Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15811
DOI URL: http://dx.doi.org/10.21474/IJAR01/15811

RESEARCH ARTICLE

FLAWS IN POLICIES OF CONFIGURATIONS AND RISKS FOR WIRELESS NETWORKS IN THE CITY OF MANAUS

Matheus Kalil Lopes De Freitas, Wellington Sousa Da Cunha and Jaqueline Silva De Souza Pinheiro

Manuscript Info

Manuscript History
Received: 05 October 2022
Final Accepted: 09 November 2022
Published: December 2022

Key words:-
Network, Information Security, Wireless Standards, Wireless Attacks, Configuration Failures And Wireless Prevention

Abstract

This article aims to inform people of the risks each of them takes when connecting to unprotected wireless networks, instructing them on the care they should take, what can happen to their data, the types of wireless standards, and how to prevent themselves today. For this purpose we did a search through Google Forms where people answered questions related to their day-to-day that provides us with the security data that can help us achieve our goal in this article.

Copy Right, IJAR, 2022,. All rights reserved.

Introduction:-

During the course of the day we spend a lot of time connected, it is common in our reality for a person to be connected to a wireless network, but the danger arises when we do not have the proper knowledge of what this network to which we are connected can offer us. Practicality allows us to have a connection anywhere we can go even leaving our homes we have wireless connections around the city, in places we frequent throughout the day, are them shopping, colleges, squares, shops and even unknown connections due to needs.

With the convenience that we have to connect nowadays we can acquire an internet in our homes where comes a responsible person do the installation and configuration what we have to do is only pay, however there are several types of configuration that we users do not understand, that up front can rather make a difference of security and here are some types of connection that are most used in places to which we do not understand.

Despite a lot of technology available for our use today, people don't care where they're connecting and what a person can extract from their victims just over the wireless network. The tools that have been innovating more and more difficult to detect, however we will see a little about networks and important points that we let pass in our daily life.

Theoretical Reference

The theoretical reference presented in this article was a qualitative research. Introducing topics about wireless networks about wireless networks, wireless network patterns, types of attacks, information security pillars, configuration failures, and security prevention.

Wireless Networks

Wireless is an English term and means "wireless" (wire – without less or less). Inrecent years it has become popular with a great growth of the internet, but this idea of wireless communication is not so recent. It began in the mid-1901s, with an Italian physicist named Guglielmo Marconi who demonstrated the operation of a wireless telegraph that transmitted the information of a ship to the coast by means of Morse code. It has become popularly known as

Corresponding Author:- Matheus Kalil Lopes De Freitas

wireless networks or wireless WI-FI.AS end up taking great advantage of wired networks. How to provide flexibility and mobility. They allow multiple providers to communicate servers without the need for cables. This type of communication occurs due to electromagnetic waves.

We have also considered, as wireless network the Bluetooth technology, which followed a different development path of the family 802.11 this technology operates in the Ad-Hoc topology in frequency of 2.4 GHz giving possibility of transmission in short distance between wireless phones, mobile phones, printers, PDAs, notebooks, fax, keyboard, that is, any digital device that uses a Bluetooth chip. The main goal of Bluetooth is simply to simplify communication and synchronization between these electronic devices that today use cables to connect and synchronize with each other. (MENDES, 2007).

Independent networks are more basic and simple wireless. These network types do not have a given topology, where there is no central element in the communication structure. In this case, the stations communicate directly with each other. One of the great advantages of this type of network is the ease of installation, the configurations of wireless interfaces on each mobile station. In this process no other element is used, costs are also reduced, and not even a design of a wired network needs to be elaborated. Its disadvantage is for an area with a certain coverage is restricted and does not contain a stable frequency in the quality of communication, failures due to physical barriers that can interfere in communication between stations, since they communicate directly. In addition to control deficiencies, there is also security vulnerability.

Networks with infrastructure have at least one area centralizing element that organizes part of the network, which are called access points, any communication passes through that element, and the quality of service can be controlled. In addition, physical barriers are rarely problems, since the network is designed to provide coverage in a certain area.

In this case, the access point is set to maximize the quality and coverage area desired. even when coverage is insufficient, other access points can be inserted, resulting in an expansion of the local wireless network infrastructure. In this way, communication between two stations at different access points can occur without problems. Another advantage is the control and security mechanisms, because each client station must join and authenticate to the access point, as will be detailed later. Basically, only networks with infrastructure are used in enterprise environments and are the most widely used type today.

Wireless Standards

Currently there are standards in wireless networks such as 802.11a, 802.11b, 802.11g, 802.11n standards. Each works on a different frequency, sand these frequencies are different one network cannot see the other.

Networks in the 802.11 standard use a logical bus topology, which controls the access of devices connected to it, through a system similar to the CSMA/CD of Ethernet networks. This bus when used on wireless networks is called Carrier Sense With Multiple Access and Collision Avoidance (CSMA). (OAK,2013)

- ✓ Padrão 802.11ª

With this standard it is possible to achieve upload speeds of 54 Mbps, and works with a frequency of 5 GHz. Because it has a higher frequency than the standard (the 802.11b), it ends up being a more expensive technology and little used in home networks.

- ✓ Standard 802.11b

This is the most commonly used standard today in home networks because it has a more affordable price than the standard (802.11ª). However its upload speed is lower, reaching 11 Mbps, and works with a frequency of 2.4 GHz. This pattern has some negative points, Because it has a frequency different from the standard 802.11a, the two are incompatible, This frequency is the same as other home appliances, such as cordless phones and microwaves, which causes interference in the signal.

- ✓ Padrão 802.11g

Seeking to have the benefit of the standard 802.11b was created the standard 802.11g as well as the standard 802.11b it possess the frequency, works with a frequency of 2.4 GHz with a speed of 54 Mbps. This standard 802.11g and compatible with the 802.11b standard. this pattern has as a negative point the signal interference

- ✓ Padrão 802.11

This standard and that has a higher speed can reach up to a speed of up to 300 Mbps, this standard has great advantage among previous priests with greater range and the best bell, its signal does not have much interference so more stable, compatible with all other standards. Due to the technology that allows to have multiple inputs and multiple outputs to the data.

These types of patterns can be used on a day-to-day business, today it is easy to buy a router that has the option to choose which standard will be configured.

Pillars Of Information Security

Information Security means protecting your data and information systems from unauthorized access and use, disclosure, modification, reading, recording, inspection and destruction. The concept of information security is related to the confidentiality, integrity and availability of information. (FABIANE RODRIGUES,2018) . Information security is extremely important in the technology market and is becoming essential for people who enjoy this technology. Companies want to ensure the protection of their data at all costs. Thinking about it, this article was developed to inform the risks of wireless networks that are widely used today. This research takes into account the 4 pillars of information security: reliability, availability, integrity and usability.

1. Confidentiality: Guarantees access to information only to authorized persons, that is, does not provide such access to unauthorized individuals, entities or processes.
2. Integrity: Ensures the veracity of the information, indicating that the data cannot be changed without authorization.
3. Availability: Ensures that data and systems are available to authorized persons when it becomes necessary.
4. Authenticity: Guarantees the true authorship of the information, that is, that the data are in fact coming from a certain source.

These points are extremely important for companies that seek better security within their network, being wired or wireless. It must have a break-even point so it won't be as secure as to the point that its employees can't use the network, and not so insecure to give permum to malicious attacks from unauthorized people who will have access to the network.

Attacks On Wireless Networks.

Nowadays our society is driven by information, connection, practicality, time savings and everything thanks to the Internet. An environment to which we have the power to navigate and to know places without having to go to it.

But the internet as all that is good is not all that wonder, there are dangers and care that we users have to look at. These days we all have access to a wi-fi in our homes, our own private network. But that comfort and safety only works in our residences, in the day to day we go out to work, college and other appointments. Where we do not always have that private connection network and due to the need to send a message or see an important subject on the Internet we end up connecting to these public networks scattered throughout the city, be they in college, sights, schools, squares or some unknown open networks. With this we raise some of the main cause of vulnerability in these networks are lack of employee information, corporate policies, access point security. These are some of the major problems encountered on WI-FI networks and wired networks. They generally don't realize when data was compromised via access points until after the incident, but there's no doubt that the cost of these errors is significant.

People who use loopholes in wireless network configurations often use planning to achieve a successful intrusion, so a sequence of procedures is required that enable the attacker to accurately. There are a number of tools and procedures such as: mapping the area to be attacked, a device equipped with Wi-Fi card, survey of what programs will be needed for the scanning of the network and breakdown of the encryption adopted (Robson Everton Sousa,2019).

Configuration Failures.

Configuration failures often come through equipment or through the companies that have their employees set up the services we pay for. If this employee does not configure the correct way there may be a security breach, something that leaves a vulnerability to some kind of attack, or even a malfunction that in a way can lead to future problems on both private and public networks. Connection problems, malfunctionof the appliance, crashes and slowdowns can be

configuration failures, whether network failures or the device itself to which the contracted company has configured. Traffic capture and attacks are done with specialized programs, due to the peculiarities present in the sub patterns of wireless networks (802.11b; 802.11; 802.11g and others). These tools are specialized and can be found free of charge. (RUFINO, 2015)

Prevention In Wireless Networks.

There is a huge scope of care that we users do not perceive when doing or do not have so much knowledge of situations that may be serious in the eyes of the attacker. There are some methods of defense by obscurity that allow a certain degree of security to wireless networks, but these methods do not allow total security to the network. Because there are several computer programs that allow you to reveal information that is encrypted or hidden.

Although we find many security flaws, we are not totally unprotected, we have some care that we can take so that we can prevent something from happening. The use of paid networking apps and antivirus are a good indication because they allow us to have greater security since it is a service for which the user would be paying for it. Care when using unknown wireless networks, or even avoid using, because most of the time we do not know whose network is or if the connection it offers is real even.

Disable Ssid Diffusion.

Disabling this function is one of the top recommendations of any wireless security manual. Through this configuration, network administrators try to prevent people outside the network from knowing their network name and trying to access it. This form of dark configuration tries to prevent malicious people from coming to use the network for illicit purposes. (RUFINO, 2015)

Currently on the market each brand of routers has the option to disable this SSID function which will vary and its interface that will be different depending on the brand of the device to do this just enter the router settings.

Modifying The Ssid-Standard Name

This procedure also tends to be categorized as security by obscurity, but the problem with this category exists only when all security is based only on obscurity, that is, the attacker in principle can not promote a successful attack, because it does not know some characteristics of the target, so if, or when he has this information, the target will be completely vulnerable. (RUFINO, 2015)

Usually manufacturers of routers for wi-fi networks put a standard ssid, making the change of that name ends up becoming obligation. However, most users do not usually exchange this name, which ends up creating a risk situation, because the data is public and can be found on the device itself or in the product manuals.

MAC Address Replacement

This change does not cause user inconvenience and, on the other hand, prevents the immediate identification of the manufacturer by a potential attacker. But this action alone does not guarantee the safety of an installation, so it should be combined with other measures to achieve an environment with the security closer to the ideal. (RUFINO, 2015) .

Disable Access To The Hub Via Wireless Network.

Most hubs offer access via HTTP and TELNET, and because these two proto-46 v.1, n.1, p-1-51, Apr., 2019 colos do not offer encryption, it is recommended to disable these options on the side of the wireless network, to prevent user and password packets from being captured by a potential attacker. This alternative leaves access to the hub to the care of the wired network, provided that it is endorsed with a protection mechanism that allows monitoring and authenticating users by restricting access to the hub. (RUFINO, 2015) . To make this setting, go to your device settings and look for the "Wireless Network" or "Wireless" option. Look now on the right side and see the "Wi-Fi" section. It will have a button that can be used to allow it to work and to disable it. Press depending on what you want to do.

Defense Of Client Equipment

Consideration should be given to the defense of the client who has two situations to be considered, one concerns the inviolability of communication, data and equipment of the user and the other precaution is to prevent attackers from

reaching the user's equipment from revealing keys and other information that access the network with the credentials captured from the client's machine. (RUFINO, 2015)

The person has the habit of leaving the routers in places of easy access and do not take away the sticker that contains all your information that is located underneath it. Ideally put in a place where only the person responsible would have access to the router.

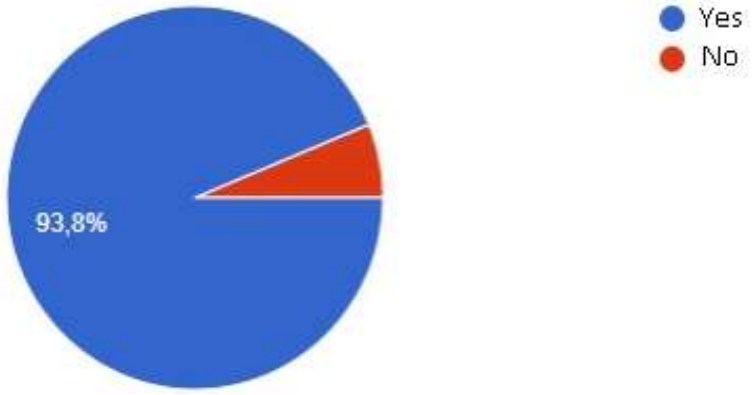
Methodology:-

The methodology used was chosen by a field research conducted in the city of Manaus, where we analyzed specific areas with a high concentration of wireless network users, we made available a questionnaire for users of these networks where we noticed. in the decision-making process, i.e. helping people make decisions in organizations is one of the main tasks of information systems, and as CHIAVENATO (2020) defines it, decision is "the process of analysis and choice between several alternatives. the course of action that a person must follow." Thus, for the condition of decisive quality means the quality of the data in the system for which it supports this decision. The organization must take care of the consistency, evaluation and filtering of the data entered in the system, because this data constitutes the information used in the decision-making process.

Findings

As we mentioned, many people connect to networks that do not know where it comes from or what this can entail, based on this we set up a search via Google Forms with 9 questions that can complement and prove the lack of knowledge and data of people.

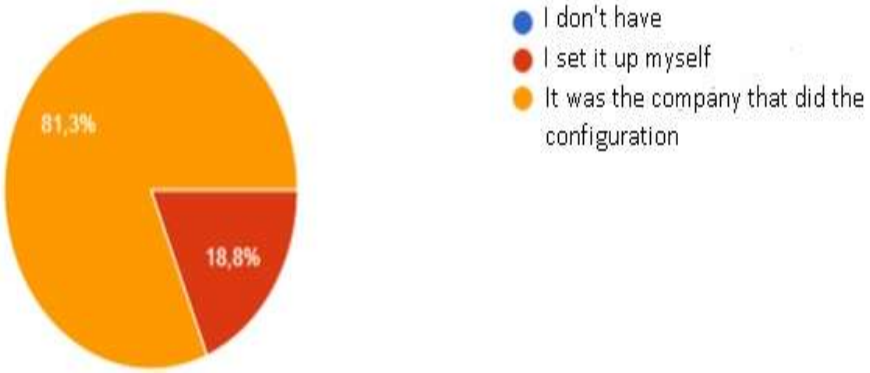
Graph 1:- Do you have a Wi-Fi connection in your home?



Source: Authors, 2022.

Based on graph 1 we can see that most people have wi-fi networks in their home, but not all 6.2% who do not have Wi-Fi connection in their homes.

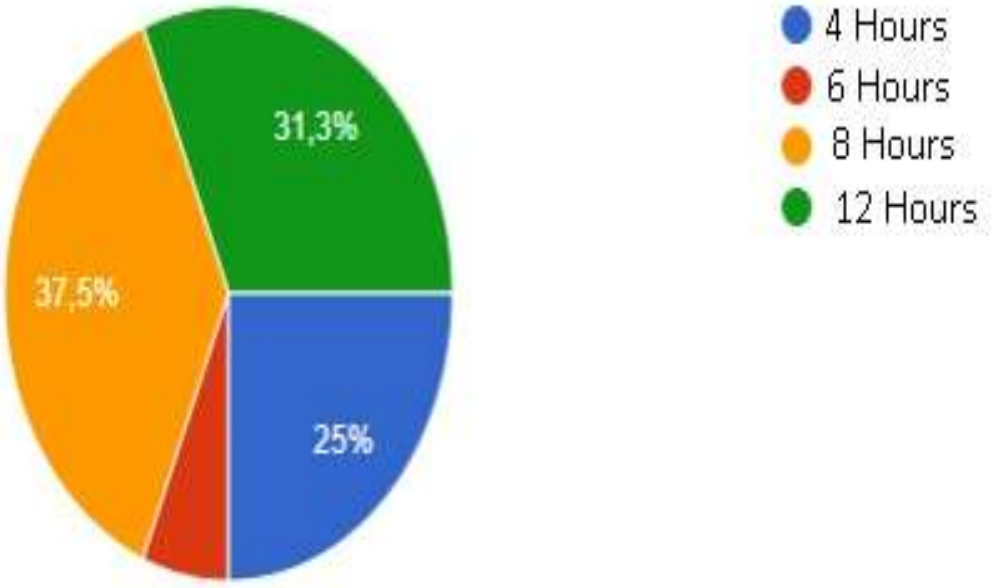
Graph 2:- If you have a router device in your home, were you the one who set it up yourself?



Source: Authors, 2022.

When analyzing graph 2 we can notice that people who already subscribe to internet plans, the company that makes the settings itself, but we can also observe that not everyone lets the company do the service, 18.8% configure their own device for their use.

Figure 3:- How long are you out of your residence?



Source: Authors, 2022.

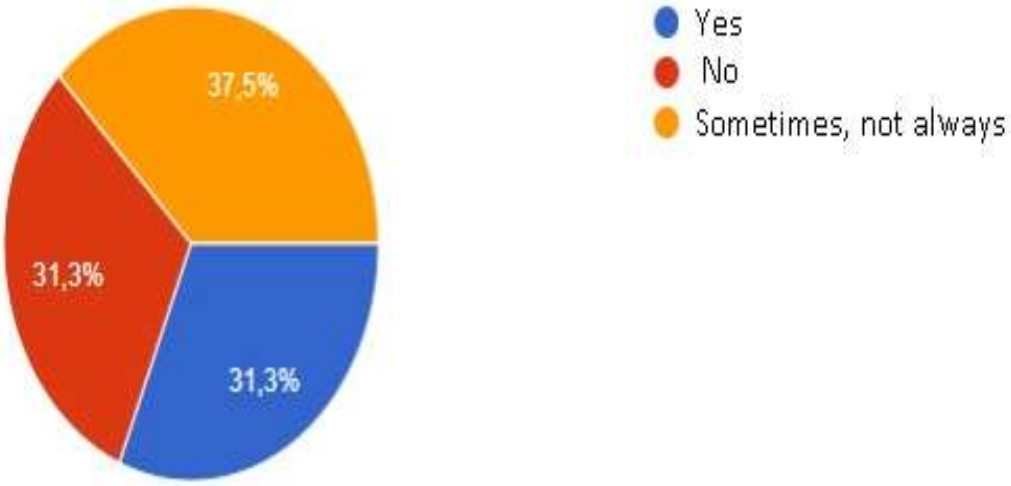
As we can see from the data, most people spend about 4 hours outside their homes, not to mention the large part that would be 8 hours to 12 hours outside the home, in which case comes into questioning about what connections they use outside their homes.

Figure 4:- Do you have mobile data on your mobile phone?

Source: Authors, 2022.

Above we can see that 93.8% of the public uses mobile networks (internet on mobile) usually that has its own mobile data is less susceptible to connect frequently on public Wi-Fi networks.

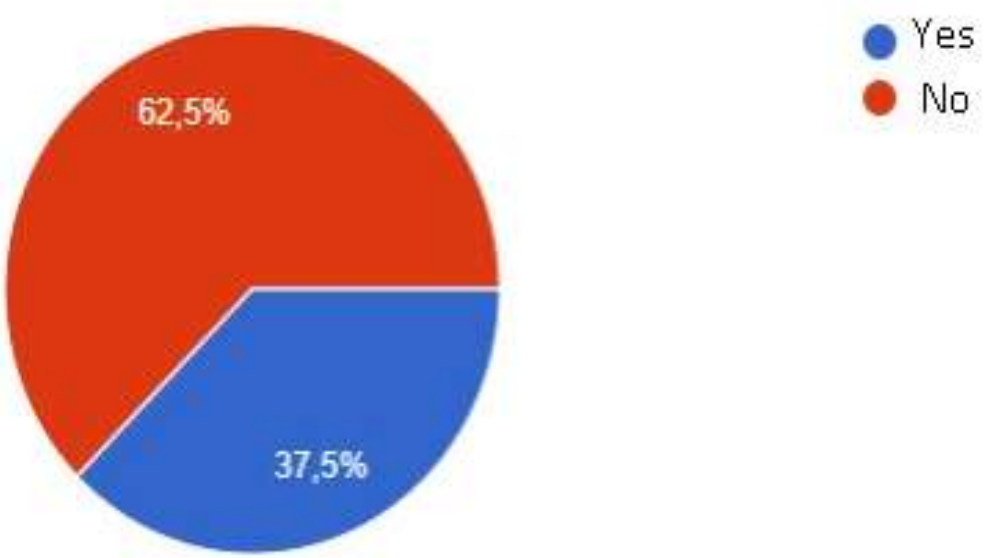
Graph 5:- When you leave home do you easily connect to wi-fi networks at your fingertips?



Source: Authors, 2022.

As we can see, most people connect on Wi-Fi networks easily, these people without proper care end up becoming targets, already 31.3% do not connect this in turn can be due to their own mobile data or their knowledge of vulnerability and to close we have 37.5% who connect time or time that in turn also end up at this risk if they do not take care and due attention.

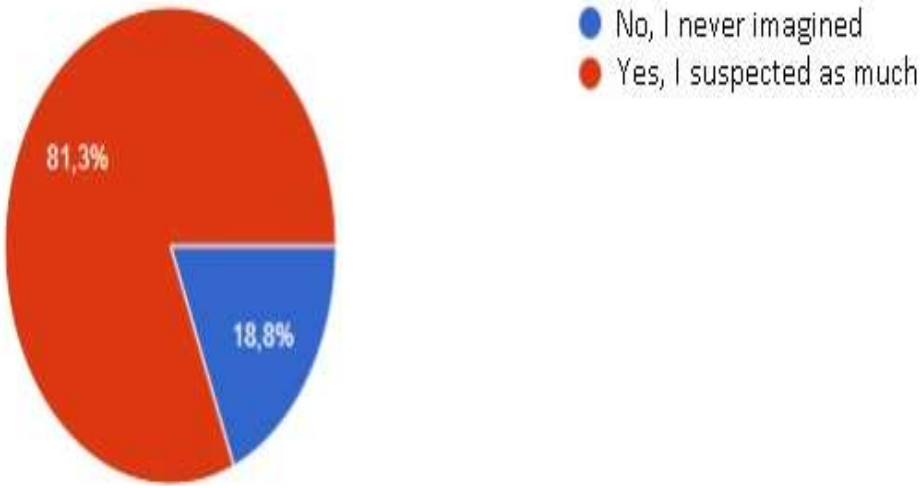
Graph 6:- In public places such as: squares, malls, cinemas, shops and colleges do you connect on wi-fi that do not have passwords?



Source: Authors, 2022.

We have a basis that some 62.5% of people do not connect to public networks, in turn this may be because they have their own mobile data or a certain care, but we still have 37.5% of people who connect to the networks.

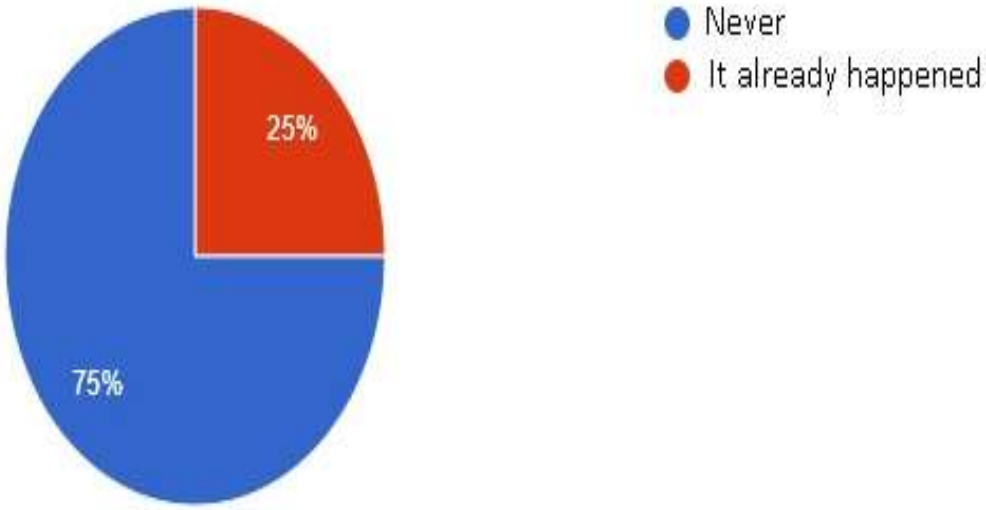
Graph 7:- Are you aware that your data is at risk on public wi-fi networks?



Source: Authors, 2022.

With 81.3% people are aware that public connections have a certain risk, even with the science of what can happen there are still many who do not take the appropriate measures and cause problems, already 18.8% are not aware that their data can be leaked simply by connecting to a public wireless network.

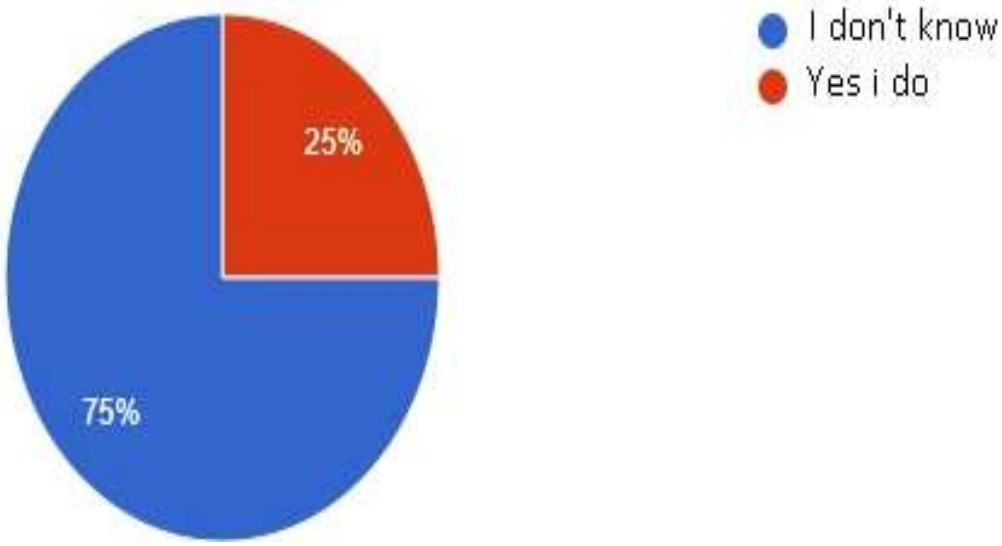
Graph 8:- Have you ever had a problem connecting to public wi-fi networks?



Source: Authors, 2022.

When connecting to Wi-Fi networks 75% of people had no problems, already 25% had problem, be it connection or even something else. Not everyone has problems connecting, but it still happens to some people and we can mitigate these problems by looking out the right way on wireless networks.

Graph 9:- Do you know how to prevent attacks made on your network or electronic device?



Source: Autores, 2022.

We see that not everyone has a certain notion of what to do if there was an attack, with 75% of people not knowing what to do and only 25% could take a preventive measure,

Discussion:-

As we can see, most people know the risks of connecting to wireless networks, but they still do. However, many people do not know the risks they run only use public networks out of necessity, we also note that most of them have a private connection network in their home, greatly reducing the use of unknown local networks.

Our survey found that 31.3% of people spend about 12 hours outside their home while 37.5% spend about 8 hours, a time that if the person does not have a mobile connection and needs to do something it will certainly connect to the first wireless network at their fingertips and if the network is closer to even an unknown public network, this due to the need for use.

Confinal Siderações

We can conclude that a large part of the population that does not have mobile networks or private networks at home, when needing to connect end up ceding to public networks, end up submitting to the wi-fi networks available on the streets even knowing that they are seriously at risk when doing this action.

Taking into account that our research was done in the city of Manaus with people who spend much of their time outside their homes, it is perceived that many people are not aware of the vulnerabilities of their own routers devices, showing the lack of information that there is. However, despite many vulnerabilities and flaws there are also ways to protect yourself or prevent failures in our wireless devices.

Due to the practicality we spend the day to day connected and even with so much information over the network, we still leave to be desired in the matter of awareness of use or even by false information circulating through the network, a small detail can make a difference in our device and in our connections that we believe to be "safe".

This article was done with the objective of informing users of these networks that there are risks when connecting to these networks that we do not know available in malls, businesses and public places. foram addressed the topics that show how users can prevent themselves by making their devices safer, about their network patterns as 802.11a the most used standard currently in wireless networks and overs the risks of a misconfiguration in the device that often users do not know how to change end up leaving the settings that are made by the device supplier.

Bibliographic Reference:-

1. ATTIE, W. Audit: concepts and applications. 3. ed. São Paulo: Atlas, 2000.
2. CARVALHO, Joao Antonio. Informatics for contests: theory and questions. Rio de Janeiro. Elsevier,2017.
3. CHIAVENATO, Idalberto. Administration in the new times. São Paulo: Campus, 2000.
4. CHIAVENATO, Idalberto. People Management. 3rd edition, Editora elsevier - campus, 2018.
5. LAUDON, Kenneth C.; LAUDON, Jane P. Management Information Systems: managing the digital company. 5 ed. São Paulo: Prentice Hall, 2015. O'BRIEN, James A. Information systems and management decisions in the Internet age.São Paulo: Saraiva, 20 16.
6. Read about information security. Available from: <https://efagundes.com/artigos/seguranca-da-informacao/> access: 10 Oct. 2022.
7. REZENDE, D.A.; ABREU, A.F. de. Information technology applied to business information systems: the strategic role of information and information systems in companies. São Paulo: Atlas, 2020.
8. RUFINO, Nelson Murilo de Oliveira(Wireless security: Learn how to protect your information in Wi-Fi and bluetooth 4 environments. Ed. São Paulo: Novatec, 2018.
9. TORRES, Gabriel. Computer Networks. 2. Ed. Rio de Janeiro: New Earth, 2014.