Article **Journal Applied Computing**
June 2021, Vol.5 No.16 6-12

# Computer security, one more reason to take care of yourself today

# Seguridad informática, una razón más para cuidarse hoy en día

DOMINGUEZ-LUGO, Alma Jovita†*, CASTORENA-PEÑA, Jesús Abraham, CANTU-GONZALEZ, José Roberto and SALAZAR-GAITAN, Pablo Arturo

*Universidad Autónoma de Coahuila, Mexico.*

ID 1st Author: *Alma Jovita, Domínguez-Lugo* / **ORC ID:** 0000-0003-4988-4911, **CVU CONACYT ID:** 260410

ID 1st Co-author: *Jesús Abraham, Castorena-Peña* / **ORC ID:** 0000-0002-8833-1159, **CVU CONACYT ID:** 411532

ID 2nd Co-author: *José Roberto, Cantú-González* / **ORC ID:** 0000-0001-5616-2947, **Researcher ID Thomson:** AAT-9346-2020

ID 3rd Co-author: *Pablo Arturo, Salazar-Gaitan* / **ORC ID:** 0000-0001-7897-8904

**DOI:** 10.35429/JCA.2021.16.5.6.12 Received January 15, 2021; Accepted June 30, 2021

**Abstract**

The pandemic did not come alone, it came with the increase in cybercrime and the world turned into chaos, because with so many technological changes in the way of carrying out activities, the opportunities for cybercriminals have been increased. Online shopping rose sharply, and they are here to stay even and after this contingency, people realized that this way to go shopping is very simple and its transactions can be easily done by young and even older people. Even these days, incredibly many of the users do not have adequate precautions to maintain the security of each movement, it has even reached high reliability since the devices have generally open sessions, some for purchases, banks, networks social, etc. There are various software packages that in the hands of malicious people, very probably could be useful to access to passwords, images and files from any computer or electronic device, thus leaving the safety of users affected.

**Pandemic, Cybercrime, Computer Forensics, Security**

**Resumen**

La pandemia no llegó sola, llegó con el incremento de delitos informáticos y el mundo se volvió un caos, pues con tantos cambios tecnológicos en la manera de realizar las actividades se han incrementado las oportunidades de los ciberdelincuentes. Las compras en línea se elevaron en gran medida, y llegaron para quedarse aun y después de esta contingencia, las personas se dieron cuenta que esta forma de ir de compras es muy sencilla y además sus transacciones pueden ser realizadas tanto por jóvenes e inclusive por personas mayores. Aun en estos días, increíblemente muchos de los usuarios no tienen las precauciones adecuadas para mantener la seguridad de cada movimiento, se ha llegado incluso a la alta confiablidad desde el momento en que los dispositivos tienen generalmente abiertas las sesiones algunas para compras, bancos, redes sociales, etc. Existen diversos softwares que, en manos de personas mal intencionadas, muy probablemente podrían ser útiles para acceder a contraseñas, imágenes y archivos de cualquier computadora o dispositivo electrónico, quedando así la seguridad de los usuarios afectada.

**Pandemia, Delitos informáticos, informática forense, seguridad**

**Citation:** DOMINGUEZ-LUGO, Alma Jovita, CASTORENA-PEÑA, Jesús Abraham, CANTU-GONZALEZ, José Roberto and SALAZAR-GAITAN, Pablo Arturo. Computer security, one more reason to take care of yourself today. Journal Applied Computing. 2021. 5-16:6-12.

* Correspondence to the Author (Email: almadominguez@uadec.edu.mx)
† Researcher contributing as first author.

 

## Introduction

With the presence of information technologies in the world, “the intelligent society” has become present, depending on three fundamental technological elements: connectivity, smart devices and software, as well as all the principles associated with sustainable development. (Ngary Njeru, 2017) When we say intelligent society, we are talking about the use of technologies, where society interacts daily with smartphones and computers, used for working, studying, socializing and shopping online.

Based on the increase in work at home, but especially the use of the internet as a consequence of the physical isolation measures imposed by the coronavirus pandemic, the digital vulnerabilities of professionals and individuals increased and revealed.

With the emergence of the telephone, during the 1960s, different computer programmers or systems specialists tried to boycott government financing of the Vietnam War through the free use of the service.

The phreakers (neologism from the English words: "freak", of rarity; "phone", of telephone; and "free", free) used blue boxes or blue boxes that reproduced ringtones similar to those used by the Bell Corporation, and the ATT established free long distance communications. The first misconduct or illegal conduct related to computers began to be reflected during the 70s, from some resounding cases portrayed by period newspapers.

The first computer crimes were of an economic nature, among which computer espionage, software “piracy”, sabotage of digitized databases and extortion stood out. In relation to espionage, these were carried out by removing hard drives from computers, stealing floppy disks or direct copying of information from devices, as well as the absorption of electromagnetic emissions that every computer radiates for capture. of data.

The espionage was commercial or industrial, as it is often called, its main objectives being computer programs, research data in the defense area, accounting information of companies and the address book of corporate clients.

Cases of computer sabotage and extortion, which means deleting, suppressing or modifying without authorization computer functions or data with the intention of obstructing the normal functioning of the system, were the crimes that most concerned organizations due to the high concentration of data stored in format digital. (ERREIUS, 2018) Before like today, when a cyber attack of any kind is suffered, it is necessary to gather the necessary information to determine the damage suffered, its consequences, try to reach the source and discover who is responsible. This work corresponds to computer forensics, which has seen a significant increase, with the automation of processes and the rise of the internet of things applied to vehicles, homes and others.

Overall, eight out of ten social media users are concerned about advertisers and businesses accessing the data they share on social media platforms. However, they use video calling platforms and applications on a daily basis that barely meet minimum standards or reasonable security practices, leaving them open to spying or cyberattacks. (Jara, 2020).

*Computer forensics*

This is responsible for acquiring, preserving and protecting data processed electronically and stored on a physical medium. Information systems are periodically investigated to detect any small vulnerabilities that could endanger the enormous amount of data that is processed and stored every second. (Technology, 2020)

Computer forensics is characterized by its preventive approach, so that through various techniques, it proves that the security systems implemented are adequate. In addition, it is also in charge of developing security policies and defining which systems are suitable for each case.

Computer forensics is an indispensable science for all companies, as it ensures that the confidential information and data of everyone who interacts with the company is properly protected and out of the reach of network criminals. (Secron, 2018).

ISSN-2531-2952


DOMINGUEZ-LUGO, Alma Jovita, CASTORENA-PEÑA, Jesús Abraham, CANTU-GONZALEZ, José Roberto and SALAZAR-GAITAN, Pablo Arturo. Computer security, one more reason to take care of yourself today. Journal Applied Computing. 2021

**Developing**

During the first half of 2020, there were 450 security threats per minute around the world. (Anton, 2021)

To support the clarification and prevention of these computer crimes, forensic computer science arises, which with its phases allows us to decipher:

*ID*

It refers to the collection of information necessary to work on the data source presented by the server administrator (forensic request).

*Preservation and Acquisition of the Elements*

To ensure that both the processes and the tools to be used are the most suitable, it must have suitable personnel who can be assigned to lead the forensic process, for this the security team must be trained and thoroughly understand the methodology.

*Identify the evidence*

It is important to identify the evidence presented at our "crime" scene, which will be subject to all the necessary processes for the presentation of final results, the evidence will be classified according to the type of device and storage mode.

*Investigation of Acquired Items*

At this stage, the following is analyzed: What happened? For what purpose did it enter? and Can you detect who has been responsible?

*Documentation and presentation of evidence*

It consists of documenting the investigation and presenting the results

**Computer forensics tools**

Almost every day we find that there are leaks of private or company data to the Internet, either due to a bad network configuration and computer systems, or because a cybercriminal has managed to circumvent the security measures implemented and has done with a lot of information that has subsequently ended up on the internet.

There are free tools for computer forensics useful for when a security incident occurs to be able to identify: Where did it come from? What has happened? And how to act so that it never happens again?

*Autopsy and The Sleuth Kit*

The Autopsy tool is one of the most used and recommended, it allows you to locate many of the open source programs and plugins, it is like a Unix library and Windows-based utilities, which greatly facilitates the forensic analysis of computer systems.

Autopsy is a graphical user interface that displays forensic search results. This tool is widely used by the police, the military and companies when they want to investigate what has happened to a computer.

One of the most interesting aspects is that it is extensible, this means that users can add new plugins easily and quickly. It incorporates some tools by default such as PhotoRec to recover files, and it even allows extracting EXIF information from images and videos.

As for The Sleuth Kit, it is a collection of online command tools for investigating and analyzing the volume and file systems used in digital forensic investigations. With its modular design, the correct data and evidence can be obtained. Also, it is compatible and works on Linux and runs on Windows and Unix platforms. (Cortez Castilla, 2017)

*Name Search Tool Analysis*

The File Name Search module can be used to perform a basic search by entering a search string and a location. For example, the search for "file" will match "file.txt", "test.file", or "MyFile.doc"; even to perform more advanced searches which can be selected from the preset options to quickly locate certain types of files, some examples of preset searches are the following:

- Images + Face-detect Al
- Images + Ilicit-detect Al
- Photo taken with iPhone

ISSN-2531-2952

- Office Documents
- Video Files
- E-mail Files
- Virtual Machine Files, among others.

We will define the first two in more detail:

Images + Face-detect

When trying to locate all images in a system or directory that contains faces; results are displayed and highlighted in green based on a percentage score.

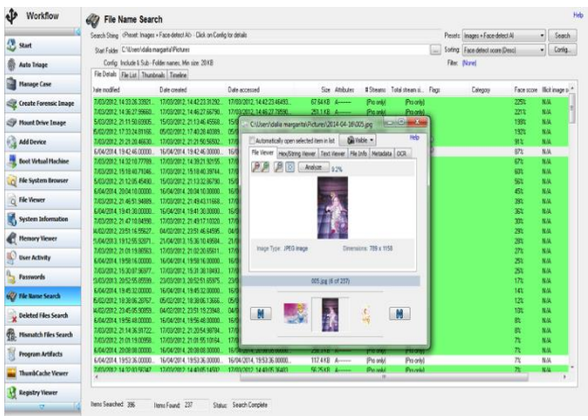

**Figure 1** Image Face-Detect

*Images + Ilicit-detect*

This feature tries to locate any image that contains nudity or pornography; results are displayed and highlighted in red based on a percentage score.

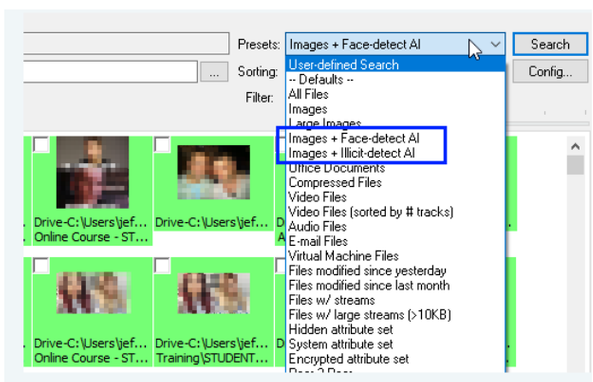


**Figure 2** Image Ilicit-Detect

*User Activity*

The User Activity module scans the system for evidence of recent activity, such as accessed websites, USB drives, wireless networks, recent downloads, website logins, and website passwords. This is especially useful for identifying user trends and patterns, and any recently accessed materials or accounts.

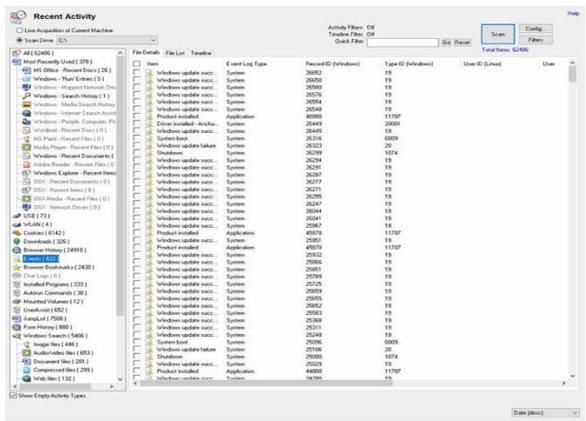

**Figure 3** User Activity

Next, we will see some information that this scan would show us:

Web browser activity

Shows users' web browser activity such as browsing history, cookies, and stored user names from web browsers. The following table shows what items can be retrieved from commonly used web browsers using this module.

Connected USB devices

Displays the details of the USB devices that have recently been connected to the computer, providing information about the last connection date and device information such as the manufacturer's name, product identification, and serial number.

ISSN-2531-2952

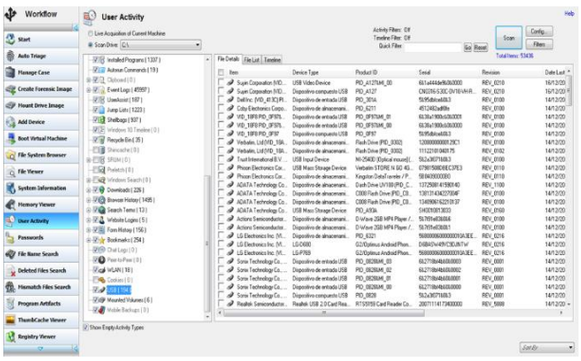

**Figure 4** USB devices that have been connected

*Wireless network connections*

Lists the WIFI access points that the machine has connected to in the past, including the date and time it was accessed.

Downloads: shows all document or file downloads made by users.

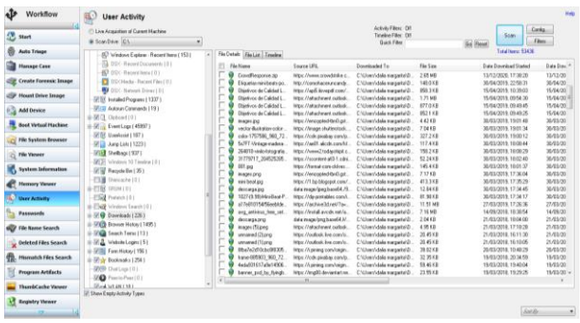

**Figure 5** Used wireless network connections

*Event log*

Scans Windows logs for system activity, such as the following events:

- Security log events, such as account login attempts, logoffs, and password changes.
- System log events such as Windows update attempts, system boot / shutdown, and driver installations.
- Application log events, such as application installation attempts.

*Password*

Recovers passwords and product keys that have been stored by various applications and web browsers on the system.

**Figure 6** Recovers stored passwords and keys

## Recommendations

- It is recommended to use passwords that are not so easy to deduce, in addition to including second levels of authentication or two-step verification, which would make it more difficult to violate the entry.
- Avoid using the same password in several applications, such as accessing email, banking applications, social networks, and any other internet resource that requires some validation to enter with the same password.
- You should also think about having a secure connection and trying to avoid public wireless networks, since anyone can access our data if the connection is not encrypted and most who connect do so for convenience without thinking about what this is. may cause.
- Having antivirus, protection with updated equipment, will allow greater security.
- Do not open emails or files that come from unknown or unexpected senders.
- Keep all types of connections disabled when not in use, for example "Bluetooth".
- Do not install unknown programs.
- Use all the filters and security services offered by the different Internet tools and systems.

ISSN-2531-2952

## Conclusion

In order to have a broader information on what society lives in a matter of cybercrimes, an instrument of 5 questions was developed, giving the following results:

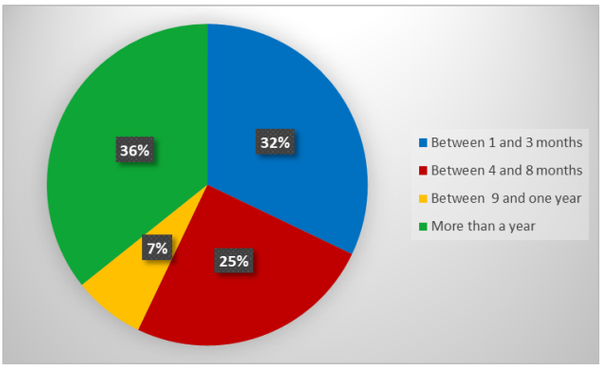


**Figure 7** When was the last time you changed your password?

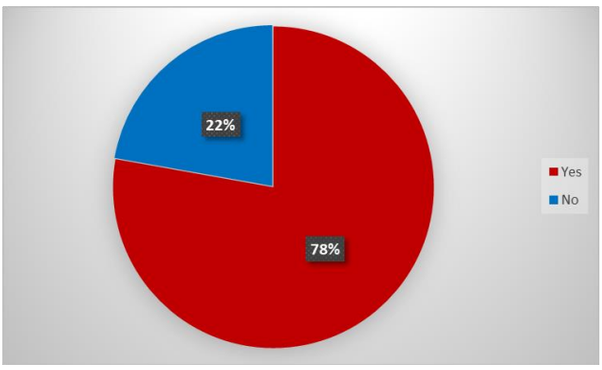


**Figure 8** Do you know what to do in case of a computer crime?

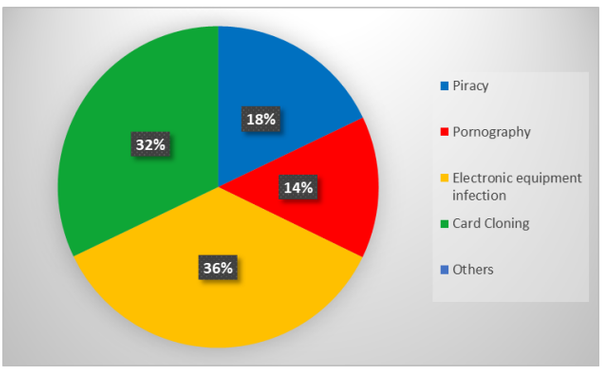


**Figure 9** What do you consider to be the most common computer crime?

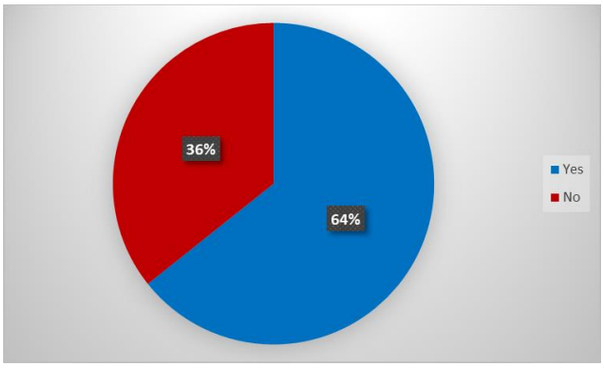


**Figure 10** Do you know what a computer crime is?

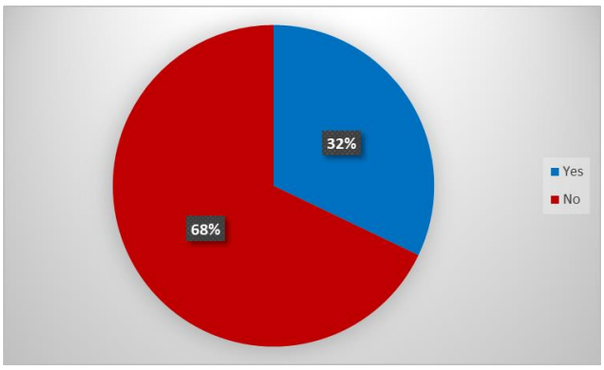


**Figure 11** Have you been a victim of cybercrime?

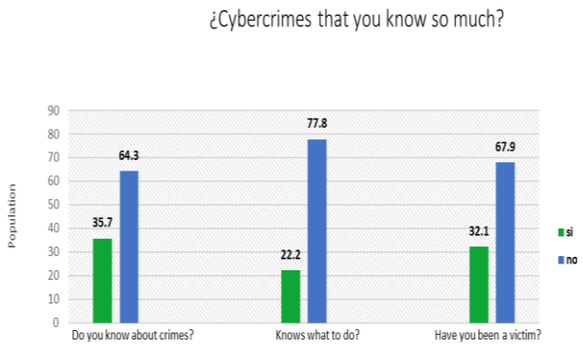


**Figure 12** How much does society know about cybercrime?

Based on the results obtained from the survey, it is presented that the majority do not know about the subject, but nevertheless they will not know what to do in the event of a cybercrime.

Likewise, it is shown that a third part of society has been a victim.

Therefore, it is concluded that it is important to keep your devices and computer equipment safe to prevent them from being victims of a cybercriminal.

ISSN-2531-2952

And if it is about companies, as a preventive measure to detect any vulnerability in it; it is highly recommended to constantly use computer forensic software such as OSForensics since it helps to carry out the case from the beginning, the creation of images and clones of the units to be investigated, the analysis and incorporation of evidence, protection of evidence with hash code, creation automatic log of the investigation carried out and final report.

**References**

Antón, M. (March 16, 2021). *yahoo/finanzas*. Retrieved from: https://es-us.finanzas.yahoo.com/noticias/ciberataques-crecieron-70-pandemia-trampas-223000777.html

Cortez Castilla, J. (2017). *SILO.TIPS*. Retrieved from: https://silo.tips/download/informatica-forense-fases-de-aplicacion

ERREIUS. (2018). *CIBERCRIMEN Y DELITOSINFORMÁTICOS.* Buenos Aires, Argentina: BluePress SA.

Jara, F. (10/22/2020). *Infoabe*. Retrieved from: https://www.infobae.com/sociedad/2020/10/22/ciberdelito-desde-el-inicio-de-la-cuarentena-los-ataques-informaticos-crecieron-cerca-del-70-por-ciento/

Ngary Njeru, J. (2017). *Creación de la sociedad inteligente: desarrollo económico y social a través de aplicaciones TIC.* Suiza: Unión Internacional de Telecomunicaciones.

Secron. (2018). *Secron Ciberseguridad & Sistemas*. Retrieved from: https://secron.es/informatica-forense/

Tecnologica, D. E. (02/14/2020). *Select Business School*. Retrieved from: https://escuelaselect.com/informatica-forense/

ISSN-2531-2952