doi: xxx/semj.xxx

Mobile Health and Its Security in the Face Cyber Attacks

B Vahidiataabadi [1,*]; M Abolverdi [2]; SJ Masoumi [3]

[1] Deputy Director, IT Incubator Center of Shiraz Medical of Sciences, Shiraz, Iran
[2] IT Expert, South-Area Management Industrial Organization, Shiraz, Iran
[3] Head, IT Incubator Center of Shiraz Medical of Sciences, Shiraz, Iran

[*] *Corresponding author:* B Vahidiataabadi, Deputy Director of IT Incubator Center in Shiraz Medical of Sciences, IT Incubator Center Building, Next to the Sina-Sadra Complex, Neshat St, Shiraz, Iran. Tel: +98-7132332771, E-mail: vahidiba@gmail.com

Received: 11 Dec 2016
Accepted: 01 Jan 2017
Epub: 23 Feb 2017
Ppub: 15 Jan 2018

Abstract

Background: Today, mobile phones are used as useful tools in medicine; however, the risks of using them have always been an important concern of doctors and the medical community. The aim of this study is to evaluate mobile device risks of being attacked in cyberspace and how to deal with them.
Objectives: As we know, mobile phones and other portable electronic devices, including laptops, tablets, and etc. are always one of the favorite targets for small theft. In addition to the financial value of them, they are good choices for online thieves and hackers to access medical databases and IT systems in the medical community. In this work, the author studies the risks of mhealth and the ways to deal with them. These approaches include strong encryption on mobile health systems and a distrust of the links in unknown emails.
Methods: This study is a review-analysis based on library sources and online articles. Data were collected using the resources available in PubMed-Medline, Springer, Magiran, and the Journal of Medical Internet Research. The results of the most common health risks were developed as an analytical method.
Results: The results showed that 'Medjacking' attacker or attackers to devices used in mobile health not only endanger the patient's health, but are also a threat to the security of information systems used in hospitals or health systems. The best approach to handle such a problem can be by choosing a strong password on the mobile device and using tools such as URL X-ray to open the contents of the emails.
Conclusion: Although, vast use of mobile devices in mhealth increases the risk of virtual attack, using a proper security system installed on the device can avoid this danger.

Keywords: mHealth; Security; Mobile; Information Systems; E-mail