ANNOTATED BIBLIOGRAPHY

Arabo, A., & Pranggono, B. (2013, May). Mobile malware and smart device security: Trends, challenges and solutions. In *2013 19th international conference on control systems and computer science* (pp. 526-531). IEEE.

The manuscript elaborates on a study conducted to identify the developments and problems of cybersecurity on smartphone devices. The article assesses the growing demand for connectivity through wireless mechanisms to enhance internet access. The manuscript also states that because of the surge in smartphone use, an increase in threats towards users' data has also been witnessed. According to Arabo and Pranggono (2013), mobile malware is considered a significant threat to internet access by using smartphones. The article also discusses the effects of cybersecurity on devices along with the possible techniques of curbing the discussed problems. Lastly, the article also offers solutions such as accessing the available applications that assist in safeguarding data during internet access. As a result, the article can provide more information on the effects of mobile handsets on cybersecurity

Bell, R. (2015). *Digital steganography: Its impact on mobile forensics, hacking, and social media* (Doctoral dissertation, Utica College).

The article provides an assessment of the effects of mobile forensics, social media, and hacking. According to Bell (2015), digital steganography is one of the current advancements in the cybersecurity space, enhancing the aspect of encrypting sensitive information. Steganography, a software, enhances the concealing of crucial messages and data from unapproved users. Moreover, the application is compatible with any operating system on smartphones and computers. The article offers wide-ranging evidence on the extensive research the numerous approaches by hackers to access user data, and the vital roles of installing the application as a cybersecurity framework. Because the article assesses the significance of utilizing applications such as steganography to avert attacks, it may be utilized as a viable source of information in identifying the impacts of smartphones on cybersecurity.

Bertino, E. (2016). Security Threats: Protecting the New Cyber frontier. Computer, 49(6), 11-14.

The article states that cyber-attacks are on the increase each year, leading to a dependence on information and communication technology frameworks. According to Bertino (2016), mobile handsets require a robust defense mechanism due to fresh threats. The technological advancements in information and communication have led to the development of smartphones and cloud computing. The article also elaborates on the new cyber frontiers being used by corporations to secure their data and restrict access to delicate and essential data. According to Bertino (2016), various corporations continue to adopt the BYOD mechanism, allowing personnel to utilize personal devices to execute work-related responsibilities. The article also discusses vulnerabilities attributed to software, and the loopholes may be sealed by using metamorphic testing. As a result of the manuscript's information, it is plausible to affirm the information can be utilized in conducting the secondary research.

Dye, S. M., & Scarfone, K. (2014). A standard for developing secure mobile applications. *Computer Standards & Interfaces*, *36*(3), 524-530.

According to Dye and Scarfonr (2014), the article articulates the standards of establishing secure smartphone applications that may not be susceptible to cybersecurity threats. The manuscript starts by providing information on the number of security challenges that arise from the development of applications that expose users to cybersecurity threats. The applications are primarily developed by amateur programmers are not conversant with safeguarding mechanisms for the applications. The manuscript also elaborates on the appropriate mechanisms that should be employed to enhance security. This proves that the article is a viable resource for accessing information due to the author's experience and knowledge.

Gelenbe, E., Görbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., &Lyberopoulos, G. (2013). NEMESYS: Enhanced network security for seamless service provisioning in the smart mobile ecosystem. *In Information Sciences and Systems 2013* (pp. 369-378). Springer International Publishing.

The article explores the enhanced security system to develop the provision of seamless services in the mobile network. Since smartphones are popular, hackers are gradually exploiting weak links by installing malware that can tap into private data. According to Gelenbe et al. (2013), smartphones are highly utilized in launching scathing cyber- attacks. Moreover, the article states that the NEMESYS mechanism proves to be the best framework to avert the increased use of smartphones to carry out cyber-attacks. It also explores the various techniques employed to acquire private data. The key aspect discussed in the article is the NEMESYS mechanism, which creates an information collection structure for safeguarding mobile handsets. This is accomplished through the provision of warnings when a threat is detected.