Telefónica Tech

Human Factors in Cybersecurity: *Protect Yourself*

Index

01. Introduction

The human factors in cybersecurity refer to the situations when human error results in a successful **data or security breach.** The human factors are the **weakest component** for the security of any ICT infrastructure and imply the greatest risks and threats for a company or organization.

Human error is the leading cause of cybersecurity breaches[1]. In 2021, it was found to be responsible for 95% of these breaches . This means that, **if the human factors were mitigated, only 1 out of 20 security breaches would take place.**

This human error is usually caused by the **misinformation** of users and workers. People can endanger their company and their personal data because of lack of awareness. In a company, this can lead to a large breach or security incident with an economic impact of millions of dollars. In the day-to-day, it can mean the theft of credit cards or compromise users' personal files and data.

During this time of pandemic, cybercriminals have adapted to take advantage of this issue and launch **massive attacks related to COVID-19.** A study conducted by INTERPOL[2] showed that, during the first four-month period of 2021 (January to April), cyberattacks increased greatly: **907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs.**

According to feedback from INTERPOL, 59% of the main COVID-19 related cyberthreats involved phishing, scam and fraud; 36% of attacks included malware; 22% contained malicious domains; and 14% involved fake news. These figures are alarming: a phishing attack costs large companies nearly $15 million a year on average. **The cost of phishing in 2021 is more than three times its cost in 2015**[3].

Cyber attackers are taking advantage of lockdowns, working from home, and online studies to steal information by posing as companies, public entities, and universities. Cybercriminals know how to take advantage by attacking lowest hanging fruit.

The aim of this report is to **fight disinformation** and to **raise awareness.** Spreading these concepts, highlighting common mistakes and good practices can help make the day-to-day of families and companies more secure in terms of cybersecurity.

1. Why Human Error is #1 Cyber Security Threat to Businesses in 2021 (thehackernews.com)
2. INTERPOL report shows alarming rate of cyberattacks during COVID-19
3. New Ponemon Institute Study Reveals Average Phishing Costs Soar to $14.8M Annually, Nearly Quadrupling Since 2015 | Proofpoint US

02. Who poses a threat?

Usually when thinking about enemies in cybersecurity, cybercriminals who want to cause some harm on purpose come to mind. Nevertheless, **a great number of security incidents are caused by accident by misinformed users.** External attackers are not always responsible for the worst incidents. **Internal threats** are of great concern due to its difficult prevention and detection since each person can have their own motivations for becoming this type of danger.

The motive behind these crimes is not the same for all types of attackers: money, information theft, elimination of competition, or having fun, are among the most frequent reasons. sGetting to know the attacker is important in order to, effectively, protect from them. Below are some of the most common adversaries:

→ **Cybercriminals:**
Individual or a group of individuals whose aim is to take advantage of sensitive information of users and companies to generate profit. They commit malicious activities on digital systems or networks.

→ **Fraudsters**:
They are criminals who use scams to steal money or blackmail people. They usually do not have as much knowledge as other cyber attackers, yet they have more knowledge than the average user. Fraudsters take advantage of users' misinformation to generate phishing campaigns.

→ **Hackers:**
They are people that have the technical skills to breach the data by exploiting any vulnerability. Not all hackers are cybercriminals. They are classified into three main types based on their intent: black-hat hackers (unethical hackers, their aim is to obtain personal benefits), white-hat hackers (ethical hackers, they use their skills in a lawful manner to determine the security risk of an organization) and grey-hat hackers (hacker who may violate some laws or ethical standards but does not have a malicious intent).

→ **Hacktivists:**
They use digital tools pursuing a political end and fighting for their cause.

→ **State-sponsored:**
This type of attackers has specific goals associating with their county political or military origin. They have unlimited resources and use sophisticated tools to achieve their goals.

→ **Insider threat (intentional):**
Dissatisfied employee who, either out of a bribe or out of anger, compromises the security of the company.

→ **Insider threat (unintentional):**
This is the case of an employee who causes unintentional damages to the company due to carelessness or lack of knowledge.

→ **Script-kiddies:**
Amateurs who learn from the internet and who use tools they find to launch attacks without fully understanding how they work. They do not usually have a malicious intent but can still cause some damage.

→ **Organized crime:**
Groups of cybercriminals who combine their skills and resources to commit major crimes that might not otherwise be possible.

03. Social Engineering

Social Engineering is a **manipulation technique** used by cybercriminals to get victims to take some act on their behalf. These attackers exploit human error to obtain valuable information, transfer money, gain access to an organization or compromise the security of its systems.

Scams based on this technique are built around **how people think and act.** Cyber attackers manipulate **victims' emotions** to make them act on impulse without realizing what are the associated risks. Scammers especially prey on victims with a **lack of knowledge** or on those who are not fully aware of **the value of their data.**

Some methods used in social engineering are phishing, Trojans, or spam calls. These examples will be discussed in depth later.

3.1 Learn to recognize it

Social engineering attacks usually rely on **real communication** between the attacker and the victim. These criminals create a **reliable process** to deceive and motivate the user that can take place in a single email or can last up to months.

Throughout different attacks of this type, a series of **characteristics** have been found that can help not to be deceived:

Urgency / Exclusivity:

Scammers usually rely on making the victim think that the time they have to fix a problem or apply for a prize is coming to an end. The victim may feel more motivated or **compromised** if they believe there is a serious problem that **requires immediate attention.** Also, the victim may be more likely to fall for a hoax if they feel they have limited time or that it is a unique opportunity.

Heightened emotions:

Emotional manipulation plays an important role in social engineering. You are more likely to take risky actions or follow instructions if you're in a heightened emotional state. Attackers can use both **positive and negative emotions** to their advantage. They will use happiness, excitement, fear, guilt, or anger to convince you.

Trust & credibility:

These attackers will try to sound convincing and show themselves with a lot of self-confidence. They will try to have **consistency** in their words and craft a **credible narrative.**

Reciprocity:

Scammers can convince the victim by promising that they will be rewarded afterwards. You will be more willing to accept a deal if you think you are going to **make a profit too.**

Authority:

Cybercriminals can employ authority to play upon their victims. Scammers may pose as government agencies or company executives to make the victim **feel compelled** to meet their demand.

Consensus:

Another method is to make the victim believe that **everyone** is part of the process. For example, they may make the victim believe that the company's security policies are being modified and that they need their credentials. In this case, they can pressure the victim by saying that he is one of the few employees left to complete the process.

04. Phishing Attacks

Phishing is a set of techniques that **seek to deceive a victim** to manipulate them and make them perform actions for their benefit. It is part of social engineering and gain their victims' trust by **posing as a person, company, or trusted service.**

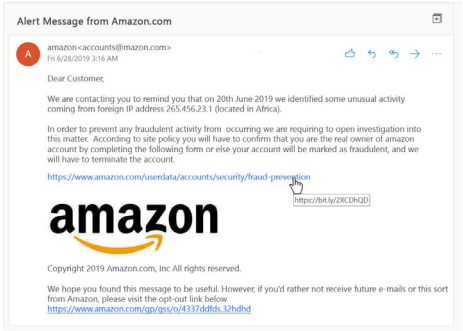


Figure 1. Mail Phishing example[4].

Phishing is a very **simple cyberattack** and yet, the most **dåangerous and effective one.** It has evolved over the years to cover most platforms. According to the route of entry and nature of the attack, the following types are distinguished:

Common phishing:
it is based on **probability** and **mass attempts.** The attempts are made to extract confidential information by requesting it from many potential victims through **apparently reliable and legitimate means.** The use of email is very common. Clone phishing will show a replica to previously received legitimate emails replacing links and attachments with malicious ones.

Spear phishing:
in this case, the phishing attack is **targeting a specific group** of people. It is a more elaborate attack for which the attacker has previously collected information from the victims. This attack is usually **more successful** as they know in advance what triggers can urge the victim.

Whaling:
spear phishing attack in which the targeted people are also the **directors and managers** of the organization.

BEC - Business Email Compromise:
spear phishing campaign that tricks employees into taking actions detrimental to the interests of the company or its customers. **Attackers pose as workers or partners** to deceive victims. They usually accomplish this by accessing to legitimate accounts or by domain spoofing.

Vishing:
voice phishing. This phishing uses a phone call as an entry point. The attacker may attempt to obtain personal data or continue a more complex attack. An example of vishing is the **technical support scam** shown in the following section.

Smishing:
this attack aims to bring the user to follow a malicious link from the SMS message. Usually, they are alarming messages that urge the victim to change their credentials through a link provided. Again, **SMS originator spoofing** will be seen in depth later.

Pharming: in pharming, scammers **clone an entire website** to trick the victim into stealing their confidential data. In pharming, traffic from a website is manipulated so that users visit the fake malicious site without realizing it.

4. How to Spot Phishing Emails and Other Online Scams • Optima Systems (optima-systems.co.uk)

4.1 Our experience: how to detect Phishing

Phishing attacks are the order of the day and Telefónica Tech team is not exempt from suffering them. The following examples are a brief compilation of the most notable and frequent attacks.

4.1.1 A "technical support scam" tale

One of our employees recently received a **vishing call.** The call was allegedly made from **Windows Service Center:** a man named John was calling her on behalf of Microsoft.

"The call seemed to come from a **call center,** hearing John's voice was difficult because of all the **background noise.** Although our employee is Spanish and the call came from such a large company, John seemed to have **problems with the language** and asked her if they could switch to English. John seemed to have problems with English too.

Once the language was settled, the tragedy began: John said that they had detected a large **traffic of illegal downloads** on her computer and claimed that the situation should be **remedied immediately.** Our employee, let's call her Lucy, pretended to be deeply worried and asked John for help to solve the problem.

He asked her to press down the keys **"Windows + R"** and to type "**eventvwr**". (This command opens Windows Event Viewer; a tool designed to aggregate and analyze event logs from apps and system).

John kept asking her to describe what she saw on the screen and guided her through the directories until she reached the **following path**:

Event viewer > Custom views > Cisco > Administrative events

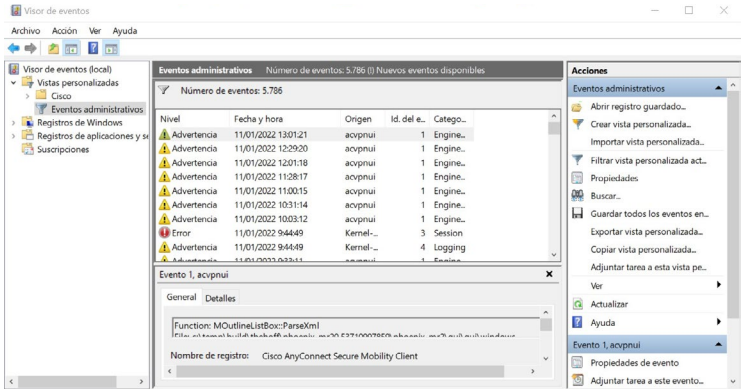


Figure 2. Event Viewer Panel

Now, Lucy could see the screen shown in Figure 2. John asked her what the number of **events displayed on screen** was. (This number usually goes into thousands, and it is a totally normal behavior). John gasped at the "incredibly high **number of viruses**" Lucy had on her computer and repeated to her that she had to remedy it **as soon as possible**.

The next step caught Lucy by surprise and almost made her get out of the role. John put a **recording** (barely audible) in which someone else's voice explained what Lucy was seeing. The voice explained that the warnings displayed on the screen were **events generated by thousands of viruses and evil hackers.**

Lucy then pretended to be scared and asked John a few questions. He put the entire recording from the beginning.

Now that John had convinced Lucy, he asked her to **download SupRemo**[5]: a software application for **remote desktop control** and assistance. From here, our employee **stopped pretending** and told John that she was a cybersecurity expert. (She also told him that the recording part had been very shabby). He did not seem very happy with it and John ended the call with not very good manners."

This case of vishing is known as '**Tech Support' scam** and it follows a well-defined pattern.

- → First, scammers **contact the victim through a phone call.** Usually, the call is made from a call center and the quality is very low.
- → Scammers ask the victim to **display on screen a series of warnings** that, although harmless, may **scare the victim.** Attackers take advantage of users' ignorance and show admin panels that users do not know about.
- → Once the victim is distressed, the **scammers use remote access software** to take control over the victim's computer.
- → From here, the attack can take several directions: scammers can **hijack the computer** or pretend they have fixed it in exchange for a sum of money. They can also **install malware** (different types of malwares will be explained later) on the victim's computer to further the attack and steal private data.

A large company is never going to call its users because of these matters. Personal information should never be given, and you should **never cede control** of your devices to anyone with whom you have **not initiated the communication.**

5. Supremo | El mejor software de escritorio remoto (supremocontrol.com)

4.1.2 SMS originator spoofing

It is quite possible that most users are familiar with the following images:

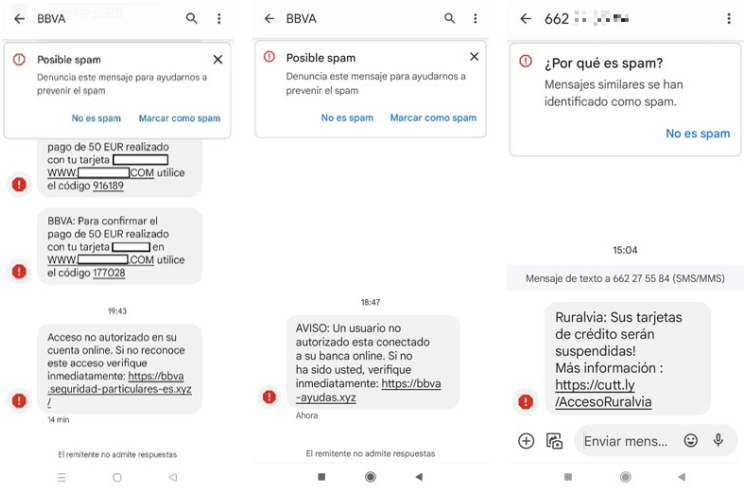


Figure 3. Spanish Banks Smishing cases

These images belong to cases of **smishing** that impersonate bank accounts. The behavior of this type of attack has already been explained, the question is why do mobiles detect that it is spam and still group it with bank messages?

SMS originator spoofing is a smishing attack in which the scammer changes the **Sender ID** number for a sender name of a trusted company or brand. Scammers' main goals usually remain the same as with other smishing attacks: financial gain or data theft.

An SMS Sender ID is the **displayed value of who sent the message.** It is the number that identifies who the message is from. These IDs can be the complete phone number, a short code (such as 1234) or an **alphanumeric** (this is the case. It is what most companies use).

Large companies such as banking companies do not always write from the same number. They write from different sources under the company's name as the alphanumeric Sender ID. It is the **mobile phones** that use these Sender IDs and **group the entering messages with the same alphanumeric associated.** Scammers only have to change their Sender ID to the name of the brand they are trying to impersonate.

It is important to **be wary of such alarming messages.** Keep in mind that you should **never enter personal information through attached links.** In case you want to check if there is a problem with your account, always access your bank's page through the **official website.**

4.1.3 Pop-ups & redirections

Intrusive pop-ups and redirects are the most **common problem** when browsing the internet. Although this is not a specific example, it is important to recognize and **avoid these warnings and websites.**

At best, they will only be **intrusive adware** that redirects the user to their website; for the most part, these pop-ups and redirects will **involve the automatic download** of infected files and **malware**.

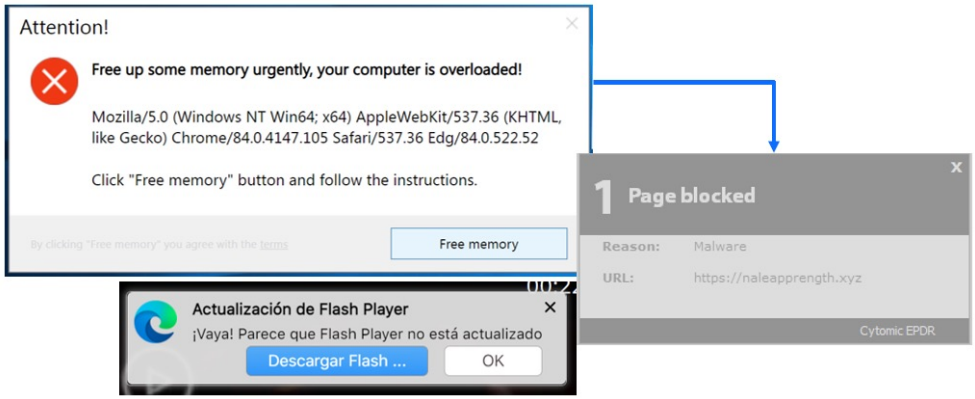
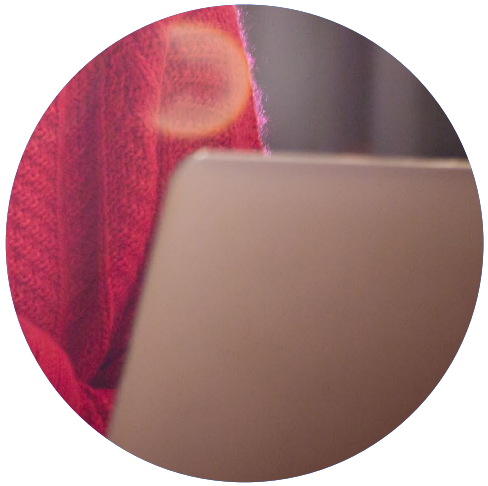


Figure 4. Malicious Pop-Ups



05. Types of Malwares

Although malware itself is not part of the human factor, many cyber attackers use it to **sabotage or disable** computers and networks. Malware is any kind of **software** intentionally designed to cause damage to a computer, server, client, or computer network without the user's knowledge. It is important for users to know how major malware attacks work.

Malware is usually channeled through **malicious links and attachments,** phishing, and other social engineering techniques. The following are some of the most common types of malwares:

Virus:
A virus is malicious software that has the purpose of reproducing programmed into itself. Its code enters an application and acts when it is running. Although it is one of the most traditional types of malwares, it keeps evolving over the years.

Keylogger:
It is a type of **Spyware**. It keeps track of user's activity and send the attacker the information the victim types on the keyboard.

Rootkit:
A rootkit is a collection of software that allows continuous privilege access to a victim's computer but keeps its presence actively hidden. This software acts as a backdoor that **allows the attacker to access the infected device** with root privilege to carry out all its purposes.

Trojan:
It is a malicious program that **disguise itself** as legitimate and valid code. It is **closely related to phishing.** Cyber attackers and scammers try to trick the potential victims into downloading it by making them think it is a legitimate update.

Worm:
Worms can quickly spread throughout a network. They are a type of infectious malware that spreads by infecting files already present on a computer and replicate themselves to spread to other computers within the network too. They are typically used to steal information, delete files or as a means of replicating other malware.

Adware:
This malware is designed for the specific purpose of **displaying ads** on your screen. The malicious form of adware can also **redirect** you to advertising sites and **change** your Internet **browsing settings.**

Ransomware:
Ransomware blocks access to a victim's data, threatening to publish or delete it until a ransom is paid. This blocking is usually done by **encrypting files** on the computer that the victim cannot reestablish. It is booming these days and it is a huge source of money for attackers. Paying the ransom does not ensure that the data can be recovered.

06. Data Exposure & Common Mistakes

As already mentioned, some attacks like phishing can be targeted. **Cybercriminals use user information to select their victims.** This makes their attacks more likely to succeed, they make more believable stories, and they know what time or by what means to launch the attack. But, to what extent can they obtain such valuable information on the Internet?

6.1 Digital footprint & social media

A digital footprint is **the trail of data you leave behind** on the Internet through online activity. This includes browsing, posts, and interactions with more users, but it also includes technical details like the operating system you use or your IP address. Although this fingerprint is not bad, it is necessary for users to know the information that is accessible on the network about them.

In addition to being able to be used by attackers (i.e. phishing, identity theft or data theft), this information can also have a **negative or positive impact** on the user's life. A **negative digital footprint** can cost a job: potential employers can eliminate a candidate based on the information they saw online. Some examples that can cause a bad footprint include the reference to weapons, alcohol, or illegal drugs, hate speech, and even bad spelling. On the other hand, having a **positive digital footprint** can increase opportunities, earn a good reputation, or bring higher profits.

With **social media,** this digital footprint has **increased considerably,** and users post daily information about themselves. It is the responsibility of users to be aware of the information they publish, and they should bear in mind that, **once the information is published on the Internet, it is never deleted.**

Besides overexposure, the use of social networks can lead to other cybersecurity risks. Some of these associated risks are data and identity theft (spoofing), scams (romance and phishing scams), bullying and stalking, and data leakages caused by whistleblowers.

6.2 What to avoid

As already mentioned, most data breaches are produced by the users themselves and the vast majority of cybersecurity issues are linked to the human factor. Lack of attention to cybersecurity remains one of the leading causes in cyberattacks. Listed below are some of the **most common cybersecurity mistakes** that users continue to make:

Weak & vulnerable passwords:
the lack of password security enforcement is one of the main reasons why an attacker gains access to the victim's account. Many users still use very short passwords that do not include enough variety of characters. It is also common for users to include personal information in their passwords, such as birthday dates, pet names or hobbies. In addition, passwords are not frequently renewed, and they are often reused across multiple accounts.

Thinking you are no one to be targeted:
although an attacker may not want to perform an attack specifically aimed at you (such as spear-phishing), you can be victim of one massive phishing attack that relies on probability.

Not paying attention to secure email practices:
users continue to fall victim to smishing. Users should be alert to alarming, suspicious, or too good-sounding messages.

Out of date tools & poor network administration:
using default settings and practices or not paying attention to software updates can lead to security issues and increased risks.

Lack of awareness:
users keep ignoring security practices and overexposing themselves due to their difficulty recognizing warning signs. Cybersecurity awareness trainings, keeping software updated and keeping good practices in mind are still the best solutions against misinformation.

07. Good Practices & Recommendations

The main cybersecurity risks, attacks and mistakes have been already mentioned. Especially in these times of pandemic and quarantine, technology has acquired a fundamental role: telecommuting, multiplied number of cyberattacks, more online purchases and increased online leisure.

Whether you are a worker looking to **reduce the risk** in your company or you are looking to **surf the Internet safer** from home, below are some of the best cybersecurity practices designed to help you **prevent fraud and scams** and surf the internet as safely as possible.

- → **Avoid unknown emails:** it is common to receive emails from senders that we do not know and to whom we have not given our address. Cybercriminals and scammers can get a user´s email address in data leakages or use their digital footprint to obtain it. **It is important to never respond these emails:** if the message is phishing, it would be **confirming to the attacker** that the address obtained is correct and therefore he can continue to use it.
- → **Avoid pop-ups and links:** malicious links and pop-ups can contain malware of different types or redirect to malicious websites that clone the original. As in the case of bank fraud, scammers can request credentials or settings changes through attached links. In this situation, it is always recommended to **access the official bank´s website** (or any other website) manually and see if there is any real problem with the account. **Never click on suspicious links.**
- → **Never enter personal data in response to an email or any other form of communication you did not initiate.** It is common for scammers to ask for personal data through mail or other messaging applications. Never give any kind of information if you are not completely sure **to whom** you are sending it.
- → **Use strong passwords and double factor authentication:** manage your credentials correctly. Passwords should contain upper & lower case, numbers, and special characters, have a length of at least 10 characters, and never be written on paper. A good practice is to use **password managers** to help change passwords regularly.
- → **Connect to secure Wi-Fi:** public Wi-Fi networks can be risky and make your data vulnerable. Do not manage or access any account in public networks. This can make you vulnerable to a **Man-in-the-Middle attack** and cause your credentials to be stolen.
- → **Use verified, secure and up-to-date applications:** do not trust or download apps from unknown sources. Unverified apps may have malicious background activity or malware installed on them.
- → **Use firewall protection at work or home and create a backup of important files.** This will help detect potential threats and make it possible to recover data in the event of a security incident.

Telefónica Tech

→ CONTACT US

Report written by NEW MARKETS Team at Telefónica Cybersecurity & Cloud Tech.