Short Communication
Volume 11:4, 2022

International Journal of Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

The Impact of Mobile Gadgets on Cyber Security

Yu Zheng*

Department of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, Jiangsu, P.R China

Introduction

The widespread use of mobile devices is a feature of contemporary society, including workplace settings. The tremendous opportunities these gadgets present and their contribution to improved communication are credited for the rise in their use. However, there have been many concerns raised about the privacy of critical corporate data and personal information held on mobile devices in conjunction with the rise in their use. Mobile devices essentially have a big impact on cyber security since the kind of data that is stored and accessed on them increases the security concerns. Even if using mobile devices more frequently has many advantages, it also creates new cyber security problems, such as higher financial risks, data loss, and non-compliance issues. Today's society has made mobile devices become enticing platforms for communication to the point where they are increasingly used for storing and accessing both personal and business data. The introduction of near field communication for mobile payment services, notably in business, has expanded the use of the devices. As a result, individuals and organisations rely on these gadgets for both communication and financial transactions. In fact, it is predicted that the use of mobile devices will increase in the next years for a variety of reasons [1].

Description

The process of securing gadgets like computers, mobile phones, smartphones, and tablets, as well as the entire internet, is referred to as cyber security. Promoting cyber security is crucial in the present world because people are relying more and more on computer networks to store and send their private data and information. If there aren't enough cyber security measures in place; hackers and other cybercriminals could invade network users' privacy and empty their bank accounts because these sensitive personal data are available to computer networks. Businesses are not exempt from these online dangers. As a result, individuals and companies are paying close attention to improving cyber security in order to safeguard their private information and eliminate dangers. Mobile Devices' Effect on Cyber security the widespread use of mobile devices is a feature of contemporary society, including workplace settings. The tremendous opportunities these gadgets present and their contribution to improved communication are credited for the rise in their use. However, there have been many concerns raised about the privacy of critical corporate data and personal information held on mobile devices in conjunction with the rise in their use. Mobile devices essentially have a big impact on cyber security since the kind of data that is stored and accessed on them increases the security concerns [2].

These groups have used the recent increase in the use of mobile gadgets as justification for their actions. As a result, there are now twice as many personal devices at the workplace as there were a few years ago. While there are certain benefits to having more personal devices connected to corporate networks, the development has also increased security threats and cyber-attacks. According to a 2012 study on the impact of mobile devices on information security, over 60% of employees in companies that allow personal devices to connect to corporate networks have noticed an increase in security threats and cyber-attacks on their employers in recent years. Over 70% of employers view these mobile gadgets as security hazards. Post-industrial nations run the risk of having higher rates of mobile device cybercrime; in fact, in 2012, the top two nations reporting mobile device compromise were Hong Kong and Brazil, while the United States and Germany (while still vulnerable to attack) reported success in containing infections. The apps that users download onto a device are also subject to cyber security risks, in addition to the device itself. According to research, "96% of apps contain an average of 14 vulnerabilities per." Countries all throughout the world anticipate an increase in cyber-attacks (over 90 percent of British companies anticipate this) [3-5].

Conclusion

It is impossible to deny the contribution of mobile devices to the rise of cyber security. Cyber-attacks would not be on the rise without the increased creativity of technological engineers (89 a week in the US). While a result, there appears to be a connection between the two: as cyber security intensifies its efforts to safeguard mobile devices, cybercriminals intensify their attempts to penetrate their defences. This cycle appears to go on forever. There is only education and being a careful and informed mobile device user as a cure-all for cyber-attacks.

Cyber-attacks can be lowered by keeping devices updated, avoiding downloading solicitations from unidentified sources, and reading material related to personal gadgets. It is important to notice the advancements made in cyber security. The extensive usage of mobile devices tends to weaken corporate networks' cyber security, which could result in data theft and significant financial losses. The Bring Your Own Device (BYOD) policy, which allows employees to use their personal mobile devices to access the company network, poses a severe threat to cyber security an increasing proportion of personally owned mobile devices are connecting to business networks. The survey revealed that the BYOD policy presents the greatest obstacle to protecting business data.

Conflict of Interest

None.

References

1. Aydeger, Abdullah. "A moving target defense and network forensics framework for ISP networks using SDN and NFV." *Future Gen Comp Sys* 94 (2019): 496-509.
2. MacFarland, Douglas C. "The SDN shuffle: creating a moving-target defense using host-based software-defined networking." *Proceed Second ACM Workshop Mov Tar Def* (2015): 37-41.
3. Van Leeuwen, Brian. "Operational cost of deploying moving target defenses defensive work factors." IEEE Military Commu Conference (2015): 966-971.
4. Eskridge, Thomas C. "VINE: a cyber-emulation environment for MTD

***Address for Correspondence:** Yu Zheng, Department of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, Jiangsu, P.R China; E-mail: yzheng123@nuist.edu.cn*

Received: 02 April, 2022, Manuscript No. sndc-22-68694; **Editor Assigned:** 04 April, 2022, PreQC No. P-68694; **Reviewed:** 16 April, 2022, QC No. Q-68694; **Revised:** 21 April, 2022, Manuscript No. R-68694; **Published:** 28 April, 2022. DOI: 10.37421/2090-4886.2022.11.158

experimentation." *Proceed Second ACM Workshop Moving Target Defense* (2015): 43-47.

5. Shen, Tao. "Improve computer visualization of architecture based on the Bayesian network." *Comput Mater Continua* 58 (2019): 307-318.

How to cite this article: Zheng, Yu. "The Impact of Mobile Gadgets on Cyber Security." *J Sens Netw Data Commun* 11 (2022): 158. .