ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Unveiling Quishing: The Dark Side Of Qr Codes In Cyber Attacks

Avtandili Bichnigauri[1], Ioseb Kartvelishvili[2], Luka Shonia[3], Daviti Bichnigauri[4], Otar Gudadze[5]
DOI: https://doi.org/10.61446/ds.2.2023.7412

Article History:
Received 18 September 2023
Accepted 20 October 2023
Published 25 December 2023

Abstract

In the ever-expanding realm of technological integration, the emergence of QR phishing, aptly termed “quishing,” has become a potent threat to digital security. This article navigates the complexities of quishing, unveiling the clandestine techniques wielded by cyber perpetrators through QR codes. It scrutinizes the evolution of these deceptive maneuvers, explores the nuanced strategies employed, and advocates essential proactive measures crucial for fortifying defenses against this insidious facet of cyber assaults.

Drawing upon the ubiquitous presence of QR codes in our daily interactions, this article illuminates the shadowy underbelly of quishing, revealing the potential risks lurking behind these innocuous-looking symbols. By delving into the core mechanisms of quishing, this exploration aims to equip individuals and organizations with insights necessary to navigate the perilous terrain of cyber threats engendered by QR codes.

Continuously evolving cyber tactics demand a proactive stance. Hence, this exposition seeks to empower readers with an in-depth understanding of quishing, emphasizing the critical need for heightened vigilance, robust security measures, and comprehensive awareness to thwart the ever-looming specter of QR-based phishing exploits.

Keywords:
QR phishing, Quishing, cyber threats, digital security, deceptive maneuvers, proactive measures, cyber assaults, QR codes, cyber tactics, heightened vigilance, robust security.

1 Ph.D., Assistant of the Faculty of Informatics and Management Systems, Georgian Technical University
2 Professor of the Faculty of Informatics and Management Systems, Georgian Technical University
3 Assistant Professor of the Faculty of Informatics and Management Systems, Georgian Technical University
4 Full-Stack Web Developer and Cyber Security Researcher
5 Master of the Faculty of Informatics and Management Systems, Georgian Technical University

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Introduction

Within the fabric of modern technological interactions, the unassuming presence of QR codes has woven a tapestry of convenience and vulnerability. Amid this intricate web, a looming threat surfaces - **QR phishing** or **“Quishing”** - an insidious tactic leveraging these ubiquitous codes as a conduit for cyber attacks.

The prevalence of QR codes in daily life has entrenched a sense of trust and reliance, yet this very trust becomes a chink in the digital armor, exploited by cybercriminals to perpetrate phishing attacks. This article endeavors to navigate the multifaceted landscape of quishing, shedding light on the deceptive maneuvers that render QR codes both a tool of convenience and a gateway for exploitation.

In this exploration, we peel back the layers of this emerging threat, exposing the shadowy underpinnings concealed beneath the surface of innocuous squares. By unraveling the complexities of quishing, we aim to arm individuals and organizations with a comprehensive understanding, equipping them to discern the potential risks inherent in these seemingly innocuous symbols. As we delve deeper into the mechanisms driving quishing, it becomes evident that our reliance on QR codes warrants a nuanced comprehension of the risks they harbor. This understanding is foundational to fortifying our defenses against the malicious intent lurking behind these deceptively simple visual codes.

Through this investigation, we seek to empower readers with insights essential for navigating the labyrinthine pathways of cyber threats ingrained within QR codes. This knowledge serves as a beacon guiding us toward a proactive stance against the looming specter of QR-based phishing exploits, emphasizing the cruciality of vigilance, education, and fortified security measures.

Main Part

Deciphering Quishing and understanding the depths: At the heart of quishing lies the manipulation of QR codes, transforming these innocuous-looking squares into gateways for cyber exploitation. Cybercriminals adeptly embed malicious URLs within these codes, Deciphering Quishing and understanding the depths: camouflaging them amidst the sea of legitimate links. When unsuspecting individuals scan these QR codes, they unwittingly open the door to a world of fraudulent websites or malware infiltration. The inherent trust and convenience associated with QR codes become the very tools exploited by attackers to orchestrate their deceit.

The Evolution of Tactics by adapting to Cyber Resilience: Quishing, like any other cyber threat, is not stagnant. It evolves. From the static codes of yesteryears to the dynamic QR codes of today, cybercriminals continuously refine their strategies. Dynamic QR codes offer a tactical advantage, enabling attackers to alter destinations post-distribution, eluding traditional security measures. Moreover, social engineering plays a pivotal role, embedding these deceptive codes within alluring promotions or contests, preying on human curiosity and trust.

Essential Preventive Measures: Mitigating the risks posed by quishing necessitates a multifaceted approach. Education emerges as a potent tool, arming individuals with awareness about the potential dangers lurking within QR codes. Implementing QR code scanners equipped with URL preview capabilities empowers users to scrutinize destinations before engagement, adding a layer of defense against fraudulent links. Rigorous security audits and robust encryption protocols fortify organizational defenses, creating formidable barriers against potential breaches.

By embracing a proactive stance and comprehending the intricacies of quishing, individuals and organizations can navigate the treacherous waters of QR-based phishing exploits. This heightened awareness, coupled with stringent security protocols, serves as a formidable shield, safeguarding against the deceptive allure of QR codes wielded for malicious intent.

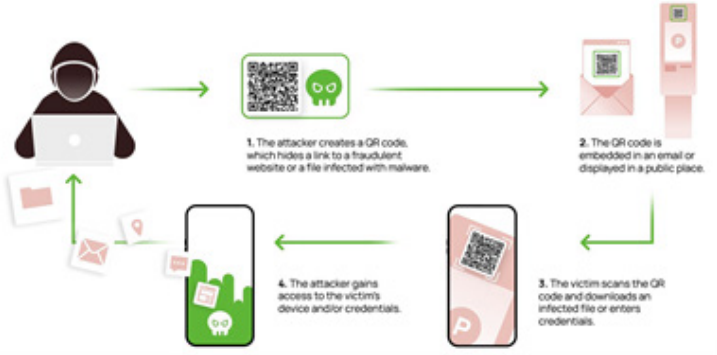

Fig. 1. Quishing attack performance diagram

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Conclusion

Quishing poses a substantial threat in the landscape of cyber vulnerabilities, exploiting the very convenience that QR codes offer. As technology propels us forward, it is imperative to remain vigilant, educating ourselves and fortifying our defenses against evolving cyber threats. Through knowledge dissemination, robust security measures, and an unwavering commitment to vigilance, we fortify our digital resilience, ensuring that the dark side of QR codes remains a conquered territory in the realm of cyber security.

References

ბიჩნიგაური ა., ქართველიშვილი ი., შონია ლ., „ფიშინგისა და მავნე კოდის მქონე ვებგვერდების პრევენციის ეფექტური მექანიზმის მოდელის შემუშავება და რეალიზაცია ვებბრაუზერის გარემოში“, ISBN 978-9941-512-06-3, საერთაშორისო სამეცნიერო - პრაქტიკული კონფერენცია თანამედროვე გამოწვევები და მიღწევები ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებში, თბ., 2023.

Chaudhry, Junaid & Chaudhry, Shafique & Rittenhouse, Robert. (2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications. 10. 247-256. 10.14257/ijsia.2016.10.1.23.

Awuah Amoah, Godwin & J.B., Hayfron-Acquah. (2022). QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing). International Journal of Computer Applications. 184. 34-39. 10.5120/ijca2022922425.

Sharevski, Filipo & Devine, Amy & Pieroni, Emma & Jachim, Peter. (2022). Gone Quishing: A Field Study of Phishing with Malicious QR Codes.

Quishing is the new phishing: Why you need to think before you scan that QR code. https://www.zdnet.com/article/quishing-is-the-new-phishing-why-you-need-to-think-before-you-scan-that-qr-code/

Latest Cyber Threat: Quishing or QR Code Phishing Method. https://cybriant.com/latest-cyber-threat-quishing-or-qr-code-phishing-method/