DOI: https://doi.org/10.31686/ijier.vol10.iss7.3827

Study of the Application of User Security Techniques in the Network

Rilmar Pereira Gomes
rilmargomes@hotmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Francisco Luan Monteiro da Silva
lluannmonteiro@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Maria Correa Rodrigues Junior
mariojunior144@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Thiago de Carvalho Caetano do Vale
caetano.thiago@outlook.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Zaida Maria Marques Tavares
zaida.tavares@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

David Barbosa de Alencar
david002870@hotmail.com
Institute of Technology and Education Galileo of Amazon - ITEGAM, BRAZIL

Abstract

Mapping user behavior on the network is one of the fundamental points for the development of security measures against intrusions, however, despite a large number of platforms and programs adopting protection standards, users are still poorly understood about their security, so, this article sought to study user security techniques on the network as a way of identifying to what extent their actions may constitute a risk or protection for their security. of a data collection questionnaire, which was prepared online and later collected responses from 222 users in Manaus-AM. From the data, a certain balance in the behavior of users can be highlighted, indicating that he is more aware of the risks, but performing actions that leave him exposed, it can be seen that through the data obtained, his behavior brings surprises to some people. situations. The main conclusion of the study reveals a certain balance of user actions regarding their security while in the network environment, so the contribution of the research is in the description and presentation of the user's security actions while in the online environment, an area little explored by the academic research. Finally, a proposal for a future research agenda on this topic is also presented.

Keywords: Actions; Behavior; Network; Safety; Users;

1. Introduction

The Internet is a great learning and information tool. However, it is also a dangerous place. Thus, there are many things that can go wrong when using the Internet or using an application, which means that there is an increasing probability of encountering risky situations. As much as platforms, websites and applications try to protect themselves against malicious attacks, none offer complete protection. Internet users must be careful when using it, and thus seek ways to protect their data and information. This research focuses on studying the application of security techniques by users on the network.

In this way, we seek to understand how users are dealing with their security in the internet environment, how they act in the virtual environment, what security measures they adopt. We sought to gather data/information to answer the following research problem: how can the study of user security techniques on the network help in the identification of failures in the use of the network by users?

Therefore, as a general objective, the present work aims to study the application of user security techniques on the network to determine to what extent their actions may represent a risk or protection to their security. One of the steps taken to achieve this goal is to conceptualize information security and issues related to Internet security. Analyze user security measures on the network and identify key behaviors that make them more exposed, and then make security recommendations based on the greatest risks. Leading us to analyze whether the actions of users on the network constitute a risk or protection for their security.

Knowing how the user behaves on the network in relation to its security is very important, especially for developers. Knowing this position, it is possible to develop more robust applications with greater focus on these user failures, in order to detect different forms of possible attacks and provide security solutions. In this context, the work proposal seeks to know how users are acting in relation to their security in the network environment.

For the development of the present work, descriptive research was used, as it requires standardized data collection techniques. The mechanism adopted to carry out the data collection was through an online questionnaire. The method of distributing the questionnaires and the call for participation were carried out through pamphlets with QR codes fixed in the premises of the study sites and link distribution through the WhatsApp application.

The technology market has provided civilians with easy access to drones of different categories that imply their ability to use. Drones ranging from small flights and minutes in duration to hours of flight and cargo transport. Control and programming systems have been improving over time in terms of safety and integrity, for example. However, there is still a deficiency regarding drone attacks by hackers, which aim to affect, mainly, the integrity of the data that is transmitted between the operator and the drone, causing the drone to deviate from its programmed path. With this scenario, a study was carried out where each tool presented in this article has the ability to help together in the fight against attacks that seek to send false GPS signals to divert drones from their original route.

2 Theorical Reference

2.1 Information Security

Information security is intended to ensure that the user's confidential or even personal data is accessed only by him or with whom he wishes to share. Security incidents are directly related to financial loss, whether due to system downtime due to viruses, theft of confidential information, or loss of important information. Worms and viruses that reached high rates of spread - such as MyDoom, Slammer, Nimda - are estimated to have caused billions of dollars of damage worldwide. We can say that there is no system that is fully protected against attacks, as a rule, it is not about how it will be attacked, but when. There are several information security tools and assumptions that must be followed to prevent these attacks, such as data integrity, confidentiality and availability policies. In addition to using features such as firewall and other more complex programs to prevent attacks.

2.1.1 Safety Techniques

Security techniques range from simple to sophisticated depending on the mechanism chosen by the IS manager, some traditional and known to most people and others just experts in the field.

Backups, known as the usual backup, are a primary mechanism to ensure the availability of information in case of malice or theft of databases where the information is stored on an external hard drive, or in the cloud. From the backup it is possible to restore in a very short time, information lost accidentally or as a result of accidents (floods, fires, etc.), sabotage or theft.

Firewall - It is a mechanism for controlling traffic between computers on an internal network and between computers on other external networks. It works according to security protocols (TCP/IP, IPSec, HTTP, etc.) that guarantee the correct functioning of the communication between the two ends to avoid intruders.

Digital signature - It is a form of identification of the user who accesses the resources of the IS, gives legal validity to digital documents and guarantees the authenticity of the sender of the information.

Biometrics - Access to information is granted only to the authorized person, taking into account their physical characteristics (fingerprint, voice or iris pattern of the eye, or of the entire face).

2.2 Cybersecurity

Cybersecurity are measures that seek to guarantee the three pillars of information security (availability, integrity, confidentiality) in cyberspace. Cybersecurity makes it possible to keep equipment and software safe from cyber attacks, keeping data and information protection intact. It is evident, given this scenario, that to avoid attacks it is necessary to adopt cybersecurity measures.

According to Ferreira (2017), cybersecurity are security criteria adopted to ensure the protection of information, IT infrastructure components and information systems. It is clear that the role is to guarantee the integrity and viability of the use of cyberspace and the entire structure that composes it in a safe and peaceful way.

Therefore, it becomes evident that Cybersecurity refers to the actions and techniques used to protect systems, programs, networks and devices from intrusion. It can be seen, therefore, that it serves to guarantee the security of information systems and their structure. Therefore, the fact that it is of

paramount importance to society in general is indisputable.

2.2.1 Cyber Attacks

With the development of technology and increasingly frequent online activities, risks arise, namely cyber attacks, which are understood as any activity of invasion, alteration and damage caused to physical equipment and software, any unauthorized access to a system and any fraudulent way to obtain sensitive information and data through these security breaches. These are currently classified into three categories: attacks on confidentiality, availability and integrity (ROSS, 2018).

As Nogueira (2021) assures us, it can be said that any activity that corresponds to deliberate and unauthorized attempts to access/manipulate information or make systems inaccessible, integrable or unavailable, whether physical or logical is called cyber attacks. It can be of the most varied types, such as: viruses, worms, spam, bots, botnets, exploits, backdoors, brute force, trojan, spyware, malware, keyloggers, screenloggers, sniffers, spoofing, phishing, DoS, DDoS.

Attacks come from all vectors: mobile devices, email, computers, web traffic and automated exploits. On the website of the Center for Studies, Responses and Treatment of Security Incidents in Brazil (CERT.BR), one can identify, for example, the most common threats in 2020, Worms: notifications of malicious activities related to automated processes that spread malicious code over the network. dos (DoS - Denial of Service): Denial of Service attack, where an attacker uses a computer or group of computers to bring down a service, computer or network. Intrusion: A successful attack resulting in unauthorized access to a computer or network. Web: Specifically targets attack cases that compromise network servers or web pages. Scan: Scans notifications on computer networks to identify which devices are active and which services are providing. Often used to identify possible targets, as it allows possible vulnerabilities to be associated with services enabled on the computer. Fraud: any act of willful misconduct with the intent to harm or deceive others, or breach of a specific duty. Others: Notifications for events that do not fit into the previous categories.

In the end, it can be concluded that a cyber attack in a simplified way is any unauthorized act against an information system and its network infrastructure, aiming to harm an individual, agency or company. When executed it will have a very specific objective, to restrict access to data/information and make the system unusable and insecure.

2.3 Internet Security

Currently the internet is a place where most of the entire population has access, but not everyone who accesses the internet knows how to use it safely. This is due to the fact that most internet users are not interested in seeking this information or even knowing how to protect themselves. According to a survey carried out by Diniz (2022), one out of two Brazilians feel insecure on the internet, the survey survey was carried out among 9,638 people and revealed that the greatest fear among these users is to have their data stolen on the internet, the of the other users was referring to suffering a blow and having the social network invaded. In addition, the survey addressed other interesting things such as, for example, asking if they have ever been a victim of a scam on the internet and the answer was that only 20.07% of respondents know that they have already suffered a scam, 23.76% could not say and 56.16% did not suffer such an

action, the most common blow suffered was the financial/banking blow, followed by product never received in online purchases and others, 42.37% of respondents said that nothing was done and only 20.50% did an incident report (B.O.).

One of the best ways to protect yourself on the internet is by using antivirus. It is always recommended to install it on your equipment, as one of the forms of attacks by cyber criminals is the use of viruses. Another technique that is also widely used is phishing, which consists of the cybercriminal impersonating people, companies or even some public entity.

Some tips that are given to all users when using the internet to ensure their safety is, always be aware of unknown sites or when accessing an unreliable source, most of these sites do not offer a secure network address (https), avoid installing suspicious software on your cell phone, desktop, notebook or any electronic device because it is possible to monitor the steps of users on the computer, record passwords, data, etc., changing the password often is something that helps a lot too , several companies use this to keep themselves safe, some have as a default force the employee to change their password every two months, avoid accessing or downloading unknown email attachments if they receive an email from an unknown or dubious source the most indicated is to delete/block the sender, because it is possible that you want to induce the user to share their personal information, and finally keeping your antivirus updated is another good thing a to stay safe, so that there is no security breach.

3. Methodology

According to Frainer (2020), research is a pillar of science and is a perpetual foundation designed for the intervention development process for implementation or practice integrated to reality. Searching is collecting data that will eventually become information after being interpreted in order to synthesize an answer about a particular study. This study aimed to carry out an applied research, since it sought to know to what extent the actions of users on the network constitute a risk or protection for their security, thus using the knowledge of fundamental research to solve this problem. For a better treatment of the objectives and better appreciation, it was observed that it is classified as descriptive research. Gil (2002, p. 42), defines descriptive research as:

[...] Descriptive research has as its primary objective the description of the characteristics of a given population or phenomenon, or else the establishment of relationships between variables.

As the population of end users on the Internet network is not registered, its population cannot be determined, therefore, a non-probabilistic sample will be used, which according to Mattos (2020) is a method that allows the researcher to select participants based on their ease and access, the sampling technique used was a convenience sample.

Analyzing the main objective of this work, the target audience of this study are people who can access the network and interact with it through mobile devices or desktops, with no specific criteria, since all people in the web environment are considered users. The research with network users was developed in companies, public and private schools, in the city of Manaus, central region of Amazonas, between April 23 and May 4, 2022.

The mechanism adopted to carry out the data collection was an online questionnaire where its distribution

and call for participation was through the distribution of links through the WhatsApp application and pamphlets with QR code fixed in the premises of the study sites.

For data collection and analysis, the quantitative method was used, where the quantitative approach (realistic/objectivist) was applied. Gressler (2004, p. 43) defines the quantitative approach.

[...] it's characterized by the formulation of hypotheses, operational definitions of variables, quantification in the modalities of data and information collection, use of statistical treatments. [...] has, in principle, the intention of guaranteeing the accuracy of the results, avoiding distortions of analysis and interpretations.

With quantitative surveys, you can measure and quantify respondents' responses and obtain data that more accurately confirms or disproves initial assumptions. The online questionnaire with pre-prepared questions, composed of 2 groups with 29 questions, and in group I, the characterization data of the respondents are requested. Group II is composed of 26 questions aimed at knowing the actions of end users in a situation of possible risks, as well as security procedures adopted in the digital environment.

4. Results

In the developed research, 221 answers were obtained, in which 15 were discarded that by chance had their answers incomplete, in this way the answer of 207 users is based on analysis. With the results obtained, we can understand how users are taking care of their security in the internet environment, how they act in the virtual environment, and to what extent their actions may constitute a risk or a protection for their security.

For data collection, closed questions were used, seeking to obtain more information about the subject object of research. The analysis method was divided into three parts that correspond to: (i) the characterization of users; (ii) Main actions that indicate security acts in the face of possible risks; (iii) The main security risk actions, and, finally, comments and suggestions regarding your actions.

Initially, to know the profile of the interviewees, 3 fields were made available for response: Gender: of the 207 valid responses, 58.94% are female and 41.6% male. As for age group: 7.73% are between 12 and 17 years old, 27.54% are between 18 and 24 years old, 42.51% are between 25 and 31 years old, 15.46% are between 32 and 38 years old, 4.83% are between 39 and 45 years old and 1.93% are over 46 years old. And finally, regarding the level of education: where 47.83% of respondents have completed higher education, 27.05% have incomplete higher education, 16.91% complete high school, 5.80% incomplete high school, 1 93% complete elementary school and 0.48% incomplete elementary school.

4.1 Main Actions that Constitute Good Security Practices

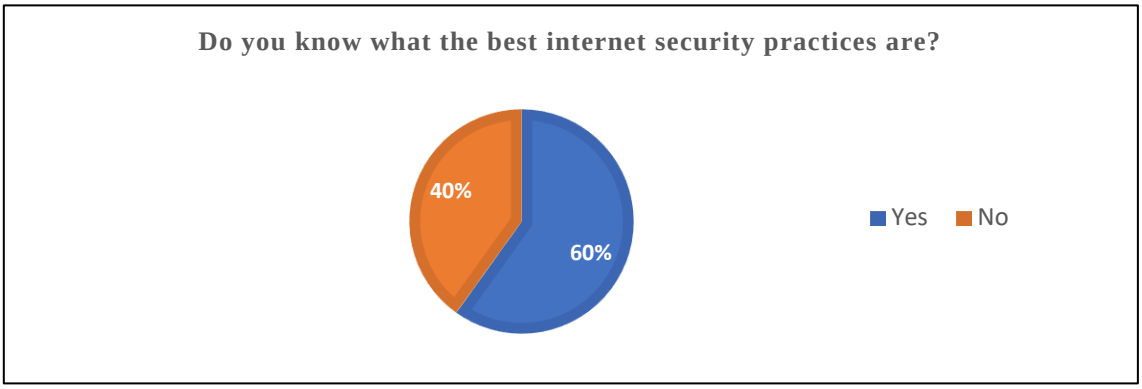

Figure 1: Internet security best practices.
Source: Authors (2022).

In Figure 1, the user is asked if he has knowledge of good internet security practices and 60% reported that they do have knowledge of good internet security practices. Therefore, through this it is possible to notice that more than half of the internet users will be less likely to fall for a scam, information theft or suffer something bad on the internet since they claimed that they have knowledge of good practices, however among the respondents 40% they do not have such knowledge and these people are already more likely to suffer a scam, theft or some malicious act on the network.

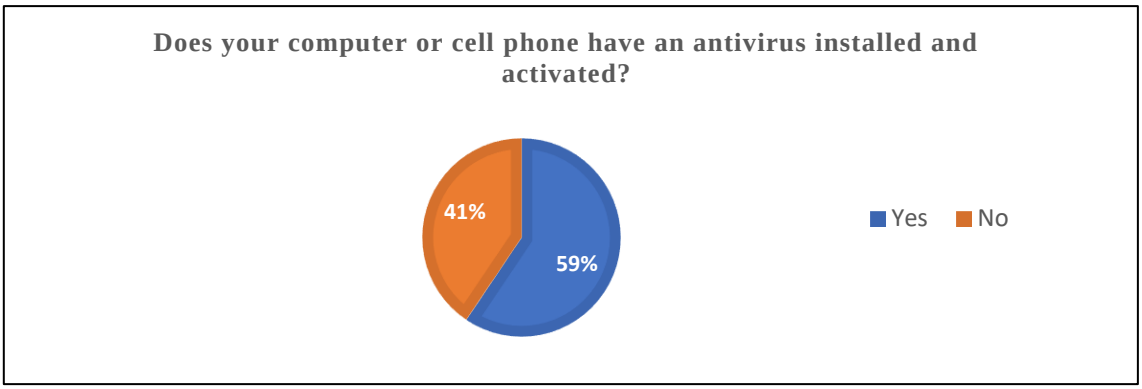

Figure 2: Does computer or cell phone have antivirus?
Source: Authors (2022).

In Figure 2, the user is asked if he has an antivirus installed on his cell phone or personal computer, 59% of the respondents do have an antivirus installed on their device or personal computer, so it is clear and easy to perceive the fact that the largest part of the respondents will not suffer attacks, virus or malware invasions and if these users suffer the attack or invasion they will be able to use the antivirus to perform a scan, identify and eliminate such threat but the remaining of the respondents that are 41%, if they suffer an attack will not know how to identify that they are in danger and putting their data and information at risk, which causes an extreme vulnerability to these users and all this caused by the fact that they do not have

an antivirus installed on their mobile device or personal computer.

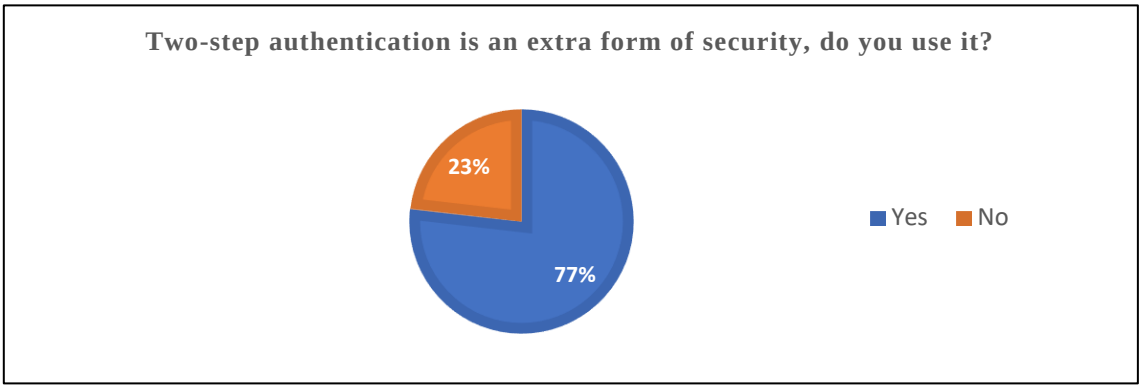

Figure 3: Do you use two-step authentication?
Source: Authors (2022).

In Figure 3, users are asked if they use two-step verification, which is also known as two-factor authentication, which has the purpose of adding an extra layer of security for the user, it is possible to notice that 77% of the respondents use yes two-step authentication, which is a very good result since these people, by using two-step authentication, are safer when logging into their account, be it bank, email or something more personal, because the two-step authentication in addition to needing the user's password to enter their personal things, it will also ask for an extra confirmation which is usually a code sent by SMS, code sent by email or app and even the use of a token, although it does not provide 100% security for the user, it is a much safer mechanism than using just the password, which leaves the other 23% drastically vulnerable since it is enough to know your password to have access to everything that these users rivers have.

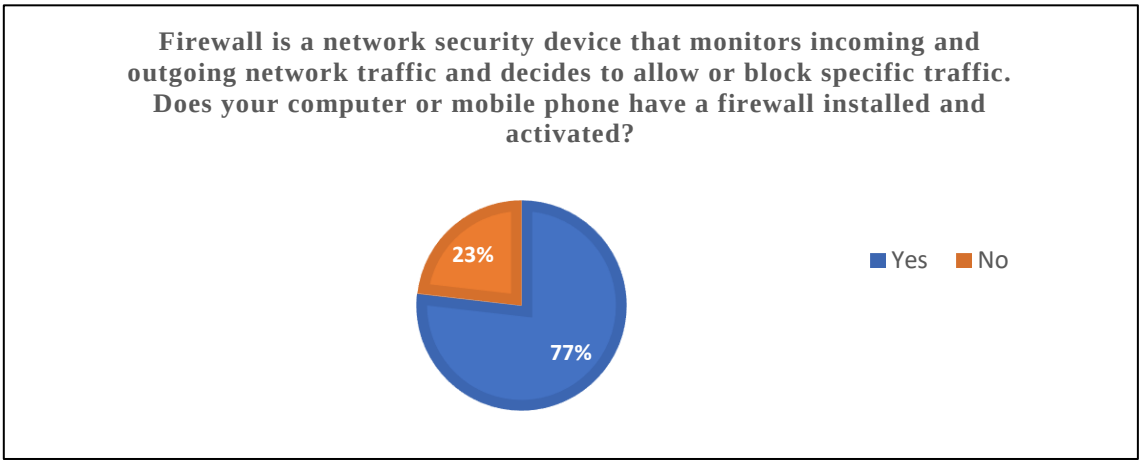

Figure 4: Firewall Usage.
Source: Authors (2022).

According to figure 4, 77% of users have the firewall enabled on their computers, the firewall is the first layer of protection against intrusion by other malicious users, it creates "invisible barriers" on the computer, acting on network traffic making a file scan to decide which files will pass through the "invisible barrier".

4.2 Main Actions that Constitute Security Risks

It is important to ensure that the connection between your computer and the Internet is secure, as this will protect you from attacks. With that it was asked: When accessing a site, do you check if the connection is secure?

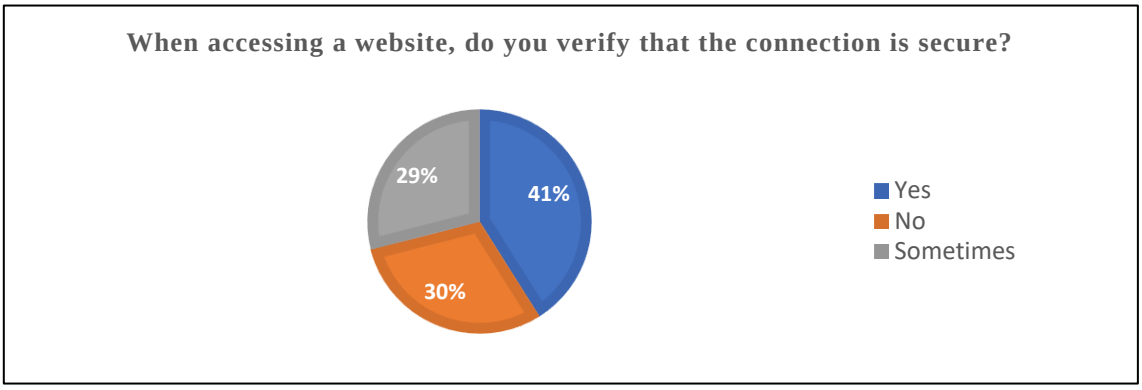

Figure 5: Usually checks if the site has a secure connection.
Source: Authors (2022).

As identified in Figure 5, 41% of respondents reported that they check whether the site connection is secure, another 30% said no and 29% only check sometimes, so if we approach it from a more technical point of view, we have a total of 69% of respondents who at some point are exposed to a security risk by not verifying the site, which according to Wendt, Vinicius and Nogueira (2012) occurs through verification of the SSL or TSL security protocol as well as the presence of a padlock on the page which indicates that it has a security certificate. One method of protection indicated is the thorough verification of the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols that encrypt data while traveling over the internet. The form of identification is to observe if the site has the following format “https://www”.
Watching a newly released movie at home seems like a good idea, since on official platforms, things change perspective when using unofficial websites. With that, it was asked: Do you have the habit of watching cartoons, series or movies on any unofficial website that offers this content?

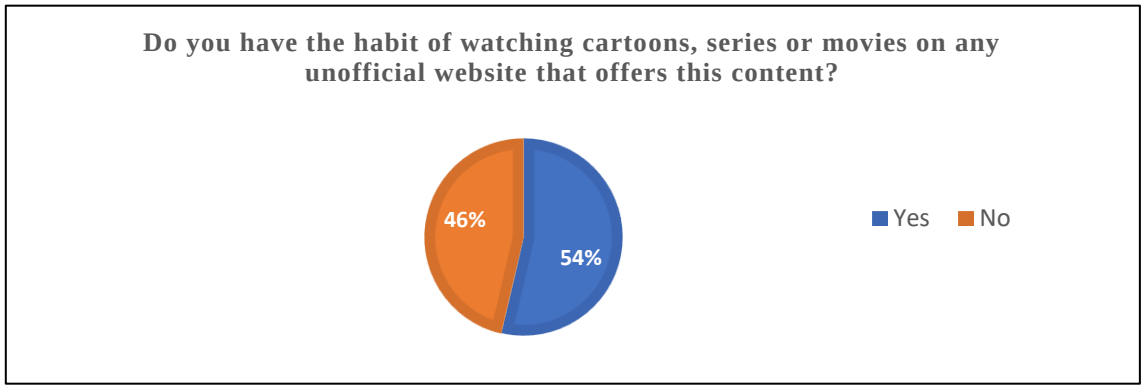

Figure 6: Habit of watching on unfamiliar websites.
Source: Authors (2022).

According to data from this research, as shown in figure 6, 54% of the respondents have habits of watching movies on unofficial streaming sites, which can be a risk factor for their safety, since, in general, sites that offer free movies can open multiple popups with each click. Where, according to the Center for Studies, Responses and Treatment of Security Incidents in Brazil - CERT.br (2012), the risks of a pop-up window can be the presentation of inappropriate content and the display of links that can lead to fake websites that contain malicious codes. One way of prevention would be to block pop-ups that are usually configured by default in traditional browsers, use an up-to-date antivirus and without a doubt try to avoid these types of sites.

The risks of getting a malicious code on the computer when downloading a program from a website and not performing the scan is very high, these are among the most common reasons for computers to be infected by viruses, so the following question was asked: If you download a file and program on website, after downloading you scan with antivirus?

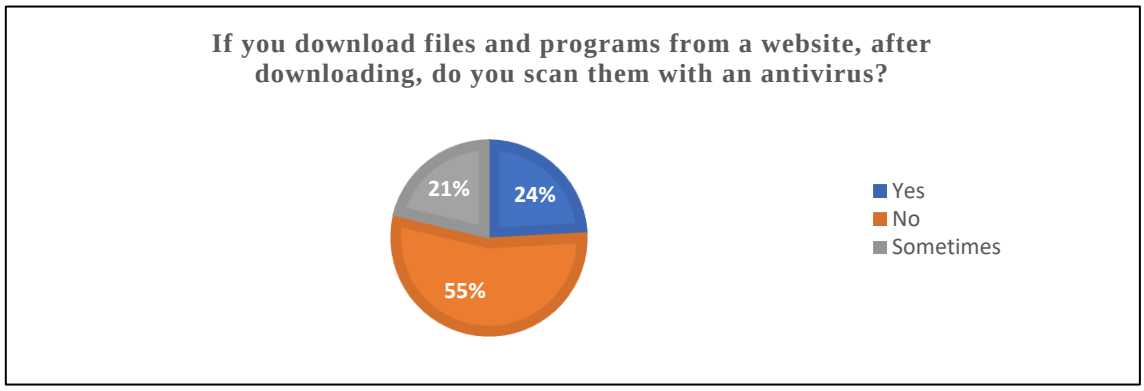

Figura 7: Scans files and programs downloaded from websites.
Source: Authors (2022).

Figure 7 showed that 55% do not usually scan files and programs when downloading, and this rate can even increase further if you add the 21% that only sometimes perform such an action, and in this interval, malicious code can be obtained. One measure to avoid getting malware is to avoid sites that offer free

software downloads, unless you are very careful about what you download (you can find out which sites are trustworthy by searching). The only way to protect yourself from viruses/malware is to practice good computing habits (including safe browsing) and keep your systems up to date as well as having an up-to-date and active antivirus. The custom of using the same password to access websites or programs is a security risk and can result in identity theft. thus, it was asked: Regarding passwords: Do you use the same password to access websites or programs?

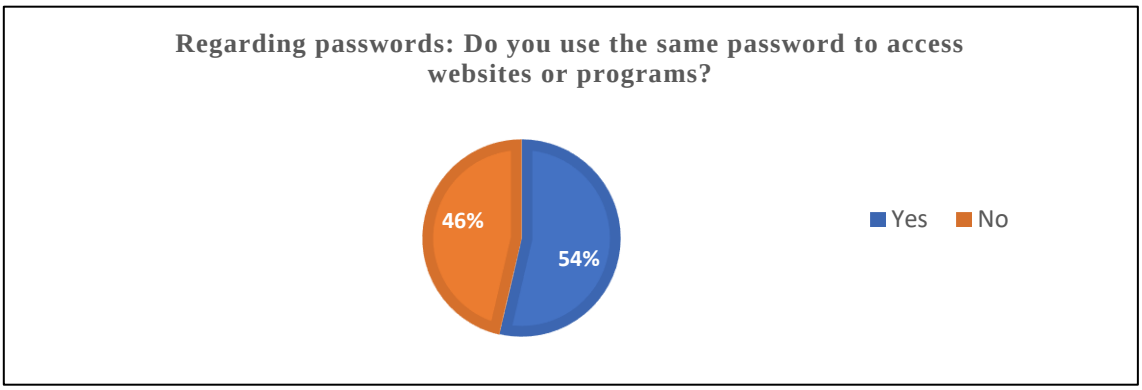

Figure 8: Usually uses the same password.
Source: Authors (2022).

In Figure 8, it can be seen that 54% of the participants usually use the same password for websites and programs, at first it may not present risks as it makes it easier to remember them, but CERT.br (2012) warns that this is a a risky practice, because if a hacker has access to the password of one account, they can easily gain access to the others. An adequate security practice would be to use different passwords for personal and professional matters and never use the same password for accounts that have more critical information such as emails and bank account websites.

5. Conclusion

The development of the present study sought to analyze the actions of users on the network in the face of the most common risks of infection by malicious code, viruses, Worms or Trojans, from which it was possible to assess whether their actions may constitute a risk or extra protection. to its security and thus to be able to understand a little more about the maturity of users during the use of the network regarding their security.

In general, network users showed knowledge about good internet security practices, which infers that they are aware of the eminent risks that the network has. Most users use up-to-date antivirus on their devices, and they also make use of two-step authentication which provides an extra layer of protection in the event of a password theft. However, it is also possible to notice that unfortunately there are many users who are still uninformed out there and who do not know how to browse or stay safe while using the network. Some points can be mentioned here such as: the fact of not verifying if they have a secure connection with a website; have the habit of watching websites with pirated content; use the same password for websites

and programs and do not scan files downloaded from websites even if you have an antivirus on your device. in view of such information collected and analyzed, it is evident that the objectives of each study proposal were actually achieved.

In this sense, users can see a maturation in the perceptions of good practices related to the use of the network and basic security care, but there is still a need for more information and guidance on the risks they run in using the network, as a way of detect and mitigate them before they become real problems.

Of course, the implementation of this work has some limitations. The main one concerns the use of non-probabilistic samples for convenience, so that results and conclusions cannot be extrapolated to the scope of network users. In future investigations, we find it interesting to cross some characteristic variables, such as education, age, and analyze whether these factors influence network security actions. It is also possible to suggest more technical and in-depth studies of the risks to which users are more exposed, such as not checking connections to websites.

6. Acknowledgement

To the Metropolitan University of Manaus - FAMETRO, the Academic Coordination for the support and assistance in the development of teaching and research.

7. References

CERT.BR. Cartilha de Segurança para Internet. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

DINIZ, Danielly. Navegação segura na Internet: 1 a cada 2 brasileiros não concorda. ln: PSafe. dfndr blog – PSafe. [S.l.]. 8 fev. 2022. Disponível em: https://www.psafe.com/blog/navegacao-segura-na-internet-1-a-cada-2-brasileiros-nao-concorda/. Acesso em: 9 mar. 2022.

DOS SANTOS, Bruna Cardoso et al. Vulnerabilidade de Dados e a Percepção de Privacidade dos Usuários de Redes Sociais. Brazilian Journal of Business, v. 1, n. 4, p. 1728-1742, 2019.

FERREIRA, Sergio D. C. Sistemas de informação em segurança. Londrina: Editora e Distribuidora Educacional S.A., 2017.

FRAINER, Juliana. Metodologia científica. Indaial: UNIASSELVI, 2020.

GIL, Antônio C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

GRESSLER, Lori A. Introdução à pesquisa: projetos e relatorios. 2. ed. São Paulo: Loyola, 2004.

MATTOS, Sandra M. N. D. Conversando sobre metodologia da pesquisa científica. Porto Alegre: Editora Fi, 2020.

NETO, Pedro Tenório Mascarenhas. Segurança da informação: uma visão sistêmica para implantação em organizações / Pedro Tenório Mascarenhas Neto, Wagner Junqueira Araújo. - João Pessoa: Editora da UFPB, 2019.

NOGUEIRA, José H. M. Fundamentos De Segurança Cibernética. 1ª. ed. Joinville: Clube de Autores, 2021.

PIMENTA, Alexandre Manuel Santareno; QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. JISTEM-Journal of Information Systems and Technology Management, v. 13, n. 3, p. 533-552, 2016.

POSITIVO TECNOLOGIA. Segurança da informação: conheça as 12 melhores práticas. [S.l.]. Panorama Positivo, 2020.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de, Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico

ROSS, Alec. As Indústrias do Futuro. Lisboa: Actual Editora, 2018.

SANTOS, Rodolfo Francisco Souza dos. Segurança da Informação: Proteção de dados em ambiente empresarial. Faculdade de Tecnologia de Americana, Curso Superior de Tecnologia em Segurança da Informação. Americana, SP. 2018.

SANTOS, Patrícia Isabel Pinho. Segurança informática: a importância para a segurança interna. 2016. Tese de Doutorado.

SILVA, Renata; URBANESKI, Vilmar. Metodologia do trabalho científico. Indaial: UNIASSELVI, 2009.

WENDT, Emerson; VINICIUS, Higor; NOGUEIRA, Jorge. Crimes Ciberneticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.