Security Matters in the Age of Information

Author: Yasemin Er

Date: June 10, 2025

Abstract

This paper explores the growing concerns and risks associated with the transformation into a more connected, global, and digitalized society. It focuses on the widespread adoption of QR codes, their benefits, and the lack of regulatory oversight, while emphasizing the importance of proactive security measures.

1. Introduction

Tools that generate QR codes are now widely available to companies, institutions managing critical infrastructure, and businesses such as airlines. The QR code, as we know it today, was invented by a team of researchers at the Japanese automotive product developer Denso Wave[1]. It's reasonable to assume that the original intent behind this barcode was to streamline the labeling of parts in industrial production settings.

2. Regulation and Adoption

There is a lack of regulatory oversight, both nationally and globally, when it comes to software tools that generate QR codes[2]. Despite this, the quick-response barcode has become ubiquitous across much of the industrialized world.

3. Benefits and Consumer Impact

When we consider QR codes being used as boarding passes to simplify air travel, the stark contrast to previous methods becomes apparent. The benefits are clear. Yet, consumers and customers often have little say when businesses decide to change how their products or services are processed, delivered, or secured. This places a responsibility on businesses to safeguard not only their own interests but also those of their customers.

4. Marketing and Security Oversight

One of the most compelling ways to promote QR codes as a modern replacement for outdated, resource-intensive, or overly complex procedures is by emphasizing their frictionless nature. No hustle and bustle, fewer interruptions, fewer challenges, just a smoother boarding process.
When companies around the world use these arguments to market their solutions to large enterprises and critical infrastructure providers, it's important to recognize that the discussion is often unbalanced. Consumers want ease of use. Businesses want streamlined processes. Tool developers want to sell their products. Security concerns, if addressed at all, are often framed as opportunities to upsell additional features or build trust with specific demographics. Rarely are they discussed within the framework of objective, standardized regulation, let alone mechanisms for audits, reviews, or ongoing monitoring.

5. Security Risks

QR codes pose significant security risks. Attackers can encode malicious links that lead to phishing sites or inject malicious code[3]. A study by MIT researchers found vulnerabilities in popular QR code scanners, including code injection and unauthorized actions[4].

6. Risk Assessment and Future Outlook

Transmitting data wirelessly without a robust authentication mechanism, whether for stadium access, concerts, flights, warehouse logistics, or financial transactions, can reduce costs and save resources. This concept has become deeply embedded in cultural, environmental, educational, healthcare, and economic sectors, and it's likely here to stay. Statistically, the greater the potential damage a technological system can suffer, the less foreseeable that damage tends to be. Without proactive reflection on potential risks, strategic mitigation becomes impossible. QR codes must be included in threat modeling and security policies to avoid being overlooked as a risk vector[5]. Once damage occurs or is recognized, reactive and untested countermeasures, often implemented in haste, can exacerbate the situation.

7. Conclusion

In the absence of unbiased regulatory oversight for the integration of widely adopted tools into critical services and infrastructure, we must find ways to critically evaluate our own strategies and approaches to implementation.

References

[1] Denso Wave. (n.d.). *QR Code Essentials.* https://www.denso-wave.com/en/technology/vol1.html

[2] ISACA. *QR Code Security Challenges.* https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-18/qr-code-security-challenges

[3] Krombholz, K., Fruhwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). *QR Code Security: A Survey of Attacks and Challenges for Usable Security*. https://www.researchgate.net/publication/263146774_QR_Code_Security_A_Survey_of_Attacks_and_Challenges_for_Usable_Security

[4] MIT. *Security Overview of QR Codes.* https://courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf

[5] SANS Institute. (2021). Threat Modeling for Modern Applications. https://www.sans.org/white-papers/40180/