5 ways to protect your digital identity

17 october, 2019 ·

Table of contents

In the era of communication, protecting our physical identity and the one on the Internet are equally important. Especially now that cyber-attacks are on the rise, affecting both individuals and entities. Under this situation we must follow certain Internet safety rules. Here are five tips.

Cyber crime is a growing concern for the authorities. Reasons for us to find ourselves in this situation are the figures published by Spanish and European Authorities and specialists in this regard.

At the continental level, a study by F5 Labs states that Europe has suffered the most online attacks in the world during the first quarter of 2019. In Spain, the *Cyber Threats and Trends 2019* report by the National Cryptological Center, explains that in recent years attacks against personal data have increased and will continue to do so in the future.

As we can see, the rise of threats directed at individuals forces us to remain vigilant and be very careful with everything related to the information and the actions performed on the Internet. For this reason we would like to help you secure your digital identity with some tips.

What is digital identity?

address or the age of digital elements.

These digital elements refer to the email address, profile on social media or other types of web portals, messages uploaded to the network, multimedia content, avatars, bank details or their digital signature.

As you can see, the digital identity goes beyond a a dataset on an identification card, but covers aspects like the online behaviour of each person.

Main threats for digital identity

Digital identity can be harmed by a set of malicious agents that must be kept in mind when performing any online action. Among these threats, we can highlight the following.

Malware

This means a malicious software that may be installed installed on the user's device without their consent.

They intend to steal confidential information, such as bank details, passwords or any type of sensitive material. They may also block the device or the user's data demanding ransomware payments.

Phishing

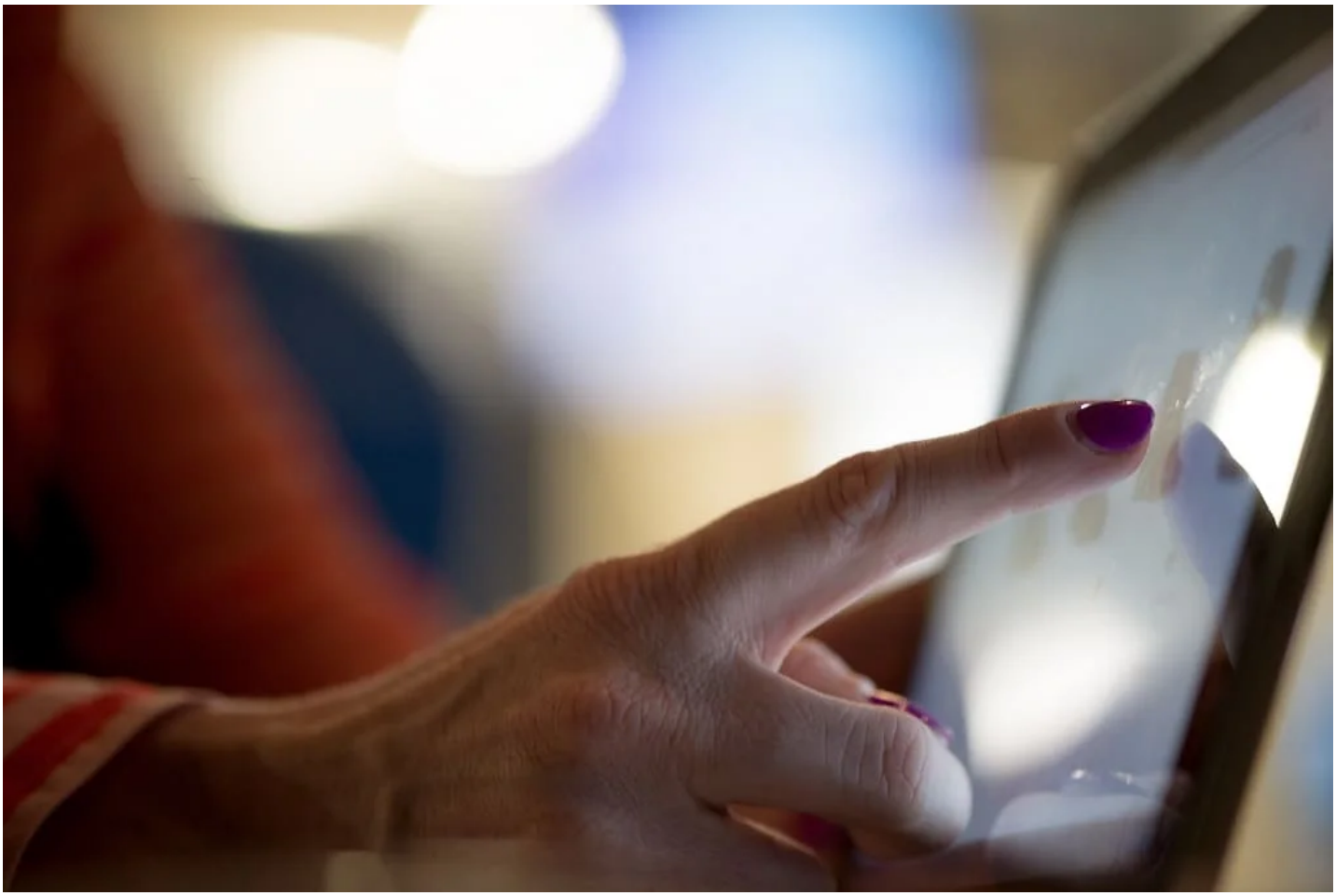
It's a set of techniques used to deceive users into providing valuable information, whether financial or personal.

Spyware

Spyware software steals valuable information from a device that is connected to the network and sends it to an external entity.

Identity Theft

In this case someone impersonates another person by using their personal data.



5 ways to protect your digital identity

Password Management

A password is the most traditional way of protecting digital identity. That is why we must take our time, as well as certain good practices, when establishing the different passwords of the online services we use. It is not a matter of taking it lightly.

When defining a password there are security actions present by the service administrators themselves, such as a minimum length or the obligation to use lowercase, uppercase or some number. But in addition, we can take other habits on our own, such as:

- They are long and complex. This password does not have to make much logical sense, thus being more difficult to steal.

- Do not use the same password for all sites.
- Do not include the name of the service that we will use in the password.
- Do not use personal information for the password, such as a family member's name or date of birth.
- Use a password manager, since it will allow access to all services only through a single password, which must be extremely secure.

We provide you with a trick to build a very complex password and, at the same time, easy to remember:

1. –Choose a song. For example: Free, by Nino Bravo. Now, go to the beginning of the letter: "I will look for a place for you, where heaven..."
2. –Select the first letter of each word: Iwlfapfywh.
3. –Add a number (it can always be the same): Iwlfapfywh9.
4. –Then, put a sign and the capital letter of the site where it will be used, for example, Facebook: Iwlfapfywh9-F.
5. –If the phrase has something that can be changed by a number, better still: 1wlfapfywh 9-F.

Now you have a very complicated password, different for each site (more or less) and very easy to remember.

Do not use open Wi-Fi networks, or use them very carefully

Many people have the habit of connecting to the internet through wireless networks available for free in coffee shops, public transport, on the street itself and in many other places. This, although it seems an advantage from the point of view of network accessibility, is not recommended for cyber security.

These Wi-Fi networks do not usually have WPA or WEP encryption, which translates into lower security standards.

If we have no choice but to do so, we must try to access websites that have secure https (Hyper Text Transfer Protocol Secure) protocol, in which the information on the website is encrypted.

Digital signature

documents have not been altered after this process.

As we have mentioned on other articles, the digital signature may be associated with a digital certificate (as in the case of qualified signatures), but it is not essential (as in advanced signatures), but both have a very high level of security, if they meet the right requirements

In the case of digital certificates, we must protect them against possible illegal uses, and for this the centralized signature is a very powerful ally, allowing safe custody in the cloud so that they can be used anywhere. To this we must add that, since the certificates are not installed on any physical device, it is therefore harder to steal.

Viafirma Fortress is a secure solution for for storing signatures and certificates. Viafirma Fortress consists of a robust identification system, or what is the same, a two factor authentication which can be: something you know, something you have or something you do or that It is the user.

These authentication factors can be, among others, email, LDAP, OTP, password, PIN number, SMS or biometric signature.

Make sure you have the updated software

Cyber criminals are constantly inventing new tools and methods to commit crimes and attempt against our digital identity.

Hackers often take advantage of security loopholes in different applications and operating systems. Therefore it is crucial to have the latest versions available.

Training is essential

One of the most important premises in terms of digital identity protection and computer security is to have the best antivirus.

Of course, to apply this common sense, at a minimum, we must be aware of the modus operandi of cybercriminals, current affairs in terms of digital threats and of the most effective measures to neutralize them.

This applies to both domestic and professional use. There are many training courses, seminars, congresses and events of all kinds in cyber security, and lot of information can also be found in the Internet Security Office.

improvement of general cyber security.

An example of the latter is the recently approved Cyber Security Law of the European Union (Regulation 2019/881), which will provide a strong boost to the European Agency for Cyber security (ENISA, by its acronym in Spanish) and standardize security criteria, as marked by the European Digital Single Market.

With these measures we can establish the bricks of a safe behaviour on the Internet that avoids as far as possible the usurpation of our digital identity. All this with the support of institutions that strive so that we can enjoy the infinite opportunities that the internet offers us safely.

VIAFIRMA EUROPE

HEAD OFFICE
+34 954 155 244
comercial@viafirma.com
Edificio Centris. Planta Baja. Módulo 8
Glorieta Fernando Quiñones S/N
41940 Tomares (Seville)
Spain

MADRID
+34 954 155 244
comercial@viafirma.com

Spain

VIAFIRMA AMERICA

COLOMBIA
+57 311 5680931
comercial@viafirma.com.co
Cra 9 #115-30 Piso 17. Edificio Tierra Firme.
110111 Bogotá
Colombia

DOMINICAN REPUBLIC (AVANSI)
+1 809 682 3928
info@viafirma.do
Edificio PIISA A, suite 102.
Lope de Vega, 19
Ensanche Naco
10119 Santo Domingo
Dominican Republic