Wireless Technology Security

Trey Bourgeois

Tony Griffin

Information Security - ISSC422

06/02/2019

**Wireless technology security.**

**Introduction**

 Wireless technology has become part and parcel of many people lives today. With the increased use of social media sites, the wireless technology has seen a great tremendous number of people using it for their personal purposes. People today cannot imagine living lives that are out of wireless technology due to the regular advancement of technologies and the benefit they accrue from them (Wang et al.,2014). Many businesses today rely on the wireless technology devices to conduct their day to day businesses. With wireless technology it is possible to transfer data as well as voices over a long distance from one location to the other.

**Statement of the problem**

Many people enjoy the advantages brought about by the wireless technology but end up forgetting the security concerns that are associated with the wireless technology. People need to take caution when using the wireless technology as a result of the security concerns brought about by the media. Over the past, the wireless technologies have been faced with security challenges but few could identify the consequences brought about by the threat.

**Topic overview**

 Wireless technology is the technology that has made it possible for us communicate easily amongst ourselves easily without having to use cables or wires. On the other hand, wireless technology security is the prevention measures that need to be put in place in order to protect illegal access or damage to information and communication technology devices such as computers by the aid of wireless networks that are common among many people in our societies today. With wireless technology it is possible to communicate with people who are further away from us with much ease (Kim & Garrison,2009).

**Wireless technology security threats.**

There are various threats to wireless technology security. Some of the threats to wireless technology security include the following:

Hackers and crackers are the main threat in the wireless network due to their abilities as well as their illegal activities. The number of hackers attacking wireless networks has been growing over the years due to the increase use of the wireless technology devices as well as the networks that we have within our homes. Hackers may use the network and pretend to be access networks only to give services to innocent people who may end up putting users to a network to a risk of losing their networks to a fake access point in a network (Rappaport,1996).

Unprotected wireless networks are dangerous since they are open to the public and some individuals within the community may choose to have ill intention and use the wireless technology wrongly to damage the reputations of others as well as to share viruses to the users of a network who may end up losing their important data. Virus attacks may end up clocking the computers used in unprotected network accessible for all. Networks need to be protected from all the public access, for the network to be protected, unique usernames together with long passwords is required to be used and to be changed regularly for security purposes.

Unauthorized access to wireless technology devices is another threat thus the data losing its confidentiality. Data need to be protected from illegal access by unauthorized users and their confidentiality should be protected when being transferred over a wireless technology. In addition, the data should be encrypted in a way that it will be hard for anyone to change any content that is made accessible to him unknowingly. Illegal access to a wireless technology can make a person easily commit cyber-crime and go against the laws that are in place today that protect the illegal access of users to a person’s data that is encrypted and stored in secret locations from illegal access by unauthorized users at regular times (Miller,2001).

**Relevance and significances**

 Without protection of our wireless technology networks it means we are exposing ourselves too much thus will be at risk of being attacked. Everything about our lives need to be protected and not everything should be shared to the public. With the use of the wireless technology people can access other people’s files as well as confidential personal pieces of information thus this might be dangerous due to the fact that we can be attacked easily without our knowledge or we may also lose the integrity of our information that should be kept out of public access. If some few individuals get our personal information, they may choose to change two or three things in the files thus damaging the integrity of a given piece of data. Having a good security basically means we are free from attacks that many people suffer due to the growth use of the social media sites as wireless technologies (Perrig, Stankovic & Wagner,2004).

**Conclusion**

Wireless technology security should be taken seriously by all and none should despise the threats brought about by the wireless technology and the advancement of technologies that we have today. A lot has to be done in order for the people to take the full responsibility of putting first their security first before the advantages that they receive from the use of the wireless technologies.

References

Kim, S., & Garrison, G. (2009). Investigating mobile wireless technology adoption: An extension of the technology acceptance model. Information Systems Frontiers, 11(3), 323-333.

Miller, S. K. (2001). Facing the challenge of wireless security. Computer, 34(7), 16-18.

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks.

Rappaport, T. S. (1996). Wireless communications: principles and practice (Vol. 2). New Jersey: prentice hall PTR.

Wang, C. X., Haider, F., Gao, X., You, X. H., Yang, Y., Yuan, D., ... & Hepsaydir, E. (2014). Cellular architecture and key technologies for 5G wireless communication networks. IEEE communications magazine, 52(2), 122-130.