A Review of Detection Methodologies for Quick Response code Phishing Attacks

Publisher: IEEE

Sikiru Subairu ; John Alhassan ; Shafii Abdulhamid ; Joseph Ojeniyi All Authors

Abstract: Recently, phishing attacks have taking a new dimension with the addition of quick response code to phishing attacks vectors. Quick response code phishing attack is when a... **View more**

Metadata

Abstract:
Recently, phishing attacks have taking a new dimension with the addition of quick response code to phishing attacks vectors. Quick response code phishing attack is when an attacker lures its victims to voluntarily divulge personal information such as password, personal identification number, username and other information such as online banking details through the use of quick response code. This attack is on the rise as more and more people have adopted mobile phone usage not just for communication only but to perform transaction seamlessly. The ease of creation and use of quick response code has made it easily acceptable to both provider of goods and services and consumers. This attack is semantic as it exploits human vulnerabilities; as users can hardly know what is hidden in the quick response code before usage. This study reviewed various methodologies that earlier researcher have used to detect this semantic-based attack of phishing. The strength of each methodology, its weakness and general research gaps identified.

Published in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS)

Date of Conference: 13-15 Oct. 2020

INSPEC Accession Number: 20198173

Date Added to IEEE *Xplore*: 24 November 2020

DOI: 10.1109/ICCIS49240.2020.9257687

Publisher: IEEE

ISBN Information:

Conference Location: Sakaka, Saudi Arabia