CCN-CERT

BP/08

Social Network Best Practices

SOCIAL NETWORK BEST PRACTICE

JULY **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit:

Release date: July de 2021

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set forth herein, expressly disclaiming any implied warranties of any kind that may be found to be related. In no event shall the National Cryptologic Centre be held responsible for direct, indirect, incidental or extraordinary damage derived from the use of the information and software indicated, even if advised of the possibility of such damages.

LEGAL NOTICE

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies thereof by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the sanctions established by law.

Index

1. About CCN-CERT

The **CCN-CERT** is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity,** by being the national alert and response center that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centers

Its ultimate aim is to **make cyberspace more secure and reliable,** preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

CCN-CERT is the Information Security Incident Response Capability of the National Cryptologic Centre, CCN.

2. Introduction

2.1 Cyberspace as an inhabited territory

Social networks are where virtual identity is configured. They can be: individuals, groups, companies or institutions. It is composed of: an alias, a personal image and a biographical statement.

Cyberspace is a domain of social exchanges that is growing exponentially every year and has established itself as a territory of its own in which individuals, collectives, companies and institutions carry out activities.

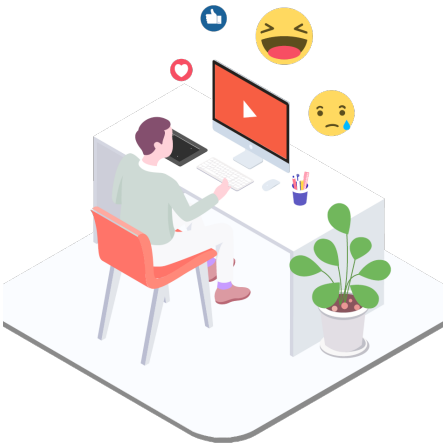
This territory is essentially made up of identities and objects connected through the internet. By 2020, it is estimated that there will be 50 billion objects connected to the Internet of Things (IoT), interacting with people through their digital identities.

However, it is not only at the quantitative level that human beings have come to "inhabit" cyberspace, but cyberspace is a virtual territory where humans "make life": they interact, communicate, engage in social, commercial, political or religious exchanges and, in short, end up "being and being".

Beyond the general presence on the web, social networks configure the virtual identity of individuals through their experiences, and their life in cyberspace.

This digital identity is composed of a name (one or several aliases); a personal image (avatar type), which represents the individual in one or several social networks; and a biographical statement, based on a series of personal or job references such as geographical location, studies or work.

More importantly, associated with these references is a significant volume of content in text, image, audio or video, where a person shows their behaviour, their affinities, their interests and, in short, a more or less detailed trace of their personal, social and, often, working life.



2.2 What are social networks?

As soon as a group of individuals sharing personal social bonds or nexus of interest in the economic, religious, political, leisure or other spheres emerges, a social network is already configured. Therefore, the social relationship of human beings through networks exists since human beings communicate and interact with each other.

However, the emergence of social networks as a global and everyday concept, associated with millions of human beings regardless of their geography of residence or culture of origin, is inherent to the appearance and exponential growth of social exchanges through the internet, the web or, in short, cyberspace.

It could be said that social networks in cyberspace are the digital or virtual equivalent to the set of personal, work or social relationships that human beings usually maintain in their *physical lives*.

In social networks, in cyberspace, individuals maintain an agenda of friends or acquaintances, converse with them and share interests and hobbies. Social networks are configured to share massive digital experiences; for example, one can virtually attend a music concert or a university lecture given in a country other than the user's physical country of residence.

2.3 What do well-meaning people use social networks for?

The main motivation for signing up to a social network, at least to those where it is necessary to create a profile, is to keep in touch with friends and acquaintances[1] or to access content of interest to the user. In other words, the main motivation for social networking is interaction with other members of the community (family, friends, professional circles, etc.).

Social networks, as a mass communication tool, enable the expansion of relationships and the formation of identity. Following Randy Conrads' creation of the website classmates.com in 1995 to keep in touch with his former high school classmates, social networking has seen rapid growth, aided by the development of applications and connectivity solutions based on mobile devices.

1. Source: "Informe de resultados Observatorio de Redes Sociales". The Cocktail Analysis. Fourth wave, 2011. April 2012

2.3 What do well-meaning people use social networks for?

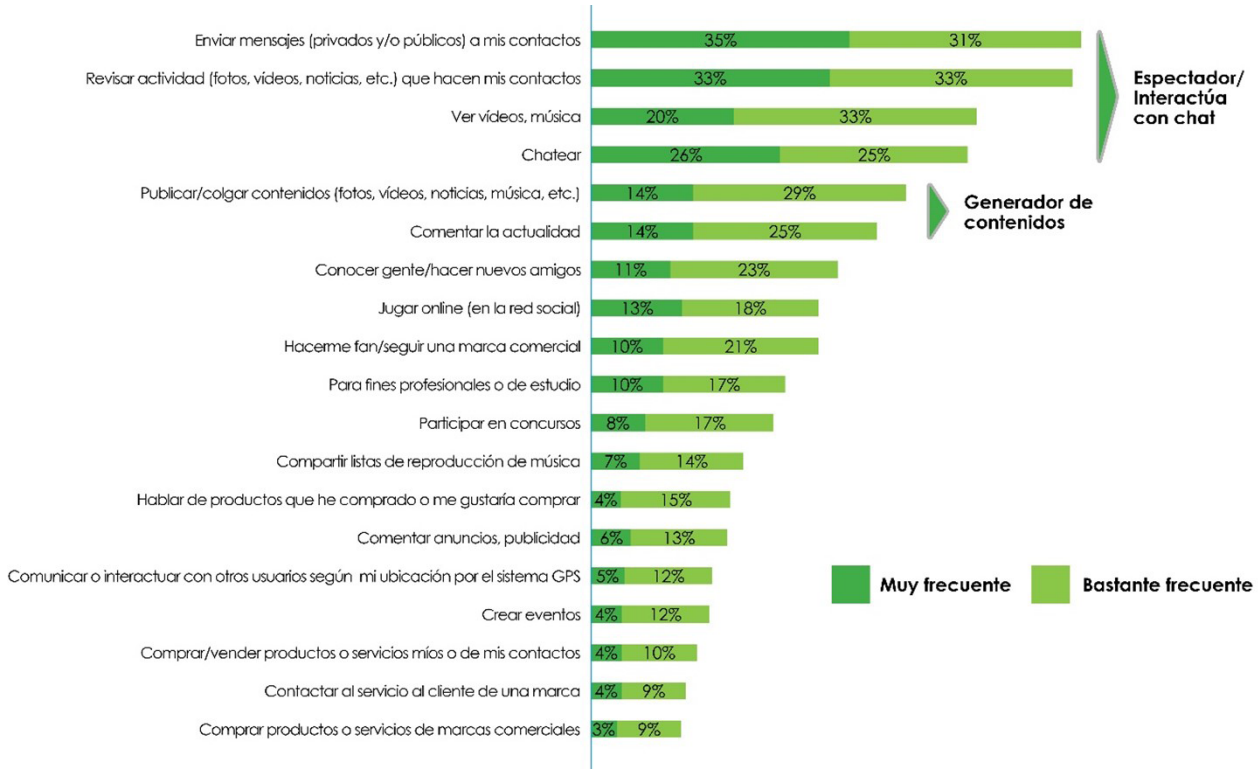


Figure 1.- Reasons for belonging to social networks (iab Spain study)

2.4 What do malicious people use social networks for?

The enormous possibilities offered by social networks and their massive use entail a series of risks of various kinds, both in the private and personal sphere as well as in the professional sphere.

Given the growing trend towards the use of such networks as a medium for cyber-attacks, it is of vital importance to be protected, to use them properly and within a secure environment.

In general, actors using social networks as a gateway for cyber-attacks and compromising users' security exploit three (3) types of vulnerabilities implicit in the networks' own "social architecture":

2.4 What do malicious people use social networks for?

Overexposure of personal information. The overabundance of personal information, which users disseminate through their social network profiles, is an attractive raw material for cybercriminals to use for harmful purposes.

Information highways. The v fluidity and openness inherent to communication turns social networks into veritable information highways through which socially innocuous and legitimate communications circulate, as well as content linked to various types of malicious code. This malware is not specific to social networks, but it takes advantage of the fluidity of social networks' communication to distribute itself and spread its infection to as many users as possible.

Massive use. With a penetration rate of 42% of the world's population (3.196 billion people)[2], social networks are the perfect vehicle to access a large number of people, potential victims of cyber-attacks.

2. Global Digital Report 2018 (https://digitalreport.wearesocial.com)

2.4 What do malicious people use social networks for?

The most common malicious use of social networks falls into the following categories:

- **Social engineering:** based on the design of deception mechanisms or schemes, aimed at getting users to perform certain actions that will harm them and will allow cybercriminals to make illicit profit.
  Social engineering draws on known patterns of human behaviour to design online behavioural processes that encourage users to perform certain actions, access certain content, provide information in different contexts or share sensitive data.
- **Identity theft:** to do so, cybercriminals take advantage of personal information disseminated by users on social networks.
- **Cyberbullying:** it uses the ability of one person to psychologically harass another, thanks to the information obtained from the victim through their profiles on social networks, and is particularly serious when it involves minors and takes place in the school environment . Some specific forms of cyberbullying are:
  - **Sexting**: this consists of sending photographs and videos with sexual content, filmed or recorded by the protagonist, over the internet, especially via smartphones (applications such as WhatsApp facilitate this practice). It is an increasingly common practice among young people and can lead to harassment or extortion if the recipient of the photographs has malicious intentions.
  - **Grooming:** a method based on a set of strategies that an adult develops to gain the trust of a minor through the Internet, and thus gain control over him/her on an emotional level, with the ultimate aim of obtaining sexual concessions.
- **Reputational damage:** in the personal, social or employment sphere, arising from content on social networks that may damage a person's relationships in those spheres.
- **Harmful or misleading advertising:** disseminated and delivered through social networks, often for the purposes of fraud or the dissemination of harmful code.

3. https://www.anar.org/wp-content/uploads/2017/04/INFORME-II-ESTUDIO-CIBERBULLYING.pdf

Crime in the physical world: it uses information obtained from social networks to carry out criminal acts in the physical world, such as holiday thefts, taking advantage of information advertised on social networks, or kidnappings, with the aim of obtaining a ransom based on a person's "standard of living" as observed on their social networks.

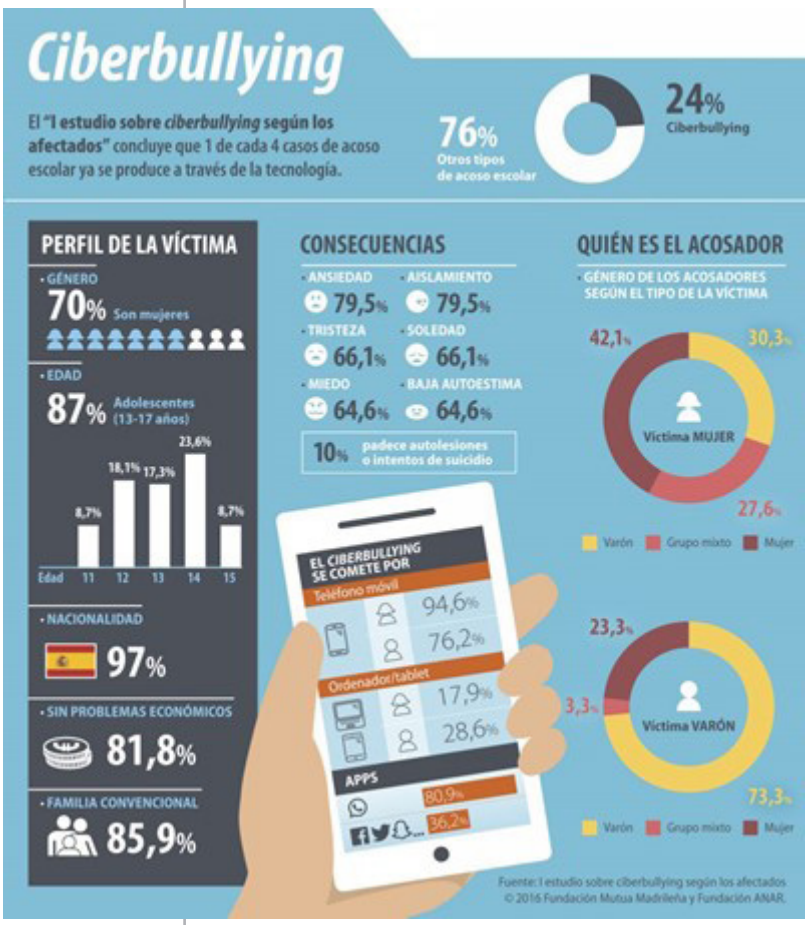


Figure 2.- ANAR Foundation

Malware distribution: to do so, they use the interpersonal information highways that social networks represent. Cybercriminal groups use social networks simply as distribution channels for all kinds of malicious code. They do not seek to exploit programming or configuration vulnerabilities in the social networks themselves, but rather to download themselves onto users' devices (desktops, mobile phones, tablets) and, once there, to exploit vulnerabilities in the *apps* and *software* installed on that device.

The most common ways of distributing malicious code through social networks are:

2.4 What do malicious people use social networks for?

Phishing and Pharming. *Phishing* is a type of attack in which social engineering is used to obtain personal information from users, mainly that which allows access to financial services. To reach as many victims as possible and increase the chances of success, they use spam to distribute themselves. The mail sent to the recipient contains links to modified websites of banks and financial companies, so that they enter their personal data such as bank account numbers, passwords, social security numbers, etc.

Pharming is the redirection of legitimate domain name requests to a fake or fraudulent website by exploiting the DNS system (DNS hijacking or DNS poisoning).
Phishing techniques are also used, impersonating homepages on social networking platforms, to collect information and try to access other services used by the victim, as it is common to share the same username and password for most services offered on the internet.

Malicious links. This type of attack usually employ the formula "message plus link", with the link leading the user to the malicious content. In the case of an attack on Facebook, for example, the victim's wall is often used to post a message, an inbox or a photo in which the user is tagged.

In the case of Twitter, this type of attack is carried out through a mention, a private message or through link shorteners, which are used on this platform, and which are exploited in *spam* and redirection campaigns.

Promising videos. One of the most common 'hooks' for social media attacks, as with email, is the promise of a shocking video, such as the one promising to show the death of Osama Bin Laden.

By clicking on these videos, information is displayed on the social network profile, publishing the same or a similar video, without the victim's consent.

2.4 What do malicious people use social networks for?

A TrendMicro[4] study suggests that cybercriminal groups prepare scam schemes (phishing campaigns) on media events between two (2) weeks before and three (3) hours after the event. In addition, up to 13% of users have been victims of identity theft via social media; 69% of adults and 88% of teens are exposed in some way to bullying or cruelty on social media; and nearly five (5) million people regularly post travel plans on social media.

Figure 3.- Information shared on social networks (TrenMicro)

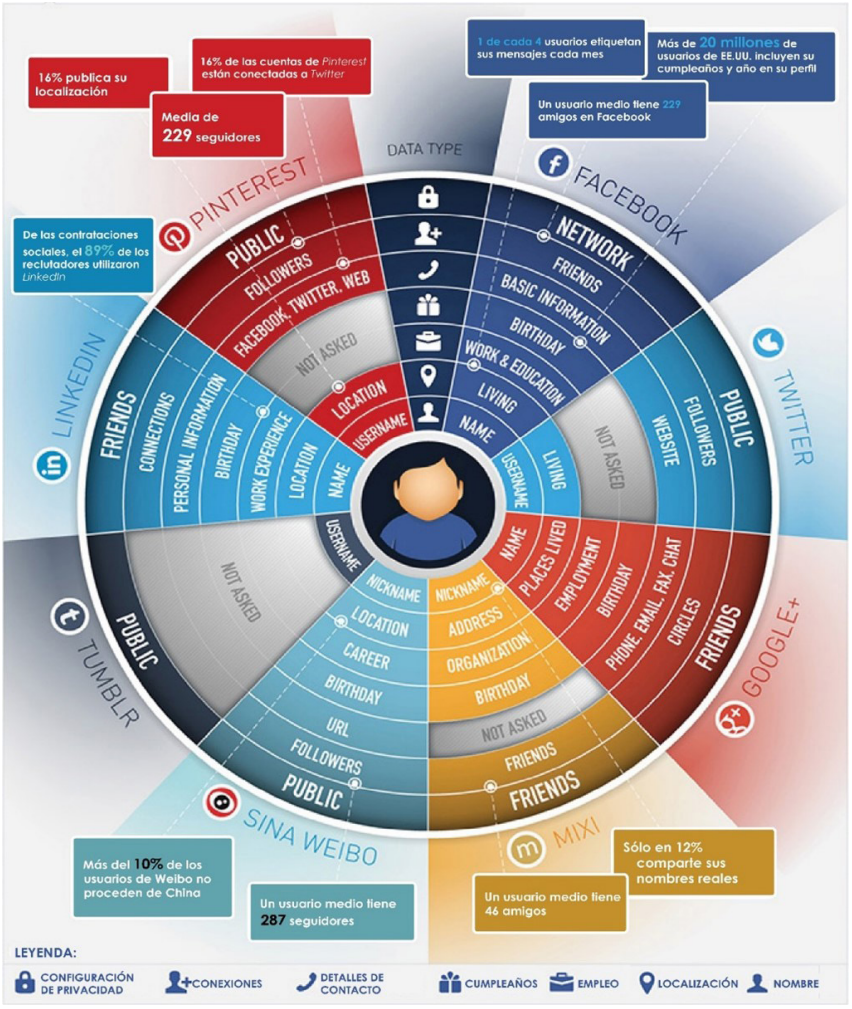
On the internet, many of the risks to which systems and their users are exposed have to do with vulnerabilities in web servers, content management systems, database configurations or access panels. It is common, for example, for a vulnerability in the code of a web server to be used by an attacker to gain illegitimate access to the website's database of users and steal users' personal data.

On the other hand, **malicious code** can be very varied in its design and functions (Trojans to steal personal information, remote access tools to take control of devices, *ransomware* to extort money, *adware* for fraud...), but they all have a common element, a kind of *genetic code* that all malware possesses: it will be designed to exploit one or more vulnerabilities, generally in software and, to a lesser extent, in the hardware of devices connected to a network, the internet being the most accessible.

4. http://blog.trendmicro.com/trendlabs-security-intelligence/the-risks-of-posting-in-social-networks/

2.4 What do malicious people use social networks for?

There is a clear difference between the vulnerabilities presented by social networks and those exposed by internet-connected devices. Social networks are a privileged channel, due to their interpersonal connectivity, for malicious code to spread and infect vulnerable user devices. In other words, the vulnerability that malware writers exploit in social networks is the very *connectivity intrinsic* to the interpersonal structure of the network.



Although social networks may have vulnerabilities related to their software programming or design that allow an attacker to gain illicit access to personal information or compromise the user's security, this is rarely the case. Sometimes a social network vulnerability would allow

an attacker, for example, to access or modify users' private information. However, these occasional vulnerabilities in social networks are not usually their Achilles' heel, nor do they draw the attention of cybercriminals to them.

In general, the most prevalent malware is developed to exploit vulnerabilities in the software of applications (programmes) or *apps* on users' physical devices (phones, tablets...). In this context, social networks are mainly used as **vehicles for the dissemination and transmission of malicious code** with the aim of infecting users' devices that are connected to the internet.

In this malicious use of social networks as vehicles for the propagation of threats, authors mainly exploit two (2) inherent characteristics of social networks: the overabundance of personal information and the large volume of data. In both cases, the key factor is the behaviour of users on the social networks themselves through their virtual identities and interaction with other users.

3. Best practices in the smart use of social networks

The greatest risk posed by social networks is not associated with the way their software is programmed, nor with the weakness or strength of their encrypted connections to users. The greatest risk of social networks is mainly related to users behaviour:

Smart extreme: smart use of social networks means making the most of them to interact with friends and contacts, share information or interests, and express feelings and emotions in cyberspace; but at the same time, it is necessary to adopt protection routines that are not very different, in philosophy, from those that any person would adopt in physical space.

People do not usually leave their homes open or exposed to intruders, do not tell intimacies to strangers, do not leave their cars unlocked in the street or try not to walk alone in the dark in an unfamiliar area. These behaviours, which are an intelligent way of preventing risks in physical space, also have their correspondence in cyberspace.

Vulnerable extreme: vulnerable behaviour implies carelessness and lack of protection of the personal and sensitive information that is disseminated and shared publicly; in the percentage of privacy that is disclosed, accessible to acquaintances and strangers alike; and in the acceptance of suspicious content that can lead to different types of malware. In short, vulnerable behaviour means going out unprotected into cyberspace, as if walking barefoot on a path full of broken glass.

As in the analogue world, in cyberspace you should not share personal data with strangers. You should also be very cautious about what data strangers share with you.

The **user** is the "*Achilles*' heel" since, although software and hardware devices may be equipped with the latest cybersecurity measures, in the end the user's protection is up to him/herself, based on his/her security awareness and his/her own protection. **Social engineering** aims to exploit precisely this potential weakness of the human component in social networks, rather than attacking software or hardware directly to breach the security of a system.

Social engineering will resort to scam and simulation to show users scenarios that are not really what they seem: ads on social networks that when clicked lead to the download of malware; fraudulent ads pretending to be from banks that lead to forms designed to steal credit card credentials; or more or less crude advertising tricks to fraudulently subscribe the user to premium rate SMS services.

Figure 4.- Good practices in the smart use of social networks

Minimising risks in social networks is not unlike reducing them in the physical space: user behaviour will increase or decrease the ecosystem for threats to operate maliciously. Good social media behavioural practices can help reduce or nullify malicious intent.

A user's intelligent behaviour starts at the moment of defining his or her own identity in cyberspace, deciding how he or she wants to appear, what he or she wants to be called, what appearance to offer or what interests to share; in short, deciding who he or she is going to be in cyberspace.

3.1 Step 1: Defining identity in cyberspace

3.1.1 Constituents of virtual identity

Identity in social networks is not only composed of the name or alias, screen name or username, which is used to open an account on any of the available platforms (Twitter, YouTube, Facebook, Instagram, Snapchat, WhatsApp, LinkedIn, etc.). Identity is everything that "stably identifies" a person, something like the permanent traits that make a person who he or she is (individualisation) and distinguishable from others (differentiation) in social networks.

Unlike in analogue space, what is defined in social networks about an individual will be archived in the hyperlinks of the internet, in the memory of cyberspace, probably forever.

Drawing a parallel between cyberspace and analogue space, analogue identity could be composed of a name, perhaps a nickname, a job, studies, a place of residence and other elements that are taken as a social reference to define an individual in a stable way -their family, their hobbies...-. This information can be transferred to the virtual realm of cyberspace, where users in social networks are defined by the name and alias they adopt, by the image they place as a profile, by the *biographical* statement they write or by the social networks in which they are present.

There are also other parameters, made up of the content shared through profiles, which define an individual's identity on social networks in a more dynamic, less static and therefore more variable way.

In social networks, an individual's personality, i.e. the *behavioural expression of their identity,* is translated through **content**, the way in which the person expresses themselves through messages that communicate actions, thoughts or feelings. Therefore, the contents that are shared communicate *personality traits*, translate the essence

of an individual's identity into behaviour in relation to other people (**interpersonal relationships**) and the environment.

Unlike in analogue space, what is defined on social networks about an individual will remain archived in the hyperlinks of the internet, in the memory of cyberspace, probably forever. Even in the case of minors, it is known that 81% of babies have a presence on the internet through their parents[5]. This is known as "*sharenting*", derived from sharing and parenting, which refers to the increasingly common practice of parents sharing photos, videos and information about their children on social networks. In many cases, without being aware of it, they provide details of their children that could lead to identity theft or have an impact on the child's honour and reputation over time.

In this sense, a good practice would be to ask oneself:

- **What is my social purpose in setting up a social media profile?**
- **What image of myself do I want to show to others on social media to achieve my intended purpose?**
- **Who do I want to be or how do I want others to see me when they visit my profile?**
- **Can the content I upload to my profile cause me any problems now or in the future?**
- **Will my friend, co-worker or parent of another child agree to the uploading of a photo?**
- **When my children are older, will they be okay with their lives being on the internet from their earliest childhood?**

5. https://usolovedelatecnologia.com/sharenting/

3.1.2 What I am, what I seem to be, what I could be: identity risks in cyberspace

In the analogue or physical world, individual identity is known, to a greater or lesser extent, to oneself and to those people with whom we relate most closely: family, friends, co-workers, etc.

In cyberspace, personal profiles in social networks are based on incomplete information and, mainly, on the absence of physical interpersonal contact, and our contacts may get a wrong or distorted impression of our identity, based more on what I appear to be than on what I really am.

On many occasions, appearing to be something other than what I am is an effect that a person intentionally seeks when defining a profile on social networks, perhaps trying to offer an improved image or highlighting a specific aspect to enhance.

At other times, the information that one's self or one's contacts disseminate means that we may unintentionally become another identity than the one we are or the one we voluntarily wish to appear to be, through manipulation or unlawful use by third parties.

Descriptive information about an identity may have a presence on social networks that is not in line with the person's wishes. The risks of such **unwanted effects of a person's loss of control over his or her identity in cyberspace** increase in the following circumstances:

The amount of personal details available in cyberspace increases the risk of malicious use: the greater the availability of data, the greater the likelihood of illicit use with malicious intent.

3.1.2 What I am, what I seem to be, what I could be: identity risks in cyberspace

When the **subject's full name** (first name and two surnames) is published on one or more social network profiles, the more statistically characteristic the subject's name is, the greater the potential for unlawful use.

Firstly, with a name such as "Epifanio Torreblanca Altaguardia" it is easier to search the internet for additional information about a subject, but if you google "Juan Sánchez", you will get thousands of results. Secondly, when impersonating, a distinguishing name is more useful than a common name, since the distinguishing name, if accompanied by additional verification information, produces a psychological effect of greater credibility.

Although it may seem counterintuitive, it is more attractive to steal a highly distinguishable identity such as "Epifanio Torreblanca Altaguardia" than "Juan Sánchez".

When the **exact location of the** person's **address** is disclosed through social networks. A person's name and address are two main features of his or her administrative identity, which in malicious hands can be very useful information for identity fraud.

The display of an **ID card or passport number,** next to a person's name, can be used for the falsification of identities impersonating the person who has disclosed his or her ID card or passport.

By transmitting a **bank account or credit card number in the** open, via any social network. Cybercriminal groups have designed procedures to immediately transfer card numbers fraudulently obtained in cyberspace to physical cards.

It is always advisable not to transmit bank account or credit card numbers, as once the message is in circulation it is no longer under control, even if social networks such as Facebook or Twitter, or internal messaging systems such as WhatsApp, have encrypted connections.

Distributing the **registration number of a vehicle** owned by the subject. The vehicle's number plate, together with the subject's name obtained in cyberspace, could be used in various scamming procedures. Sometimes googling a licence plate number yields a person's postal address, or at least his or her possible area of residence due to an administrative sanction that has been published.

3.1.2 What I am, what I seem to be, what I could be: identity risks in cyberspace

- Disseminating the **e-mail address** together with the name of the person assigned to that address. Uncontrolled dissemination can result in the address being used as the source or destination of *spam* or *phishing* campaigns.

- When friends or contacts of a person disseminate, without malicious intent, **identifying information about another person** - such as their home address, car registration number, full name or other sensitive data. This dissemination can take the form of text, but also of images or tagging. For example, a person who does not have a social network profile can be tagged in full name by another person who does have a social network profile in a photograph where both pose with the former's vehicle, leaving the full registration plate visible.

Identity information, which a user provides on social networks, can create scenarios favourable to losing control over their identity, being exploited by individuals or groups with malicious intentions to impersonate their identity, to deform it or make it appear to be something other than what it is.

In order to maximise the possibilities of control over one's own information in cyberspace, one of the best practices recommended is to think before registering on a social network: to think about what one intends to do with one's presence on that social network, what image one wants to give and what part or parts of one's life one intends to share socially, often with strangers.

3.2 Step 2: Think before you sign up

3.2.1 Identity: protecting our image and reputation in cyberspace

Digital reputation is "googling" your name to see what people say about you on the Internet or in social networks, companies, universities and other groups. It is very difficult to delete or modify content on social networks.

Digital reputation, the positive or negative image in cyberspace, very often depends on the content that one (or acquaintances) places on social networks. And this image, once established in cyberspace, is difficult to erase or modify because, as we are constantly warned, once a piece of content enters the internet it is very difficult to make it disappear from the ecosystem.

Digital reputation, and even the profiling of a subject's behavioural or personality traits, are increasingly taken into account in cyberspace. It is not just that in order to get an idea of a person we have just met in the analogue world, the first thing we do is "google" their name to see what is said about them on the internet or what they say about themselves on their social networks; companies, universities and other groups are increasingly resorting to observation, or even professional analysis of social networks as an element of screening or acceptance.

It should not be forgotten that users are the ones who have the first control over the content that is disseminated on social networks so that, by applying a minimum of reflection on what is done before doing it, it is possible to prevent undesired consequences on the published identity.

As a general rule, when providing basic identity information when setting up a social network profile, it is advisable to consider the following aspects:

3.2 Step 2: Think before you sign up

Screen name or profile name. Regarding the screen name, the first thing a user should think about is whether to use a digital alias or the same name they have in the analogue world. If an alias is chosen, it should be borne in mind that it will be linked to the person and therefore define their digital identity in some way. Other people will therefore be able to make a priori judgements, without knowing the person, solely on the basis of the alias.

If the user's name is chosen, it is advisable not to provide all the information about the name, especially if the name is very distinctive. The more distinctive a person's full name is, the easier it will be for people with malicious intentions to appropriate it. In general, it is advisable to use the first name and surname, without giving middle names or surnames.

It should be noted that, even if a social network profile is defined as absolutely private by the subject, at least its screen name, username and profile icon will be fully public.

Username. This is the short name used to register on a social network. It is usually made up of alphanumeric characters and cannot coincide with that of another registered user.

A good practice to prevent your username from being used by malicious individuals or groups is to **avoid using the same username of your regular email address.**

Although it is common practice for a person to try to maintain the same username on several social networks - which may coincide with an alias as if it were an identifying feature for that person in cyberspace – using the same username of our regular email address makes it easier for a cybercriminal individual or group to obtain our email address.

This practice is known as the **guessing** method and is common in fraudulent practices or cyber-attacks, based on obtaining mass email addresses, such as **phishing** or mass distribution of spam or **scam** emails.

Obtaining the name of a person's email address is also a very useful step for impersonating a digital identity.

3.2 Step 2: Think before you sign up

Figure 5.- Example of a user name already registered on Twitter

If a person uses the user 'poppy' in Skype, Facebook, Twitter and Instagram accounts, even if they have never publicly communicated their email address and keep it protected in their privacy, if that email address is poppy@gmail, poppy@hotmail or poppy@yahoo, a malicious cyber group or individual will guess it in a matter of seconds.

Icon or profile image. It is the visual representation of a person's identity on social networks, secondarily accompanied on some platforms by the so-called "cover image".

The most obvious good practice in managing profile pictures on social networks stems from understanding that profile icons, like the bio posts or alias you use on social networks, are going to speak about you in cyberspace.

Figure 6.- Example of profile icon and cover image in Facebook

3.2 Step 2: Think before you sign up

Therefore, the smartest way to use social network profile icons, for the purposes of protecting and managing your digital reputation, is to think carefully about what you want to convey about yourself through your social media identity images.

The first thing to bear in mind before posting a representative image in a stable manner on social networks, such as the profile icon, is to think that from the moment it is uploaded, you have no longer control over it. In this context, it should be considered that images can be downloaded, manipulated and circulated by others with unknown intentions.

An additional general recommendation is not to choose images of an official administrative nature for the profile icon, e.g. a photograph of a National Identity Card, passport or employment identification card, as such images make it easier for people to falsify documents and impersonating our identity.

Location. Most social networks include a field at the time of registration of the profile for the location of the subject. In this case, the location required is their usual location, for example, the city where they live, where they were born, the city where they work or with which they feel identified for whatever reason.

In addition, social networks such as Facebook or Instagram allow you to add a location tag individually to each post in your profile.

The most obvious best practice for personal profiles on social media is not to post specific postal addresses as the location of the profile user. Companies, businesses or institutions usually have their postal address located through a map on social networks, which facilitates their business or contact relationships. On the other hand, personal profiles that communicate their postal address on social networks may expose themselves to risks and unforeseen events.

A criminal gang specialised in locating and stealing high-end vehicles could use information obtained from social networks to, with a little more digging, locate the usual position of the vehicle and steal it. The same can happen with characteristic places of residence.

Biography posts. On most social networks it is common for the profile overview to have a space reserved for the user to make a statement, which most people use to self-describe themselves.

It is quite common to enter the user's profession on social networks intended for personal contacts (such as Facebook or Twitter), not to

mention social networks specifically intended to promote professional or work-related contacts, such as LinkedIn or Viadeo.

Not because it is a common practice that it is free of risks, both connected to the analogue and physical world and generated and developed in cyberspace. In addition to the well-known risks of identity theft, which are facilitated by the more specific information about a subject that is available on their social networks, there is also the possibility that the declaration of a subject's profession on social networks may be the attack vector used by a cybercriminal group to make them a target for the dissemination of malware.

If such a group knows which individuals are occupying certain positions in a company and has their email address, users could become the target of a targeted phishing operation to steal sensitive company information, to install a software tool in the company to infiltrate corporate information systems or simply to infect the company's network with malicious code such as ransomware[9].

Telephone number or email address. Although both telephone and email are contact details that the user is obliged to provide when setting up a profile on most social networks, these details remain private, without public exposure, only accessible by the subject and by the company to which the user has transferred them under the terms of service that the user accepts when registering.

It is advisable to **do what almost nobody does**: read the terms of service of that social network, where it will be established whether or not the private data communicated by the user, when setting up a profile on the network, will be shared with other companies and under what conditions.

Cybercriminal organisations operate continuously with **automatic** internet harvesters, whose purpose is to detect and store email addresses and telephone numbers in databases that will later be sold to the highest bidder on the cybercriminal black market.

6. Ransomware is a type of virus or malicious software whose purpose is to block the user's access to their own information stored on a device, computer, tablet or phone, usually by encrypting that information and demanding a financial ransom from the user to release it.

3.2.2 Security: protecting access to your profile on social networks

The username, or email address, and a password are a user's access credentials to a social network. Specifically, the password is the element that protects the user against illegitimate access and attempts to access their private information and contacts on the social network.

One of the main causes of illegitimate access to sensitive information, which should be protected, is the **weakness of the passwords** chosen by users to protect this information[7].

Among the most common passwords for accessing web services, including social networks, are "123456", "qwerty" or the word "password" itself. These simple passwords offer zero protection against an attacker to illegitimately access a web service and violate the user's rights.

Some social networks require certain alphanumeric characters to be entered in passwords (combinations of upper and lower case, numbers and letters, or additional characters such as an asterisk, hash or underscore), and most report with a colour code (green and red) the strength of the password the user is choosing to set up a profile on a social network.

But what are considered **strong or secure passwords**? Ideally, strong passwords are those that tend to be randomly generated, i.e. there is a very low probability that they will be guessed or predictable by someone who does not know them. A strong password will be long in length; it will combine numbers, letters and special characters in a way that avoids any pattern and will have the disadvantage for the user that it will be very difficult to memorise.

The most common passwords are "123456", "qwerty" or the word "password" itself. These simple passwords offer zero protection against an attacker to illegitimately access a web service, violating the user's rights.

7. For example, a report from January 2017: https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

3.2.2 Security: protecting access to your profile on social networks

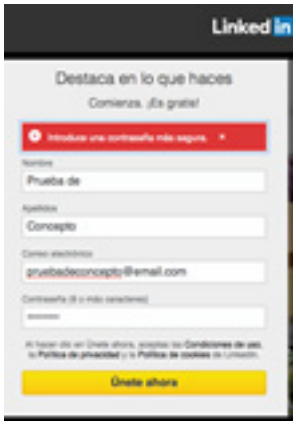


Figure 7.- Example of a registration attempt with weak password on LinkedIn

A weak password is usually predictable because it follows a pattern (one or more words followed or not followed by a number, numerical sequences, dates meaningful to the subject). It is almost always the case that an insecure password is weak because it has been designed to be remembered by the subject and not to have a minimum guarantee of reliability in terms of providing security.

The following actions are considered good practice when accessing a personal profile on social networks:

1

Adopt personal self-protection awareness. The company is obliged to maintain security standards to protect the network, in its hardware, software and human (its own employees) components, with which it provides services, but there is a point where the user's security relies on the user him/herself.

No matter how secure a network is in cyberspace, it still is as weak as its most insecure component, usually the human being. If a social network provides encryption, password authentication and continuously audits its security to avoid vulnerabilities exploitable by attackers, but a user leaves access to his or her profile unprotected by a weak password, it will be easy for an unauthorised third party to gain illegitimate access to that profile.

Therefore, the first factor for a user to provide protection for their own profiles on social networks is to be aware that they should be concerned about and responsible for their own security by making use of the mechanisms provided by the network.

2 **Use pseudo-random passwords.** That is, passwords that include numbers, letters and special characters so that they do not follow any pattern and are sufficiently long (six characters or more; the longer the password, the less likely it is to be broken). For example, a strong password would be "89Jy$+_'1VwqÇ#", as it mixes all kinds of characters without following any pattern.

Obviously, such a password is difficult not only to remember, but also to type continuously by the ordinary user. Therefore, other tactics will have to be adopted to avoid having to remember and type complex passwords that are secure, but "make life impossible".

One way is to have the access passwords to the different social networks written down in a text file, in turn protected by a password, stored on the device to be used (computer, phone, tablet), with access also protected by a password.

Another way is to have the **"remember password"** function activated in the internet browser for the most common authenticated accesses. This option is reasonably secure only if access to the device is password protected.

A third way is to use "password managers", which are applications or programmes that we install on our devices and which not only store the passwords for our network services, but also generate them with security guarantees and integrate with web browsers to authenticate us in our services. If the "password manager" software has its security audited and updated by its manufacturer and if access to the manager is protected by a strong password, it will be a reasonably secure method.

These three (3) options for storing passwords will require the user to memorise at least one difficult password (**master password**): the one for accessing the device, the password file or the password manager.

3 **Do not use the same password for several social networks.** In this way, if a user's password to one network is compromised, the others will remain secure (unless the compromised password is the so-called master password).

4 **Do not use leet-formatted passwords[8] for common words.** The hacker world began in its infancy to communicate in this language, and therefore software dictionaries for brute-force attacks may incorporate leet variations of common words.

If you add capital letters and special characters at the beginning and end, such as the dollar or the slash, you have a strong password that is easy

8. Leet: substitution of letters by numbers or special characters

to remember by mnemonics by having a favourite colour and number chained in leet by a hash: "$R0j0#s13T3/".

5 **Do not use passwords that contain personal details**, such as birth dates or anniversaries, important places, nicknames or middle names. An attacker will try all the personal information they know about a user if they are trying to guess their password.

6 **Alternatively, use two-step authentication.** Social networks such as Twitter, Facebook or Google have implemented the two-step verification option for users to access their profile from their devices.

In addition to the password (first step), the user will be asked to enter a numerical code (second step), usually sent by SMS to the telephone number that the user has registered in that social network profile. In all cases of two-step authentication, it is essential that the user has registered his or her telephone number in his or her social network profile.

Figure 8.- Facebook two-step authentication setup menu

3.2.3 Privacy: what's shown and what's hidden

In social networks, privacy is the parameter that regulates what the user shows and hides publicly on social networks. Privacy is usually associated, in most social networks, with two types of information:

- The profile's own descriptive information, e.g. contact email, phone number and identity of friends and contacts.
- The individual content that the user disseminates through messages, images, audios, likes or comments on the social network.

When creating a profile, each company operating a social network presents the user with the "terms of service" in the form of several dozen pages which the user is asked to "read" before continuing and finally "accept", if he/she agrees to those terms. No user can open a profile on a social network without accepting the terms of service presented to them by the social network operator.

The terms of service for a user to join a social network are in the nature of a legally binding contract between the parties (between the user and between the operator of the social network, e.g. Facebook Inc. or Twitter Inc.), and that contract governs the relationship between the operator and the user.

All companies that operate social networks have published their privacy conditions, i.e. how they manage and treat the data that users are hosting on the web servers of those companies when they create a profile on the social network[9]. These privacy terms set out not only how social network operating companies share information that is voluntarily provided by users, but also what additional user data the companies are collecting automatically, with the user's consent, without the user being aware of it.

For example, among the information that Snapchat states it collects from its users, in addition to the content that each user discloses and shares in their daily interaction with the social network, there is metadata about the disclosed content, activity information, information

9. For example, Facebook [https://www.facebook.com/about/privacy/], Twitter [https://twitter.com/privacy?lang=es], Instagram [https://www.instagram.com/about/legal/privacy/?hl=es], Snapchat [https://www.snap.com/es/privacy/privacy-policy/]

3.2.3 Privacy: what's shown and what's hidden

Figure 9.- Companies with which Facebook claims to share user data

of the subject's location (if the subject enables this option) or access to the subject's camera and photos stored on their device, subject to Snapchat's request for permission.

The service contract usually includes clauses in which the company specifies what other companies are being authorized by the user to receive his or her data, no longer sent by him or herself, but by the social network company itself. Each of the third-party companies with which a social network operator declares to share data has its own privacy and service provision terms and conditions (the user is assumed to be aware of such a data sharing scenario when he or she first agrees to sign the contract to sign up to a social network).

With regard to the privacy of the contents disclosed by each user on social networks, each network has established the possibilities of protecting the contents totally or individually so that they can only be accessed by the subject himself and by his contacts/friends.

For example, Facebook allows to protect with a privacy filter each individual content disseminated on the social network, by clicking on a drop-down associated to each individual content; however, Instagram or Twitter allow to define privacy in the configuration menu of each profile by protecting all the content of messages sent by the user, so that they are only visible to the followers of the profile, but they do not have the option to configure each message individually as private.

3.2.3 Privacy: what's shown and what's hidden

Figure 10.- Privacy drop-down menu for each individual Facebook content

Figure 11.- Option to protect all messages on Twitter with a privacy filter.

With regard to the privacy of the descriptive information of a user's profile on social networks, some social networks have the possibility to configure the visibility of the profile. The option for other people to locate a profile, by searching by email or phone number, is usually enabled by default on Facebook and Twitter in the profile settings menu.

Figure 12.- Facebook profile visibility settings

3.2.3 Privacy: what's shown and what's hidden

Another relevant issue that social network users have to take into account when reflecting and acting on the privacy of their profile is the geolocation of both the profile and its contents.

Figure 13.- Configuration of content geolocation in Twitter

On Snapchat, for example, geolocation is not available by default at the moment, but there is a feature called "geofilters", which allows users to use graphical location tags to show where (the city) they are or which location the shared content identifies with.

Figure 14.- Examples of geofilters on Snapchat

Another functionality that social networks have incorporated in recent times, in relation to user privacy, is the **encryption of messages and content** shared through the social network.

However, encryption is a property that does not prevent anyone from reading or viewing content that we share with the intention of making it public; encryption is not intended for that purpose in the case of social networks. What encryption provides is protection to prevent that, if an attacker with malicious intent is able to intercept data traffic between

a user's device and their social network, the content of that intercepted data will not be made clear.

Some private messaging social networks, such as WhatsApp, have encryption between users by default, so that communication between users is automatically encrypted. Other social networks, such as Facebook, provide the possibility of configuring, within the security tab, the user's use of their own PGP encryption key for their communications with other users.

Figure 15.- Encryption settings tab in Facebook's settings

Another chapter linked to the privacy of a user's personal information on social networks is related to sharing the contact book that the user has on the mobile device with which he or she connects to that social network, or the **list of contacts** that the user has on another social network.

In most cases, granting permission to the social network to access the mobile phone's address book is mandatory if you want to install the Android or iOS app and connect to a social network. In some cases, such as Facebook or WhatsApp, permissions even include the possibility for the *app* to "modify" the user's contacts in the phone's address book, e.g. by adding some data in a specific field.

3.2.3 Privacy: what's shown and what's hidden

Figure 16.- Permissions related to contacts that Snapchat, Facebook and WhatsApp mobile apps request

Contacts accessed by a social network app in the address book are not inserted into the subject's profile, unless the subject "imports" and adds them, nor are they disclosed, unless the subject expressly does so through their privacy settings. However, all such contacts become part of the database of user links maintained by the social network operator, legitimately authorised by the users through the terms of service contract.

3.2.4 Security and privacy risks

Both the privacy and security of a social media profile regulate the subject's control over the information shared and the channel through which it is shared. Potential security and privacy risks will be those that compromise or diminish the level of control the user has over their channel (their profile) or the visibility of their content.

3.2.4 Security and privacy risks

Security regulates the subject's ability to prevent other users from accessing and thus controlling the information and the communication channel itself (the social network profile).

Privacy regulates what content shared by the subject himself/herself on the social network is shown, is visible to other people in cyberspace, whether they are users or not (general internet users) of the social network.

Among the threats and vulnerabilities, i.e. risks, most directly associated with security or privacy issues on social networks there are:

- **Use of weak passwords or passwords based on** publicly known **personal details** of the user, such as their birthday, pet's name, band or favourite movie.

- **Sharing passwords with others,** even if they are trusted. By definition, sharing a secret increases the likelihood of that secret being revealed, as it increases the sources through which it can be divulged.

- **Lack of awareness of identity in cyberspace.** When a subject has several profiles on different social networks, the features of his or her identity in cyberspace are not a function of each of the isolated profiles, but of all the profiles as a whole. In other words, a user may avoid declaring his location or profession on his Facebook profile, but do so on his Twitter or Instagram account.

  Therefore, it is advisable to be aware that all the information about oneself that is disseminated through any medium on the Internet will be a piece to compose the puzzle in which one's own face will finally appear. An individual with the intention of "solving the puzzle" will collect each piece until he or she has a more or less clear image of the user.

- **Images that expose unwanted information**. For example, personal portrait photographs or selfies of a subject against the background of their office, workplace, home or any other personal location are common. Sometimes the backgrounds of such images, which are not the focus of the photograph to be shared, reveal identifying information about the subject or their company that the user themselves may not wish to disclose.

  In these cases, the recommendation is to review the identifying content (company name, vehicle registration number of our vehicle or the vehicle of a friend or relative) that the user intends to keep protected for privacy reasons.

3.2.4 Security and privacy risks

Tagging third parties. The privacy of individuals, even those who do not even have social media profiles, can be violated by tagging their name in photographs or images.

In other words, through tagging, someone who does not have a voluntary presence on social networks may end up having an involuntary presence, exposing their privacy, their name, their face and their contacts and friends. To prevent these risks, it is recommended to be cautious about tagging people in photographs, requesting the person's prior consent before tagging their name in an image that is going to be disseminated on social networks.

Revealing geographic trajectories. The geo-tagging of content, or geolocation, could allow a significant percentage of geographic trajectories to be known and, therefore, allow itinerary control (mapping of times and places) on a user on social networks, which could be used maliciously.

It is recommended to deactivate by default the geolocations of profiles and content on social networks, activating them individually and only for specific content.

Inadequate configuration of the profile when registering on the social network, to the extent that the level of privacy offered by the platform itself is not correctly configured. In fact, it is advisable not to choose the default options but to carefully analyse each of the settings offered for displaying certain content.

Obtaining personal data with malicious intent. The greater the amount of identifying information is published, the greater the likelihood that this data will be used, for example, to attempt to answer security questions and illegitimately authenticate in order to gain access to the profile.

Impersonation. Since registering on a social network is only a matter of having an email account, anyone could register under their real name or someone else's name.

Similarly, if our mobile phone is lost or stolen and is not protected, anyone who has access to it can impersonate us on our social networks (especially those that do not require authentication, such as WhatsApp). It is therefore necessary to use the terminal lock and, if you realize that someone has impersonated you, report it.

3.3 Step 3: Think before you write

The nature and purpose of social networks is not merely to create a profile with identifying data in the manner of a modern telephone directory. The founding principle of a social network is to socialize by sharing content through the network.

Shared content is what gives a social network its nature and what shapes its characteristics. Some networks are more focused on the dissemination of multimedia content, such as Instagram; others are multi-purpose, such as Facebook; others are more focused on the quick and brief message, such as Twitter; and some are more focused on composing a professional curriculum vitae, which allows us to establish relationships of a basically work-related nature, such as LinkedIn. These different orientations are determined by the content that users share through a social network.

The relevance of the content shared on social networks lies essentially in the fact that it defines and characterises the user who shares it personally and professionally. To such an extent, shared content and the users who share it can be considered mutually identifiable, since the global audience that inhabits cyberspace often turns to a person's social network profile to get a first impression of that person, looking at how he or she has self-described in the personal identifiers, but, above all, observing what type of content he or she shares.

Therefore, precisely because of its relevance, as has been suggested for the description of personal identifiers when opening an account on a social network, it is advisable to develop a **minimum instinct of cyber-conservation**, a minimum culture of thinking before writing content to be disseminated through social networks.

The relevance of the contents shared on social networks lies in the fact that they define and characterise the user who shares them personally and professionally. We will have to think before writing content that can be harmful through social networks.

3.3.1 Content sharing: what is shared on the network

The smartest best practice a user can adopt when it comes to disseminating content on social media is to realise that once the content has been transmitted, the user has already lost control over that content.

Regardless of how the user has configured the privacy of his or her profile on a social network, the user should be aware that once he or she transmits content, he or she has generally granted the operator of that social network significant rights of use over that content.

A general element of confusion regarding legal rights over content transmitted by a user on a social network stems from the distinction (or lack thereof in terms of user perception) between ownership of content and use of the same:

- The **intellectual property of content** disseminated through a social network is held by the user who shares it, unless that content is affected by prior intellectual property rights: for example, the user is sharing content for which the intellectual property is already legitimately owned by a third party.
- The **right to use the content** legally owned by the user can be transferred with extensive rights of use for the party to whom the rights are transferred.

In essence, even though the user owns the rights to a content, the signing of a legally binding contract with a company that manages a social network necessarily implies the transfer of the rights to use the content that the user owns. The user remains the owner, but the company managing the social network is the usufructuary, using the content with a wide margin of manoeuvre, legally and legitimately granted by the user.

Basically, registering a profile on a social network means that an individual grants a company, under a legally binding contract between the parties, a licence to transfer rights for a wide range of uses of the user's content

and personal information. In this context, the user may own the content, but no **longer has control** over its dissemination.

With regard to the transfer of rights of use over the content hosted on a social network, this transfer to the social network's management company is made under a contract with a clause to be complied with by both parties.

However, when content is disseminated by a social network defining its privacy as public (i.e. visible to all users of that social network and, in most cases, to any inhabitant of cyberspace), the **user is implicitly ceding control over the circulation and dissemination of that content to any inhabitant of cyberspace.**

It is true that when users sign up to a social network they commit themselves, by the contract on the signed terms of service, to "play by the rules" and therefore to be respectful of the limited broadcasting rights over other users' content.

Even if a user chooses to privately broadcast certain content among his or her contacts, followers or friends, once that content is sent, it is already part of the information that is accessible to other people, mostly the private list of contacts, followers or friends of the person who has disseminated the content.

In this way, any of them can publicly disclose that content initially marked as private by its original disseminator, giving rise to a "de-privatisation" of the original privacy. In social networks, content privacy is not an absolute parameter that is fixed when a person defines a content as private, but **content privacy is a relative and interactive parameter,** which depends on whether other users, who receive a private content, continue to keep it private.

Therefore, **before disseminating content through a** social network profile, the following questions should be asked:

3.3.1 Content sharing: what is shared on the network

Am I revealing any personal information that I would like to keep private only among my family and friends? If the answer to this question is yes, it is best not to disseminate the content on social networks since, even if it is marked as private, it may be voluntarily or unwittingly re-disclosed by a contact who has accessed that content.

In this regard, it should be borne in mind that there is personal information that could put the user or their loved ones at risk, since public disclosure could be used maliciously by individuals or cybercriminal groups for identity theft or social engineering, among others.

Would someone viewing that content think that it represents my opinion or my way of being, thinking or behaving? If the answer to the question is yes, think again about whether the content represents the user and what it will say about him or her - not only on a personal level, but also in the workplace. And not only now, but also in the future, as someone might form an opinion based on social media content, and maybe that opinion will matter.

Is there a chance that I will regret posting the content and want to delete it immediately after sending it because it is offensive or inappropriate? If the answer to this question is yes, it is better not to send the content. Once it has been published on a social network, it can take seconds for the content to appear on a contact's profile, which takes another second for them to repost it, so that by the time you want to delete it, the content has reached the speed of light in cyberspace and can no longer be deleted.

Does the content I am going to disseminate contain an image of me or my close ones that, with a simple manipulation, could be transformed from an innocuous image to an offensive or inappropriate one? If the answer to this question is yes, it is better not to post it, as it may end up in an unwanted exchange forum, after being slightly retouched with an image editing programme.

This is particularly sensitive in the case of minors, whose distribution of images on social networks should always be supervised by the adults responsible for the minor.

Does the content I am going to disseminate contain images of other people who do not have social media profiles or whose profiles are fully protected for privacy? There may be people close to you who for legitimate reasons of way of thinking or understanding life do not have profiles on social networks, but who appear in photographs representing family, social or work-related moments. It may also be the case that these persons occupy social or professional positions where a certain control of their public image is desirable.

In such cases, before distributing an image that involves the protected privacy of others, it is advisable to consult with them about whether or not to disseminate the content.

If I forward to my contacts someone else's content that I have just received, will I be contributing to the dissemination of offensive, inappropriate or harmful, or outright illegal content? Social engineering is a procedure that attempts to camouflage harmful content through apparently innocuous content, even content that is attractive or necessary for users (information notes, invoices, shocking videos, etc.).

The success of dissemination of such harmful or inappropriate content lies essentially in the **chain of rebroadcasting**. That is to say, that a user who receives it sends it again. Therefore, when receiving content from other contacts, whether known or unknown, it is advisable to think about it for a moment and analyse the content a little.

Am I sure that I can use the content that I am going to disseminate through my profile? Some content that is disseminated contains trademarked images, documents that are protected by rights. Sometimes the difference between what content is protected and what is not is subtle.

For example, disseminating a *selfie* taken by a user showing the logo of a company's building in the background would not, in principle and in the absence of other circumstances, be limited by rights, or at least it is doubtful that the company would claim such rights. However, using a company's logo or the identity of a person with a public image without the consent of a third party to promote a product that one wishes to promote through social networks could lead to claims for image rights by the company or public person whose image is being used.

Am I sure that I want the content I am going to disseminate to be on Google forever and that anyone can find it with a search? In the face of this question, it is necessary to think preventively that any content we disseminate is going to be forever in cyberspace. Once we disseminate content through a social network, whether publicly or privately, we have lost control over the content and, therefore, that content may end up indexed in Google, forever.

3.3.2 Malicious or unintended uses of disclosed content

Both the content that is disseminated and the content that is received can be subject to unwanted or malicious use:

Unwanted use occurs when another identity in cyberspace sends content to people who are not interested in it, circulates content at a high frequency ("no message flood"), forwards content that is deemed inappropriate, or makes an undesirable, for any reason, use of the content.

In this case, the sender of the content is not engaging in an activity that implies malicious intent or intent to harm, but ultimately ends up being annoying or showing an inappropriate conduct on social networks.

Malicious use would imply the use of any kind of content disclosed on social networks to obtain an unlawful and/or illegal benefit generally to the detriment of third parties, or directly to harm those third parties.

Examples of malicious use are the transmission of computer viruses (malicious code) via social networks or the use of fraudulent content for the purpose of misleading the user into subscribing to premium-rate services.

One of the first areas of unwanted use that third parties could make of the content we transmit through social networks is framed in **virtual reputation**. The content we transmit on social networks, in some way, defines users, says something about them, about their tastes, thoughts, ideologies and behaviour.

Less intuitive to see, however, is the use that interested third parties could make of the content disseminated on social networks to **build psychological or behavioural profiles** of a user, profiles that will later be used for employment purposes or to predict and influence the user's behaviour.

3.3.2 Malicious or unintended uses of disclosed content

Another unwanted use of content that is disseminated on social networks, which in addition to being unwanted can lead to the malicious use of this content by other identities, is the **use of intimate content of a user to damage their image or to make them a victim of cyber-blackmail**. Sexting is the exchange of erotic images that a user carries out, initially, in the privacy of communication with another user through social networks -usually through applications such as Messenger on Facebook, direct messages on Instagram or Twitter, or via WhatsApp-.

The most commonly used procedure for spreading malicious content through social networks is **social engineering**. In other words, the use of deception techniques through messages to make the user download a file with malicious content (a virus, for example) or click on a link that will take them to a website where they will be exposed to a scam, among others.

As its name suggests, social engineering is about manipulating the levers of social relations to achieve a purpose, or constructing a specific context to produce an effect. In cyberspace, social engineering procedures are commonly employed to lead users to one of three (3) destinations:

1. Downloading a **virus** to your device.
2. A **scam by which you will be** asked to subscribe to a payment service, e.g. subscription to premium SMS services.
3. Obtaining personal data (telephone or e-mail) and financial data (credit card details) of the user for money **theft**, identity theft, fraud or other illegal purposes.

Figure 17.- Most common targets of social engineering

3.3.2 Malicious or unintended uses of disclosed content

The most commonly used social engineering and social networking **scams** could be classified into the following categories:

- **Eye-catching or attractive content,** such as shocking videos that are recommended, or links to content about curiosities, celebrities, alarming news or the like. Social engineering, in this case, makes use of the natural human curiosity for shocking or novel content to increase the likelihood that users will click on the content and, from there, they are directed to the virus or scam.

- **Surveys**, which circulate daily on social networks, especially via mobile devices, with the apparent purpose of soliciting the user opinion on different purchasing behaviours in order to hide the real purpose of the survey.

  Their aim is usually to get the user to sign up for a pay-per-content, premium rate SMS service or, in the worst case, to ask for the user's contact email address, which will immediately become part of a database that will be sold and used to turn the subject into a recipient of huge amounts of spam.

- **Advertising of new or highly sought-after apps,** which in most cases are fraudulent apps that the user downloads via a message on social networks only to find that the app was not what was promised - latest version of the favourite video game, space optimiser on the mobile phone, free antivirus, utility to look for new contacts on social networks, a device to get free Wi-Fi - but rather apps that contain some kind of malicious code with the purpose of taking control of the mobile device, stealing sensitive information such as passwords or credit cards, hijacking content for ransom or, if benevolent, displaying unwanted advertising.

- **Offers of vouchers or discount coupons** in well-known commercial establishments in which, behind the deception of the fake discount coupon that may arrive via social networks or by e-mail, sometimes masked in a prize draw, the hidden purpose is to obtain the user's personal data in order to trade with them or to subscribe them, by trickery, to premium rate payment services[10].

- **Claims of sexual contacts or free pornography,** which, under the guise of identities offering intimate relationships, suggest users to click on links or multimedia content that will end up directing them to websites where they will be asked for personal data in order to traffic them, they will try to make the victim subscribe to paid services through manipulation and deception, or they will download malicious code with various harmful effects for the device being used by the subject.

10. For an example of fake discount coupons: https://www.osi.es/es/actualidad/avisos/2016/05/de-nuevo-vales-descuento-de-lidl-que-te-vacian-la-cartera

Troubleshooting technological problems or user account issues, where warning messages pretending to be from technical services of known providers to which the user may or may not subscribe (PayPal, Google, Facebook, Netflix or others) are used to inform the subject of problems with their device or user account, suggesting that they click on links or download content that will lead to fraud, a virus or theft of data, passwords or money. An identical procedure to traditional phishing is used; however, in this case, the scam is distributed via social media messages instead of email.

3.4 Step 4: Nurturing personal relationships

While the creation of a profile on a social network is determined by the definition of identity traits - who we are or who we would like to appear to be - and subsequently the content that is disseminated will determine how people behave, it is the contacts and friends that provide meaning to the very meaning of "social network"

.

Indeed, a social network is an instrument, a **tool for socialisation in cyberspace**; socialisation that is materialised through contacts, friends or followers, that is, the other identities with which we relate to on the network through the *cybersocial* level.

The social network is determined by the definition of identity traits and the content that is disseminated will determine the way people behave; contacts and friends.

3.4.1 Relationship, contact and friendship management

Regarding contact management, social network users will have to make mainly two (2) types of decisions:

- **Choosing contacts:** mainly when you create your profile on the social network, but also throughout the life of your profile, where you will make new contacts and lose some of your existing ones. In some social networks, making new contacts involves making friend requests to other identities and having them accept you as a friend.

- **Protect with the veil of privacy,** either by keeping your contact list open, so that the whole of cyberspace knows who you relate to (or intend to relate to), or by keeping your list of friends and followers hidden, so that it is only visible to you and your contacts.

Before deciding whether you want to make your list of followers, contacts or friends invisible through the privacy options set by the different social networks, the first step is to choose them, i.e. to start clicking "follow" or to start making friend requests to other identities.

Some social networks ask the user to access their existing contact list in order to create an initial list of friends from which to start building the newly created profile. This access request is common in social networking apps for mobile devices where users often have their phonebook contacts saved. In an *app's* request to a user's contact book, two (2) concepts must be distinguished:

- **Permissions request by the app.** Some social networks, as a mandatory requirement for their *apps* to be installed by the user, request permission to carry out certain actions in the contact book (mainly reading and modifying it). This permission **does not imply** that the user's contacts in the phone book will be incorporated as friends or followers in the profile of the social network that has been created.

3.4.1 Relationship, contact and friendship management

Request to import contacts. Some social networks, when a user is in the process of creating a new profile, ask for permission to import contacts from other social networks where the subject already has friends, or from his or her address book. By importing contacts, the social network is trying to absorb the entire list of friends from a profile that the subject already has on another social network or on their phone.

Initial requests to access the address book or import contacts do not in themselves present security threats (unless there are other risky circumstances, e.g. malware infection of the device), but they do present **relevant instances of the subject's privacy in cyberspace.**

In both cases, rich information about the user's contacts on several social networks is being transferred to the operator of the social network. This is not a problem a priori, but it is good practice to be aware of the implication of handing over information to several social networks, which are managed by the same corporate group, such as Facebook, Instagram and WhatsApp, all under the Facebook group; or Skype, LinkedIn or Yammer, owned by Microsoft.

On the other hand, in most social networks, a user's contact structure is made up of those other identities that the subject follows on social networks, plus users who follow the subject's profile. In some networks, such as Facebook, the addition of new contacts involves "friending" that contact in order to be accepted into their network of relationships.

In either case, either by direct addition of a contact or by friend request, that contact becomes part of the information that other identities access on social networks. If the profile is publicly disseminating information without privacy protection, other people will know through his/her profile not only who we are (the biographical statements made), what our interests, tastes and to some extent our behaviours are (the content we post), but also what other people we relate to or would like to relate to.

A subject's relationship structure is a primary source of information for inferring his or her ideology, studies, area of employment, likely place of residence and other factors which, although not expressly stated by the user, can be inferred. This information that could be inferable about a subject from his or her contacts on social networks can be hidden by restricting, through privacy controls, the visibility of the list of contacts, friends or followers on the user's profile.

3.4.1 Relationship, contact and friendship management

The privacy settings for a profile's contacts are available in the settings menu of all social networks, in the same way that privacy is activated and deactivated for content. In this regard, Facebook allows hiding the list of friends while keeping the contents of the profile open, while Twitter or Instagram require the subject to privacy-protect the entire profile (contents and friends) so as not to make the subject's contact list visible to identities other than the user's friends or followers.

Friend requests is related to the privacy protection of the contact list. This intention of new *friendships* is part of the very nature of social networks, meeting new people in order to establish new relationships. It is therefore a positive contribution of social networks as communication tools.

However, there are risks involved that a user must be aware of and manage. The most obvious risk of adding (accepting a friend request) a new identity to the contact list, if it is protected by privacy, is that the newcomer will have access to information about the user's contacts and the structure of the user's relationship network in that social network.

3.4.2 Social engineering and risks of networked relationships

The visibility of the structure of friends and contacts in a social network entails potential risks. The most obvious of these is associated with bringing unknown identities into the circle of contacts, which is an opportunity to broaden and enrich the universe of personal, social and work relationships, but involves an initial risk phase in which one person may approach another with hidden intentions.

A preliminary concept to bear in mind with respect to the contacts that are acquired in a social network is the **framing of the friendship relationship.** Since people relate to each other virtually, the lack of physical proximity is compensated by a tendency to overvalue the virtual link, giving it more sentimental weight than it would be given in a normal process of mutual acquaintance between people in the analogue world.

Another element that contributes to the overdimensioning of interpersonal relationships in social networks, **where mere contacts may be viewed as friends**, is the very mask or character that the profile in a social network represents for each user. In social networks, one can exaggerate one's virtues or even play a role with the qualities one would like to possess, and it is easier to hide defects; in this way, when meeting someone new, making a new contact and interacting with him or her, one tries to self-affirm as far as possible the *character* constructed in the social network.

The particular psychological and perceptual structure that is generated when a user has many contacts on a social network can lead to a false sense that these contacts are friends, in the same sense as friends in the analogue world. This phenomenon can lead to lowering one's guard, **lowering the perception of risk in interpersonal relationships**

The persona that is constructed as a "virtual self" to represent a person on social media can make people believe that they are "friends".

with strangers, and thus leading to trust faster and more than it may be appropriate.

With access to the network of friends, a malicious identity can not only infer information about a person that is not originally intended to be explicitly stated, but could use that information to carry out cyberbullying behaviour of various kinds.

Among the range of cyberbullying behaviours, *sexting* of intimate content has already been mentioned. The perceptual distortion of virtual friendship is more common among children and young people, in front of whom people with malicious and illegal intentions can engage in sexual harassment, which on the internet and social networks is known as *grooming*. *Grooming* is the "set of strategies that an adult develops to gain the trust of a minor through the internet in order to obtain sexual concessions"[11].

Another form of bullying through social media, which particularly affects children and minors, is *cyberbullying*, whereby an aggressor tries to undermine the emotional stability of a victim by using social media channels, but also SMS, emails or WhatsApp messages, making the victim the target of threats, insults or intimidating messages (which may include blackmail).

In terms of risk control in relation to maintaining a 'healthy' list of contacts on social networks, an additional element of prevention is to monitor followers and friend requests in order to remove, as they arise, both followers and requests that are suspected to be **bots**.

Bots, short for *robots*, are automated profiles set up on social networks to perform repetitive behaviours that do not require human intervention to be carried out. For example, a bot on Twitter or Instagram can be programmed to issue *likes* or make comments (always the same, such as "bravo", "great" or "it can be improved") to specific content; for example, when talking about a film, a book, an exhibition or a government or political leader.

Other *bots* are programmed to automatically follow profiles that talk about certain topics. *Bots* are useful tools in cyberspace when it comes to automating tasks and are increasingly used in online marketing campaigns, in opinion polls, in testing the behaviour of new software solutions or to boost traffic on social networks or websites.

However, social media *bots* can also be used to generate unwanted, annoying or outright malicious traffic. The following are examples of scenarios to avoid in which *bots* may be involved:

11. http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/grooming-acoso-a-menores-en-la-red.shtm

3.4.2 Social engineering and risks of networked relationships

- **Create a negative image of a person or brand.** These bots are programmed to post negative messages by broadcasting pre-designed content, seeking to get followers to reproduce and rebroadcast that content.

- **Harassing or pressuring certain people or groups,** which is known in social media slang as **trolling** (*trolls* are the *bots* that troll), behaviour that can be carried out with pre-programmed *bots* to insult, disqualify or reproach certain content or people who meet certain characteristics (for example, a certain ideology, personal orientation or hobby).

- **Spreading spam, advertising or unwanted services**. This is the most common ecosystem for *bots*, which are able to transmit a programmed set of advertising messages and disseminate them relentlessly. Sometimes bots are designed to contain misleading advertising, which aim at capturing users' clicks and redirecting them to malware download websites. In other words, different types of viruses that will infect the user's device with cybercriminal intentions.

- **Artificially increase the volume of users' followers.** This type of bots are created en masse, in the order of several hundred thousand, to be added to the list of followers or friends of certain users in order to generate a false sense of *popularity* in that user's profile - usually related to the sale of followers on social networks, when a user has just set up a profile on social networks and needs to "have friends and followers". It is common to sell packages of followers (5,000, 10,000, 100,000).

In these cases, the **recommended good practices** are:

- Keep **privacy-protected** the information that is considered more personal on profiles and that could expose a person if it were publicly known. In general, it would be a wise practice not to enter on a social media profile any personal information that could be considered sensitive.

- **Be more cautious about friend requests from unknown identities.** Before accepting them, it is preferable to check the person's profile on that social network, to make sure that you have common interests, or at least that what they say about themselves does not set off any alarm bells. If the profile is hidden or restricted, or if it has any features that a priori "do not fit", the recommendation is not to accept the friend request.

3.4.2 Social engineering and risks of networked relationships

Block identities with malicious or annoying intentions. Block any identity that insults or shares inappropriate or uncomfortable content with the user, such as unwanted advertising or services, and block profiles that follow users or request friendship in order to "get more followers" or artificially increase their followers.

Report unwanted identities to the service provider. If you are receiving inappropriate content, are being harassed or feel that an identity is behaving inappropriately, it is a matter of principle to report that identity to the social network service provider. All social networks have an established "whistleblowing" procedure[12].

Save and report content that is deemed inappropriate or harassing. If you start receiving content specifically targeted at you that is considered suspicious because it looks like insults, inappropriate propositions, threats or other expressions that cause annoyance, you should keep a copy of that content, as it could be useful if you need to file a report about the annoying or malicious identity.

Systematically activate privacy protection on minors' profiles. It is advisable to ensure that minors who create a profile on social networks activate privacy controls, both for content and for lists of friends, keeping them to a minimum and not providing personal data, such as information visible to the general public in cyberspace.

If privacy controls are combined with monitoring of the profile by the adults in charge of the child and a minimum of education on the use of social networks, an acceptable standard of good practice in the management of the child's social networks will be maintained.

12. https://support.twitter.com/articles/108038

3.5 Step 5: Adopting a personal culture of cyber protection

The prevention and management of risks in social networks cannot be achieved in isolation, by intensifying and strengthening the security of the websites or apps from which the service is provided in each social network; nor can it be achieved only by increasingly reducing the vulnerabilities of the devices used to connect to cyberspace, such as phones, computers, watches and, little by little, any object of daily use such as a car or a television.

The best risk prevention is achieved when, in an ecosystem where several factors come together, such as cyberspace with websites, devices, objects and people, **the security of the weakest link is substantially increased**; and in cyberspace, the weakest link in terms of security is the human being, who, unlike machines, cannot be programmed.

Human cybersecurity in cyberspace can be partially achieved by "forcing" humans to perform certain tasks that involve security behaviours. For example, by preventing them from choosing passwords that are not alphanumeric and longer than eight characters or by limiting in web browsers the use of certain types of files that are considered potentially vulnerable. However, both the very free will of human behaviour and the malicious techniques used by social engineering demonstrate time and again that **the most effective cyber security starts with the internet user's own self-protection in cyberspace.**

Humans need to protect themselves from threats in cyberspace. For example: alpha-numeric passwords of more than eight characters or by decreasing vulnerabilities of devices.

3.5.1 Defining the savvy cybernaut

Self-protection in cyberspace requires the internet user, the user of social networks, to adopt personal cybersecurity behaviour:

Situational awareness of risk. Self-protection in cyberspace requires understanding that, just as in the analogue world, there are also spaces in social networks where malicious identities will try to obtain illicit benefit by causing harm to others.

Be informed about threats and vulnerabilities. Be generally aware of the potential dangers that can lurk on social networks. The best way to stay informed is to subscribe, on the social networks themselves, to a news channel with daily updates with advice and warnings about internet security. In Spain, the National Institute of Cybersecurity has set up the Office of Internet Security precisely for this purpose, with informative channels on the web and social networks[13].

Internalise and apply good cyber-protection practices, being aware of which behaviours put users at risk on social networks and which ones prevent them from being exposed to cyber-threats. These preventive behaviours should be put into practice and gradually internalised as part of a **safe way of navigating in cyberspace.**

13. www.osi.es, www.facebook.com/osiseguridad, www.twitter.com/osiseguridad, www.youtube.com/user/OSIseguridad.

3.5.1 Defining the savvy cybernaut

Therefore, the **intelligent cybernaut** is an aware and informed person, who takes advantage of the content that circulates daily on social networks to include among it alerts or notifications about new risks and best practices; who is aware of the latest forms of *phishing*, the latest harmful content or unwanted advertising that may affect them, the latest fraud schemes or the latest malicious codes that are being transmitted through social networks with the intention of stealing personal data or money.

In other words, the intelligent cybernaut takes advantage of what social networks represent as immediate and continuous information channels to provide him/herself with a **personal culture of cyberprotection and cybersecurity;** a culture that makes them less vulnerable inhabitants of cyberspace, reducing the surface of exposure and allowing them to extract all the personal, social and work-related value that social networks could provide them with. By incorporating simple guidelines for protection and good practice into their daily internet browsing routines, preventable risks are set aside.

4. Decalogue of recommendations

The following are ten (10) safety recommendations for the use of Social Networking sites

Security Decalogue on Social Networks

1. A permanent site headed by photographs, personal data and information about studies, profession, tastes, interests, friends and family provides much more information about the person than his or her ID card or passport. Moreover, it would be visible to the whole world. It is key to pay attention to how you define your profile on social networks, as it will be the letter of introduction of your identity in cyberspace.

2. Reflect on the content that is shared on social media. More and more people and companies are watching and analysing social media to make a judgement about other people. If you want a fair judgement, take control over your own content.

3. Do not share sensitive content about your personal life or the lives of others on social networks: identification documents, telephone numbers, postal addresses, exact locations, vehicle identifiers, etc. The more such content you share, the more likely you are to be a victim of identity theft, cyberbullying or other unlawful action that uses your own information to harm you.

4. The principle "beware of the unknown" applies in cyberspace. Do not click on content whose origin or purpose is unclear, and increase caution in the face of messages from unknown identities. In short, avoid the temptation of anything that the more unknown, the more attractive it seems.

5. Protect access to social media profiles with strong passwords using two-factor authentication where feasible.

6. Control the geolocation of profiles and content on social networks. Deactivate the default geolocation in the profile configuration menu and make intelligent use of it, thinking in each case whether you want others to have a map of your life or part of it.

7. Check the privacy settings on both your profile and the content you share. Be aware that cyberspace is full of digital eyes and that you should only show what you are sure anyone can see. When in doubt, keep information private to friends and contacts.

8. Do not disseminate private information about other people without their consent and do not tag by name other people who do not have a social media profile without first seeking their permission to do so.

9. Take care and protect relationships in cyberspace. Keep your contact list private and carefully scrutinise friend requests from strangers.

10. Be aware that the first line of defence for protection in cyberspace is oneself. In this way, the help provided by cybersecurity institutions and organisations will be much more efficient and you will be of invaluable help in keeping social networks safe.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es