NIPES

Journal of Science and Technology Research

Journal homepage: www.nipesjournals.org.ng

A Conceptual Examination of Computer Networking Using Wireless Network

[1]Nwelih, E. and [2]Oghenekaro, L. U.

[1]emmanuel.nwelih@uniben.edu [2]Linda.oghenekaro@uniport.edu.ng
[1]Department of Computer Science, University of Benin, Benin City, Edo State, Nigeria
[2]Department of Computer Science, University of Port Harcourt, Rivers State Nigeria

Article Info

***Keywords*:**
Network; Wireless; Wi-Fi; Communication; Ethernet

Received 29 February 2022
Revised 16 March 2022
Accepted 27 March 2022
Available online 30 March 2022

https://doi.org/10.37933/nipes/4.1.2022.27

https://nipesjournals.org.ng

Abstract

Computer industry has made spectacular progress in short time. During the first two decades of their existence. Computer systems were highly centralized, usually within the single large room. The merging of computers and communications has had a profound influence on the way computer systems are organized. The old model of a single computer serving all of the organization computational need has been replaced with a large number of separate but interconnected computers to do the job and these are called computer network [1]. The study is based on computer networking using wireless network. The study aims to provide an overview of computer networking with more emphasis on wireless networks, while covering all the types of wireless network that exists, including their structure and components. The research information and data was elicited from residents of Ovia North East Local Government, Edo State as a case study due to easy assessment. This study was conducted to critically examine the concept of computer networking using wireless network. The study delved into the concept and structure of computer networking and wireless network. The study also critically assessed connection types in computer networking, organizational computational methods, network security and surveillance. The findings revealed wireless network constitute security threats in computer networking.

1. Introduction

The invention of the computer and the subsequent creation of communication networks can be hailed at the most significant accomplishment of the 21st century. This invention has transformed the way in which communication and information processing takes place. The network functionality of computer systems has been exploited by the government, businesses, and individual with immense benefits being reaped by all [2]. A network is a group of two of more computer systems sharing services and interacting in some manner. This interaction is, accomplished through a shared communication link, with the shared components being data. A network is a collection of machines which have been linked both physically and through software components to facilitate communication and the sharing of information. [3], defines computer network as a collection of computers, printers and other equipment that is connected together so that they can communicate with each other. [4], defines computer network as a system of interconnected computers and computerized peripherals such as printers which facilitates information sharing among them. Computer networks are made up of interconnected computing devices which communicate with each other and these networks are categorized by their sizes. The smallest is the Personal Area Networks (PANs) which extend to a few meters and connect adjacent devices together. Wireless PANs make use of technologies such as Bluetooth to replace cabling as data is moved from device

to device. Local Area Networks (LANS) extend from a few hundred meters to a few kilometers and they were designed to cover buildings which are close together or large facilities. Wireless LANs are implemented in facilities such as campuses and busy business locations. Metropolitan Area Networks (MANs) connect different buildings and facilities within a city. These networks mostly make use of wired connections with fiber optic transmissions providing the fastest speeds. The biggest networks are Wide Area Networks (WANs) which connect cities and countries together and they typically make use of fiber-optic cables which operate at speeds of up to 40Gbps. Networking is referred as connecting computers electronically for the purpose of sharing information [5]. Basically, networking consists of hardware component such as computer, hubs, switches, routers and other devices which form the network infrastructure. [6], defines wireless networks as networks that uses radio waves to connect devices, without the necessity of using cables of any kind. The term 'wireless network' refers to two or more computers communicating using standard network rules or protocols, but without the use of cabling to connect the computers together. Instead, the computers use wireless radio signals to send information from one to the other. A wireless local area network (WLAN) consists of two key components: an access point (also called a base station) and a wireless card. The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling.

Wireless networks have been a crucial part of communication in the last few decades and a truly revolutionary paradigm shift, enabling multimedia communications between people and devices from any location. Early users of wireless technology primarily have been the military, emergency services, and law enforcement organizations [7]. As the society moves toward information centricity, the need to have information accessible at anytime and anywhere takes on a new dimension. With the rapid growth of mobile telephony and networks, the vision of a mobile information society is slowly becoming a reality. It is common to see people communicating via their mobile phones and devices. With today's networks and coverage, it is possible for a user to have connectivity almost anywhere. In all forms of communication, security is of vital importance. Securing a network is a challenging task since hardware and software keep evolving and as old threats are overcome, new ones keep presenting themselves. Security implementations of a previous year may therefore not be able to effectively handle the threats being presented in the current years. Wireless networks are prone to a number of security risks and the most significant one is wireless eavesdropping [8]. Due to their wireless nature, it is easier to eavesdrop on them than it is with wired networks. [9], elaborate that wireless networks are more vulnerable to eavesdropping than wired networks because "access to the network can be gained by proximity rather than a direct physical contact". With wireless networks, an intruder simply has to set up his equipment in the area where the wireless signals are being transmitted and from there he can access packets that are intended for other devices in the network. By using a network sniffer, an intruder can capture all network traffic and try to decipher the information contained in the packets [8].

1.1.Merits of Wireless Network

Wireless networking is potentially a quick, easy and economical alternative that works between nodes and is executed without the use of wires around our home or office. It also opens up possibilities for connecting buildings which are up to several kilometers apart. It offers consistent and effectual keys to a number of instant applications therefore at present it is used under numerous diverse platforms such as health care, education, finance, hospitality, airport, and retail. The usage of wireless network increases day by day, because it has significant impact on the world. [7] Summarized the benefits of wireless networks as follows:

i. User can move about and get access to the wireless network while working at an outdoor location.

ii. User can send information over the world using satellites and other signals through wireless networks.
iii. Allows LANs to be deployed without cabling, potentially reducing costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless networks.
iv. Wi-Fi silicon pricing continues to come down, making Wi-Fi a very economical networking option.
v. Wi-Fi products are widely available in the market. Different brands of access points and client network interfaces are interoperable at the basic level of/service.
vi. Wi-Fi networks support roaming, in which a mobile client station such as a laptop can move from one access point to another as the user moves around in the building areas.
vii. It is relatively easier to set up a wireless network infrastructure
viii. Expansion of an existing network is easy since connectivity is already available within the range of the access point.
ix. The mobility of wireless networks

1.2.Demerits of Wireless Network

i. Power consumption is fairly high, making battery life and heat a concern.
ii. The most common wireless encryption standard, Wired Equivalent Privacy or WEP has been shown to be breakable even when correctly configured.
iii. Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g standard with a stock antenna might have a range of 45 Meters (Indoor) and 90 Meters (outdoor).
iv. Wi-Fi networks can be monitored and used to read and copy data (including personal information) transmitted over the network when encryption is not enabled.
v. The frequency which 802.11b and 802.11g operates is 2.4GHz which can lead to interference with cordless phones in the super high frequency range.
vi. Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications.

1.3.Working of Wireless Networks

The typical Wi-Fi setup contains one or more Access points (APs) and one or more clients. AP broadcasts its SSID (Service Set Identifier, Network Name) via packets that called beacons, which are broadcasted every 100ms. The beacons are transmitted at 1 Mb/s and are relatively short and therefore are not of influence on performance. Since 1Mb/s is the lowest rate of Wi-Fi it assures that the client who receives the beacon can communicate at least 1Mb/s. Based on the settings (e.g. the SSID), the client may decide whether to connect to an AP. Also the firmware running on the client Wi-Fi is of influence. Wi-Fi uses spectrum near 2.4 GHz, which is a standardized and unlicensed by international agreement [10].

1.4.Wireless Security

1.4.1. **Wired Equivalent Privacy (WEP):** is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physical of their structure, having some or all part of the network inside a building that can be protected from unauthorized access [11]. WLANs, which are over radio waves, do not have the same physical structure and therefore are more

vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security [12]**.**

1.4.2. **Wi-Fi Protected Access (WPA and WPA2):** is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi- Fi Alliance to secure wireless computer networks [11]. This protocol was created in response to several serious weaknesses researchers had found in the previous system. The WPA protocol implements the majority of the IEEE802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. Specifically, the Temporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP could be implemented on pre-WPA Wireless Network Interface Cards that began shipping as far back as 1999 through firmware upgrades. Because the changes required fewer modifications on the client than on the Wireless Access Point, most pre-2003 APs could not be upgraded to support WPA with TKIP. Researchers have since discovered a flaw in TKIP that relied on older weaknesses to retrieve the key stream from short packets to use for re-injection and spoofing. The later WPA2 certification mark indicates compliance with an advanced protocol that implements the full standard. Products that have successfully completed testing by the Wi-Fi Alliance for compliance with the protocol can bear the WPA certification mark [13]

1.5. Gap in the Literature

Despite the fact that research has been carried out on computer networking and wireless network, however there is no much direct empirical work available on the research topic in Nigeria, hence this paper intends to fill that gap. The outcome of the study would also help enlighten the government and various institutions on the significance of computer networking using wireless network, and to acknowledge how wireless network can be utilized to enhance various changes in the contents, methods and overall quality of computer networking thereby ensuring optimum utilization.

2.0. Methodology

The descriptive survey method was used to carry out this study. The opinion of respondents of the study population was sought because a survey research is interested in accurately assessing the characteristics of the population through the study of a sample considered to be a full representation of the population. The researcher used the modified likert four points scale of measurement for the purpose of this study. This is shown below to include the following option used in responding to the questionnaire. Strongly agree (SA) - 4, Agree (A) - 3, Disagree (D) - 2 and Strongly Disagree (SD) - 1.

2.1. Population of the Study: The population of this study comprised of all residents of Ovia North East Local Government Area in Edo State.

2.2. Sampling Technique and Size: The sample for this study was drawn from the population of all residents of Ovia North East LG. Questionnaires are to be administered to one hundred (100) residents randomly selected from the Local Government.

2.3. Research Instrument: The instrument used for data collection was a self-developed questionnaire. The questionnaire was designed to determine the frequency of responses.

2.4. Validity of Research Instrument: For the purpose of this study, the face and content validity of the instrument was carried out by the supervisor and experts in the field. The content of the questionnaire was assessed to determine whether items generated were relevant to the objective of the research.

2.5. Method of Data Collection: The questionnaires were distributed to residents of the local government by the researchers. While administering the questionnaire to the randomly selected residents, appeals were made to each of the respondents to complete the questionnaire accurately and honestly. Complete questionnaire were collected back on the spot.

2.6. Method of Data Analysis: This research employed descriptive statistical; charts, simple percentages and mean to analyze and interpret data collected. The statistical mean scores were used in analyzing the four-point questionnaire while the frequency count and simple percentage are to be used in analyzing respondents' characteristics.

2.7. Analysis of Data Collected from Respondents: The data collected for this study was analyzed using the simple percentages statistical technique.

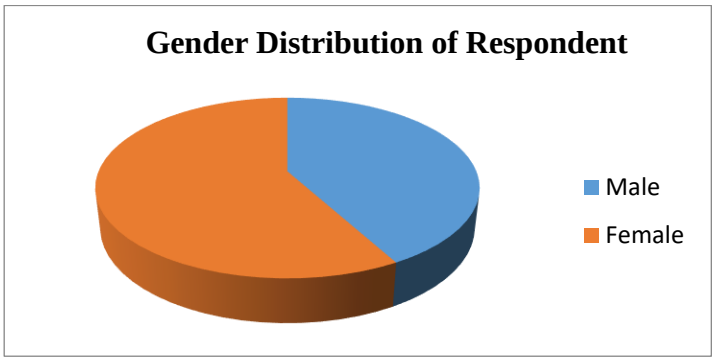

Figure 1: Distribution of respondents

Figure 1 shows the gender distribution of respondent. 42% of respondents were male while the remaining 58% were female.

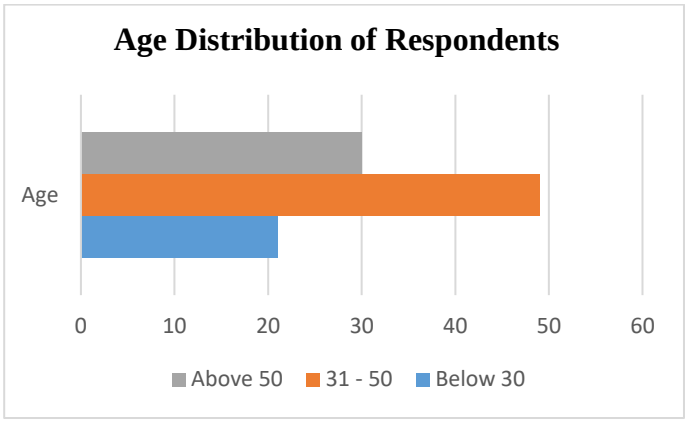

Figure 2: Age distribution of respondent

Figure 2 shows the age distribution of respondent. 21% of respondents were below age 30 while 49% were between the age bracket of 31 and 50, the remaining 30% were above 50.

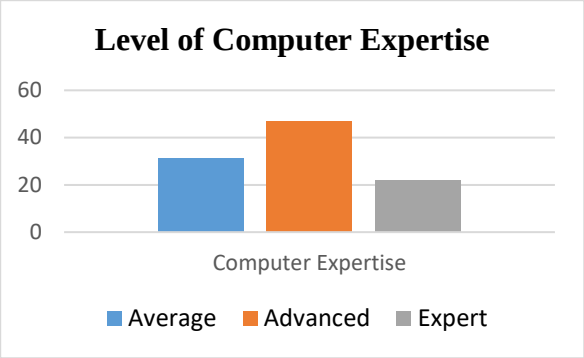

Figure 3: Computer expertise

Figure 3 shows the level of computer expertise of respondent. 31% of respondents are average, 47% are advanced and 22% are expert.

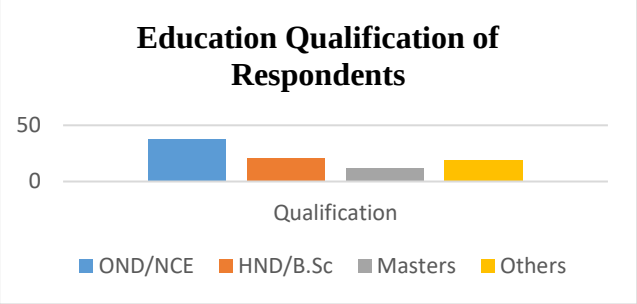

Figure 4: Qualification of respondents

Figure 4 shows the educational qualification of respondent. 38% of respondents were OND/NCE holders, 21% were HND/B.Sc holders. 12% were Masters holders while the remaining 19% were holders of other educational qualification.

3.0. Questionnaire Analysis

Table 1: Accessing the computer system and passwords

S/N	Variables	SA	A	D	SD	Mean
1.	People use the same password to access multiple systems/applications	33 (33%)	61 (61%)	4 (4%)	1 (1%)	3.24
2.	People do write passwords down	32 (32%)	58 (58%)	8 (8%)	2 (2%)	3.2
3.	People write their username/passwords in an electronic file (e.g. Word document)	2 (2%)	44 (44%)	46 (46%)	8 (8%)	1.91
4.	People use software to keep track of their passwords (e.g. Internet Explorer password manager, Firefox password manager, Password manager, Google Chrome etc.	41 (41%)	51 (51%)	5 (5%)	3 (3%)	3.3
5.	People share their password(s) with other people	24 (24%)	47 (47%)	18 (18)	11 (11%)	2.84
6.	People use a password protected screensaver	63 (63%)	22 (22%)	8 (8%)	7 (7%)	3.41
7.	People use a screen lock	40 (40%)	59 (59%)	1 (1%)	0 (0%)	3.39

Source: Analysis of Survey data 2022.

Table 1 shows the responses on accessing the computer system and passwords. For item 1, 33% and 61% of the respondents showed strong agreement and agreement to the statement that people use the same password to access multiple systems/applications, obtaining a mean score of 3.24. For item

2, 32% and 58% of the respondents strongly agree and agree with the statement that people write their passwords down, obtaining a mean score of 3.2. For item 3, 44% of the respondents agreed while 46% disagreed that people keep their username/passwords in an electronic file, obtaining a mean score of 1.91. For item 4, 41% and 51% of the respondents strongly agreed and agreed with the statement, the obtained mean score of 3.3 showed that the respondents agreed with the statement that people use software to keep track of their passwords. For item 5, 24% and 47% of the respondents strongly agreed and agreed with the statement. The mean score of 2.84 obtained showed that people share their password(s) with other people. For item 6, 63% and 22% of the respondents strongly agreed and agreed with the statement that people use a password protected screensaver with a mean score of 3.41. For item 7, 40% and 59% of the respondents strongly agreed and agreed with the statement that people use a screen lock with a mean score of 3.39.

Table 2: Security settings of the computer

S/N	Variables	SA	A	D	SD	Mean
8.	People install an anti-virus program on their computer	43 (43%)	42 (42%)	15 (15%)	0 (0%)	3.28
9.	People update their anti-virus program on a regular basis (newer versions of the program are installed, etc.)	33 (33%)	38 (38%)	16 (16%)	13 (13%)	2.91
10.	People have firewall installed on their computer	21 (21%)	29 (29%)	28 (28%)	21 (21%)	2.48
11.	People use anti-spyware tools (e.g Max Spyware Detector, Ad-Aware SE, etc.) on their computer	15 (15%)	20 (20%)	35 (35%)	28 (28%)	2.18

Source: Analysis of Survey data 2022

Table 2 shows the responses on security settings of the computer. For item 8, 43% and 42% of the respondents strongly agreed and agreed with the statement that people install an anti-virus program on their computer. A mean score of 3.28 was obtained. For item 9, 33% and 38% of the respondents strongly agreed and agreed with the statement respectively. This had a mean score of 2.91 which shows an agreement with the statement that people update their anti-virus program on a regular basis**.** For item 10, 29% and 28% of the respondents agreed and disagreed with the statement that people have firewall installed on their computer. For item 11, 35% and 28% of the respondent disagreed and strongly disagreed with the statement. The mean score was 2.18 showing that the respondents disagreed with the statement that people use anti-spyware tools on their computer.

Table 3: System maintenance and downloading software

S/N	Variables	SA	A	D	SD	Mean
12.	People update/upgrade the software on their computer (e.g. Windows, Internet Explorer, Microsoft Office, etc.) on a regular basis	18 (18%)	15 (15%)	37 (37%)	30 (30%)	2.21
13.	People install software that they downloaded from the Internet for free (Freeware or Shareware)	34 (34%)	39 (39%)	15 (15%)	12 (12%)	2.95

Source: Analysis of Survey data 2022.

Table 3 shows the responses on security maintenance and downloading software. For item 12, 37% and 30% of the respondents disagreed and strongly disagreed to the statement that people update/upgrade the software on their computer on a regular basis. In response to item 13, 34% of the respondents strongly agreed and 39% agreed with the statement. A mean of 2.95 shows an agreement to the statement that people install software that they downloaded from the Internet for free.

Table 4: Electronic Mail

S/N	Variables	SA	A	D	SD	Mean
14.	People Email program have an Email spam filter (also known as "bulk Email" or "junk Email" filter)	30 (30%)	64 (64%)	5 (5%)	1 (1%)s	3.23
15.	People open Emails if they don't know who the sender is	44 (44%)	48 (48%)	7 (7%)	1 (1%)	3.35
16.	People open Email attachments even if they don't know who the sender is	52 (52%)	43 (43%)	4 (4%)	1 (1%)	3.46
17.	People use encryption when sending Email	6 (6%)	9 (9%)	48 (48%)	37 (37%)	1.84

Source: Analysis of Survey data 2022.

Table 4 shows the responses on electronic mail. For item 14, 30% and 64% of the respondents showed strong agreement and agreement to the statement that people Email program have an Email spam filter. A mean of 3.23 was obtained. For item 15, 44% and 48% of the respondents strongly agreed and agreed with the statement that people open Emails if they don't know who the sender is. A mean of 3.35 was obtained. Responses on items 16 show that 52% and 43% of the respondents strongly agreed and agreed with the statement. In response to item 17, 48% and 37% of the respondents disagreed and strongly disagreed to the statement that people use encryption when sending Email.

Table 5: Remote access and working from home

S/N	Variables	SA	A	D	SD	Mean
18.	People use remote access (dial in, wireless system, cable, satellite) to access their organization's network	31 (31%)	29 (29%)	23 (23%)	17 (17%)	2.64
19.	People secure their wireless network connection (e.g. encryption enabled or access restriction) when using wireless network at home	5 (5%)	9 (9%)	51 (51%)	35 (35%)	1.82
20.	People use a VPN (Virtual Private Network) to connect to their organization's network when working from home	3 (3%)	5 (5%)	62 (62%)	30 (30%)	1.81
21.	People share their computer with others (spouse, family, friends, etc.) when using their computer at home	54 (54%)	38 (38%)	5 (5%)	3 (3%)	3.43

Source: Analysis of Survey data 2022.

Table 5 shows the responses on remote access and working from home. For item 18, 31% and 29% of the respondents strongly agreed and agreed with the statement. The mean score was 2.64 showing that the respondents agreed with the statement that people use remote access to access their organization's network. In response to item 19, 51% and 35% of the respondents disagreed and strongly disagreed to the statement that people secure their wireless network connection when using wireless network at home. For item 20, 62% and 30% of the respondents disagreed and strongly disagreed to the statement that people use a VPN to connect to their organization's network when working from home. For item 21, 54% and 38% of the respondents showed that they strongly agreed and agreed. The mean score of 3.43 shows a strong agreement with the statement that the people share their computer with others when using their computer at home.

Table 6: Sharing your computer and social networking

S/N	Variables	SA	A	D	SD	Mean
22.	People allow others to use their computer at the work place	31 (31%)	29 (29%)	23 (23%)	17 (17%)	2.64

23.	People are part of a social or professional networking site (e.g. Myspace, Facebook, LinkedIn etc)	46 (46%)	39 (39%)	15 (15%)	0 (0%)	3.31
24.	People's social page or blog contain personal information (Email-address, telephone number etc)	37 (37%)	34 (34%)	17 (17%)	12 (12%)	2.96
25.	People use a secure (encrypted) connection (for example Secure Shell software) when uploading information (files etc.) to the Internet (your website, your webpage, your blog, your company's network, etc.)	3 (3%)	5 (5%)	31 (31%)	57 (57%)	1.46

Source: Analysis of Survey data 2022.

Table 6 shows the responses on sharing your computer and social networking. For item 22, 31% and 29% of the respondents strongly agreed and agreed with the statement. The mean score was 2.64 showing that the respondents agreed with the statement that people allow others to use their computer at the work place. For item 23, 46% and 39% of the respondents strongly agreed and agreed respectively with the statement that people are part of a social or professional networking site. A mean score of 3.31 was obtained. A total of 37% of the respondents and 34% strongly agreed and agree with item 24, with a mean response score of 2.96 showing an agreement with the statement that People's social page or blog contain personal information. For item 25, 31% and 57% of the respondents disagreed and strongly disagreed to the statement that people use a secure connection when uploading information to the internet.

Table 7: Computer and Information Security Risks

S/N	Variables	SA	A	D	SD	Mean
26.	Spyware and adware are software programs that quietly sit on people computer and can deliver pop-ups or other advertisements to them. Based on this description, do you think people have any spyware or adware on their computer right now	34 (34%)	39 (39%)	15 (15%)	12 (12%)	2.95
27.	A phishing scam means that someone or a website tries to get personal information from people, for example by accidently signing into a website or filling out a form placed on web site? Have you, or do you believe people have fallen victim to a phishing scam	26 (26%)	28 (28%)	23 (23%)	23 (23%)	2.57

Source: Analysis of Survey data 2022.

Table 7 shows the responses on computer and information security risks. In response to item 26, 34% of the respondents strongly agreed and 39% agreed with the statement. A mean of 2.95 shows an agreement to the statement that people have any spyware or adware on their computer. For item 27, 26% of the respondents strongly agreed and 28% agreed with the statement. A mean score of 2.57 was recorded

3.1. Discussion of Findings

From the findings of research work of [1] and [2] were they presents an overview of wireless local-area networks (LANs) and wireless personal area networks (PANs), with emphasis on the two most popular standards: IEEE 802.1 1, and Bluetooth. It was noted that in spite of their merits, there are a few significant issues with wireless networks which are primarily: quality assurance and security issues. Our research findings showed similarities, in the areas of the analysis on computer networking using wireless network, it can be inferred from Table 1 that people use the same password to access multiple system application and they write such password down. Although people don't write their username/password in an electronic file, people use different software's to keep track of their passwords. Also, people use screen lock and password protected screensaver but also share their password with others. In Table 2, it can be deduced that people install anti-virus program on their computer, update such program on a regular basis but don't have firewall and anti-spyware tools installed on their computer. From Table 3, it can be assumed that people don't

upgrade/update the software on their computer on a regular basis and install software they downloaded for free. In Table 4, it can be induced that email program have a spam filter and people don't use encryption when sending email. Also, people open emails and download email attachment even if they don't know the sender of such email. From Table 5, it can be concluded that people use un-encrypted remote wireless network to access their organization network and share their computer with others when working from home. In Table 6, it can be summarized that people allow others to use their computers at the work place, are part of a social or professional networking site and their social page or blog contain personal information. From Table 7, it is deduced that people have spyware or adware on their computers and it is believed that people have once or twice fallen victims to a phishing scam.

3.2. Summary of Findings and Conclusion

Arising from data analyses, the major findings of the study are:

1. Wireless network constitute security threats in computer networking
2. People use un-encrypted remote wireless network

The study was conducted to critically examine the concept of computer networking using wireless network. The study delved into the concept and structure of computer networking and wireless network. The study also critically assessed connection types in computer networking, organizational computational methods, network security and surveillance. The findings revealed wireless network constitute security threats in computer networking.

4.0. Conclusion and Recommendations

Based on the above findings the following recommendations for improvement are:

Use strong passwords: Passwords shouldn't be repeated on different sites, and changed regularly. Passwords should be complex (i.e. using a combination of at least 10 letters, numbers, and symbols). A password management application can help keep passwords locked down. Strong passwords that can't be easily guessed and not recorded anywhere or a reputable password manager to generate strong passwords randomly should be used.

Software should be updated: This is important with operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in a software to gain access to a computer. Patching those exploits and flaws can make it less likely that to become a target.

Manage social media settings: Personal and private information should be locked down. Social engineering cybercriminals can often get personal information with a few data points, so the less shared publicly, the better.

Strengthen the home network: A strong encryption password as well as a virtual private network should be used. A VPN will encrypt all traffic leaving the computer until it arrives at its destination.

Never open attachments in spam emails: A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

Secure the computer: Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers. Anti-virus/malware software prevent viruses from infecting the computer by installing and regular update. Anti-virus software can scan, detect and remove threats before they become a problem. Anti-spyware software prevent spyware from infiltrating the computer.

References

[1] Ramiro, J., and Abdallah, C. T. (2002), "Wireless communications and networking: an overview", IEEE Antenna's and Propagation Magazine, 44 (1): 185-193.

[2] Nassar, E., and Muhanna, G. H. (2013). "Computer Wireless Networking and Communication" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8,

[3] George, M., Silviv, F., Teodora, S., and Liviu, M. (2015) "Communication in Cyber-Physical Systems" 19th International Conference on System Theory, Control and Computing (ICSTCC), October 14 – 16, Cheile Gradistei, Romania IEEE
[4] Tutorialpoint (2014). Learning DCN, Data Communication, Computer Network. Pp 1 – 6 https://www.tutorialspoint.com
[5] Saravanan, Anna Malai (2012), "Introduction to Networking", https://www.researchgate.net/publication/323511648
[6] Jordi Salazar (2017). "Wireless Networks", TechPedia European Virtual Learning Platform for Electrical and Information Engineering http://www.techpedia.eu
[7] Robert, M. M., and David, R. B. (1999). "Ethernet: Distributed Packet Switching for Local Computer Networks" Communications of the ACM. 19 (5): 395–404.
[8] Chenoweth, T., Robert, M., and Sharon, T. (2010). "Wireless Insecurity: Examining User Security Behavior on Public Networks", Communications of the ACM, 53(2): 134-138.
[9] Schmidt A., Lian S. (2009). Security and Privacy in Mobile Information and Communication Systems, Springer, Boston.
[10] Jochen, H. S. (2003). Mobile Communications Addison-Wesley, ISBN0321123816, 9780321123817
[11] Conklin, W. D., Williams, G. White, R. Davis, C. and Cothern (2004). "Principles of Computer Security," McGraw Hill Technology Education.
[12] Deng, J., Varshney, P.K., and Haas, Z.J. (2004) "A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function," Proc. Of Communication Networks and Distributed Systems Modeling and Simulation (CNDS), January 2004.
[13] Kumar, A. (2010). "Evolution of Mobile Wireless Communication Networks: 1G to 4G", International Journal of Electronics & Communication Technology, 1(1): 68-72.