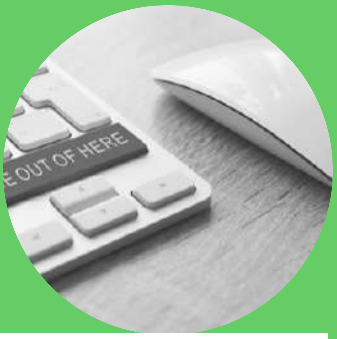
ODS
OPEN DATA SECURITY

CYBER SECURITY GUIDE FOR DUMMIES

A BEGINNERS GUIDE

opendatasecurity.io

TABLE OF CONTENTS



PART I

This is the Internet, the oasis in which we live in

Wake up and look at the phone. Have a shower, get dressed and close the door when leaving your house. Get in the car, put on the seat belt and drive to work.

It is not until you have your very first coffee, when you realise you have been acting on **autopilot mode**. Without thinking.

It is logical to close the house door; **we assume** that for safety you have to put on your seat belt when getting in the car. We know that using a helmet when riding a motorcycle protects us, and for the same reason, we try to look before crossing the street.

We integrate these actions in order to survive the dangers of real life. But the question is: **are we prepared to survive in the online world?**

While reading this, you are one of the 3,764 million people connected to the Internet.

You are part of that exorbitant amount of users in the network that generate information every time you:

- Connect to a wifi network.
- Do a search on Google or any other search engine.
- Click on a link.
- Register in a web or application.
- Download and install an application on your device.
- Send or receive an e-mail or an instant message.
- Buy something in an online store.
- Like a publication on social networks.
- Publish content on a social network, blog, application or web.

And the list does not end here. It is much longer because **we are doing more and more things from our Internet-connected devices**.

That's why we produce much more information than we can imagine.

Data speaks for itself: the amount of information we generate about us is immense and users underestimate not only the quantity, but also their value. So the question becomes inevitable:

Why should we be concerned about the information we generate on the Internet? Even if you don't believe so, **there are people and entities that want that information**, that are willing to pay for it or to obtain it using methods of doubtful ethics.

Companies, organisations, governments ... Our data is gold and from the moment we own an electronic device connected to the Internet, we start living in glass houses. The ones who are able to see through that glass and are aware of those facts, are commonly known as hackers.

Hackers, the bad guys of the oasis

"*Hacker*" is a widely used term today. Its meaning may vary according to the context in which it is used.

For example, the first meaning that appears in the dictionary of hackers, points out that it is "the person who likes to investigate the intricacies of programmable systems and how to squeeze their capabilities, unlike the majority of users who prefer to learn the minimum."

That definition does not speak of someone who commits criminal acts on the network. However, through the literature that has emerged around the Internet and the media, you can easily verify that **"*hacker*" is the most common way of referring to cybercriminals**. Individuals who are also known as "black hat" hackers, "crackers" or simply "attackers".

The main objective of a cybercriminal is usually to **earn money**. We say this because there are also cases in which the motivations may be ideological (hacktivism), or the intention may simply be to boast of what one is capable of doing.

What matters to users is **cybercriminals design complex attack methods** every day to obtain sensitive information about us. And they get it. Of course they do.

According to the data, we are talking about **the criminal activity that generates the most money in the world**. In fact, in a recent report by the Accenture consultancy, it is pointed out that a cyberattack can have higher costs than a natural disaster.

> A hacker is a person who likes to investigate the intricacies of programmable systems and how to squeeze their capabilities

Attack techniques with which they get what they want

The danger on the Internet exists for absolutely everyone. In cybersecurity, it is often said that **zero risk does not exist**. For that reason, we should not stop trying to protect ourselves.

The attacks we will see below are the most common ones, those that generate the most headlines, and to complicate this situation even more, the way in which they can be presented can be very varied.

Knowing how cybercriminals think and attack could prevent you from turning into another victim

That is why it is so important to **know what we are facing**, as well as knowing the way in which the attackers act and the way in which we can prevent ourselves from being victims of a cyberattack.

PHISHING OR IDENTITY THEFT

It is the most common scam on the Internet. It is based on posing as a person of trust or in a company of which we are customers to obtain our data: passwords, banking information, among others.

To do this, the cybercriminal uses social engineering to make the deception credible. This means they design and send very similar corporate e-mails to those customers who usually receive these kind of emails.

In a phishing email, they usually ask for one of these three actions:

1 To answer the e-mail by providing user information.

2 To answer the e-mail by providing user information.

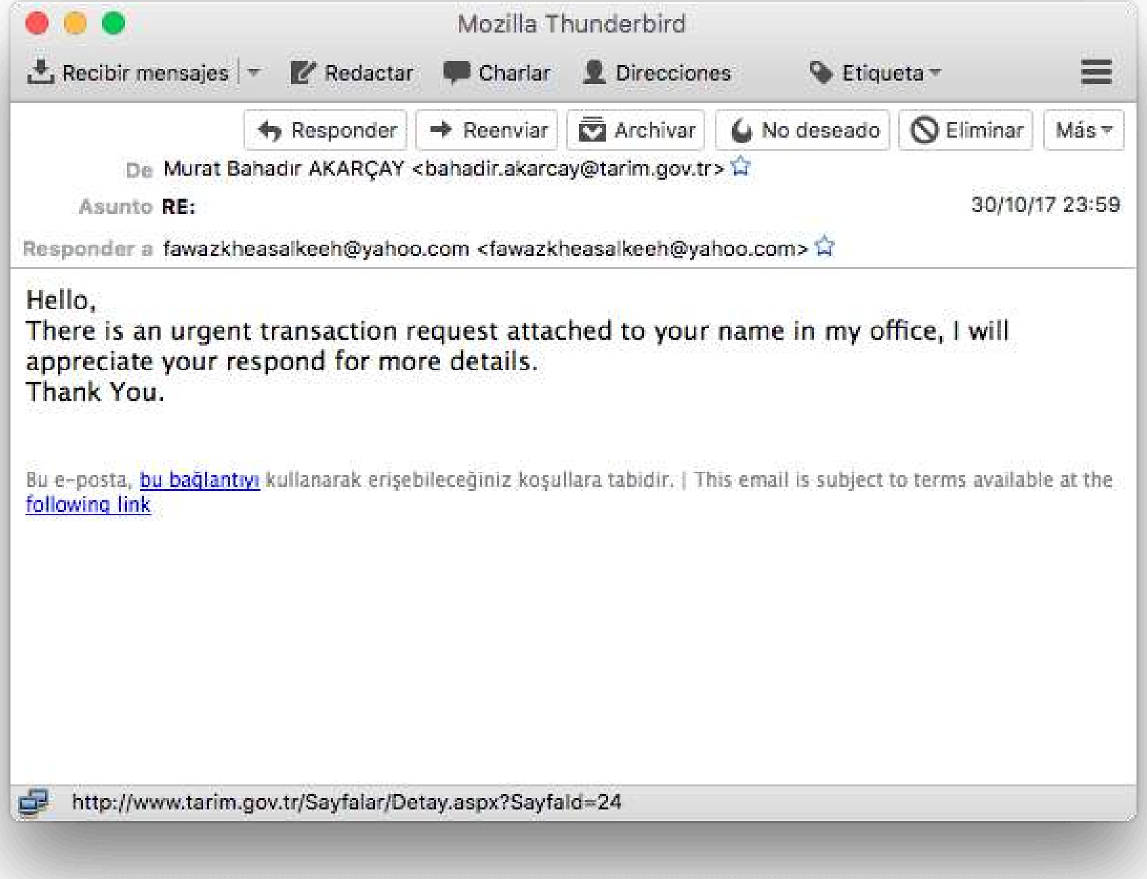
3 To click on a link that leads to a fraudulent web page in which the attacker can ask for other actions such as putting personal data that will be used by the attackers.

Phishing attack scenarios are not limited to email. It is possible to be attacked **by instant messaging or by phone calls** if you pose as a trusted person.

Phishing is also present in **fraudulent websites** you can access because they havemanaged to appear in Google results or because they are in the profile of a user of a social network.

For all the above, **the best prevention for phishing is based on distrusting** the content we receive through e-mail, instant messaging, social networks and even distrust when someone calls us to ask for private information over the phone.

There are also antivirus and tools that scan the attachments of our emails or block potentially damaging links. These are recommended and valid solutions, but not as effective as caution.



De Murat Bahadır AKARÇAY <bahadir.akarcay@tarim.gov.tr>

Asunto **RE:** 30/10/17 23:59

Responder a fawazkheasalkeeh@yahoo.com <fawazkheasalkeeh@yahoo.com>

Hello,
There is an urgent transaction request attached to your name in my office, I will appreciate your respond for more details.
Thank You.

Bu e-posta, bu bağlantıyı kullanarak erişebileceğiniz koşullara tabidir. | This email is subject to terms available at the following link

http://www.tarim.gov.tr/Sayfalar/Detay.aspx?SayfaId=24

Screenshot of a phishing email requesting the download of an attachment. In it you can see a strange email address and there's no return address.

RANSOMWARE, THE WORM THAT BLOCKS ACCESS TO YOUR COMPUTER

It is the most feared virus of recent times. The ransomware has been the protagonist of many headlines for affecting users, companies and institutions around the world. Its modus operandi is to **infect devices by blocking their access** and asking for a ransom in exchange for returning things to normality.

Some variants of ransomware also **encrypt the information** we have in our devices. In these situations a reverse of that encryption should be performed.

The most important thing we should know about a ransomware is that **you should not pay the ransom the attackers request**. The reason is that there is no guarantee we will recover our information, so paying could involve not only the loss of data, but also money.

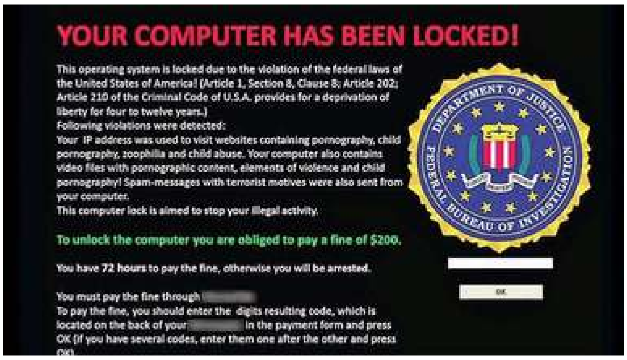
> **Every 10 seconds, a user suffers a ransomware attack.**
> **Source: Barkly.com**

The way in which this virus enters our systems is also diverse. It can be **through phishing**: a message in which we are asked to download a malign file or program.

It is possible for ransomware to infect computers and infrastructures by **exploiting vulnerabilities** in the system or an application installed on it. The possibilities are as complex as they are diverse.

So how should we prevent a ransomware from attacking us? The truth is that it is difficult, since new variants are emerging every day.

Therefore, it is best to **have the backup copies of your files updated** so that we can restore it in case our equipment is blocked and the information is encrypted.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

Screenshot of a ransomware in which the FBI logo appeared to demand the rescue of $200 from those affected.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

Every time we visit a web page, a request is made to a server, so that it responds with the data (web page) to which we want to enter.

Imagine for a moment many requests are made at the same time, so many that **the server is not able to stand and stops providing a service**, so you can not access the web page.

This is what is intended to be achieved with a **DDoS (Denial of Service) attack**, in which a saturation is achieved by overloading the servers from a single machine, whereas in a DDoS attack (Distributed Denial of Service), the attack comes from several points such as a network of bots (machines).

As users, the only thing that can be done when you can not access a web page or application that might be suffering from this type of attack is to **wait for normality to be reestablished.**

EXPLOITING VULNERABILITIES AND ERRORS

It is usual that we have to update our devices every time a new version of the operating system or the applications we have installed is released. Many times, this happens because they bring news, such as new functions.

Sometimes, what they do is solve a security breach that could compromise the information of the users. That's why is is important to keep the latest updates.

Occasionally, the security breaches of a system are not fixed until attacks already occurring. Therefore, most of the time we are not aware of when they have attacked us and a long time passes until we find out. A time in which attackers take advantage to extract private information from users.

> **DDoS attacks have been registered with a duration of 277 hours.**
> **Source: Quarterly Report on Malware of Securelist 2017**

What harm could a cyberattack cause us?

As we said at the beginning, the main objective of cybercriminals is to **earn money**. Therefore, when they steal information from us through a computer attack, their next step is to sell it on the black market or take advantage of it.

Any sensitive data can be very precious, from the content we keep in our email, to our computer or mobile phone; logically, e-mail addresses, bank and credit card information are also of great value.

> We make the mistake of thinking that our data has no value, when it's actually the main reason why cyber attacks occur

And the way in which cybercriminals do business does not end there. We can also filter applications that directly take money from bank accounts. Android.Fakebank is one of them. The Trojan infected Android devices mainly from South Korea and Russia during the summer of 2016, according to Symantec.

It was installed through an application that apparently seemed to be Google. Once installed, it worked in the background and **stole banking information from the user**.

To make things worse, when he realized there were strange transactions in his bank account, the Trojan blocked any bank call made from the infected device.

This made the user take longer to block the activity of his account, and therefore, gave advantage to cybercriminals to extract more money. The result is to be expected: a bad experience ending up as a looting.

This is another example of the risks users run from the moment we have in our hands a device with an Internet connection. Now, each problem has a solution, but that is something we will raise in the next article.

PART II

PART II

A home with all doors closed, the key to cybersecurity

In the last few years, technology has advanced in such a way that nowadays we can do practically everything without moving from home. Thanks to the Internet we have everything in our hands, literally. Our finger is the only thing that separates us from clicking on “Buy”, “Download”, “Tweet”, “Send”, etc.

It is no longer necessary to go to the cinema to see the latest releases; nor go to the physical stores to buy any product we want to buy. We can even shop in the supermarket from home.

But, what if instead of buying some shoes or downloading a game, we were actually giving away our bank details to a criminal? It is totally possible, and we would not even notice it.

This is how some cybercriminals act. As we explained in the first Part of this dummie’s cybersecurity guide, there are multiple risks and dangers on the Internet. And all of them **take advantage of the ignorance or misleading of the users**, whose information can be very precious.

A click on the wrong place can cause great damage not only to large organizations, but also to people. In our daily life we carry out a series of simple and daily activities that **can represent a very high risk for our security**.

We arrive home and, normally, the first thing we do is turn on the router (in case we ever turn it off). We connect our smartphone or our device to the Wi-Fi network of our home and we are ready to navigate. And your neighbor may know about this.

Wait, how will my neighbor know that I am connected to the Internet? In fact it’s very easy. **They may have used your Wi-Fi on more than one occasion**. If ever the speed of navigation has been particularly slow despite having a very high bandwidth, it may be due to this: someone is accessing the Internet from your network.

Although public Wi-Fi connections are the ones that receive most of the cyber attacks, **domestic networks are not exempt from this danger**, as they can be easily accessed.

The problem? The passwords

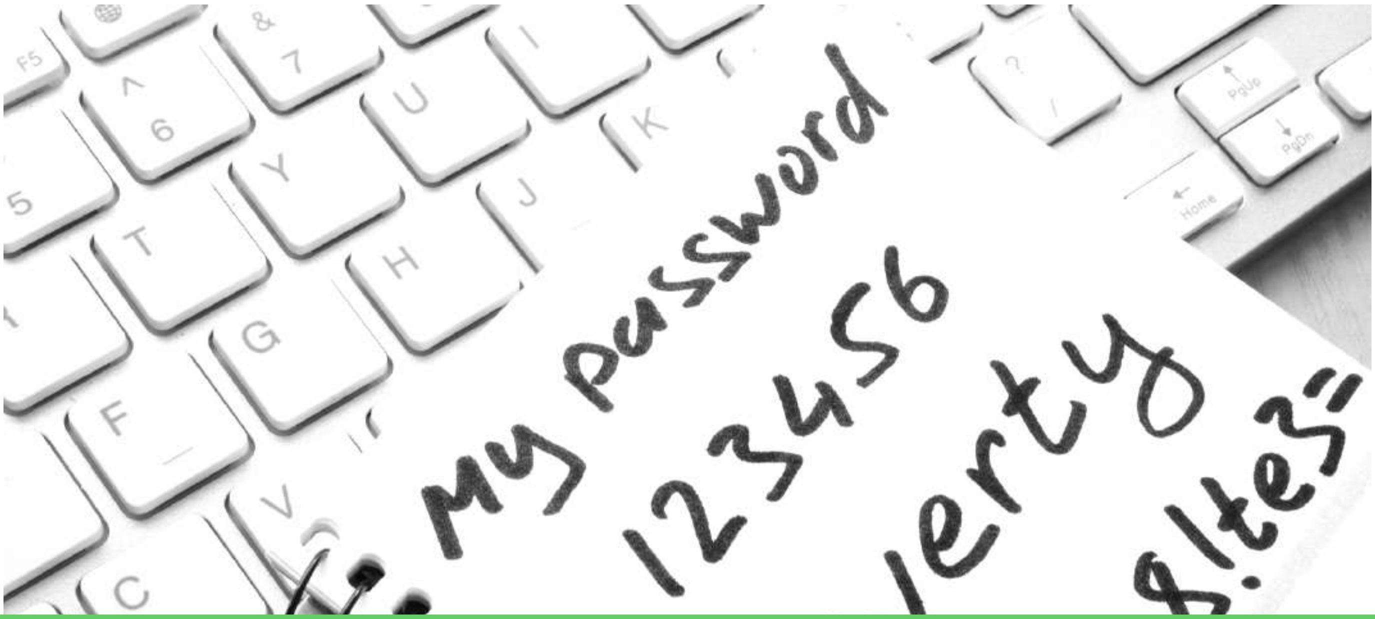
To prevent unauthorized users from connecting wirelessly to our router, stealing our Internet connection and even accessing other computers in our local network, these are usually protected with a password.

Without it, access can not be possible.

However, these passwords **are often weak and easy to hack**. In fact, if we check our router we will surely find one of these 3:

- admin/admin
- admin/password
- admin/

> ”
> **One of the most widely used passwords in the world is “123456”. Source: Keepersecurity.com**



The solution? Changing the password

Once they have accessed our router, hackers have total freedom to change the Wi-Fi password and prevent us from accessing any device we use.

To avoid this, **we must change the default access password of the Wi-Fi network** supplied by our Internet provider. These passwords are configured with an algorithm that is available to anyone. So by simply reading a tutorial on the Internet we might be able to misuse that information ourselves.

Therefore, we must assign a password that complies with **all security measures**:

- Contain lowercase, uppercase, numbers and letters.
- Do not use birthday dates, pet names, favorite foods and other easily guessable data.

Another of the most important steps to protect your home network is to activate the Wi-Fi protected access protocol (WPA) of the network. The WPA is just an industry standard which ensures that when you are connected to a router, external individuals can not analyze traffic and obtain information. Although you will have to check the router's manual to activate this protocol, the most current routers have a configuration that allows wireless encryption to be activated at the touch of a button.

We must change the default access password of the Wi-Fi network supplied by our Internet provider

It is important to note wireless encryption only protects us against hackers who try to see our Internet traffic. When we connect to a secure wireless network, we are still exposed to malware, spam and other harmful cyber threats.

What other methods are there to protect our devices?

We must be careful with what we publish on our social networks. They store large amounts of information about the activities we do, the places we visit, the people with whom we interact, our hobbies, the food we like, etc.

All this information can be used by an attacker to know our profile or plan and launch custom attacks such as the phishing that we mentioned in the first part of this guide. In addition, the information collected can be used even for kidnappings or extortions.

How to know which application is safe?

In mobile technology, most messaging services such as WhatsApp, for example, offer an **encryption system** in all our conversations. This means only we and the person with whom we communicate can read the messages, preventing access to third parties.

In fact, and even if the cybercriminal could get all the shared information, they would only see **codes that could not be deciphered**.

When surfing the Internet, it is recommended to do it on those websites where **HTTPS** is placed in the address bar, which also give the user an extra encryption. When the URL of a website starts with https: //, your computer is connected to a page that is speaking to you in a coded, invader-proof and more secure language. And we must navigate in these type of websites especially when we make online purchases, as long as they are linked to recognized electronic payment gateways as Visa, Mastercard, Paypal, among others.

FIREWALLS

An additional tool to protect against Internet threats is the use of a firewall. It is simply a security tool that controls which applications have access to the Internet and which connections are allowed to access our computer. Firewalls are usually programmed to automatically recognize threats, which means they are usually easy to use and do not interfere with the way we use the computer.

VPN OR PRIVATE VIRTUAL NETWORK

Another very good measure is to use a VPN (Virtual Private Network), which is a network technology that allows us to create a local network (LAN) even if we are browsing remotely and we need to pass the information through a public network. An VPN creates a kind of tunnel and prevents anyone from catching and using that information.

Thereby, we make sure everything that comes out of our devices is encrypted until the receiver of the message gets that information. This can prevent man-in-the-middle attacks, atype of threat in which the cybercriminal acquires the ability to divert or control communications between the two parties.

ANTIVIRUS

And of course having an antivirus. It is essential to keep our operating system updated and use the best antivirus to alert and protect us against possible threats. It is also important to run it periodically in order to find and remove malware, as well as perform automatic updates.

If you are debating whether to buy an antivirus license or get one for free, we must bear in mind that although most of the free software are of high quality and offer a reasonable level of security for home users, they do not always offer the same level of protection.

The best option would be to consult with an expert, and if possible, choose an antivirus that has technical support to help us with the configuration.

The distrust attitude, the best one

The best option is not to trust innocently in the first thing that comes in to our email inbox, in that link offering us a free product, in that user who wants to add us to a social network and that we do not know, etc.

We must think twice before doing any of those actions: **if something is too good to be true, then it is very likely to be fraudulent or harmful**.

It is always advisable to use spam filters which help block bulk emails that may contain malware.

We have to be careful if someone, even a friend with good intentions or a member of the family, gives us a USB or removable disk to insert it into our computers. They could have hidden malware in it without even knowing. Therefore, **it is essential to scan with an antivirus** every element we introduce in our devices or download from the web.

Last but not least, we should get used to **backing up** our device periodically to minimize data loss.

It is esential to scan with an antivirus every element we introduce in our devices or download from the web

Everything stays at home, or not?

Devices such as a smartphone, a tablet, a smart TV; smart appliances such as refrigerators or ovens; even thermostats, blinds, doors and lights controlled from your own phone. This is the **Internet of Things or IoT**.

Currently all these devices **are connected to**

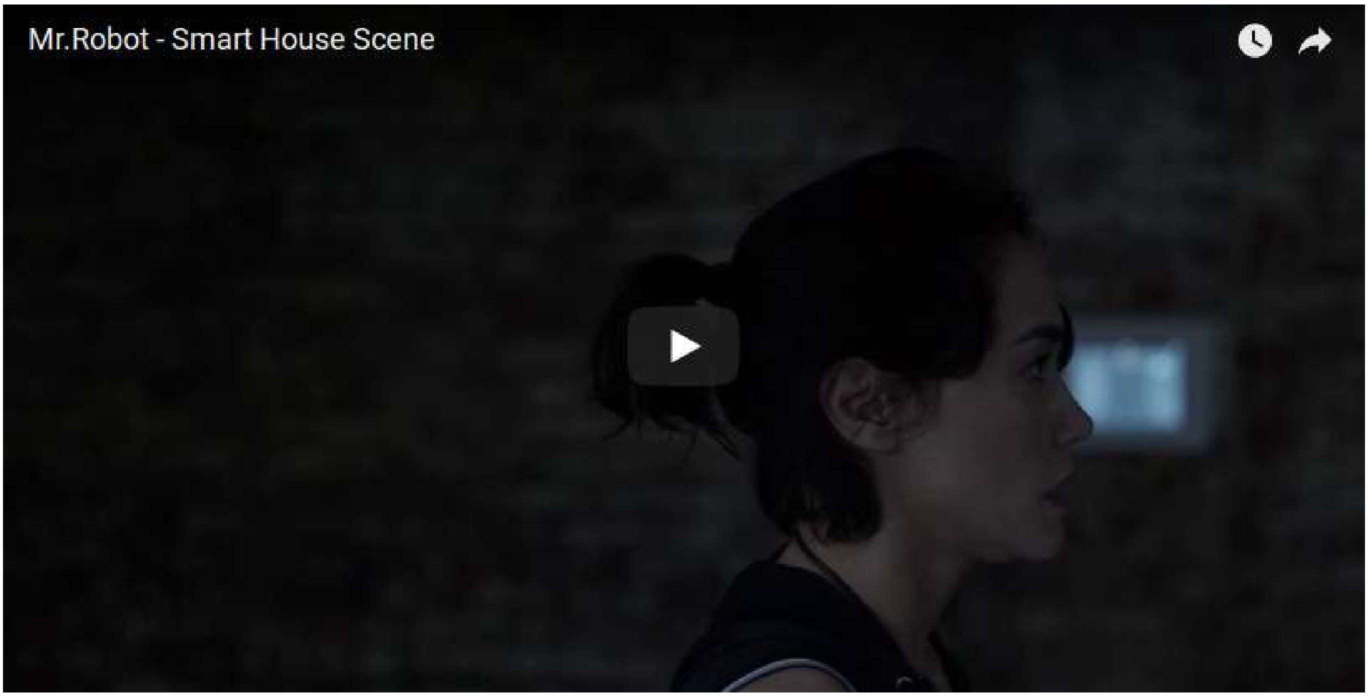
each other through Wi-Fi, Bluetooth or infrared connections and communicate with a central control which is usually found in the same domicile or in the central server of the manufacturer.

The tendency shows there will be more devices than people in each house. And these devices play an increasingly important role in domestic life.

However, **the IoT represents a difficult challenge for security**. The sensors of all Internet of Things devices collect data about us: they know what television programs we see, what we say inside a room, at what time we arrived home, etc.

And as the number of networks, operators, consumers and devices increases, so does the risk of a breach.

A great example of that risk is one of the scenes of the Mr. Robot serial, in which the network of a house is hacked, altering the behavior of all the devices that are in it.



Even the vacuum cleaner robots that have become so well-known in the last few years can store valuable information about our homes. The internationally known brand Roomba stores information about the dimensions of the houses and plans to sell it to other large technology companies.

According to its CEO, Colin Angle, the intention is to improve the technology of smart homes, and Google, Amazon and Apple are the possible buyers of that information.

But should we trust this information will not be shared with third parties? Our privacy is at stake, and as we said, we can not trust anyone, we can not even control what happens in our own home.

If we can not feel safe at home, how would it be in our workplace? We'll leave that for the third part of this cybersecurity guide for dummies.

The IoT or Internet of Things represents a difficult challenge for cybersecurity, as it collects data about us

PART III

Cybersecurity for the workplace

The principle of scarcity says that we value an asset higher when it has a scarce availability, while we tend to think that what exists in abundance has little or no value. It is possible that this theory explains why **we do not give importance to the information** that we generate as users.

Possibly, this is the reason why cybercrime has turned into **one of the most profitable criminal activities** of these times, and this situation will continue as long as we ignore how much data our email address or ID number can provide anyone who asks for them.

Things get worse when **cybercriminals target companies**. The corporate information and the data of the clients are an important part of the economic activity. That is why **protecting information should be one of the priorities of companies**, but in most of them it is not yet.

The Internet has given us a window of business opportunities that sometimes makes it difficult to perceive real threats. This means that, in terms of cybersecurity, **companies are reactive and not active**, which means that they only look for solutions when they have been hit by an attack instead of preventing it by the implementation of cybersecurity policies .

But let’s go back to the beginning of the problem.

Why do hackers attack when you are working?

Remember, how was your first day of work?

Surely, it was not one of the easiest. You had to learn the names of your mates not without delay. They explained to you details of the company while you thought that it was possible that you would forget everything after a while.

But none of that information had to do with how to protect yourself from cyberattacks or how to perform your job more safely.

And why is that a problem?

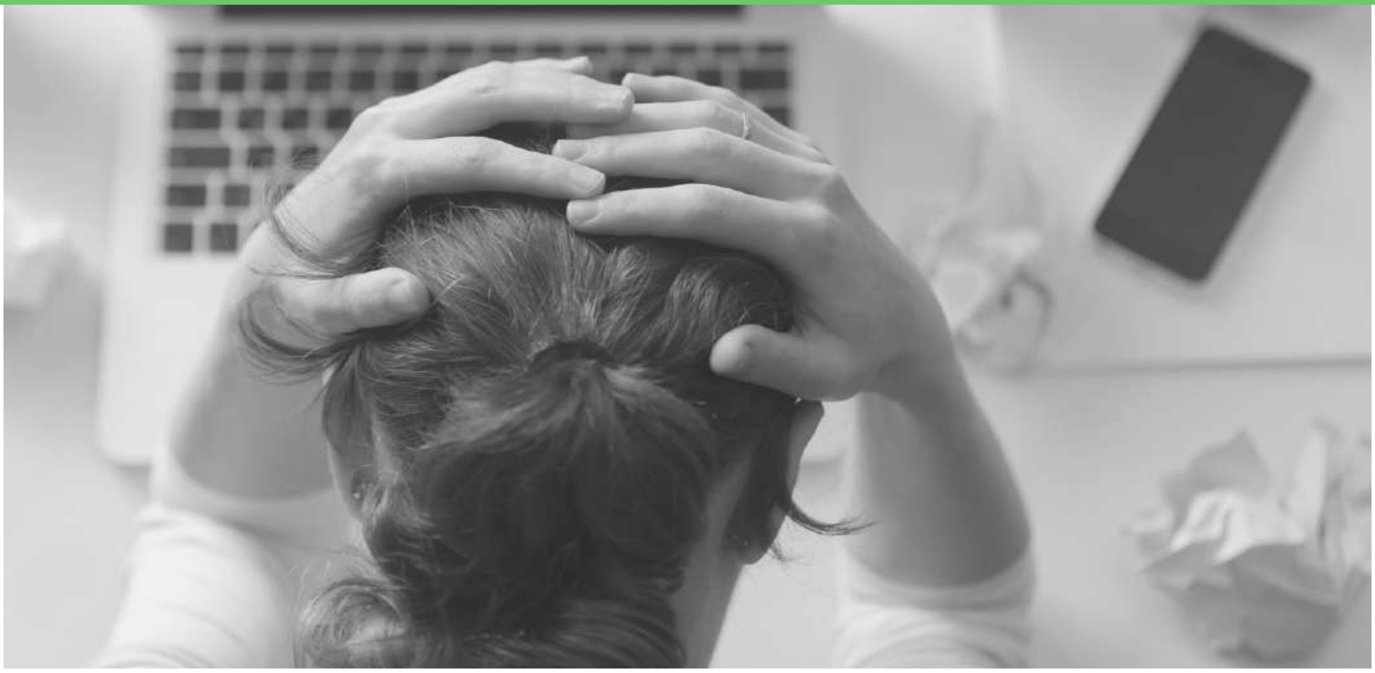
Because every day we receive dozens of emails from customers, suppliers and advertisers; we manage orders through corporate or third-party applications; and in short, **we carry out tasks proper to the activity we perform without the necessary security training**.

The next click might end with the ransom of the equipment and the encryption of the data stored in it. Cybercriminals are aware of the lack of security training of most users. They take advantage of it, just as they do with the **frenetic rhythm that many workers have** in their offices.

Lack of awareness and rushing make up the perfect context for an attack with high probability of success. And part of that success is determined by the methodology that cybercriminals use, like for example, social engineering and phishing.

Lack of awareness and rushing makes the perfect setting for an attack with high probability of success

What methods do they use? This is how social engineering and phishing works



An exercise of persuasion. This is how you could define what people do when performing social engineering.

Through a set of **psychological techniques and social skills**, the social engineer aims to gain sensitive information.

An **example of social engineering** could be receiving the mail of someone who supposedly is your manager. In the mail, he asks you to send certain confidential information that you have or, depending on your responsibility, to make a bank transfer to an account number that provides you with the excuse that it is necessary to make that payment as soon as possible.

It seems that the CEO Scam is quite obvious, but the reality is that it has achieved a high level of sophistication, so it is **a fairly common attack** among companies.

Also, **this example can be even more terrifying** if possible. On the one hand, it is making you think that the mail comes from a manager (social engineering); on the other hand, it could not only ask you to make a money transfer, but also download a malicious file that can compromise your company's infrastructure (phishing).

Like this case, cybercriminals create every day new ways to carry out attacks using social engineering and phishing. In this scenario, **learning to recognize a cyberthreat** becomes a need for all the people who work with electronic devices connected to the Internet.

A phishing attack may seem obvious, but the reality is that it is more common than most imagine

What happens when the threats come from within the company?

"The truth is out there". Do you remember? That's what they said in the X-Files series, letting us know that we had to look for the dangers outside, but how wrong they were.

When it comes to cybersecurity, the people who make an attack possible do not have to wear a hooded sweatshirt or be in front of their computer at dawn. They can wear a suit and tie or have an office schedule.

60% of attacks that occurred in companies were committed by people from within the organization. Source: IBM

They may be the people you spend more time with than your family. It is possible that they are your work mates.

According to a study that IBM published in 2015, 60% of attacks came from within an organization. From that number, **44.5% of the attacks were perpetrated by evil**, while 15.5%of those attacks originated by accident, which means by a worker who has allowed access to the company's infrastructure without wanting to.

If the bad news is that you do not just have to defend yourself from what is out there, the good news is that there is a small percentage of those attacks that occur by accident. These situations that can be avoided by complying with the basics in cybersecurity.

What are the basics of cybersecurity for a company?

Information is power, but more powerful is the one who knows what to do with information.

The really important thing is to know what to do with that information, acquire the necessary knowledge to protect yourself, and ultimately, it is important to have security training.

1. PERSONALIZED SECURITY TRAINING ACCORDING TO THE ACTIVITY OF THE COMPANY

We often think that we need a good antivirus to protect our equipment. The truth is that having these types of tools installed is fine, but they are useless when we allow (by mistake) all kinds of malware to access our systems.

If there is a reason why cybercrime has become the most profitable criminal activity in the world, it is because **the majority of users are still not aware of how to identify and proceed** when there is a potential cyberthreat.

The objective of computer security training is precisely that.

We distrust when a stranger tries to call our attention in the street. With the security training, you take the same attitude when browsing the Internet, despite not being able to see the face of your interlocutor.

But you also learn the importance of other protection methods: setting secure passwords or trying to keep computers and applications updated.

On the other hand, security training for a company should have some characteristics:

- **Personalized security training** according to the activity of the organization: because it is not the same to train bank workers as those who manage a computer in a textile store.
- **Different security training depending on the department**: because the financial department will be more susceptible to receiving potential threats than the people who are in customer service. Also, keep in mind that hackers can design attacks for positions with more responsibility because they have more privileges and critical information of the company.

2. ASK YOURSELF, HOW OFTEN DO YOU BACK UP?

The first thing we think when the disaster takes place are the backup copies. They are always ready to be used if those copies are made...

Maybe this is one of the most repeated computer security tips, but we are going to say it once again.

Backup copies must be done.

They have to be performed periodically and, if possible, save several copies of the same backup copy: one in local (offline) and another one can be uploaded to the cloud.

Nowadays we have countless tools for all types of media with which we can schedule backup copies every so often. In this way **we take away the fact of being aware of doing them** and we can go to sleep peacefully, since if we are the victim of a type of attack that erases or encrypts our data, then at least we can recover them.

3. SPECIFIC POLICY FOR SENSITIVE DATA OF THE COMPANY AND CUSTOMERS

Does the acronym GDPR sound familiar to you?

They respond to the General Data Protection Regulation, a regulation that came out in May 2016 to be applicable in May 2018. This time frame was granted so that all organizations operating in Europe will implement the necessary policies and procedures.

This regulation will give consumers more control over their information, as it implies a lot of changes for organizations that handle user data and we have talked about it at length here and here. For the privacy of the users it is good news, because the companies (only those that operate in Europe) should take care of the information they store about us.

> Learning to recognize a cyberthreat is a fundamental exercise to protect the resources of a company

4. PROTOCOL OF ACTION: WHAT TO DO IF YOU SUSPECT THAT YOU HAVE BEEN HIT BY A CYBER ATTACK?

Do you know who to call if your company is being attacked by a cyber attack?

You may think that it is not your responsibility to know that, because most organizations have a technical department that deals with it.

But not all cyberattacks are like the famous Wannacry ransomware, which infected thousand of devices around the world. **There are attacks that go unnoticed** and it takes months to know that there has been information theft.

For example, you download (unintentionally) a file from an email that seemed trustworthy.

You execute it and, despite nothing happened at this time, you suspect that something went wrong…

For these cases and many more, there should be an action protocol: like contacting a cybersecurity company or an IT security expert, if there is no one within the organization.

But how much does it cost?

In the business world, costs are everything.

One of the first issues that arise when improving the safety of companies is if it is an expensive service.

Well, the answer speaks for itself:

A single cyberattack is enough for a company to have to cease its activity.

On the one hand, there are the **recovery costs**: recover lost information, quantify how much data has been leaked, reestablish infected equipment… costs vary according to the type of attack that has been suffered.

Cybersecurity is not expensive compared to the cost of having a cyber attack

On the other hand, here is what is probably **the highest cost: the image cost**. This means that it is not a good look for a company to have customer information stolen from its customers. And ultimately, the consequences of a cyberattack can affect the sales of the organization.

And finally, with regard to cyberattacks against companies, we must bear in mind that cybercriminals have stopped targeting large corporations. The reality is that **medium and small companies are affected every time**. And campaigns like the ransomware are designed to go against organizations of all sizes to ask for a rescue according to the size of the company.

PART IV

PART IV

Symptoms and remedies: how to face cyberthreats

Prevention and distrust are two concepts we can not forget when putting ourselves in front of a device. This is definitely clear after seeing how we are affected by the lack of security at home and at work, as well as knowing how to prevent a cyberattack.

And we will not stop saying it: conscience and good practices. Always remember that in terms of cybersecurity, every precaution is helpful.

But what happens when it's too late? **What should we do if we have been attacked by a cybercriminal?**

In this fourth and last part of the guide, we will make a list of steps and recommendations to follow once we have been victims of some of the multiple threats already mentioned throughout this manual.

From knowing how to detect them, to how to face them, we bring you an index in which the emphasis will be on **reacting in time and trying to minimize risks**.

1. What to do if they impersonate your identity?

Among some of the symptoms that we can find if they have supplanted our identity are the following:

- You can not access your personal accounts with the credentials with which you normally use to login.
- You receive emails from purchases you have not actually made.
- Content is shared on your social networks from your account even if you have not published it.
- You do not get some of the bills you usually receive.

If we believe that we have been victims of identity theft, there are a series of steps we can take to respond to the incident and recover from it.

CLOSE AFFECTED ACCOUNTS IMMEDIATELY AND CHANGE PASSWORDS

Luckily, we can avoid in time the attacker taking advantage of our resources if we freeze or change credit cards or bank accounts, as well as all access passwords, even those of our social networks or email.

It is always advisable to go to the financial institution in which we operate. We must ask for advice about the possible repercussions and the steps we must take in case the account has been affected by an attack.

SUBMIT A REPORT TO THE AUTHORITIES

It is important to gather all the information possible, through screenshots, paper documents, links, email addresses, emails, messages... and give a report to the Police.

CONTACTING GOVERNMENT AGENCIES

It is not usual for cybercriminals to be behind this type of personal data, but if they have stolen documentation regarding the driver's license or the social security number, we must contact the relevant social security offices.

> If our identity has been supplanted, we must close our personal accounts and change all passwords

2. What to do if I am a victim of a ransomware attack?

If they are asking us for a ransom to re-establish the normality of our equipment and return the decrypted information, then we are facing a ransomware attack.

Again we must act as soon as possible. First we must **turn off our device**, as it stops the encryption process.

On the other hand, **trying to pinpoint the exact moment of the infection** can help when identifying the type of ransomware or determine the extent of the attack once it has occurred.

If we have backups, consider returning to a previous state in the system.

We should never pay the ransom since we will not know with certainty if we will recover the information

We should never pay the ransom. In this way we will only be encouraging the cyber criminals to commit these type of attacks and we are not sure that we will recover the information.

Once again, we must **report the attack to the authorities of our country** and contact a company specialized in cybersecurity so that it can help us solve the incident.

> **On average, a cyberattack takes 170 days to get detected and 45 days to solve it.**
> **Source: Panda Security**

3. What do I do if my website goes down due to a DDoS attack?

Sometimes it is difficult to know if we are suffering a Distributed Denial of Service (DDoS) attack. If your website is down, it may be because of legitimate traffic and not because of an attack. The key to distinguishing it lies in the amount of time the service is down.

There are cases in which cyber criminals send an email to notify of the incident and force payment so the attack is avoided. In fact, to show that it is not a joke, they cause a brief interruption or an unexplained peak of traffic as a test.

What we must do once we confirm we are facing a DDoS is to contact specialists in mitigating these attacks to help us. It will be key to stop the attack.

To prove it is not a joke, cybercriminals cause a brief interruption as a test

Second, notify the place where we have hosted our website. In most cases the threats end up being false. However, it does not hurt to give the alarm and have as many resources as possible on our side.

Under no circumstance should we pay or get in touch with the extortionists, since we could encourage them to attack us again in the future.

4. USB infection and external memories

Having a virus or malware **causes them to spread from one device to another**, acting just like any other infection.

The pendrive is a frequent attack location, but also external hard drives, memory cards, iPods or MP3 players, digital cameras, etc.

A computer can be infected through an external device that contains a virus. The infection will be made automatically by simple connection if automatic execution is active for external devices. The simple fact of making a double click on our pendrive or external hard drive will infect the operating system.

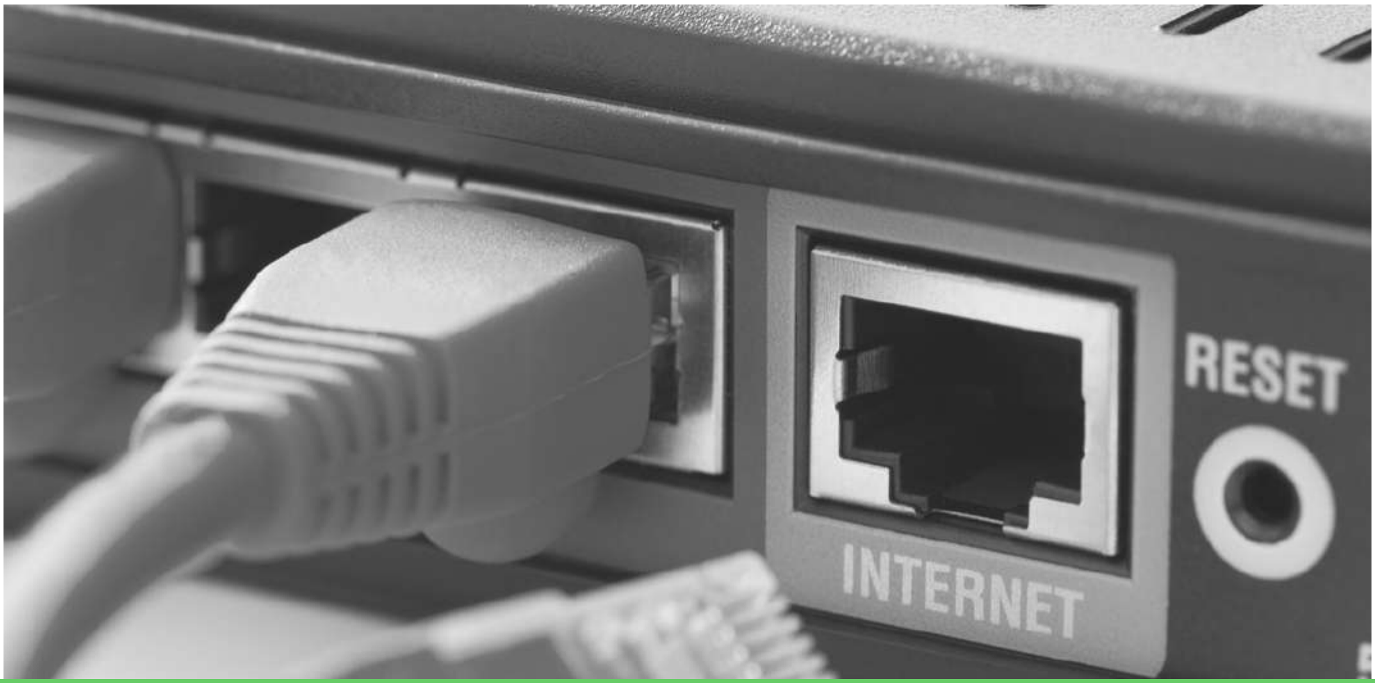
The simple act of making a click on our pendrive or external hard drive will infect the operating system

We will know that we are infected if:

- By double clicking to open the external devices connected to our computer, nothing happens.
- When viewing hidden files and folders, we realize it contains some unknown files. We must never click on them, since we will be activating the virus if it has not been activated yet.

To eliminate any threat, the antivirus plays a very important role, so we want to remind everyone that having it always updated can avoid many setbacks. We must **scan the external memory and the devices to which we have connected with the antivirus**, as well as avoid using it on others if we have not made sure before we have completely eliminated any threat.

In any case it will always be recommended to **reset the USB**. However, we must bear in mind that by doing this, we have eliminated the risk this USB will continue to infect other devices, but our computer may still be infected, so we will have to make sure that we also eliminate the infection on all our devices. If not, our USB would get infected again when connecting it to a computer.



5. What to do if we have a virus on our computer

When our computer contains a virus we know it because all kinds of pop-ups and messages on the desktop usually appear, either announcing things, saying that the PC is infected and must be protected, etc.

It may be the case the virus is performing tasks that consume resources, which is why the computer can slow down. **Another symptom is the fact that applications do not start**, or another one we did not want to start is executed.

When we connect to the Internet, many

windows may open or the browser displays unsolicited pages. This often happens since **many of the threats are designed to redirect traffic to certain sites that the user has not chosen**, and even to falsify directions making us think that we are entering a legal site when it is actually a copy of the original.

If we realize that some documents like photographs, certain folders, text files, etc. have disappeared from our computer, we should worry. It can be an infection.

Another feature of many computer threats is the **disabling of the security system installed**, such as antivirus or firewall. If just one gets closed, it can be coincidence; but if they are all disabled, it is almost an unequivocal symptom that we have become infected.

In the same way, if the languages of the applications are changed, the screen turns inside out, etc. we will have to apply the following recommendations:

- **Disconnecting from the network**: We must unplug the network cable, telephone or data from the equipment to try to prevent the data from reaching the attacker. The bots can also use our equipment as a zombie in a coordinated attack on a larger scale.
- **Analyze our computer with an antivirus**: A program with antivirus and antispyware functions can detect and often eliminate software threats from illegal activities that would otherwise remain hidden in the computer.
- **Make backup copies of important information**: A backup of our most valuable files, such as photos, videos and other work or personal files on a hard drive or removable media, such as a CD or DVD.
- **Reinstall the operating system**: Sometimes the only solution is to start over from scratch and reinstall the operating system of the computer.

6. What if I have a virus on my smartphone?

We must control the permissions we grant to the applications, since most establish permissions automatically

The use of smartphones is increasing and spreading among all generations.

This results in the increasing creation of viruses by hackers, who take advantage of the large amount of data traffic, which can put our privacy at risk.

The most common situation is **when advertising starts to appear in the notification bar**, also affecting the battery consumption or the speed of Internet connection. With this type of virus or malware it will be easy to deal with, while others, in the worst cases, **will block the device completely** and force us to pay to unlock it.

We must control the permissions we grant to the applications when we download them, since most establish some permissions that are configured automatically. For example, Google Maps asks to know in which location you are at all times, or certain applications have permission to the microphone or the camera of our electronic devices.

We must ask ourselves this question, is it really necessary? And the obvious answer is no.

If we do this, we will be able to know more easily which is the problematic application and which has the most probabilities of being the culprit of the infection of our smartphone.

Even if you think that by eliminating the application you have solved the problem, **you should scan it with an antivirus to make sure**. Once the analysis is finished, we can see not only the applications that are causing the problem, but also the files that have been affected.

After this, it is advisable to permanently delete those files, at least that way we will stop the infection and eliminate the virus or malware.

It never hurts to perform a second analysis to make sure that we have completely rid ourselves of the problem. And **in case our passwords have been affected, we will have to change them**.

> ”
> **Mobiles have changed and the interest of the cybercriminal does not reside in personal recognition, but in economic profit.**
> **Source: PandaLabs**

We must always be prepared

Taking into account all the recommendations mentioned, we could summarize them in 5 stages or steps that we must follow to face any cybersecurity issue:

- **Preparation**: Have a safety plan to know how to act.
- **Identification**: Detect the attack, determine the scope of the attack and keep the parts involved up to date.
- **Containment**: Try to minimize the risks and the impact of the attack.
- **Remediation**: Stop the attack once the situation is controlled.
- **Recovery**: Return to normality.

Now that we know it is all about time, having the help of a cybersecurity company will make the process easier and faster. Therefore, do not hesitate to **contact Open Data Security** and we will advise you on how to avoid and deal with the main cyberthreats, as well as how to protect your privacy.

Whether you are a company or a private user, **you can call our 24/7 line in case of an emergency**.

SPAIN: +34 910 601 739
UK: +44 203 034 0056
USA: +1 347 669 9174

ODS
OPEN DATA SECURITY

A LITTLE MESSAGE FROM THE OPEN DATA SECURITY TEAM:

Thank you for reading this Cybersecurity Guide for Dummies. Share it and you will be helping other people to make a more responsible use of technology and to face the main threats that unfortunately appear every day in the world.

NEED HELP? CONTACT US

Open Data Security

opendatasecurity.io

@ODSops

info@opendatasecurity.io