented within a continuous improvement environment, allowing the organization to continuously optimize its security controls and scale to higher levels within the framework.

II.3. NIST CSF in ProTego

Within the NIST CSF, the subcategories and informative references are the elements that need to be measured and evaluated to define the current profile of the organization, and also it is needed to take decisions about the objective profile, in order to make possible to measure the gap and build the action plan.

Both the evaluation of the current profile of the healthcare organization and the definition of the objective profile are out of the scope of the ProTego project. In the first case because ProTego is providing a set of technical tools (toolkit) that are going to be incorporated to the organization's IT infrastructure, but it is the whole IT infrastructure that need to be analysed in the NIST CSF. In the second case because the definition of the objective profile has to be defined based on the resources and possibilities of the organization, and has to be defined by those who can provide the means to perform the emerging action plan. For this reason, it is highly recommended that before starting any strategy, the CISO takes as a fundamental goal the appropriate awareness of the organization managers, because they are who must provide the resources needed and, thus, will implicitly decide the scope of the ISMS.

Nevertheless, the aim of the ProTego project is to develop data-protection toolkit reducing risks in hospitals and care centers and because of that the toolkit and educational framework will be of utility to improve a subset of the NIST CSF items. The following table identifies the NIST CSF items that will be impacted in an organization that incorporates the ProTego toolkit and educational framework to its IT map, or in other words, the items that the ProTego project will help to improve by facilitating to accomplish the related controls:

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1**: Asset vulnerabilities are identified and documented	**ISO/IEC 27001**:2013 A.12.6.1, A.18.2.3
		ID.RA-3: Threats, both internal and external, are identified and documented	**NIST SP 800-53** Rev. 4 RA-3, SI-5, PM-12, PM-16
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to	**PR.AC-1**: Identities and credentials are managed for authorized devices and users	**ISO/IEC 27001**:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

PROTECT (PR)	authorized activities and transactions.	**PR.AC-3**: PR.AC-3: Remote access is managed	**ISO/IEC 27001**:2013 A.6.2.2, A.13.1.1, A.13.2.1
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**ISO/IEC 27001**:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		PR.AC-5: Network integrity is protected, incorporating network	**ISO/IEC 27001**:2013 A.13.1.1, A.13.1.3, A.13.2.1
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1**: All users are informed and trained	**ISO/IEC 27001**:2013 A.7.2.2
	Data Security (PR.DS): Information and records (data) are managed	**PR.DS-1**: Data-at-rest is protected	**NIST SP 800-53** Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	**ISO/IEC 27001**:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		PR.DS-5: Protections against data leaks are implemented	**ISO/IEC 270**01:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**ISO/IEC 27001**:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**ISO/IEC 27001**:2013 A.9.1.2
DETECT (DE)	**Anomalies and Events (DE.AE)**: Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-2**: Detected events are analyzed to understand attack targets and methods	**ISO/IEC 27001**:2013 A.16.1.1, A.16.1.4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**NIST SP 800-53** Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-4**: Event detection information is communicated to appropriate	**ISO/IEC 27001**:2013 A.16.1.2
RESPOND (RS)	**Improvements (RS.RP)**: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.RP-1**: Response plan is executed during or after an event	**ISO/IEC 27001**:2013 A.16.1.5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1**: Response plans incorporate lessons learned	**ISO/IEC 27001**:2013 A.16.1.6
RECOVERY (RC)	**Recovery Planning (RC.RP)**: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1**: Recovery plan is executed during or after an event	**ISO/IEC 27001**:2013 A.16.1.5

Table 5: ProTego-related items within the NIST CSF

For each subcategory, the NIST CSF provides various informative references to choose among them. In this document, the ISO/IEC 27001 has been chosen whenever possible as the preferred option.

The previous table has identified the NIST CSF items that are included in the scope of ProTego. The description of the controls regarding each item (subcategory) and the feature that ProTego toolkit makes possible to perform such controls are described below.

ID: 1

Subcategory: ID.RA-1: Asset vulnerabilities are identified and documented

Controls: ISO/IEC 27001:2013 A.12.6.1

Description: Management of systems audit controls - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

ProTego Feature: ProTego includes the System Security Modeller (SSM) where the assets and the processes of a given IT system are identified generating a System Model of that. SSM provides the means to automatically identify cyber security and compliance threats and get help on how to address those threats by suggesting potential preventative controls. The domain model of SSM is subject to constant refinement to incorporate new system modelling requirements and new threats and can be updated in an SSM installation by its administrator. ProTego toolkit is able to retrieve information on software vulnerabilities and revaluate risks at runtime.

ID: 2

Subcategory code: ID.RA-3: Threats, both internal and external, are identified and documented

Controls: NIST SP 800-53 Rev. 4 RA-3, PM-12

Description: RA-3: Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

PM-12: To establish insider threat programs. The standards and guidelines that apply to insider threat programs that include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns

ProTego Feature: SSM allows to conduct risk assessments, including the likelihood as a parameter to determine the magnitude of harm. The System Model acts as centralized point of analysis. It will take as entry the technical information gathered by the SIEM that will detect information that needs to be analysed based on the policies defined by the organization.

ID: 3

Subcategory: PR.AC-1: Identities and credentials are managed for authorized devices and users

Controls: ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

Description: A.9.2.1 User registration and de-registration - A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.2 User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9.2.4 Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process.

A.9.3.1 User responsibilities - To make users accountable for safeguarding their authentication information

A.9.4.2 Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure

ProTego Feature: In ProTego this is done via the IAM systems of the hospitals. The design of the access control and key management system enforces that the identities and credentials of all authorized devices and users are registered and managed by these IAM systems. The reason for this is that the access control system requires a valid authorization token for each data access. These tokens will be issued by the IAM systems in place.

ID: 4

Subcategory: PR.AC-3: Remote access is managed

Controls: ISO/IEC 27001:2013 A.13.2.1

Description: A.13.2.1 Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities

ProTego Feature: Data stored in external storage is encrypted. In order to decrypt the data, one needs to get the decryption key from the KMS. The KMS will only send the decryption key to the data gateway via a secure channel, and will only do this if a valid authorization token is presented to the access control system, and when the remote data access is granted by the access control system (based on the content of the token and the security permissions in place).

ID: 5

Subcategory: PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

Controls: ISO/IEC 27001:2013 A.6.1.2

Description: A.6.1.2 Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets

ProTego Feature: The goal of the access control system is exactly to manage and enforce the access permissions to assets.

ID: 6

Subcategory: PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

Controls: ISO/IEC 27001:2013 A.13.1.1, A.13.1.3

Description: A.13.1.1 Network controls - Networks shall be managed and controlled to protect information in systems and applications

A.13.1.3 Segregation in networks - Groups of information services, users and information systems shall be segregated on networks.

ProTego Feature: Network Slicing technology allows the definition of segregated slices within a communication channel, providing isolating and encryption to protect data in transit.

ID: 7

Subcategory: PR.AT-1: All users are informed and trained

Controls: ISO/IEC 27001:2013 A.7.2.2

Description: A.7.2.2 Information security awareness, education and training- All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

ProTego Feature: Educational Framework developed in ProTego covers the required training to different categories of users, addressing different needs. For health staff it focuses on cybersecurity awareness, while IT staff will be trained on more technical details to allow a proper deployment of the toolkit and the included security features.

ID: 8

Subcategory: PR.DS-1: Data-at-rest is protected

Controls: NIST SP 800-53 Rev. 4 SC-28

Description: SC-28: The information system protects the confidentiality and integrity of the information at rest. The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of information on information system components.

ProTego Feature: Apache Parquet based encryption system ensures the confidentiality and integrity of the data at rest. To prevent unauthorized accessions, accesses will only be performed with the grant of the KMS. To ensure integrity, any file tampering will be detected and raise alerts to advice of such situation.

ID: 9

Subcategory: PR.DS-2: Data-in-transit is protected

Controls: ISO/IEC 27001:2013 A.13.1.2

Description: A13.1.2 Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced

ProTego Feature: The definition of slices defined by Network Slicing provide isolation in terms of both encryption and performance. That allows the definition of service levels according to the needs of each slice.

ID: 10

Subcategory: PR.DS-5: Protections against data leaks are implemented

Controls: ISO/IEC 27001:2013 A.9.1.2, A.9.2.3, A.9.4.1, A13.2.3

Description: A.9.1.2 Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.2.3 The allocation and use of privileged access rights shall be restricted and controlled

A.9.4.1 Access to information and application system functions shall be restricted in accordance with the access control policy

A13.2.3 Information involved in electronic messaging shall be appropriately protected

ProTego Feature: The combined features of ProTego toolkit minimizes the possibility of a data leak due to:

- the protection of data in transit provided by the network slices

- the protection of data at rest provided by the parquet data encryption
- the access control provided by the Key Management System
- the client device control provided by the continuous authentication
- the detection mechanisms provided by the SIEM

ID: 11

Subcategory: PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Controls: ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3

Description: A.12.4.1 Event logging - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information - Logging facilities and log information shall be protected against tampering

and unauthorized access

A.12.4.3 Administrator and operator logs - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

ProTego Feature: ProTego SIEM provides a centralized point of systems, services, and application logs. So even if a host is somehow compromised and the logs tampered, they will still be available in the SIEM. The communications between the hosts producing the logs and the SIEM are encrypted to prevent to maintain the Integrity and Confidentiality needed. The regularity of the review process has to be defined by each organization. The synchronization of the clocks has to be performed by the IT staff of each organization.

ID: 12

Subcategory: PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

Controls: ISO/IEC 27001:2013 A.9.1.2

Description: A.9.1.2 Access of networks and network services - Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

ProTego Feature: Data stored in external storage is encrypted. In order to decrypt the data, one needs to get the decryption key from the KMS. The KMS will only send the decryption key to the data gateway via a secure channel, and will only do this if a valid authorization token is presented to the access control system, and when the remote data access is granted by the access control system (based on the content of the token and the secure permissions in place). Without a valid token, one cannot access the data.

ID: 13

Subcategory code: DE.AE-2: Detected events are analyzed to understand attack targets and methods

Control: ISO/IEC 27001:2013 A.16.1.1, A.16.1.4

Description: A.16.1.1 Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.4 Assessment of and decision on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

ProTego Feature: Security incidents and management has to be defined in the security policy of each organization. To define security policies, it's recommended that both, IT department and the other administration and management departments of the hospital, participate. Rules extracted from the security policies can be applied as rules in the ProTego SIEM to detect those compromising situations.

ID: 14

Subcategory: DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

Controls: NIST SP 800-53 Rev. 4 AU-6, CA-7, SI-4

Description: AU6: Reviews and analyses information system audit records for indications of inappropriate or unusual activity and reports findings to appropriate personnel or roles. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. The organization analyses and correlates audit records across different repositories to gain organization-wide situational awareness. The information system provides the capability to centrally review and analyse audit records from multiple components within the system.

CA7: The organization develops a continuous monitoring strategy and implements a continuous monitoring program.

SI-4: The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives and unauthorized local, network, and remote connections.

ProTego Feature: ProTego SIEM provides the mechanisms to collect, store, correlate, and analyse in a centralized location. Metrics and frequencies are defined by each organization.

ID: 15

Subcategory: DE.DP-4: Event detection information is communicated to appropriate parties

Controls: ISO/IEC 27001:2013 A.16.1.2

Description: A.16.1.2 Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.

ProTego Feature: ProTego provides the means to generate reports. These reports will be defined by each organization and may be shown in a dashboard.

ID: 16

Subcategory: RS.RP-1: Response plan is executed during or after an event

Controls: ISO/IEC 27001:2013 A.16.1.5

Description: A.16.1.5 Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures.

ProTego Feature: ProTego toolkit will also provide decision support information at run-time for the security operators. The information will help them better understand the current risk level and how to respond to an attack suggesting some reactive control strategy, e.g., disablement of an asset.

ID: 17

Subcategory: RS.IM-1: Response plans incorporate lessons learned

Controls: ISO/IEC 27001:2013 A.16.1.6

Description: A.16.1.6 Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

ProTego Feature: The Domain Model can be refined by adding new information and knowledge gathered from previous incidents.

ID: 18

Subcategory: RC.RP-1: Recovery plan is executed during or after an event

Controls: ISO/IEC 27001:2013 A.16.1.5

Description: A.16.1.5 Information security incidents shall be responded to in accordance with the documented procedures.

ProTego Feature: This section will be completed in D3.3-Final description o Educational Framework as it needs details on how the ProTego toolkit to be deployed to be used.

III. PEOPLE-CENTRIC SECURITY MODEL

There is a gap between attitudes and actual behaviour about data privacy and, thus, information security. To better explain this: most individuals, when asked or surveyed, affirm that data privacy is a primary concern, but their behaviour is not coherent with that idea: they reveal personal information for small rewards, like discounts on purchases, access to websites or small gifts. This dichotomy of information privacy attitude and actual behaviour has been coined the term “privacy paradox” (Brown, 2001; Norberg et al., 2007) [8] or, to be more accurate, “information privacy paradox”.

This situation that has been documented through different empirical experiments as "*Privacy Choices Behavioural Economics Review*" conducted by Sören Preibusch in 2015 [9], or "*Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*" by Spyros Kokolakis in 2017 [10].

This reality is materialized in more customary practices that have implications on cybersecurity as well: users from healthcare staff are aware about the password policies regarding length and strength and in the survey executed in ProTego Deliverable 3.1, it was concluded that the most of the MS staff that responded to the survey were able to find and remember strong passwords. But if those good practices are not applied outside of the work environment, it would be risk due to the BYOD trend, that causes private and working environments interlace each other.

This reveals the necessity of reduce that divergence between attitude and behaviour and that is only possible through a change of mentality.

To explain how we get to this point it is needed to look at the evolution of Information Security.

III.1. Evolution of information security

First wave: when it first appeared, IS was "Technology-centric", meaning that in that time the main points were algorithms, systems and protocols. The main contributors to this were STEM (Science, Technology, Engineering and Mathematics) that tried to come up with **technical artifacts**. This was the first wave. And how they were used takes us to the second wave.

The **second wave** was "Economic-Centric": once those technical artifacts were available, **cost and benefit parameters** were attached to it, to maximize payoffs and minimize cost. In this phase optimum policies were developed. The main contributors were classic economists and science management science experts. And in this phase, it was developed optimum security incentive mechanisms, **policies and regulations**.

But obviously from the earlier examples showing real cases regarding the privacy paradox, something was lacking. Technology and optimum design of policies were still not sufficient. What is lacking? To explain this, it is needed to observe this matter from a different angle, from the angle of people that attack systems.

Kevin Mitnick was one of the most famous hackers and he currently works as a security consultant. He stated that "*Companies spend millions of on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems*" [11].

People that have a direct relation with the systems has to perform decision making in the real world. They can follow or not the recommendations stated in the policies. And that's de main focus of this **third wave**: **design and offer technology and policies that regular people** not only understand and agree with, but also **be able, capable and willing to use**.

The main contributors to this third wave are phycology, neuroscience, behavioural economics and sociology, that is, all the fields that will affect decision making. And the goal of this new wave of Information Security will be developing technical artifacts and protocols that will be actually used.

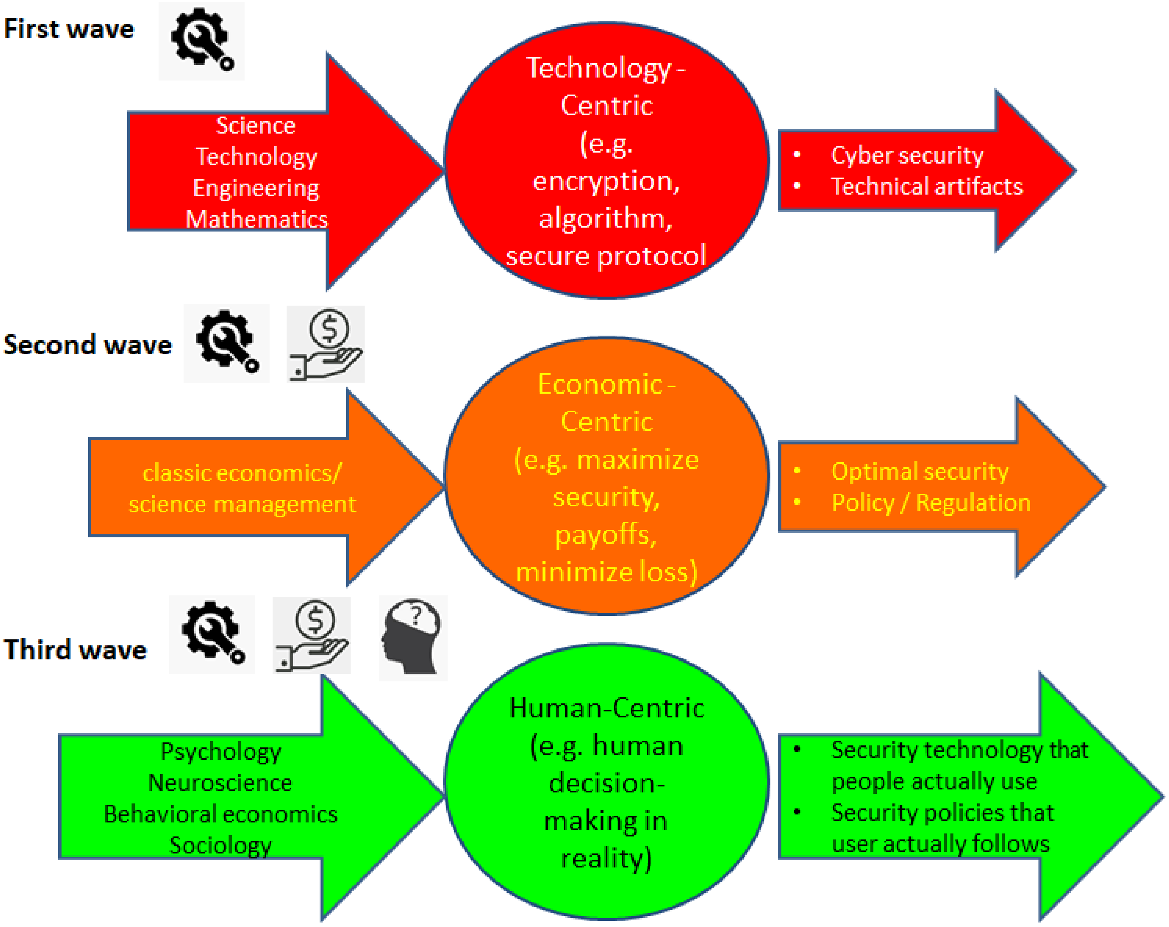

First wave
Science
Technology
Engineering
Mathematics
Technology - Centric (e.g. encryption, algorithm, secure protocol
• Cyber security
• Technical artifacts
Second wave
classic economics/ science management
Economic - Centric (e.g. maximize security, payoffs, minimize loss)
• Optimal security
• Policy / Regulation
Third wave
Psychology
Neuroscience
Behavioral economics
Sociology
Human-Centric (e.g. human decision-making in reality)
• Security technology that people actually use
• Security policies that user actually follows

Figure 7: Three waves of Information security

III.2. Cybersecurity in the organization

From the psychological approach suggested by the third wave of Information Security we can extract some basis that will surround the design of the ProTego educational framework. The main objective is to actually engage people and probably the main challenge is to achieve that in the healthcare sector, which is a particular sector in terms of its final users because the most of them are health staff and they have been historically focused in patient safety and right care [12], deep-seated concepts that have never included cybersecurity concerns. Technology, applications and cybersecurity are considered tools that hospital's support services (as IT department) must provide and that are completely out of physician's scope: physicians, nurses and health staff in general must care about "*material safety*" and IT department about "*virtual safety*".

Cybersecurity is about people

First concept is that cybersecurity is about people because it is created as a result of the interactions between people and technology. Without technology, cybersecurity would not have anything to protect. And without people nobody would try to attack IT systems. Is this intersection that creates and necessitates security.

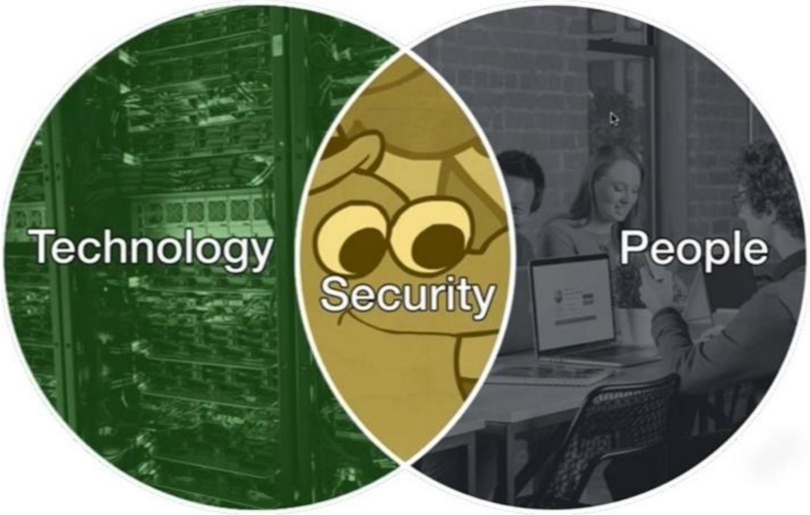


Figure 8: Cybersecurity scope

If each side of that equation is forgotten, it likely ends up without a good security solution in the organization. If we only have the security to technology but we don't address the people element, people would try to circumvent defined policies because they don't understand whether important, and on the contrary if technology is not addressed even the best policies can't protect unsecure systems by design.

Culture as a system

Culture is a fundamental portion of keeping an organization secure. It defines a complex social system, encompassing the behaviours, traditions, values, and interpersonal dynamics of a group. Its major inputs are shared norms, values, routines, and what the business reward or punishes. And its major outputs are user behaviours, employee retention and organizational health.

The goal is to create those unseen incentives and disincentives that promote the desired cybersecurity behaviours.

We can use drives or incentives towards the goal of getting staff to do certain things, in these three lines:

- Economic: we can introduce monetary bonus incentives if and only if, we can define measurable indicators that allow to objectively evaluate the achievement ratio. For example, if they attend to cybersecurity awareness trainings, the response to phishing simulation campaigns, the result of information security internal audits to different sections, etc.
- Social: this is about how the cybersecurity is perceived in the organization. Is it a roadblock or an enabler? A good example for this is when early on IT people started to talk about cloud. Many organizations decided it was not a possibility at all because of information security. This is an example of "*culture of no*". But instead of it, other companies decided to "*create a culture of yes*". They decided to open themselves to this new technology and create policies to address risks.
- Moral: this concept treats of mutual trust with users. Are users incentivized to report things that they think are relative to security violations? Or do they fear to be punished or shamed if they report that? We obviously want users that report because one of the main problems is that attacks remain undiscovered for a long time or even they are never discovered.

All these drivers work together and have unforeseen effects that can make that the same worded policy would be accepted completely different in an organization.

Communication in the organization

It is also important how we communicate about information security in the organization. This communication can be explicit but also implicit in the actions and decisions taken.

It is not about power: If any cybersecurity initiative is taken into an organization, it is very important that it would be applied from the top level of the organization. It is a usual error that just before a system is going live one of the terms discussed is whether or not the managers (e.g., CEO and directors) will consent on being applied by the security concerns, rules and protocols. And that is an error because if we have leaders talking about security but make themselves exceptions to the rules, it launches a message that security is about power: if you have power enough you are out of the scope of cyber security. And it is easy to imagine how different it is if the CEO not only talks about security but is also subjected to the same rules than the rest of the organization: that launches the message that cybersecurity is so important that nobody is about it.

It is not a lost cause: cybersecurity initiatives must not be approached with the objective of being completely safe. As many experts affirm, it is inevitable to fall victim of a cyberattack. There is no phishing simulation campaign where at least one people clicks the malicious link. There is no way to be out of it, but what can make the difference is how we deal with that, how do we respond to that vulnerability. If staff feels worried about being punished rather than encouraged to report breaches, it is a dangerous situation because security can be compromised and nobody is taking actions because the breach would not be detected. But if that is not assumed as a lost cause and a culture is created in the organization where nobody fears about punishment for a potential breach but rather staff feel incentivized to report immediately, the exposition time is minimized and the problem can be fixed with a minimized impact.

How cybersecurity often makes users feel can be illustrated with a phrase from the film WarGames (1983, John Badham) [13]: "*A strange game. The only winning move is not to play.*", and that is what should be avoided.

Make it easy: The easiest the cybersecurity mechanisms are, the higher adoption they will have into an organization. And taking it to the extremes, if users ran into a problem using a process, they will probably just ignore it. This idea can be illustrated with the example of the lock screen systems in phones. Several studies [14] demonstrated that the ratio of users that lock their device if it is equipped with biometric systems (fingerprint, face id) is higher than the same on devices that don't have these capabilities. Here the important point is not if those biometric systems have vulnerabilities or not (as it has been proved they have) but it is always better locking the screen that keeping it unlocked. That is, the best security mechanisms are those that are adopted by users. Here the message is that don't let perfect security obstructs good security.

Make cybersecurity team visible: In most organizations, cybersecurity team is an abstract person or team that users receive emails from, often to punish regarding some incorrect behaviour, or to give instructions perceived as obstacles to the job. To change that situation, it is a good idea that those people (cybersecurity team) will be known by the rest of the organization, that users can put face to that person or team, and understand that their job is to keep them safe. It is a psychological factor, human have a cognitive bias towards people we trust or people that we don't.

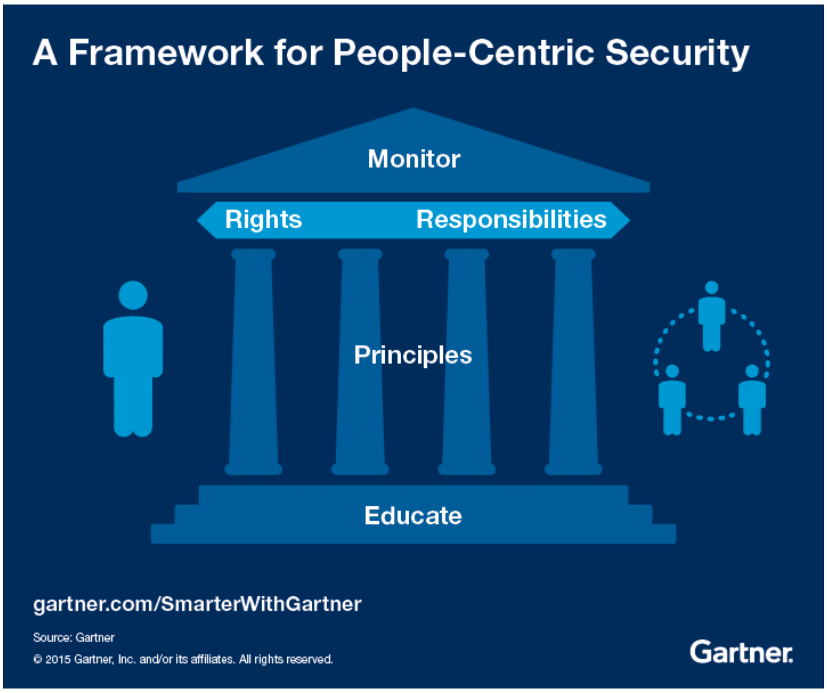
Teach differently: like in traditional education the difference between having a passionate teacher that explains why you should care about what you are learning and not only pay attention to what you are learning makes the complete difference. And for people whose job is not so related to cybersecurity (like health staff) repetition is very important. As it is not feasible to repeat the training sessions quite often, this repetition can be achieved by making cybersecurity more present, by creating visual material as posters, digital banners, etc. with key concepts that refers to the main subjects of the training sessions, and place it in physician work places, corporate intranet, etc.

III.3. People-Centric Security model

The cybersecurity awareness strategy for final users designed by ProTego is based on the People-Centric Security (PCS) model. Within the following sections the model will be presented and its concrete adaptation to ProTego.

This model aims to achieve an effective cybersecurity culture within the healthcare organization, increasing the global level of cybersecurity and reducing the risk of incidents directly related to one of the key components in this matter: people.

It is framed within a cybersecurity management strategy in which people play an active and relevant role, acquiring responsibilities in the management of the information they handle. To define this new cybersecurity management model Gartner has coined the term "*People-Centric Security*" [15].


A Framework for People-Centric Security

gartner.com/SmarterWithGartner

Source: Gartner

© 2015 Gartner, Inc. and/or its affiliates. All rights reserved.

Figure 9: Concept of Gartner's People-Centric Security

In keeping with this name, PCS is a strategy in which the person has rights and responsibilities in the cybersecurity management of the technologies they use and the information they manage through them, and must manage the associated risks.

PCS aims to make the people who work in an organization part of its line of cyber defence: "human firewall". To achieve this objective the framework defines three main lines of work:

- **Training**: Provide the person with the attitudes and skills necessary to carry out adequate risk management.
- **Personal risk management**: Definition of an appropriate methodology that allows people to carry out practical and effective risk management.
- **Monitoring**: Continuous review of risk management carried out by each person who works in the organization.

Training is the most essential part of this strategy: it is necessary to approach the training of people so that they can adequately manage the risks that affect them through continuous awareness-raising and training. In the PCS model training splits in three sections:

- Awareness: Through awareness it is about involving the person in the protection of the technologies and information it manages. To do this, it shows people the threats they face and their possible impact, making them understand why they must properly manage cybersecurity.

- Training: Through training, the necessary knowledge is transferred to people to put into practice adequate cybersecurity management. They are trained in how to do it.
- Simulation: By executing training actions, people are helped to keep their knowledge up to date in order to effectively manage risk

In ProTego, an awareness program has been designed to improve correct behaviours in cybersecurity (see Section IV). Training and simulation are not suitable in the most of healthcare organizations because clinical resources are precious and limited, and increase awareness is the basic element that should be performed, as a synonym of “understand why”. From this point other objectives can be examined, as more specific trainings with a deeper technological component.

IV. EDUCATIONAL MATERIAL FOR HEALTH STAFF

It is a globally accepted fact that the contents in education need to be adapted to those they are addressed to. In this case the objective people are health staff that has its own particularities. In this concrete scope, to impart a right awareness training is about:

- designing the right content: every possible item that can be included in a cybersecurity training can't be covered so it is needed to select and cover those contents considered more relevant and that keep students connected and interested.
- demanding the right effort: it is known that health staff perceive any issue outside of healthcare as an extra content that should probably not be addressed to clinical personnel. Therefore, any training program should mind the time required to be attended. In the case of ProTego, it is about 90 minutes.
- communicating through the right channel: for clinicians in general and physicians in particular it is a proven fact that their perception and understanding of any matter get better if it is transmitted from a colleague, this is, from another physician. This strategy has been followed in many healthcare organizations by involving clinical key users in relevant IT committees, where they are the receptors of the change requests, prioritize them and communicates to the rest of the health staff. This strategy is going to be followed in ProTego, involving the heads of clinical services in the communication strategy, so the final users perceive this awareness program more related to their clinical responsibilities.
- making messages persistent in time: cybersecurity awareness program should not be a sort of technical training where you are teaching someone about how to do a concrete task to reach a touchable or a least countable objective. This is about impress the necessity of perform correct behaviours that are not mandatory to reach the objective, and that is the point: users don't necessarily need to apply the right behaviours to reach their goals, but even so we need them to feel the necessity to act correctly. And for this objective is important that the messages transferred become persistent. And this have been addressed by the creation of reminders with visual and direct messages that make users remember the concepts treated in the training.

IV.1. Execution of the user awareness training

The correct execution of the training implies a top-down communication process to ensure required resources and engage participants. The following table resumes the plan:

STEP ID	NAME	PARTICIPANTS TO ENGAGE	OBJECTIVES
1	Quick-off	Organization managers	Communicate the awareness training plan. Ensure material and personal resources.
2	Engage clinical managers	Managers of clinical services	Prepare first communication for final recipients by clinical managers
3	Present training to users	Health staff	Present cybersecurity training as a clinical subject
4	Perform training sessions	Health staff	Explain risks derived from user's normal behaviour. Teach how to act to avoid those risks.
5	Reminders	Health staff	Place graphic material as reminders

Table 6: Phases of awareness program for health staff

This is the explanation of each step:

- Communicate to organization managers: First of all, it is important to advice organization managers to ensure the clinical resources needed will be available, mainly those referring to clinical managers as head of medical services.
- Engage clinical managers: Then it is needed to engage heads of medical services. The first talk to the final receptors of the training will be given during a clinical session. There, the intermediate clinical managers will introduce this plan. They will talk about the importance of cybersecurity, highlighting the risk from the patient safety perspective: from the modification of clinical images leading to a bad diagnose, to the change of medical prescriptions, or the ransomware attacks that can stop completely the normal work in a hospital. They will insist in the fact that the major part of these attacks came from exploiting vulnerabilities derived from a bad cybersecurity behaviour and that's why it is a responsibility of each user to know how and to behave in the correct way.
- First contact with final users: Clinical managers will design this first communication step to make this message to reach every single user under his responsibility. They will notify the following step: training sessions offered in different timetables to make possible all users to assist. As rotatory shifts are usual in healthcare it is important to offer a wide range of possibilities, making that this training doesn't interfere in staff's regular work.
- Training sessions: At this point it will take place the awareness training sessions that is the trunk activity of the plan. This will be organized in 90 minutes sessions, given by communication professionals that will be accompanied by IT technical staff if they come from different curricular areas such as pedagogy or human resources. These sessions will be divided in four sections, developing four different subjects described later on, plus a last 5 minutes slot for questions. Each training session should admit from 10 to 30 people, promoting the participation and discussion. The four topics threated will be:

TRAINING BLOCK	KEY CONCEPTS
Block: 0 **Name: Introduction** **Length: 10 minutes** **Channel: Live session**	Healthcare as a target for cyber criminals Dimensions of information security Expected impacts regarding each dimension
Block: 1 **Name: Passwords** **Length: 10 minutes** **Channel: Live session**	Strong passwords. Different passwords for different services. Password managers Multifactor authentication
Block: 2 **Name: The good employee** **Length: 30 minutes** **Channel: Live session**	Digital print Terms and conditions in cloud services Apps permissions Hidden metadata in files Manage paper and digital information Connect to public Wi-Fi Information leaks

	Untrusted USB devices Cypher USB contents
Block: 3 **Name: <u>Phishing and Social engineering</u>** **Length: 30 minutes** **Channel: Live session**	Email Phishing Spare phishing Non corporate phishing Malware installation Smishing Vishing Deepfakes The CEO fraud Baiting
Block: 4 **Name: <u>Cell phones</u>** **Length: 10 minutes** **Channel: Live session**	Apps from certified sources Control permissions granted Stay updated Antivirus and other complements

- <u>Reminders:</u> Finally, to make the messages and risks explained persistent in time, graphic material addressing the main subjects will be set in posters and placed in usual work places of health staff as nursery controls, physician work rooms, etc. This paper-based material will be digitalized and included in the hospital intranet as a banner that randomly will show them, among other messages that the organization needs to communicate.

IV.2. Block 0: Introduction

To put this training in context, it is important to understand why the information security is essential in healthcare, and it is closely linked to interest of cyber criminals on healthcare information and the severity of the impact that security breaches may have.

Healthcare organizations are special targets for cyber criminals due to the high value of healthcare information on the black market. Healthcare services are expensive and being able to identify potential customers would be a high valued item for companies. In addition, any other information about individuals has or may have caducity: credit card numbers, addresses, even names or passport numbers can be changed. But biometrical and medical information is stored as part of the citizen personality and accompany them forever.

The previous is the most immediate reason we can think of when trying to imagine why somebody would perform a cyber-attack against a hospital. But technology has evolved and each time its presence, and thus impact, is greater in every single healthcare workflow.

To better explain this idea, we're going to introduce the concept of dimensions of information security and the impact that a breach on each of them can have on the patient's safety.

The three main components (also called dimensions) of information security are confidentiality, integrity and availability. These three components put together conform the CIA triad [16] which is a security model created to guide information security policies within an organization.

- **Confidentiality**: Confidentiality is the security principle that controls access to information. It is designed to ensure the wrong people cannot gain access to sensitive information while ensuring the right people can access it.

Access to information must be restricted only to those who are authorized to view the required data. Data can be categorized according to the type and severity of damage that could happen to it should it fall into unauthorized hands. According to these categories, strict measures can then be implemented.

Protecting confidentiality may also include special training for those who share sensitive data.

Strong passwords and password-related best practices must be used as well as information about social engineering attacks to prevent them from unwittingly avoiding proper data-handling rules and potentially causing disastrous results.

An example of a method used to ensure confidentiality is the use of data encryption. Two-factor authentication is now becoming the norm for authenticating users to access sensitive data, while user IDs and passwords should be considered standard practice.

Users should also be cautious to reduce the number of places where the information appears and where sensitive data is transmitted in order to complete a transaction.

Healthcare information has the highest level of sensibility because the unauthorized access or diffusion of healthcare information may cause serious social detriments as denegation of insurances, barriers to access jobs or social discriminations.

- **Integrity**: The second component of the triad, integrity assures the sensitive data is trustworthy and accurate. Consistency, accuracy, and trustworthiness of data should be maintained over its life cycle. Sensitive data should not be altered in transit, and security measures, such as file permissions and user access controls, should be taken to make sure that it cannot be modified by unauthorized users. To ensure this dimension of information security, there are other technical strategies to put in place as cryptographic checksums for verification of integrity and backups or redundancy plans to be able to restore any affected data in case of integrity failure or security breach in order to restore data back to its correct state.

To understand the impact that a breach on the integrity dimension may have it is important to be aware of that the most of the clinical decisions are taken based on antecedents and the falsification of that information may lead to wrong decision as inadequate drug prescription, wrong diagnosis, etc. That risk is getting higher with the inclusion of automated or semi-automated CDSS

- **Availability**: Availability is the guarantee of reliable and constant access to sensitive data by authorized people. It is best guaranteed by properly maintaining all hardware and software necessary to ensure the availability of sensitive data. In addition, organizations should provide disaster recovery plans with safeguards against interruptions in connections and data loss, considering unpredictable events such as a fire or a natural disaster.

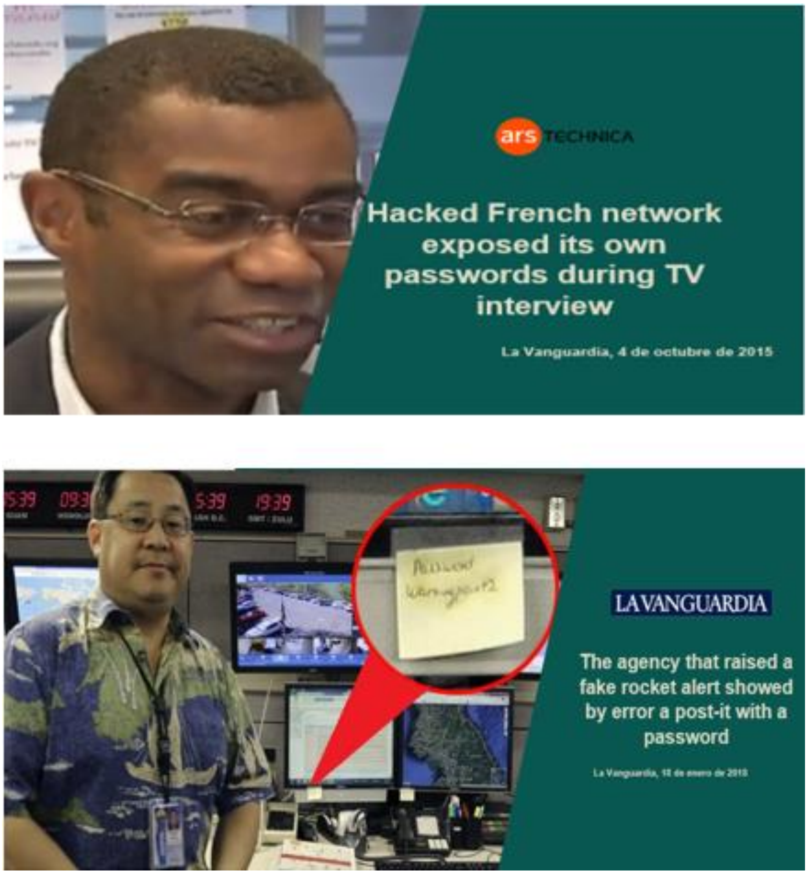
The unavailability of healthcare information may preclude the adequate provision of healthcare services. This risk is higher as the organization is more IT dependent, what use to come with the process integration and efficiency. It might make impossible the provision of services or obligate to take decisions without all the required information, which may lead to errors in the provision of appropriate cares and health services in general.

The following sections describe which risks users are exposed to and how to perform feasible, correct behaviours to avoid them.

IV.3. Block 1: Passwords

In this block of content, the presenter will transmit the importance of a correct password policy at personal level, covering from the selection and creation of a strong password, to the management of the different passwords for different services that is a recommendation for users.

Introduction: The section will begin by presenting some articles showing real cases of involuntary diffusion of passwords in relevant organizations.



Hacked French network exposed its own passwords during TV interview

La Vanguardia, 4 de octubre de 2015

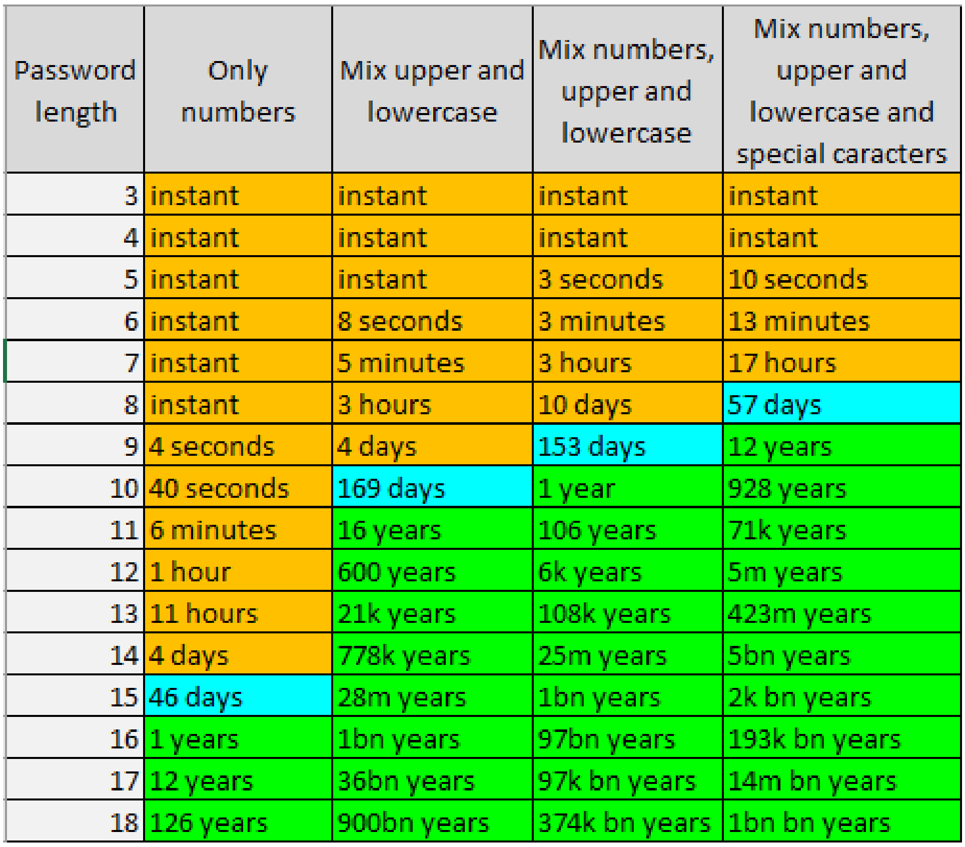
The agency that raised a fake rocket alert showed by error a post-it with a password

La Vanguardia, 18 de enero de 2018

Figure 10: Real password expositions

Password strength: In this section the presenter will explain the concept of hashing, brute force attack, and password salting techniques by playing a video. [17]

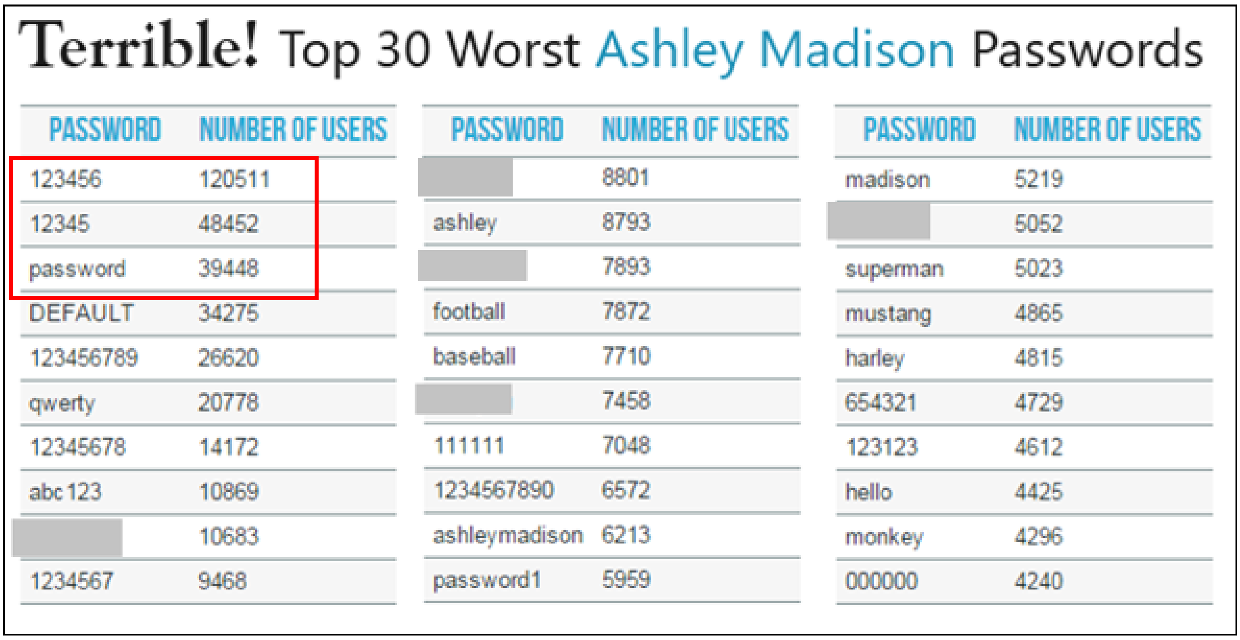
And then will show a table explaining how the time needed to break a password increase with the strength of the password. More than concrete values that depend on hardware capacity, it is important to transmit the curve evolution with the type of characters used and the password length.



Password length	Only numbers	Mix upper and lowercase	Mix numbers, upper and lowercase	Mix numbers, upper and lowercase and special caracters
3	instant	instant	instant	instant
4	instant	instant	instant	instant
5	instant	instant	3 seconds	10 seconds
6	instant	8 seconds	3 minutes	13 minutes
7	instant	5 minutes	3 hours	17 hours
8	instant	3 hours	10 days	57 days
9	4 seconds	4 days	153 days	12 years
10	40 seconds	169 days	1 year	928 years
11	6 minutes	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2k bn years
16	1 years	1bn years	97bn years	193k bn years
17	12 years	36bn years	97k bn years	14m bn years
18	126 years	900bn years	374k bn years	1bn bn years

Figure 11: Cost curve in cracking passwords

Real example of Ashley Madison hacking on 2015. It is shown an extract of the weakest passwords used by members:



Terrible! Top 30 Worst Ashley Madison Passwords

PASSWORD	NUMBER OF USERS	PASSWORD	NUMBER OF USERS	PASSWORD	NUMBER OF USERS
123456	120511	[redacted]	8801	madison	5219
12345	48452	ashley	8793	[redacted]	5052
password	39448	[redacted]	7893	superman	5023
DEFAULT	34275	football	7872	mustang	4865
123456789	26620	baseball	7710	harley	4815
qwerty	20778	[redacted]	7458	654321	4729
12345678	14172	111111	7048	123123	4612
abc123	10869	1234567890	6572	hello	4425
[redacted]	10683	ashleymadison	6213	monkey	4296
1234567	9468	password1	5959	000000	4240

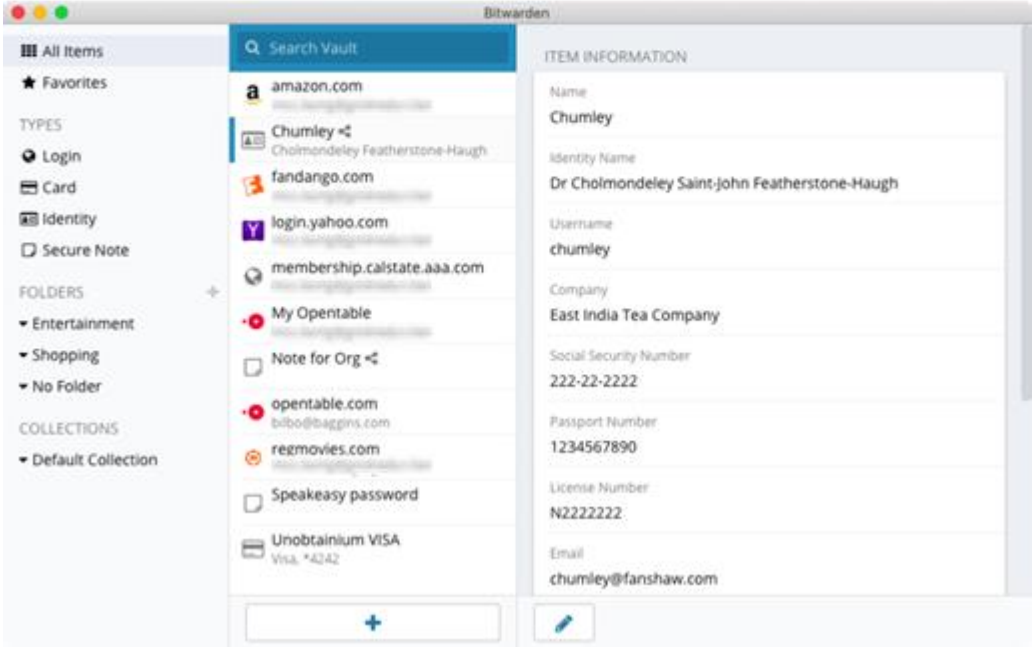
Figure 12: Ashley Madison weakest passwords

The following matter is that it is not recommended to use a unique password for every service:

Figure 13: Different passwords for services

And the previous advice introduces the recommendation of using password managers. Different alternatives as Keepass or Bitwarden will be presented:

And it will be explained how these tools work over the ”Bitwarden” tool: that can be used in different devices, from laptops or PCs to mobile phones:



amazon.com

Chumley
Cholmondeley Featherstone-Haugh

fandango.com

login.yahoo.com

membership.calstate.aaa.com

My Opentable

Note for Org

opentable.com
bilbo@baggins.com

regmovies.com

Speakeasy password

Unobtainium VISA
Visa, *4242

Name
Chumley

Identity Name
Dr Cholmondeley Saint-John Featherstone-Haugh

Username
chumley

Company
East India Tea Company

Social Security Number
222-22-2222

Passport Number
1234567890

License Number
N2222222

Email
chumley@fanshaw.com

Figure 14: Bitwarden password manager

The last section of this block will introduce the multifactor authenticator, explaining the ”something you know – something you have – something you are” concept, and how it is used in some common services as online banking. The recommendation will be to active at least double factor authentication whenever possible.

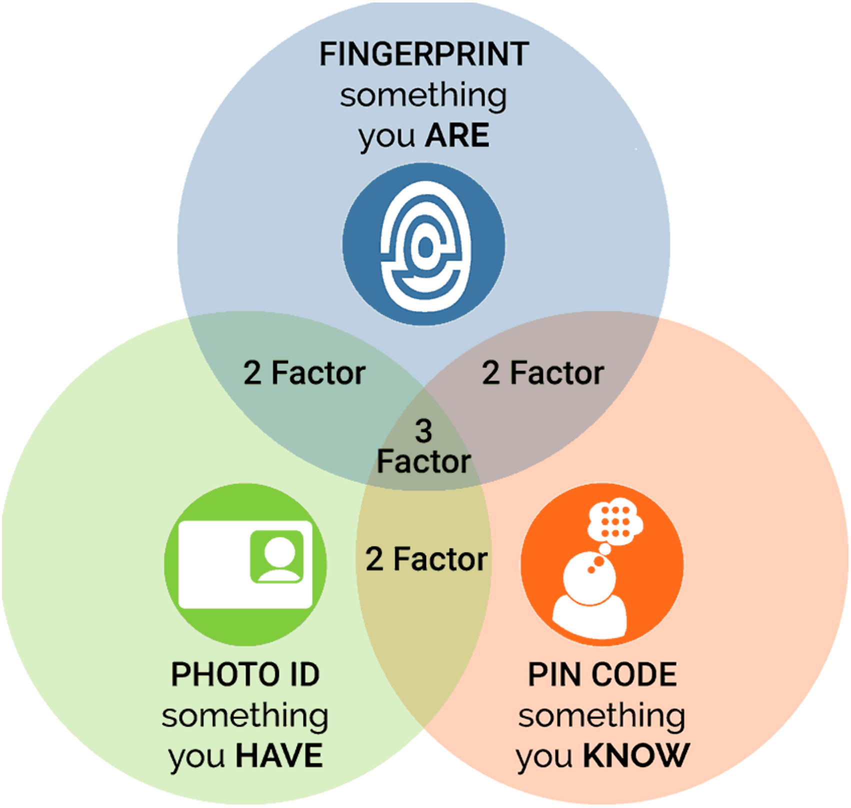
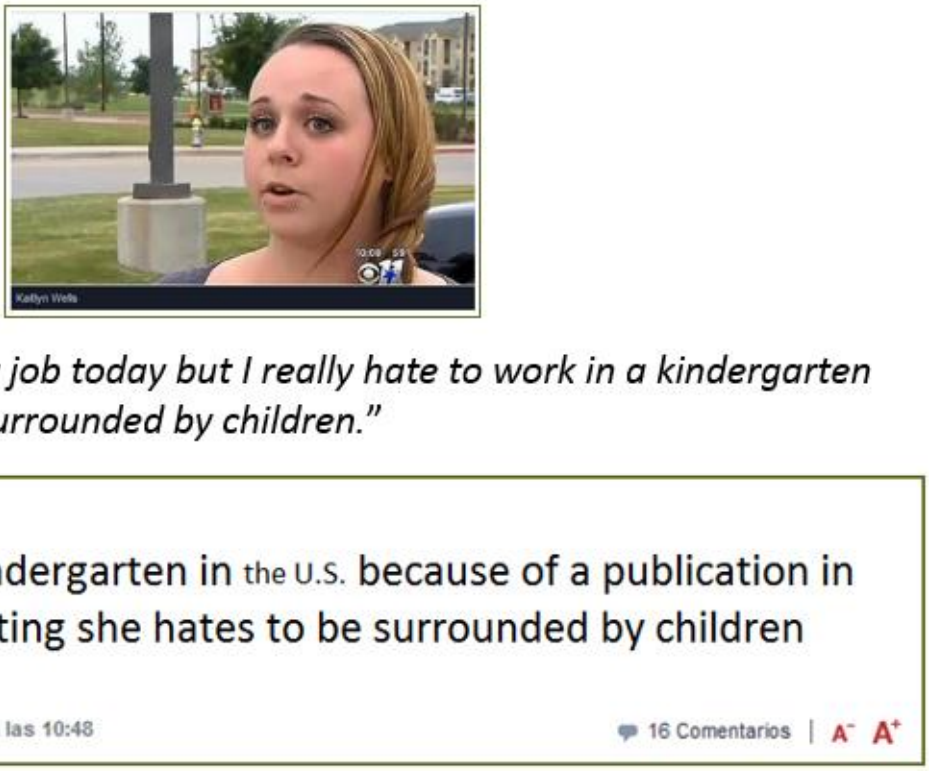


Figure 15: Multifactor authentication

IV.4. Block 2: The good employee

In this block and over the example of a working day of a fictitious persona, it will be shown how daily actions of a well-intentioned employee can hide cybersecurity threads and risks.

It will first introduce the concept of **digital print** showing an example of a real person that was fired due to declarations made in her social networks. The intention beside this is to show that the activity in the network actually matters because it is part of our real live and may have consequences.



“Starting my new job today but I really hate to work in a kindergarten (…) , hate to be surrounded by children.”

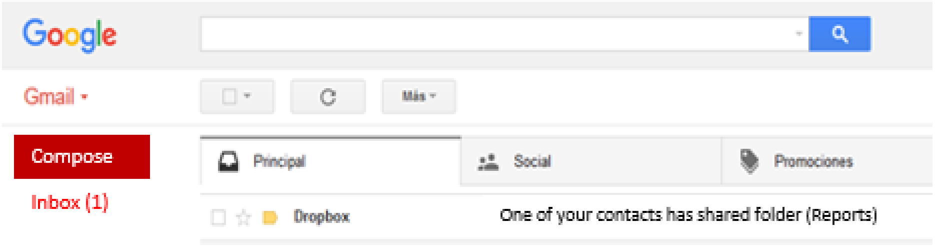
In the United States

Fired from a kindergarten in the U.S. because of a publication in Facebook admiting she hates to be surrounded by children

Heraldo.es | 30/04/2015 a las 10:48 16 Comentarios | A- A+

Figure 16: Impact of digital print

The Good Employee day starts, by reviewing his email at home before departing to the office. There he finds an email from a colleague that has shared content in the cloud.

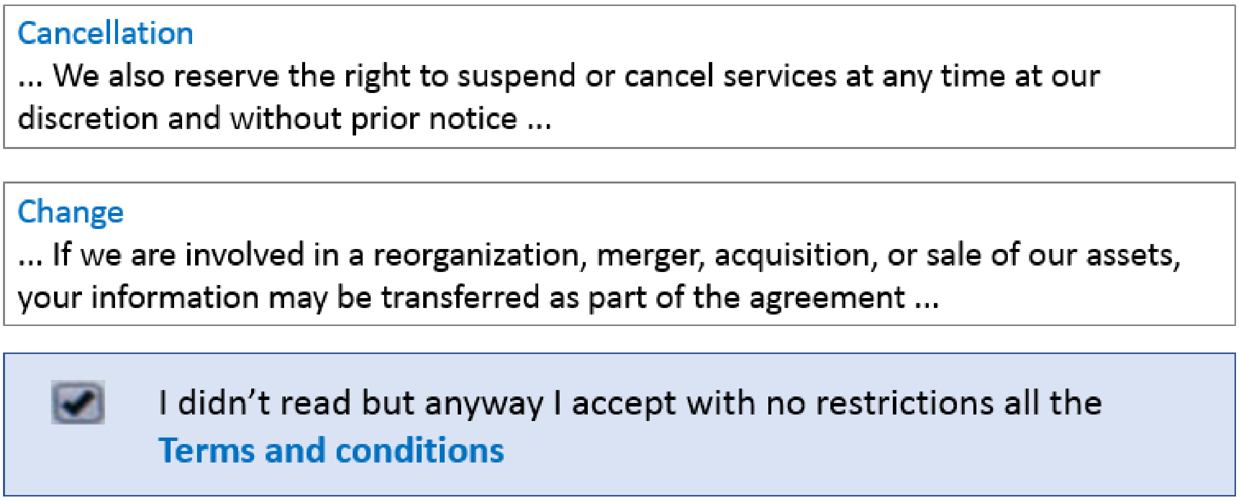


Dropbox One of your contacts has shared folder (Reports)

Figure 17: Invitation to cloud-share documents

Here there are two concepts to focus on:

- Do not click links from emails or communications always as possible. Access directly to the website by typing the URL
- Read carefully the terms and conditions when using cloud repositories and, as a rule, do not use unauthorized sites to store and share corporate information.



Cancellation

... We also reserve the right to suspend or cancel services at any time at our discretion and without prior notice ...

Change

... If we are involved in a reorganization, merger, acquisition, or sale of our assets, your information may be transferred as part of the agreement ...

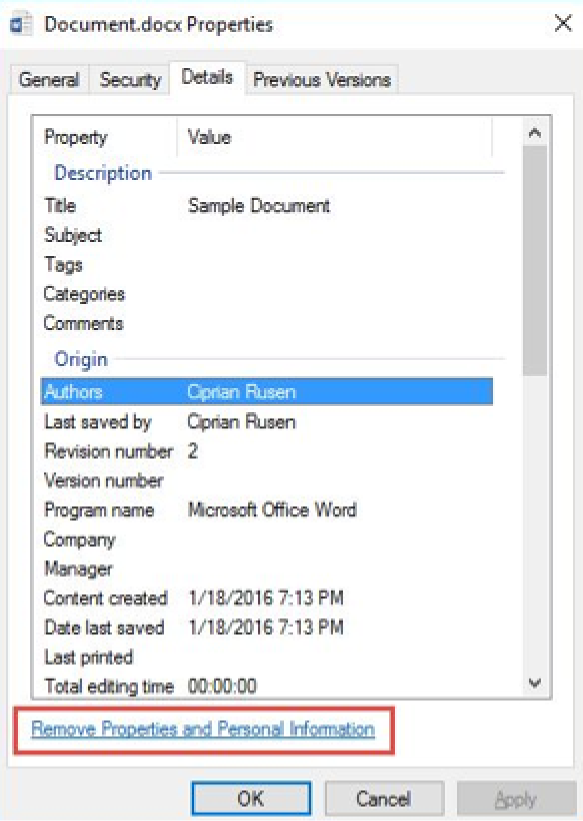
☑ I didn't read but anyway I accept with no restrictions all the Terms and conditions

Figure 18: Terms and conditions on cloud services

The Good Employee arrives to the office. There he logs into the corporate system and continues editing an internal document. Once done, the document needs to be transmitted to an external email and printed in paper as well.

By this, two more cybersecurity concepts are explained: by sending the document outside the organization he will take care of the *metadata*. There is hidden metadata that can store information that can lead attackers to be able to exploit vulnerabilities of the corporate systems. Transparent to the user, a document can contain information about internal servers, disc folders and routes, credentials of users that worked with the document, etc.

The recommendation here is to review the document metadata, to know that there are tools to remove any hidden metadata and to use it whenever possible, both in working or private scopes.



Property	Value
Description	
Title	Sample Document
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	Ciprian Rusen
Last saved by	Ciprian Rusen
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	1/18/2016 7:13 PM
Date last saved	1/18/2016 7:13 PM
Last printed	
Total editing time	00:00:00

Remove Properties and Personal Information

- Metadata may contain sensible information
- Review them before sending documents to external sources

Figure 19: Metadata in files

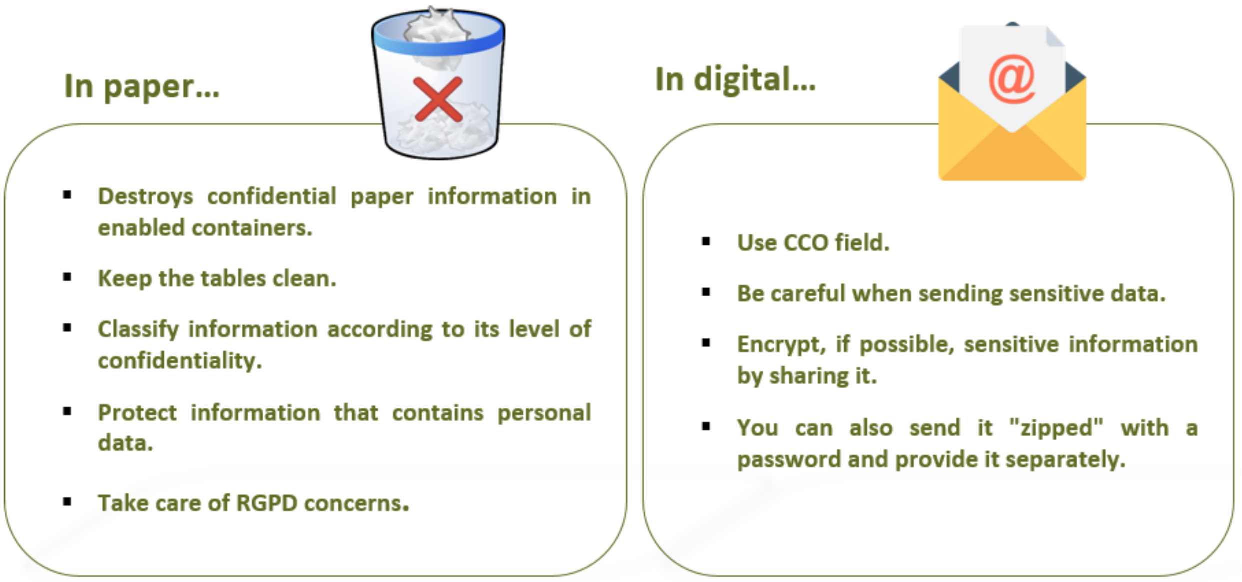
By printing the document, it will be explained that even seeming a silly mistake, leaving documents forgotten in a printer has historically been away to filter sensitive information. And it is a realistic possibility if we think about large organizations with printers covering work zones and sometimes users can actually ignore the printer assigned, so sent documents can rely unattended for hours or days, and if those documents include sensitive information ... the threat is clear.

The use of printer pins may lower the thread.

This risk links directly with the risk of an information leak:

Paper information: It is commonly covered the way that papers should be stored in physical archives, but the destruction of paper documents is often not defined. Documents with sensible information should be managed through a certified system that ensures that paper will not be accessible until its final destruction, with paper shredder, or locked waste bins and certified companies managing it.

Digital information: users must use the CCO field, cypher the information sent to external sources or at least apply simple obfuscation mechanisms as zip the information with a password and send it through a different channel.



In paper…

- Destroys confidential paper information in enabled containers.
- Keep the tables clean.
- Classify information according to its level of confidentiality.
- Protect information that contains personal data.
- Take care of RGPD concerns.

In digital…

- Use CCO field.
- Be careful when sending sensitive data.
- Encrypt, if possible, sensitive information by sharing it.
- You can also send it "zipped" with a password and provide it separately.

Figure 20: manage paper and digital information

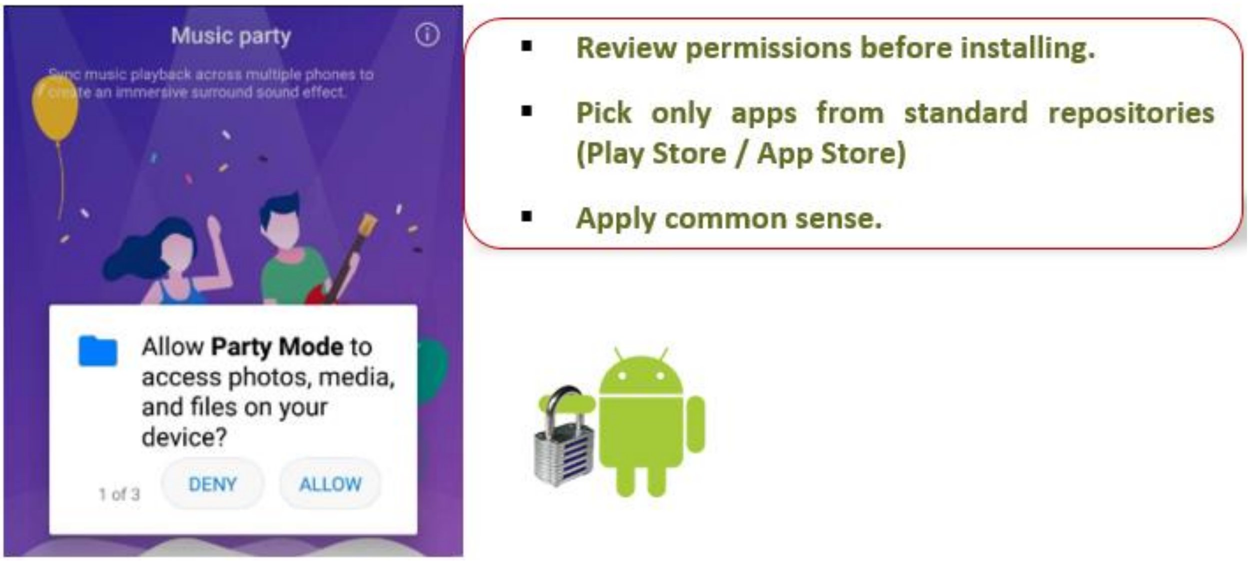
It is lunch time and the Good Employee goes to a restaurant near the Hospital. There he connects to the restaurant free Wi-Fi, writes some comments in the social networks. At the same time, he opens the email client and reads an email from work.

Here there is an incorrect behaviour. It is not recommended to connect to untrusted networks and if connected, no sensible information should be treated. It is pretty easy for attackers install sniffers and capture information sent.

There he attends a link to download an APP to make funny photos and he decides to download and test it to see if can be of interest to his children. When installing it, the app asks for permissions to the camera, microphone, location, contact list and filesystem. He accepts all, test it and keeps it installed, it is a funny app and children will enjoy it.

With this, two incorrect behaviours have been performed: first no software should be installed when connected to an untrusted network. And second, it is required to think about the permissions given to apps, trying to give them strictly what they must need to perform its intended functionality. In this example, access to microphone, location and contact list should not be given because are features not related to the app intended functionality.

Figure 21: Open Wi-Fi hidden risks


Music party

Sync music playback across multiple phones to create an immersive surround sound effect.

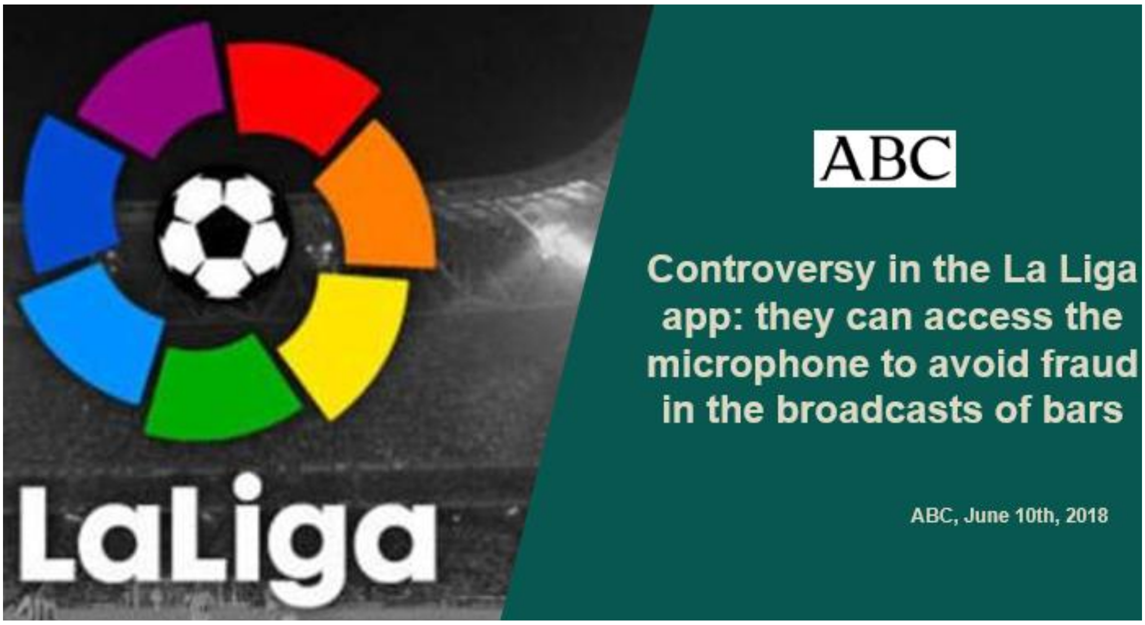
Allow **Party Mode** to access photos, media, and files on your device?

1 of 3

- **Review permissions before installing.**
- **Pick only apps from standard repositories (Play Store / App Store)**
- **Apply common sense.**

Figure 22: Check app permissions

As an example of what can be done by providing unnecessary permissions to apps, the enterprise La Liga which manages the soccer league in Spain asked for permissions to the location and microphone in their app. They used it to locate bars where soccer matches were video transmitted by turning on a listen mode of mobile phones and locating them. Then they checked if each of those bars had license to broadcast the match.



ABC

Controversy in the La Liga app: they can access the microphone to avoid fraud in the broadcasts of bars

ABC, June 10th, 2018

Figure 23: La Liga app controversy

After lunch time, he takes a taxi, before coming back to the office he needs to pick a shirt from the laundry. In the taxi he receives a call from the User Call Centre of the hospital related to an incident he logged the previous day. He responds the call as being in the hospital, talking completely free about his account parameters, login user, etc.

It is an incorrect behaviour because he was spreading sensitive information in an environment where external people (taxi driver in this case) can listen to it and gather sensitive information. Imagine the same situation responding the call in the restaurant, laundry or any other environment with more people being able to listen.

Figure 24: Information leak by unauthorized listeners

After the travel, he arrives to the Hospital and takes the lift to his office in the third floor. In the lift he finds a usb key. He thinks some of their colleagues in the hospital can lost it and decides to take a look to the content to figure out who can be the owner, or at least the department or medical service to address. He is not willing to break any confidentiality right, after all he is a Good Employee, but just with the names of the files it would be possible to figure out where to address to restore it to its owner.

He plugs in the USB to his laptop and see some documents containing articles about cardiology, that leads him to think it should be submitted to the Cardiology area.

In this situation two recommendations are highlighted:

- First is from the perspective of the Good Employee: he should never connect any untrusted usb key to a corporate or even personal device. It is a commonly used attack vector, attackers might have prepared it with malware to infect the device it gets connected to, if no appropriate corporate controls are applied to prevent it. But the recommendation can be extended to other kind of pluggable as mobile chargers, that make the impression that can’t contain any logic and thus don’t represent a thread, but the fact is that attackers are able to introduce malware on they.

Figure 25: USB Trojan

- Second, from the perspective of a real employee that may have actually lost the key. The recommendation is to never share sensitive information through an usb and, if necessary, it is recommended to encrypt it with tools like Bitlocker.

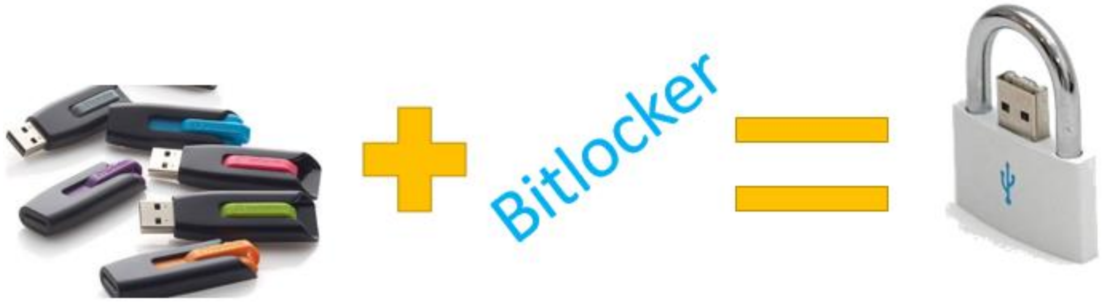


Figure 26: Bitlocker to protect USBs

As a final epigraph to this presentation, the objective is to explain the idea that even with appropriate controls stablished from the organization, there will be always a realm depending on user's responsibility. It was also intended to show some daily situations that may not seem threating in terms of cybersecurity but they actually are, depending on the interest an attacker would have to break organization's security. And this interest is high in healthcare organizations and it's being increased as the time goes by.

IV.5. Block 3: Phishing and social engineering

The block begins with a definition of the terms "Phishing" and "Social engineering" with the objective that users understand both widely used terms, but that may be confusing to the major part of non IT users.

Social engineering is a broad term used to describe a range of techniques to trick people into giving fraudsters what they want. **Phishing is a specific technique within social engineering**, designed to gain personal information. Phishing has been performed usually via email but, as will be shown in this training, different and new variants are arising and it is important that user be aware of them. In this section we present different ways of social engineering to make user familiar with them and to create awareness.

Email Phishing

In resume, email Phishing consists in sending to the victims an email that emulates a trusted source, and giving them instructions to perform some action. This action should be taken from the fraudulent email, normally by clicking a link, and here is where the fraud takes place: the link takes the user to a fake site that emulates the site that users expects to reach, and here (s)he is asked to log in by providing username and password or any other information that allow the attackers to supersede the user. In other variants, the link installs some malware in the client PC and then spreads along the reachable network. There are many variants and the requested action may be open an attachment.

With this scheme, any damage can be avoided if the required action is not performed (the link is not clicked, the attachment is not opened, etc.). To avoid it, users must follow the following instructions:

I. Do not open attachments or click on email links from users that we have not requested: in case of doubt, contact USC to assess the risks

II. Doubting any email that requires us for any URGENT action, even if it comes from a recognized person (e.g., a colleague or the CEO). Urgency is a factor that attackers commonly use to prevent us from scanning email. Remember that we should always be able to contact someone who can ask us for something urgent by another way (by phone, in person).

III. Do not click on email links from any unexpected recipient.

   a. Example of legal mail: a password change in an account in which, in response to our request, they send us a link to confirm the process

   b. Example of potentially illegal mail: an email arrives to us, without having requested it, indicating that we must access a page to update our data or attend to an important matter

   As a rule, directly access the page of the company in question (bank, facebook, amazon, etc.) without doing it through the link provided in the email

IV. Confirm that the email address corresponds to that of the sender, especially in emails that ask us to download files or click links, For example, USC<cxv@cybyx.ru> could be an example of someone trying to impersonate our USC.

V. Never respond to any suspicious email, and notify USC.

Spare phishing

Phishing started with rude emails translated automatically from one source language to many others, what normally included errors. They also talked about few common issues like heritages, denied payments or business opportunities. Those were happy days for cybersecurity because it was less probable that a user can take the bait. But as in many other fields the future is already here. It has evolved to a more fine-grained methodology where hook emails are prepared specifically to its recipient. That is known as *spare phishing* and are much more difficult to detect. Imagine you receive an email from a known person in human resources asking you to review an attached document concerning your contract. Of course, if you take your time and review the real address from the sender, the domain will not correspond with the organization real one, but it is necessary to "*think fast and type slow*" as the best strategy.

Anyway, always as possible both attachments and links should be avoided and the emails should explain the requested task and the way to reach the website, application or file necessary to perform it. This objective can be accelerated from the organization by providing advanced tools that allow to perform the tasks inside them and minimizing the necessity of downloading or managing corporate information from outside (word or excel files, or even papers). System integration is also vital to perform this objective.

Non corporate phishing

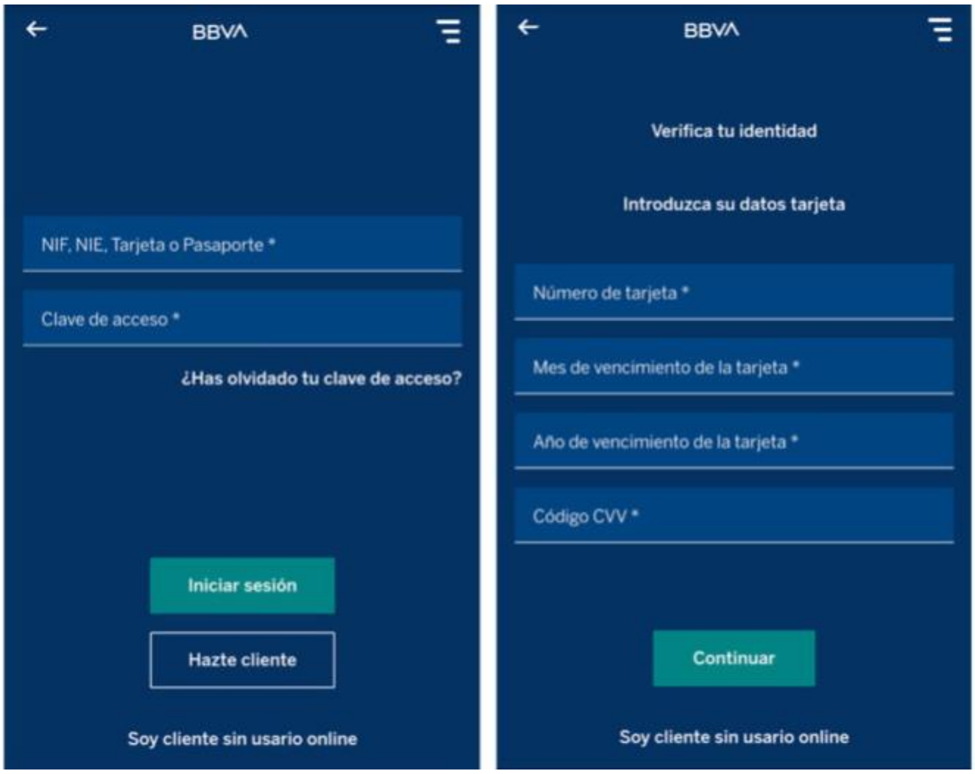
Outside spare phishing things has evolved as well. Those rude emails have become very elaborated emails that, through the included link, take users to a very elaborated website emulating the real one.

The most known cases have been related to banking. In Spain some of the bigger banks have suffered this kind of phishing:

EL PAÍS
A dangerous trojan scams apps of seven Spanish Banks in Android
El País, November 23th, 2019

Figure 27: Article about scams in banking apps

And you can make judgements if you would be able to detect the fraud:

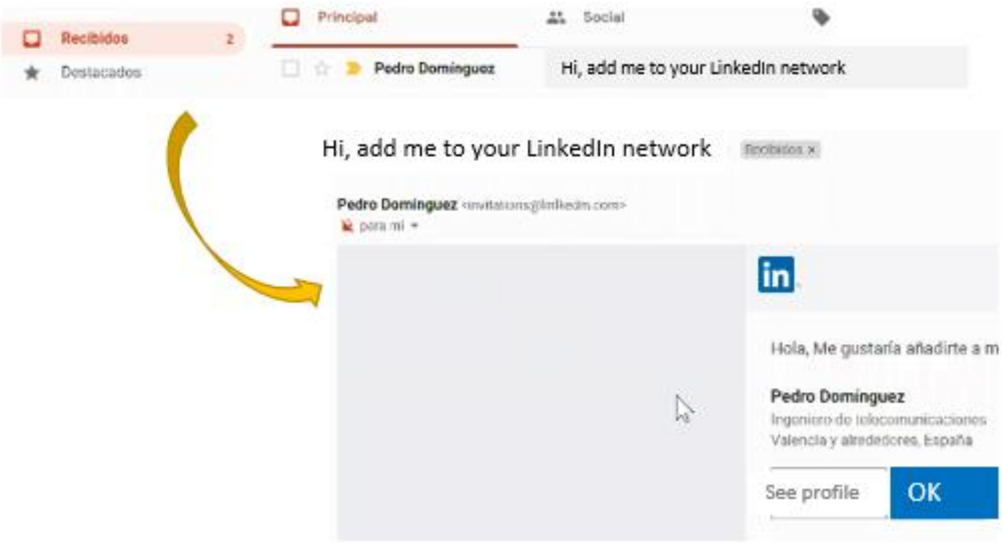


BBVA
NIF, NIE, Tarjeta o Pasaporte *
Clave de acceso *
¿Has olvidado tu clave de acceso?
Iniciar sesión
Hazte cliente
Soy cliente sin usario online
BBVA
Verifica tu identidad
Introduzca su datos tarjeta
Número de tarjeta *
Mes de vencimiento de la tarjeta *
Año de vencimiento de la tarjeta *
Código CVV *
Continuar
Soy cliente sin usario online

Figure 28: BBVA bank phishing example

It seems fairly clear the reason to get our credit card information, but think about any other password for a less sensible service and mix it with an unappropriated policy of sharing same passwords for many services: it is quite easy that the effect of a breach can be spread for many other fields, including the hospital workplace. Imagine a phishing attack using LinkedIn, a social network with a consideration of a serious place related to work career:

1.-The victim may receive an email with an invitation to join other's circle. When opening the email, it seems the same LinkedIn message that the victim has seen so many times before:



Pedro Dominguez Hi, add me to your LinkedIn network

Hi, add me to your LinkedIn network

Pedro Dominguez <invitations@linkedin.com>

Hola, Me gustaría añadirte a m

Pedro Dominguez
Ingeniero de telecomunicaciones
Valencia y alrededores, España

Figure 29: LinkedIn fraudulent invitation

By clicking the "Accept" button, it is apparently guided to the LinkedIn page where as many times he needs to log in to proceed with the desired action:

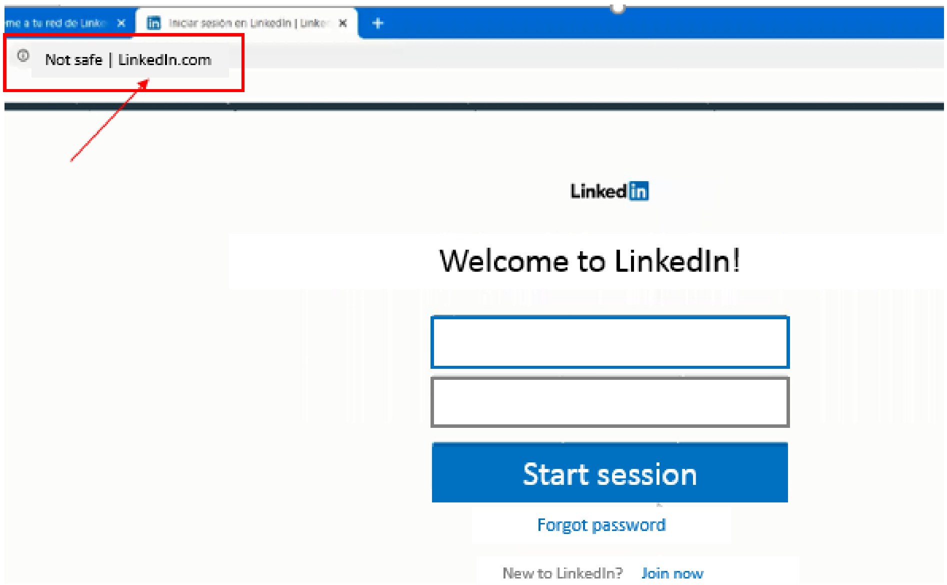


Figure 30: LinkedIn fraudulent page

But that page is not the real one, as it is shown in the previous image by two details:

1. The Internet navigator is showing a message indicating that the site **is not safe**
2. The URL of the site is “linkdin.com” and not “link**e**din.com” (missing ‘e’)

But let’s assume the user is no aware of this fraudulent situation and tries to log in by providing user and password and clicks “Start session”. Then (s)he may see the same page again requesting for user and password and may think there’s been some kind of problems, then he provides it again ang gets into the LinkedIn site.

But what actually happened is that the first try has been performed in the fake site and with it he did provide credentials to the attackers, and then the page redirected to the correct site, and the user did not notice the fraud.

As a result, an attacker got user’s credentials for a site, that may be used for other sites as well, and the user is completely agnostic to that situation so he is not taking any preventive action like change passwords, inactivate accounts or advising the emulated site.

How can it be avoided?

I. By entering the LinkedIn URL instead of following the link in the email, or

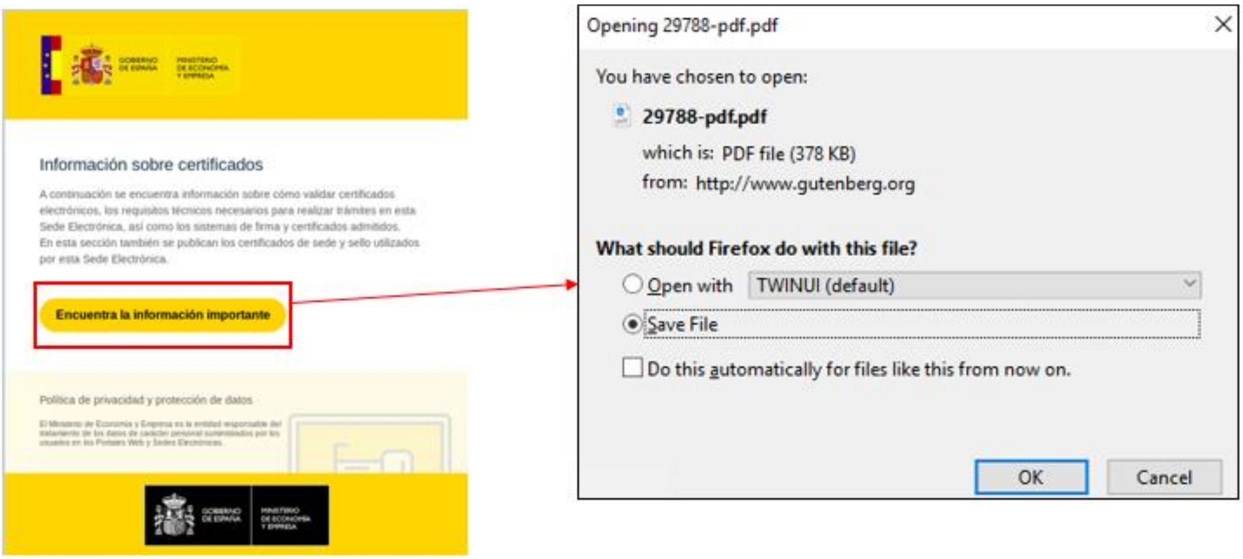
II. By checking the URL once in the website, and the alert in the internet navigator regarding the security of the website

But email is not the only vehicle for Phishing, there are different variants as *vishing* (voice) or *smishing (sms)* that will be covered in the following sections about social engineering.

Malware installation

Some phishing emails are not intended to lead victims to a fake site, but aim to make them a different action: open or download a file that can be attached or linked, and through this action a malware gets installed into the victims PC and can be spread along the network, causing different damages.

Those are fine-grained attacks that may emulate emails from both corporate origins or persons (colleagues, human resources, etc.) and external sources. As an example, in Spain were detected this kind of attacks emulating emails from the Spanish Ministry of Economics, with a link to a file and instructions to open and read it:



GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA

Información sobre certificados

A continuación se encuentra información sobre cómo validar certificados electrónicos, los requisitos técnicos necesarios para realizar trámites en esta Sede Electrónica, así como los sistemas de firma y certificados admitidos. En esta sección también se publican los certificados de sede y sello utilizados por esta Sede Electrónica.

Encuentra la información importante

Política de privacidad y protección de datos

El Ministerio de Economía y Empresa es la entidad responsable del tratamiento de los datos de carácter personal suministrados por los usuarios en los Portales Web y Sedes Electrónicas.

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA

Opening 29788-pdf.pdf

You have chosen to open:

29788-pdf.pdf

which is: PDF file (378 KB)

from: http://www.gutenberg.org

What should Firefox do with this file?

○ Open with TWINUI (default)

● Save File

□ Do this automatically for files like this from now on.

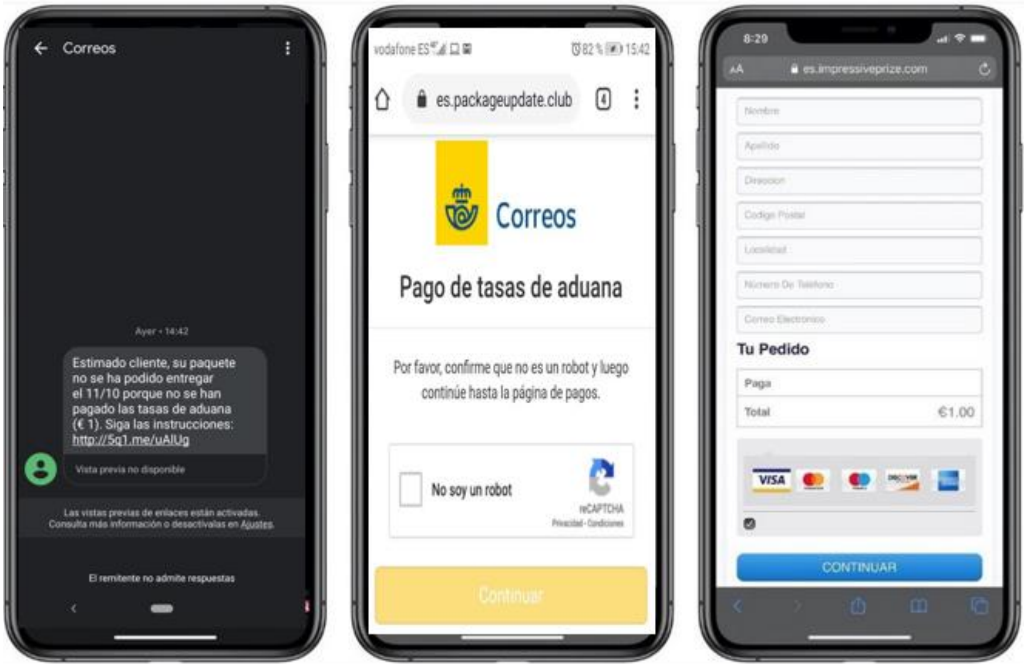
Figure 31: Malware email emulating official sender

Again, no security breach nor damage can be done if the victim does no perform the required actions. Aligned with the previous recommendation, official organizations ask users to access their official sites and access to any pending notification, so it is a good recommendation to never access this kind of content directly from the received emails.

Smishing

Smishing is a branch of phishing performed through SMS messages. The pattern is the same: the hook is a notification (SMS in this case) that requires an action from the victim, both provide sensitive information or to open or download something.

The following figure illustrates it by three mobile phone screenshots:



Estimado cliente, su paquete no se ha podido entregar el 11/10 porque no se han pagado las tasas de aduana (€ 1). Siga las instrucciones: http://5q1.me/uAlUg

Vista previa no disponible
Las vistas previas de enlaces están activadas. Consulta más información o desactívalas en Ajustes.
El remitente no admite respuestas
vodafone ES 82 % 15:42
es.packageupdate.club
Correos

Pago de tasas de aduana

Por favor, confirme que no es un robot y luego continúe hasta la página de pagos.

Figure 32: Smishing example

- ➢ In the left one a SMS has been received telling the victim that some product couldn't be delivered because there is a fee pending for payment. It is quite probable that someone has pending delivers so it may seem veridic. The SMS includes a link that take victim to the second screenshot.
- ➢ In the second (middle) screenshot, attackers emulated the deliver company page and logos, simulating a payment gateway.
- ➢ In the third the victim is required to provide credit card information to complete the payment. Only a small fee of one euro is required so the user can easily accept to perform it.

In general, users should not trust this kind of notifications. Real ones would not include the link to the payment site in the SMS and would ask user to access the company site by themselves and complete the pending action.

Vishing

Vishing is another modality of phishing but changing the vehicle: this time the hook is a voice conversation. Attackers impersonate a person or legitimate business to scam victims and retrieve personal, sensitive or confidential information.

These *vishers* even create fake Caller ID profiles (called 'Caller ID spoofing') which make the phone numbers seem legitimate.

Deepfakes

Deepfakes is an acronym of *deep learning* and *fake*. It is an artificial intelligence technique that allows the edition of fake videos of people who are apparently real, using unsupervised learning algorithms, known in Spanish as RGAs (Antagonistic Generative Network), and existing videos or images.

Cybercriminals are leveraging deepfake-as-a-service toolkits to wage disinformation wars on corporates and, worse, to power sophisticated phishing attacks.

Deepfakes can be performed only with audio or adding video as well. To show an example of what can be done, it is recommended to access this video [18].

The CEO fraud

The CEO fraud is a BEC (Business Email Compromise) scam that works by spoofing or impersonating the email account of the CEO or another business executive in order to send a fraudulent wire transfer request to those who manage company wire transfers (CFOs, Financial Controller, or accountant). Believing that the request is legitimate, the unwitting employee will then transfer funds.

There have been found two main techniques being used in the campaigns against institutions, including healthcare. The first spoofs the *From* field to make it seem that the email came from the CEO or executive, while the *Reply To* field is filled with the scammer's email address. The second technique uses copycat domain names, where the scammer uses a domain name that's very similar to the target healthcare institution. This can be done by using an email extension that could be off by just one character, for example 'mariasalud.es' instead of 'mari**n**asalud.es'

The scammer then crafts a simple and innocuous subject line, which commonly includes the following phrases:

- Extremely Urgent
- Treat As Urgent
- Treat Very Urgent
- Due Payment
- Urgent Payment

In addition to the urgency, the scammers ask for confidentiality, so the attack can remain unnoticed as long as possible.

Baiting

Baiting is like a real "Trojan horse", using a physical medium, and based on the victim's curiosity or greed. It is similar, in several ways, to phishing attacks. However, what sets them apart from other types of social engineering is the promise of an item that hackers use to lure their victims. Baiters (as these attackers are called) can use music or free movie downloads, if they offer their credentials to a certain page.

For example: a "lucky winner" receives a digital audio player which he does is compromise any computer to which he connects.

Here applies the concept of "*To good to be true*".

These attacks do not occur exclusively on the internet. Attackers can also focus on exploiting human curiosity through physical means. An example can be a mobile phone charge cable. At a first glance if any user finds a charge cable on his work table he will not hesitate about using it because it is a logic-less item that can't lead to risks or security breaches. But far be it from this case. Attackers can attach logic components to that kind of simple items and infect the device it gets connected to.

Xataka
O.MG Cable
It seems an USB cable, but it serves to install malware and control other devices instead
Xataka, February 16th, 2019

Figure 33: Baiting example

IV.6. Block 4: Cell phones

It is mandatory to make a specific reference to cell phones and smartphones because they have acquired capabilities like those of personal computers and business users are granted high-level access from personal mobile devices , smartphones and tablets are effectively replacing desktops for many business tasks. However, personal mobile devices don't offer the same level of built-in security or control as the organization-owned desktop computers they are replacing.

This trend is known as BYOD (Bring Your Own Device) and it is getting even more common in healthcare because of the necessity to allow physicians to monitor patients even not being physically near.

That is causing that a high percentage of workers now routinely access corporate data from smartphones, and that means keeping sensitive info out of the wrong hands is an important concern.

Many, if not all, the previous hacking techniques may be applied through a mobile phone, and the general recommendations of not clicking links from emails, SMS, check websites URL, etc. are relevant on smartphones as well. But there are, moreover, some specific comments to be made in reference to cell phones

Install apps only from certified sites

When new Apps are developed, they need to be certified in terms of security, performance, resource needs, etc. This certification is made before allowing the apps to be uploaded to the certified sites (Play Store for Android and App Store for iPhone's IOS) so if the apps are downloaded from these sites, users can be sure those controls have been performed and the apps are safe, among other features.

That will ensure that, for example, it is not a fake app emulating a banking, insurance company or government app that is asking us to enter sensitive information that can be used against us. Some examples of this have been explained before, being bank apps the most common in this kind or attacks.

Therefore the recommendation is to always download apps from the certified site corresponding to our smartphone type, and never do it from links contained in emails, SMS, websites or any other place.

Control permissions granted

By downloading Apps from the official sites users can be sure that they are not fake apps or apps that have been reported for security issues. But there is something else that user must take care of. Each app will need permissions to some functionalities or contents into the phone and users are asked to allow access to them during the app installation.

It is extremely important to give permissions according to the app expected functionality, and if more than reasonable permissions are required for the app to work, discard and uninstall it.

Some examples:

App_1: Lantern

Expected functionality: To illuminate using smartphone camera flash

Expected permissions: Access the camera

Required permissions: Camera, microphone

Correct behaviour: Not allow the app to use the microphone or any other feature apart from the camera. If the app can't be started without those extra permissions, discard it and uninstall.

App_2: Funny sound recorder

Expected functionality: To record voice or sound in general and apply filters to introduce distortion.

Expected permissions: Access the microphone. Access to the disk folders.

Required permissions: Camera, disk folders, camera, contact list.

Correct behaviour: Not allow the app to use the camera nor access the contact list. If the app can't be started without those extra permissions, discard it and uninstall.

Note: At each moment it is possible to review permissions given to each app and modify them, by granting some news or declining others previously given.

The reason for this is that official app stores don't evaluate if permissions required are appropriate to the app expected functionality, and final user common sense is the only filter to be applied at this point.

Stay updated

Even official and well-intention apps can have security vulnerabilities that might be discovered once the app have been installed by users. When this occurs, the source app is updated with a fix to the detected vulnerability and published with a new version.

That's why it is also important to keep devices and apps updated. Periodic updates are a good policy to keep safe.

Install antivirus and other complements

Installation of antivirus is a good recommendation in smartphones as well. They keep users protected from known vulnerabilities in real time, in the same way that PCs.

In addition, there are other kind of apps complementary to the antivirus that help to identify potential risks in our smartphone. One example for Android is *Conan mobile*. This app scans our smartphone and offer security information in different sections:

- ➢ Configuration: It analyses Operative System's configuration detecting risky situations, and classifies them in base of its level of risk.
- ➢ Apps: It alerts if any dangerous app is found installed, classifying them into:

  - Malicious: if it is included in the lists of falsified apps
  - Suspicious: in case it would have been detected as dangerous by some antivirus
- Permissions: It gathers permissions declared by apps, grouped by potential threads.
- Proactive service: It alerts if abnormal and potentially dangerous behaviours, in two sections:
  - Events: it recovers:
    - Changes in important files as /etc/hosts
    - Detections to untrustworthy networks
    - Check new apps installed
    - Calls and messages to special tariffication numbers
    - Detection of potential risky connections
    - Detection of botnet related threats
  - Connections: It shows the network connections established by the apps and alerts when may be considered dangerous. In addition, geolocation of the destination can be performed.

IV.7. Recommended behaviours

From the previous training sessions and as conclusion the following table includes recommended actions that will reduce risks and can be easily performed by any user. They must be kept on mind on daily actions and both in work and private scopes, as they are not clearly delimited and incorrect behaviours in one of them may have consequences in other:

SUBJECT	RECOMMENDATION
Passwords	Chose strong passwords. 8 characters length as minimum. Combine letters and numbers.
	Don't reuse passwords for different services
	Use a password manager
	Don't reuse passwords for different services
	Never write passwords in paper
	Use multifactor authentication
Digital print	Network activity is part of real life. Beware what you write.
Terms and conditions	Read carefully the terms and conditions accepted when acquiring online services
Metadata	Delete hidden metadata
Paper data	Use certified protocols to destroy data in paper format
Email data	Encrypt digital data when sending it to external sources
Public networks	Don't share nor access sensitive data through public networks
Smartphone apps	Take care of permissions required for apps.
	Download apps from trusted repositories
Spoken data leaks	Take care of who is listening when speak about sensitive data
USB devices	Never plug USB from unknown or untrusted sources
	Never plug cables from unknown sources
	Encrypt content of USB devices

Phishing	Don't use links contained in emails or SMS. Go direct to the site instead.
	Don't take quick decisions, urgency should always lead to suspect
	Don't open nor access attachments from not required communications
	Check email addresses, not just descriptive names
	Voice calls can also be spoofed. Check identity by another way
Device security	Keep the devices updates
	Install antivirus

IV.8. Reminders

The live training sessions described in previous sections will take place, in the best case, once per user. Said in other way: non IT users, mostly clinicians, will be listening for a period of 90 minutes about cyber risks, thread types and recommendations. It is much content to be remembered and make it persistent, even offering presentations, links or even extra training by demand.

It is important to make those messages and recommendations persistent and familiar and to achieve this graphical material is going to be developed.

That material must include short and direct messages, straight to the point and that may be easily related to contents previously explained during the training session. Each concept included will be developed by one illustration a one short message, and they will be combined and used in different ways:

i. Posters in paper format, including a group of concepts and illustrations, placed in clinical work places as nursery controls on the wards or physicians' workrooms.

ii. Same posters in digital format, inside a specific folder on the corporate document management system.

iii. Banners in the corporate intranet, changing each few days and being interlaced with other important messages addressed to the staff.

Similar graphic material will be used as educational material for patients, as described in Section V.

The concepts included here will be:

ID	TITLE	SUBJECT
1	Who wants to know	Don't friend anyone you don't know in real life
2	Take it slow	Don't attend to urgency requirements when sharing sensitive information
3	Lock, lock, ... LOCK!!	Always lock your devices
4	Caution with permissions	Don't give more permissions that those really needed
5	Source smart	Download apps from verified sources
6	Vaccinate your device	Install antivirus in your devices
7	Size really matters	Choose at least 8-character length passwords
8	2 better than 1	Use multifactor authentication when possible
9	It's in your eyes	Add biometric authentication factors when possible
10	Look for the "S"	Legitimate sites use HTTPS
11	Linked ... and lost	Links on websites and emails can be spoofed

12	Too good to be true	Scams are usually performed through amazing deals
13	Shield with auto-update	Maintain updated your apps and devices
14	Free Wi-Fi ... or not	Don't share sensitive information through free Wi-Fi
15	Was I expected it?	Think if you started the communications or not

Table 7: Index of graphical material

The whole content will be included in **D3.3- Final description of educational framework**. Below there are included a subset as a descriptive sample:

Size really matters

Your password, **the longer the safer** . Never less than 8 characters!

... and how to do it?

- Think of **sentences** to be able to remember better.
- **Mix** languages, symbols or anything, so it only makes sense to you.
- ... and **never reuse** passwords!

2 better than 1!

There are different **types of authentication**: what you **know**, what you **have** and what you **are**.

If you **combine at least two** of these guys, you will make the bad guys

they have to work very hard to hurt you.

It’s in your eyes

Add the **“something you are“** factor always as possible

Take it slow

Attackers will try to lead you to take quick decisions.

Think fast but type slow and they will not hurt you

Figure 34:Sample of reminders for health staff

V. EDUCATIONAL MATERIAL FOR PATIENTS

The contents previously presented for health staff can be perfectly used to train patients as well. But the main handicap about extending cybersecurity awareness education to patients is to find the appropriate ways to reach them.

In the case of the staff a communication program can be defined in a way that it is no eligible to join it or not, or at least it is difficult to avoid it. But in the case of patients most of them have fleeting contacts with the healthcare organization and the time is used to give the requested cares and services, with no possibility to place any extra activity.

In this context the way to reach patients should be to introduce them in parallel with the ”normal” healthcare activity and make them accessible to deepen into it by requesting it or make them available online resources.

Following this strategy, the following channels are going to be used in this educational framework:

- Clinical apps: ProTego toolkit will be used by two apps, Pocket EHR and FoodCoach. These apps allow to push information to the users (patients) and to show it cybersecurity tips in the form of the graphical reminders presented in the previous section. Those materials will include a ”know more” button that will open a recorded webinar explaining the same content than live sessions. Future apps that should be ProTego ready will be required to accept the same behaviour, this is, to have a dedicated cybersecurity section where reminders will be placed. Those reminders and cybersecurity contents will be provided by the healthcare organization.
- As mentioned before, posters in paper format will be placed in different places, some of them reachable by patients as nursery controls on wards.
- Calling monitors: it is common that hospitals use automatic procedures for calling patients to external consultancies. Those monitors, except when the call is made, are showing TV signal or any other content of interest for the hospital, like remembering flu vaccination. Those monitors can be used to show graphical contents in the form of slices, with a simple URL at the bottom, leading to the recorded training sessions.

In all these channels the strategy is to reach patients without requiring effort from their side, and let them to access further information.

VI. EDUCATIONAL MATERIAL FOR IT STAFF

This section will be completed in D3.3-Final description o Educational Framework as it needs details on how the ProTego toolkit to be deployed to be used.

VII. EDUCATIONAL MATERIAL FOR EXTERNAL PROVIDERS

This section will be completed in D3.3-Final description of Educational Framework as it needs details on how to integrate new apps to the ProTego toolkit, and use its cybersecurity features.

VIII. CONCLUSIONS AND NEXT STEPS

In this document, we presented the initial description of the ProTego educational framework. In line to what discussed in the Description of the Action we provided training material for health staff that will increase situational awareness, what will help to reduce cyber risks. This training material is also in line with the conclussions of the survey designed and executed in D3.1, whose proven hypothesys has been taken as requirements to cover, in order to promote correct behaviors regarding cybersecurity.

Future deriverables will analyze the impact of the execution of this training by comparing the results of the survey with the Risk Awareness Profile tool presented in the D3.1 as well. The final version of the reminders will aso be included.

They will also include educational material fot IT staff, covering the deployment and configuration of the ProTego toolkit, and recommendations regarding the use of IO(M)T in healthcare organizations as they represent a widely present item that use to implement few security controls due to provider’s restrictions on configurations.

Finally, they will describe the instructions for external providers and developers in order to develop ProTego-ready applications.

IX. REFERENCES AND INTERNET LINKS

[1] ISO 27001:2013, A.6.2.1, “Segregation of duties”

[2] EU GDPR, recital 81

[3] https://whatis.techtarget.com/definition/information-security-management-system-ISMS

[4]https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[6] https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[7] https://www.nist.gov/cyberframework/framework

[8] Brown (2001). "The Privacy Paradox"

[9] Sören Preibusch (2015). "Privacy Choices Behavioural Economics Review"

[10] Spyros Kokolakis (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon"

[11] https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

[12] https://rightcarealliance.org/about/what-is-right-care/

[13] John Badham (1983). “WarGames”

[14] https://www.hindawi.com/journals/scn/2019/8715264/

[15] https://www.gartner.com/en/documents/2410615/definition-people-centric-security`

[16] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[17] https://www.youtube.com/watch?v=YiRPt4vrSSw

[18] https://www.youtube.com/watch?v=5rPKeUXjEvE