Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.11, 2022

Security of Wireless Networks

Irida Gjermeni[1*] Jehona Hoxha[2]
1. Department of Mathematic and Informatics, Agricultural University of Tirana, "Pajsi Vodica" St., 1029 Tirana, Albania
* E-mail of the corresponding author: igjermeni@ubt.edu.al

Abstract
Wireless networks today have become a normal standard, a technology that could not even be imagined a few years ago. We have them everywhere: at home, in schools, in offices, in restaurants, in airports, in squares or main streets. These wireless networks have become an inevitable, as well as a necessary part to carry out our daily tasks, from the simplest to the most sophisticated ones. Thanks to them, we can study, work, buy, order or book in a very short time and feeling comfortable; all sitting on a chair with a cell phone or laptop in front connected wirelessly.However, the world is somewhat more complex. Things are not as simple as they seem. There are many malicious individuals who have devised hundreds of ways to make these networks vulnerable. A minimum of 800,000 individuals are hacked each year according to Norton, the American antivirus company, but not only. Thousands of businesses, organizations or institutions have also fallen prey to these attacks.In this study, some of the types of attacks that are encountered more often against wireless networks are dealt with. Some key but simple security measures that can be taken by anyone to gain minimal security have been identified, as well as some practical tips for homes, organizations and public spaces have been summarized.The purpose of this study is to clearly show the danger that wireless networks can have, the possible threats and the security measures that can be taken to prevent them.
Keywords: network, wireless, security, attack, hacker, privacy
DOI: 10.7176/CTI/11-02
Publication date: October 31st 2022

1. Introduction

Today, at the time when technology has managed to occupy a fairly significant part of human life, wireless networks represent an equally important field of this virtual world. Over the years, these networks have been developed and improved, have gained reliability and have been implemented in home organizations, but many times wireless networks have also faced failures.

We see wireless networks applied not only in work or school environments, but also in homes, in various social, cultural and entertainment environments. Based on the fact that all phones of the last decade support wireless, we once again prove the importance and spread of this technology. This wide spread is due to the fact that these networks are very simple to install and use, as well as having low costs. Mobility, the ability to move easily and quickly, is one of their main advantages.

On the other hand, the integration of the virtual world into our lives is so great that most of the previously known activities, such as sending letters, job applications, shopping, banking, etc., have been digitized. The large amount of information that is transmitted online, which includes personal and often sensitive data, is exposed to various risks created by people with malicious intentions. In such a situation, the focus should be on safety.

This thesis will discuss the threats and vulnerabilities that wireless networks have, security measures that can be taken to protect the virtual environment where you operate, practical advice on networks for three different operating environments: in organizations, at home and in public environments . Also, through a survey with 200 participants, a study was conducted on the impact of wireless networks in society, informing the public about risks, security measures and the degree of their applicability in everyday life. 1 **Wireless networks**

Wireless networks are computer networks that are not connected by any type of cable. The beginnings of these networks date back to the 1950s, when the Bell telephone company in the United States introduced a new service to customers, the radio telephone. This was the first case of a radio-telephone network for commercial use.

Figure 1: Wireless Networks

By 1980, these networks were spread all over the world. After the 1980s, researchers and scientists began to study the idea of building a wireless broadband network that would be functional for personal computers (PCs). In general, these studies were led by the Apple Corporation, taking as a platform the European Telecommunication Standards Institute (ETSI, European Telecommunication Standards Institute). The first standard appeared in 1993 and the final version in 1995. Also, an initiative was taken in the United States to standardize WLAN at the IEEE (Institute of Electrical and Electronics Engineers). By 2002, wireless access had become widespread. Laptops manufactured after 2003 included wireless network interface cards.

Advantages of wireless network

Nowadays, a wireless network uses radio waves to connect devices such as laptops to the Internet, network and business applications. This communication between wireless users is done through the transmission medium, air (electromagnetic waves). The application of WLAN in various environments such as homes, offices, campuses, universities, etc., has many advantages, but also shortcomings. Specifically, we can clarify these by considering businesses. How can businesses benefit from a wireless network?

Since the digitization of work is always increasing, the attitude of employees only on the office computer seems ineffective, especially when there is a need for cooperation in work groups. Generally, employees are equipped with small computers (notebooks), which brings them more freedom in accessing the network, ease in their work and higher productivity. So businesses of all sizes, by implementing a wireless network that provides a combination of the bandwidth of wired networks with the flexibility and mobility of wireless networks, can benefit from:

1. Mobility. The employee will no longer be "tied" behind the desk. It can access the network from the meeting office, from a colleague's office, from the conference room, from the coffee shop, etc.
2. Productivity. Access to the Internet and key company applications from any work environment helps staff accomplish tasks successfully and encourages collaboration.
3. Simple installation. Since there is no need to lay cables, installation is quick and low cost.
4. Expandable. A network with existing equipment can be easily expanded, while a wired network may require additional wiring.
5. Cost-effective. There is no cost for laying cables, especially when it comes to solid walls
6. Convenience. Access network resources from any location within the wireless coverage area

This freedom of movement offers several benefits to users in different work environments such as:

- Immediate access to patient information by the doctor or hospital staff.
- Simple real-time network access for consultation or audit.
- Improvement in accessing the database for supervisors such as: construction engineers, etc.
- Faster access to customer (buyer) information by sellers, resulting in faster and better service, as well as increasing customer satisfaction.
- Network access regardless of location for network administrators, avoiding any problems and providing support for users.
- Real-time access to study groups and students.

Also, some of the other benefits of the wireless network are: The ability to share materials, printers, scanners, as well as high-speed Internet.

2. Methods

Purpose: To understand and draw conclusions about the level of public information on the risks of attacks on

wireless networks, the security measures that can be taken and the applicability of these measures.

This study was conducted by means of a questionnaire consisting of 10 questions. The number of respondents is 200. In the following, the answers to each of the questions are analyzed, attached with the relevant tables and graphs.

Question no. 1: Your Age is?

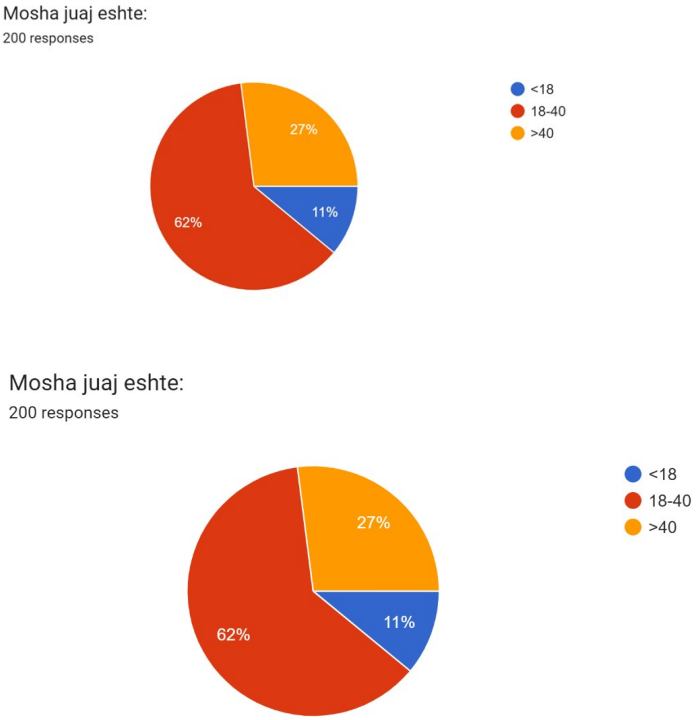

Figure 2-1 Question 1 report

The division into these 3 main age groups is done to judge who are more likely to have information and take action on wireless network security. These age groups include: minors, the most active online adults, and the least active.

11% of the respondents are minors, 27% are over 40 years old, while the rest of 62% are in the 18-40 years segment.

Question no. 2: The most frequent types of activities carried out online?

Nowadays, a number of online activities can be performed that save us time and money. On the other hand, some types of activities involve the exposure of general, personal or sensitive information that may be compromised in the event of an attack.

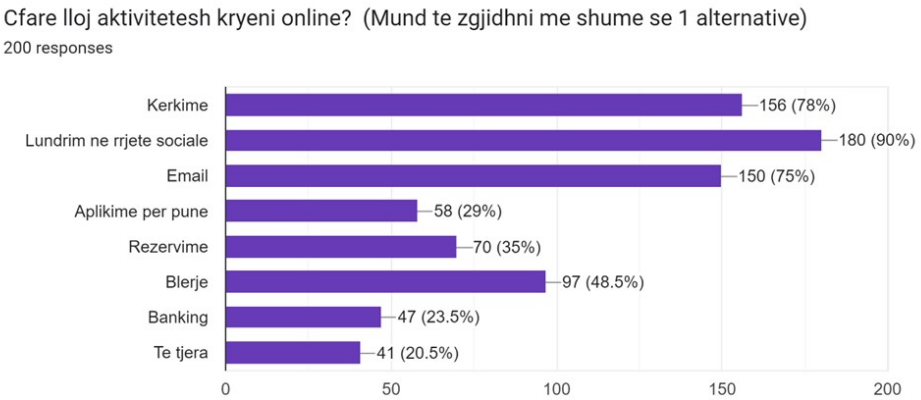

Figure 2-2 Question 2 report

In the table above we see a list of some of the possible activities and the corresponding percentages of their use by the respondents. We see that the most used activities are: Navigating social networks, Searches and

Emails, respectively with 90%, 78% and 75%.

Mainly, no personal or sensitive information is required from the user during searches, so this can be considered as one of the activities with the lowest risk. On the other hand, Shopping or Banking require very sensitive information and their websites have several layers of security. However, until a few years ago, users were quite averse to these services, while today the level of their use has increased significantly.

Question no. 3: Use of public wireless networks?

The use of public wireless networks brings higher exposure to various attackers. From the survey, we see that 86% of the respondents use these wireless networks, while 14% do not. So, 172 of the 200 individuals interviewed are users of these networks and are therefore even more vulnerable to attacks compared to the rest.

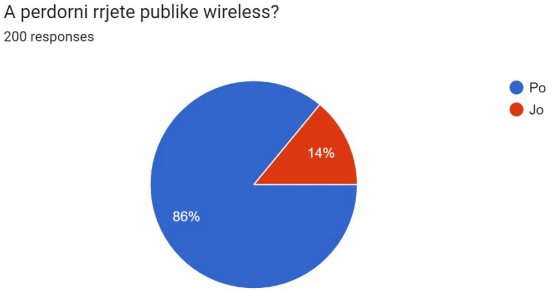

Figure 2-3 Question 3 report

In security matters we have mentioned open networks, WEP and WPA/WPA2/WPA3 and we have talked about their protection, how secure they are, etc. Questions 4, 5 and 6 are somewhat related to each other as in each one a type of wireless security is provided and respondents are asked to rate how secure they think they are. It is not without purpose that their ranking has not followed an ascending or descending order of security, but they have been placed irregularly in order not to give clues about the correct answer, but to have a somewhat more realistic picture of public information regarding wireless security . The questions serve to see how familiar users are with these terms, whether they know them and how safe they think they are.

Question no. 4: Trusted WPA/WPA2/WPA3 security level?

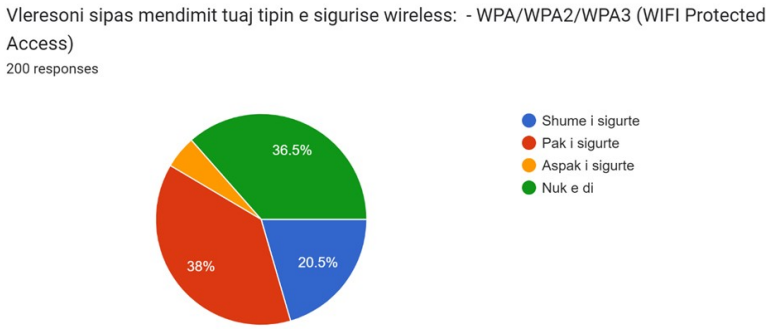

Figure 2-4 Question 4 report

From the graph above we see that 36.5% (or 73 people) do not know how secure they are or do not know the mentioned terms at all, 5% (or 10 people) have the wrong idea that these types of security are not secure at all and 38% think they are a little safe.

Only 20.5% had the correct idea that the mentioned terms are very safe and if we have been a little attentive we have seen them in the home internet modem or in the settings of our mobile phone or laptop at the moment we will connect it to this wireless.

Question no. 5: Trusted Open Wireless Network security level

We remind you that open wireless networks are those that do not have any security protocol implemented. When we try to connect to one of them, next to them we will notice the text "open" instead of "secure" and the lock icon will not be present.

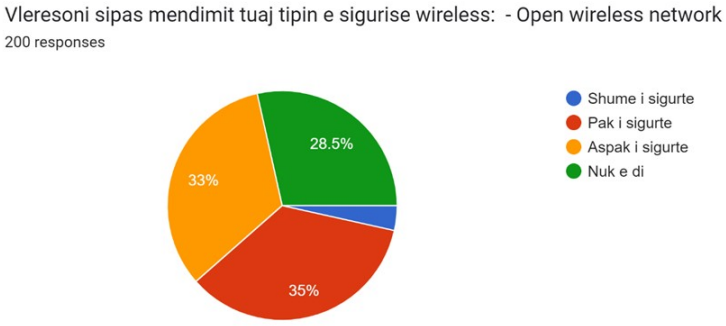

Figure 2-5 Question 5 report

35% of people who participated in the survey state that the Open Wireless Network is somewhat secure, followed by 28.5% of respondents who have no knowledge and 3.5% who think that it is very secure. While the rest of 33% have the correct idea that the type of security in question is not safe at all.

Question no.6: Trusted WEP security level

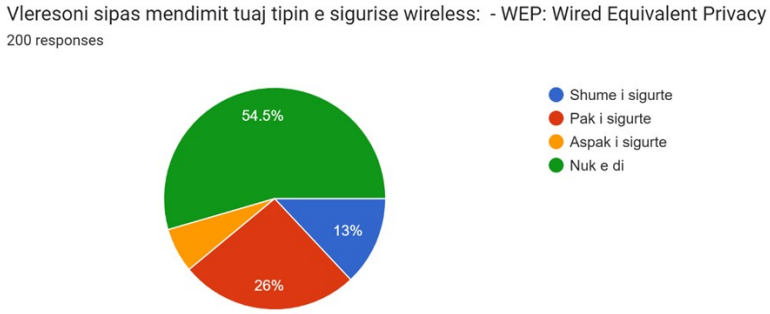

Figure 2-6 Question 6 report

More than half of the people surveyed, 54.5%, have no knowledge of WEP. 13% answered that WEP is very secure and 6.5% that it is not secure at all. Both of these assumptions are wrong. In fact, WEP offers minimal protection and is better than "nothing," so only 26% correctly answered that WEP is somewhat secure.

Question no.7: Information on computer attacks

Figure 2-7 Question 7 report

Information on attacks is extremely necessary in security matters. But in order to protect ourselves, we must first know what to protect ourselves from. If users don't know the consequences of unprotected navigation, then there is no reason for them to take action.

From the survey we noticed that 17% do not have any information on network risks, while the majority of 69% have little information. Only 14% declare that they are well informed on this issue.

Question no.8: Information on security measures against attacks

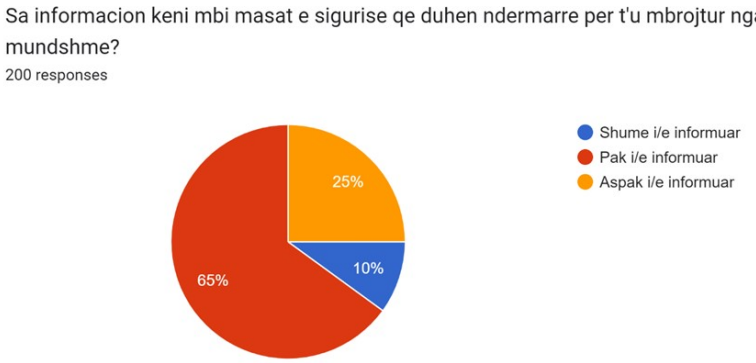

Figure 2-8 Question 8 report

There are indeed many types of attacks, but there are many measures that can be taken to prevent them. The lack of information in this aspect increases to 25% of the people surveyed. Only 10% have sufficient information about the security measures to be taken to protect themselves, while the remaining 65% have little information.

Question no.9: Information on security measures against attacks

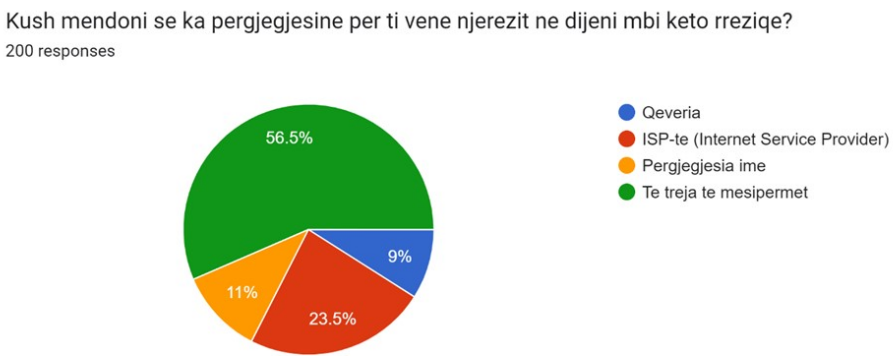

Figure 2-9 Question 9 report

This question is designed to see who users think is responsible for not being informed about potential dangers in wireless networks. We see that 23.5% of people think that ISPs, i.e. those that enable internet service, have the duty to inform their users about these risks. 9% think that information should be provided by the government, while the remaining 11% see obtaining information as a personal responsibility.

More than half, 56.5% state that the responsibility should fall on all three alternatives; government, ISPs but also on the user himself.

Question no.10: Security measures against attacks

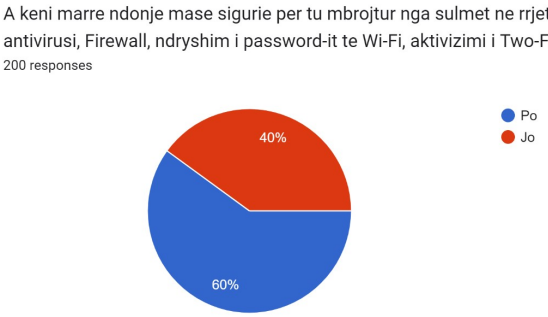

Figure 2-10 Question 10 report

Of the people surveyed, 60% of them considered it reasonable to take some security measures to protect themselves from malicious attacks on wireless networks, while the rest declared that they did not take any protective measures.

Measures taken by persons may include: Antivirus activation; Firewall; Changing the default password, and frequent Wi-Fi password changes; Two-Factor Authentication; Using VPN (Virtual Private Network) to access email when outside the work environment; Other security measures offered by ISPs (Internet Service Providers).

3. Conclusions

In addition to the above conclusions, we can draw some others that come from combining the answers to the questionnaire and observing the individual answers. It is noted that:

- People younger than 18 have little or no information about the risks and measures that can be taken for network security.
- Respondents over the age of 40 have little or no information on the dangers of the network and its protective measures.
- The majority of individuals who state that they have not taken any security measures for wireless network protection belong to one of the above age groups.
- Only 10% of people who send financial information online use security measures.
- 29% send online documents containing personal data (eg in job applications)
- Despite the fact that 11% of respondents think that it is only their responsibility to obtain information on risks and safety measures, only 2 people out of 22 have actually asked for this type of information.

It is recommended that the types of information mentioned above on the risks of using wireless networks and measures to protect against attacks, be made widely available by ISPs (Internet Service Providers), but also by the relevant state institutions competent for security. This would lead to a higher awareness among people of the need for security, which would lead to a greater applicability of protective measures, not only in company workplaces, but also at home and on public wireless networks. .

References

1. Scalable VoIP Mobility Integration and Deployment 1st Edition - July 30, 2009, Author: Joseph Epstein
2. Fixed/Mobile Convergence and Beyond Unbounded Mobile Communications 1st Edition - October 9, 2008, Author: Richard Watson
3. Advances in Computers 1st Edition - March 13, 2010, Editor: Marvin Zelkowitz
4. Wireless Communications & Networking 1st Edition - June 13, 2007, Author: Vijay Garg
5. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
6. https://www.gartner.com/en/information-technology/glossary/wimax-worldwide-interoperability-for-microwave-access