




## The user: an unavoidable vulnerability in health information security

*El usuario: una vulnerabilidad inevitable en la seguridad de la información en salud*

María del Carmen Roche Madrigal <sup>1</sup> \* 

<sup>1</sup> Universidad de Ciencias Médicas de La Habana. Facultad de Tecnología de la Salud. La Habana, Cuba.

**\*Corresponding author:**  
[marycarmen@infomed.sld.cu](mailto:marycarmen@infomed.sld.cu)

**Received:** April 16<sup>th</sup>, 2023  
**Accepted:** May 17<sup>th</sup>, 2023

### Cite as:

Roche-Madrigal MC. The user: an unavoidable vulnerability in health information security. Rev. Cubana Tecnol. Salud [Internet]. 2023 [cited:]; 14(2):e4075. Available from: <http://www.revtecnologia.sld.cu/index.php/tec/article/view/4075>

The world is a frantic place, and the speed at which it changes is growing exponentially. Information is *the* king. Protecting that information, whether it is personal or business-related, has become one of life's greatest challenges.

Information security, computer security, and cybersecurity may seem the same. Currently, the prevailing model is to digitize and manage any type of information through a computer system.

However, these are three areas of knowledge that, although they must work in harmony and together, were conceived to protect informational assets or goods. Specifically: information, the infrastructure that supports it, and the users who utilize it each have different objectives and activities.

Information security is the discipline responsible for ensuring the confidentiality, integrity, and availability of information. It refers to the protection of informational assets essential for the success of any organization.

It is responsible for regulating and establishing the rules to follow for information protection. Its purpose is to protect recorded information, regardless of where it is located: printed on paper, on computer hard drives, or even in people's memories.

While information security is the strategic line, computer security describes the tactical and operational aspects of security and cybersecurity. It is the process of protecting networks, systems, and data from unauthorized access, modification, and destruction.

There is a security axiom: no information system is secure, meaning that no measure can guarantee a threat or risk-free environment for the information, organizations, or users that require it. Why? Because there are people involved in managing the system, and they make

mistakes or errors. Therefore, humans, who are part of any system, will always make it vulnerable.

Some authors believe that the implementation of adequate security measures for information protection requires considering technical and legal aspects. However, in many cases, too little attention is paid to the importance of the human factor in information protection. People represent the weakest link in information security.<sup>1</sup>

It is essential to consider the role of humans and their relationship with the organization's computer systems and networks. A fundamental principle to prioritize from the perspective of information security is that all technological solutions implemented by the organization can be rendered useless due to ignorance, lack of information, disinterest, or malicious intent of an employee.

The security level of an information system is effective only if the security level of the weakest link is also effective. You can have the best technology, firewalls, intrusion detection systems, biometric devices. All it takes is a call to an unsuspecting employee, and access to the system is gained without much effort. They hold everything in their hands.<sup>2</sup>

If one thinks that technology can solve security problems, then they do not understand either the problem or the technology. Information security must be addressed globally. A reinforced door won't protect a building if the windows are left open.<sup>3</sup>

Users are often unaware of their role in compromising confidentiality, integrity, and data availability. They may ignore errors and fail to rectify them. Therefore, user training is key to mitigating the human factor. People can be careless and make mistakes, but with proper training, they can be taught to avoid them and keep data secure.

The need to protect information and the system must become a culture of work. Users must be taught to identify and avoid human errors that can lead to incidents or security breaches. They should recognize social engineering scams, spam emails, and hoax messages. Additionally, they must protect their access credentials and exercise caution when sharing them with others.

The Faculty of Health Technology is not exempt from the need to educate network users. The Health Information Systems (HIS) program includes the Information Security in Health subject in its core curriculum, which covers topics related to the safekeeping and ethics of information resources. These topics are present in all program courses.

Therefore, in the context of health information management, HIS professionals must implement effective information security measures, stay updated on the latest trends and threats. Since information security is not just a technical issue but also an ethical and legal one, awareness of the human factor in this field is essential.

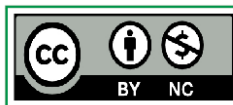
**Keywords:** *Information Security, Information Security, Cybersecurity, Information User.*

**Palabras clave:** *Seguridad de la Información, Seguridad Informática, Ciberseguridad, Usuario de la información.*

## **BIBLIOGRAPHIC REFERENCES**

1. Bogantes A. El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. *Sistemas, Cibernética e Informática*. 2020;17(1):24-29
2. Alabdan R. Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*. 2020; 12(10):e168.

3. Almanza AR. XIX Encuesta Nacional de Seguridad Informática. Evolución del perfil del profesional de seguridad digital. Revista Sistemas [Internet]. 2020 [cited: 12 Jan 2023]. Avalilable from: <https://doi.org/10.29236/sistemas.n151a3>



Los artículos de *Revista Cubana de Tecnología de la Salud* se comparten bajo los términos de la Licencia **Creative Commons Atribución-No Comercial 4.0. Internacional**