



IEEE.org | IEEE Xplore | IEEE-SA | IEEE Spectrum | More Sites **SUBSCRIBE** SUBSCRIBECard Create Account | Personal Sign In

**IEEE Xplore**® Browse My Settings Help **Institutional Sign In** 

**Institutional Sign In**

All  **ADVANCED SEARCH**


Conferences > 2020 2nd International Confer...

# A Review of Detection Methodologies for Quick Response code Phishing Attacks

**Publisher:** IEEE

[Cite This](#)

[PDF](#)

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

**1** Paper Citation **104** Full Text Views

Export to Collabratec

### Alerts

Manage Content Alerts Add to Citation Alerts

Abstract	
Document Sections	
I. Introduction	
II. QR Code Phishing	
III. QR Code Phishing Detection Methodologies	
IV. Review Summary	
V. Findings from Literature Review	
Authors	
Figures	
References	
Citations	
Keywords	
Metrics	
More Like This	

Downl PDF

**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

**ISBN Information:** **Publisher:** IEEE

**Conference Location:** Sakaka, Saudi Arabia