Abuse of QR Codes: Threats, Attacks, and Countermeasures

Igor Kumichev Dias Yerzhanuly

Department of Computer Science
University of Salzburg
5020 Salzburg, Austria

16th of January 2026

Content

- Introduction to QR Codes
- Why QR Codes Are a Security Risk
- Threats and Attack Scenarios
- Attack Techniques and Exploitation Methods
- Countermeasures and Best Practices

QR Codes - Introduction

- Our presentation introduces a general background on the technology of QR code, as well as the most important security aspects.

[1] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. QR Code Security. In Proceedings of the Workshop on Trustworthy Ubiquitous Computing (TwUC), Paris, France, 2010

QR Codes - Introduction

- Our presentation introduces a general background on the technology of QR code, as well as the most important security aspects.
- Quick Response (QR) codes are two-dimensional matrix barcodes that have become an intricate part of our digital lives.

[1] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. QR Code Security. In Proceedings of the Workshop on Trustworthy Ubiquitous Computing (TwUC), Paris, France, 2010

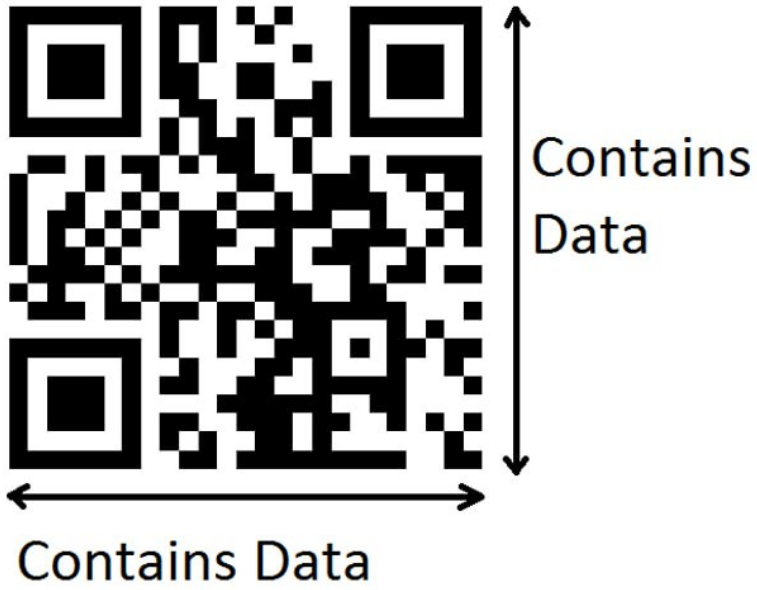
QR Codes - Introduction

- Our presentation introduces a general background on the technology of QR code, as well as the most important security aspects.
- Quick Response (QR) codes are two-dimensional matrix barcodes that have become an intricate part of our digital lives.
- The QR code was designed in 1994 by Denso Wave in Japan with the intent to provide quick and efficient information retrieval. [1]

[1] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. QR Code Security. In Proceedings of the Workshop on Trustworthy Ubiquitous Computing (TwUC), Paris, France, 2010

Barcode vs. QR Code

Barcode vs. QR Code



Advantage of QR Codes

- Traditional barcodes store data in one direction only, while QR codes store data both horizontally and vertically, allowing much higher capacity in a much smaller space.

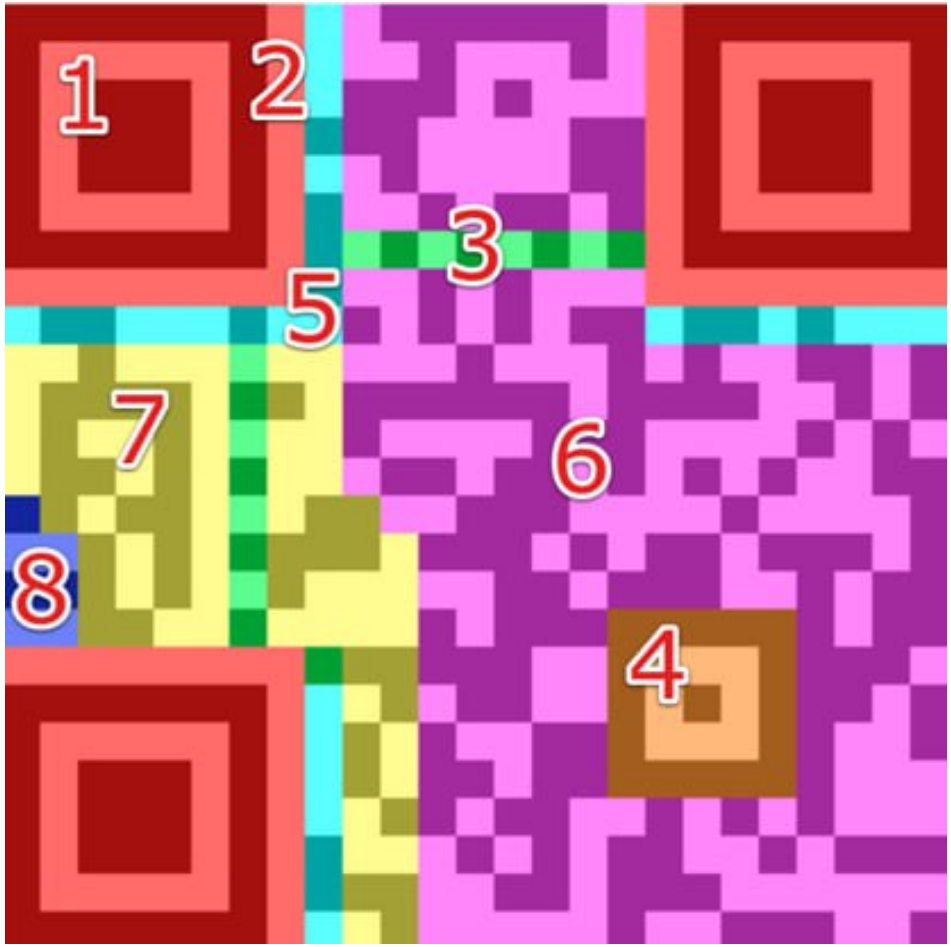
Advantage of QR Codes

- Traditional barcodes store data in one direction only, while QR codes store data both horizontally and vertically, allowing much higher capacity in a much smaller space.

- QR codes can store many data types, including numbers, text, binary data, symbols, and Kanji, making them suitable for a wide range of applications.

QR Code Structure

- 1. Finder patterns
- 2. Separators
- 3. Timing Pattern
- 4. Alignment Patterns
- 5. Format information
- 6. Data
- 7. Error correction
- 8. Remainder Bits



Common Use Cases of QR Codes

- Offline
- Online
- Mobile payments
- Ticketing
- Menus
- Authentication
- Marketing activities

Reasons for Widespread Trust and Adoption

- The key benefit is independence of orientation. The QR code has the advantage of being able to be scanned from any angle as the scanning software is able to interpret it in the proper orientation using the finder and alignment pattern

Why QR Codes Are A Security Risk

- Lack of Human Readability
  - QR codes are not human-readable
  - Reckless scanning behaviors
  - Weaknesses within QR code software and web browsers

[2] Marvin Kowalewski, Leona Lassak, Markus Durmuth, and Theodor Schnitzler. Scanned and scammed: Insecurity by obsqrity? measuring user susceptibility and awareness of QR code-based attacks. In Proceedings of the 34th USENIX Security Symposium (USENIX Security 25), Seattle, WA, USA, August 2025. USENIX Association.

Why QR Codes Are A Security Risk

- Lack of Human Readability
  - QR codes are not human-readable
  - Reckless scanning behaviors
  - Weaknesses within QR code software and web browsers

- QR code social engineering attacks are very effective because they exploit the human trust, convenience, and curiosity
  - Since the scanning of the QR code automatically facilitates interaction, users feel the link is more secure compared to the conventional link, thus reducing critical scrutiny but rather vulnerable to manipulation [2]

[2] Marvin Kowalewski, Leona Lassak, Markus Durmuth, and Theodor Schnitzler. Scanned and scammed: Insecurity by obsqrity? measuring user susceptibility and awareness of QR code-based attacks. In Proceedings of the 34th USENIX Security Symposium (USENIX Security 25), Seattle, WA, USA, August 2025. USENIX Association.

Comparison to Traditional Phishing Links

- Studies show that QR codes can increase vulnerability to phishing and scams, as users are less likely to verify authenticity when scanning them.

Threats and Attack Scenarios

- Quishing (QR Code Phishing)
  - These attacks also commonly involve directing the victim to phishing websites where they are tricked into entering their login credentials or performing other operations using single sign-on methods

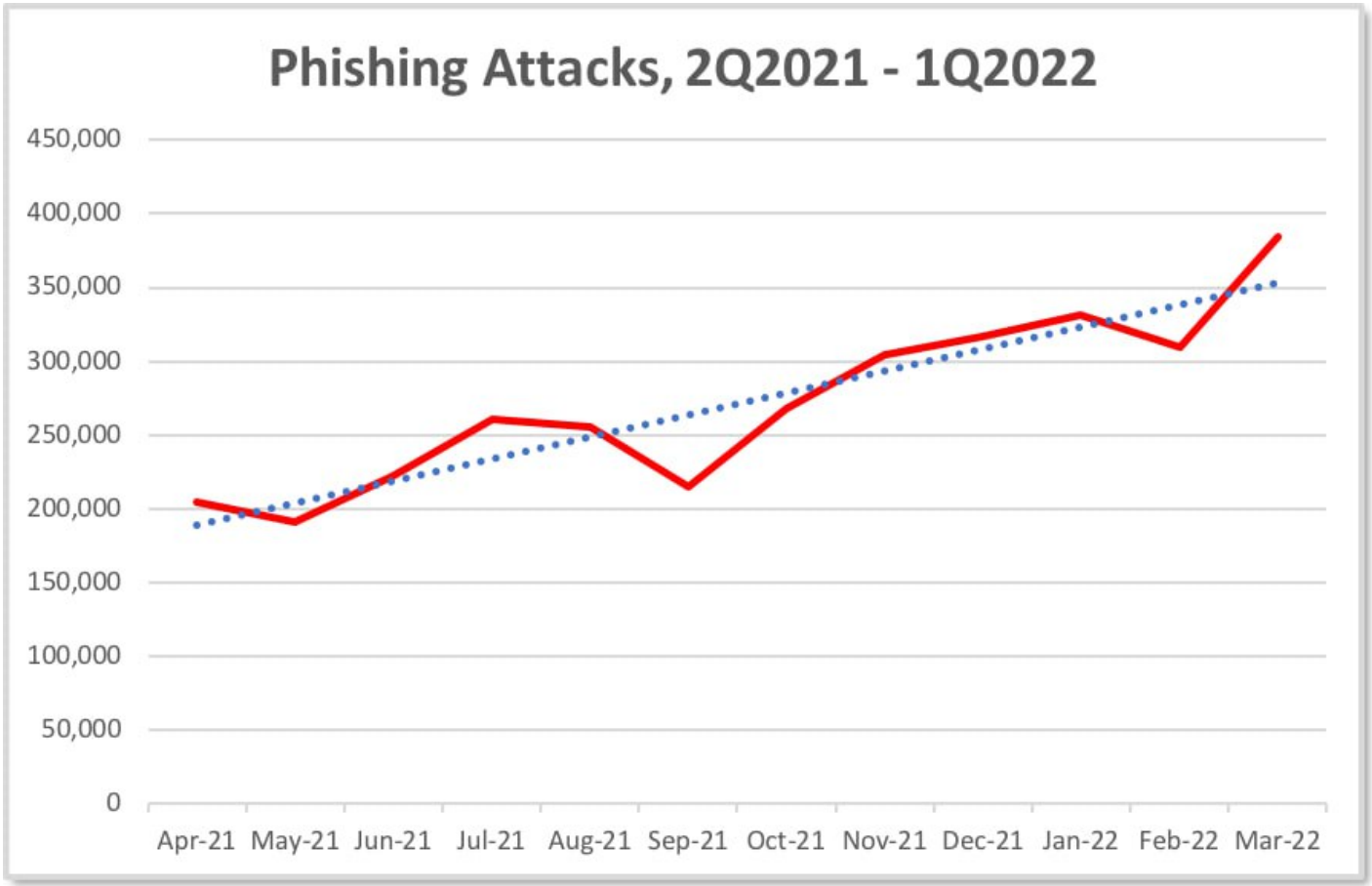
[3] Godwin Awuah Amoah and J. B. Hayfron-Acquah. QR Code Security: Mitigating the issue of quishing (QR Code Phishing). International Journal of Computer Applications, 184(33), 2022.

Threats and Attack Scenarios

- Quishing (QR Code Phishing)
  - These attacks also commonly involve directing the victim to phishing websites where they are tricked into entering their login credentials or performing other operations using single sign-on methods
- Malware Distribution via QR Codes
  - Some QR codes create an automatic download, forward users to malicious websites, or exploit mobile application vulnerabilities [3]

[3] Godwin Awuah Amoah and J. B. Hayfron-Acquah. QR Code Security: Mitigating the issue of quishing (QR Code Phishing). International Journal of Computer Applications, 184(33), 2022.

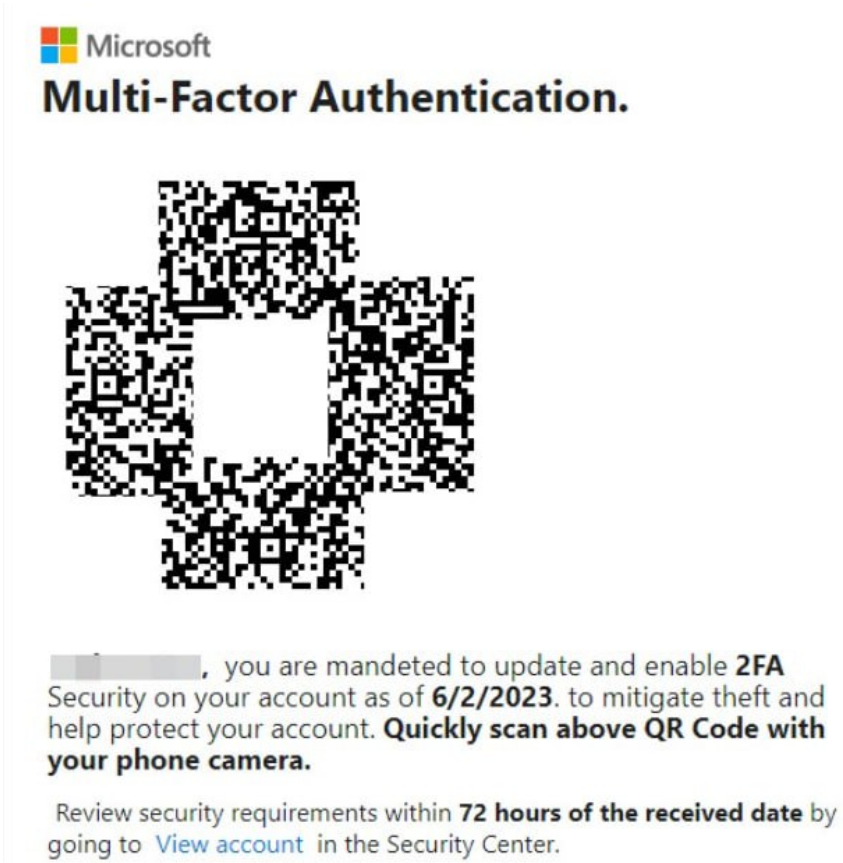
Real-World Examples and Incidents



Yahoo Finance (2022)

https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Real-World Examples and Incidents



TechRepublic (2023)

https://www.techrepublic.com/article/major-us-energy-company-hit-by-qr-code-phishing-campaign/

Attack Techniques and Exploitation Methods

- Creation and Distribution of Malicious QR Codes

Attack Techniques and Exploitation Methods

- Creation and Distribution of Malicious QR Codes
- Exploiting Mobile Device Permissions

Attack Techniques and Exploitation Methods

- Creation and Distribution of Malicious QR Codes
- Exploiting Mobile Device Permissions
- Attacks Targeting Payments and Authentication Systems

Creation and Distribution of Malicious QR Codes

- In cyber space, the attacker will embed malicious QR codes in phishing emails that will mimic trusted institutions. The recipient cannot determine the authenticity even before scanning the QR code, making this method extremely successful

Exploiting Mobile Device Permissions

- The scanning usually involves the automatic processing of the encoded information, such as the opening of the browser or filling of payment details, without the need for verification

Attacks Targeting Payments and Authentication Systems

- In the context for payment purposes, QR codes are able to automatically fill transactions, thereby limiting the ability for users to recognize anomalies. Likewise, for authentication purposes, QR codes lead to phishing pages resembling genuine services, with the aim to steal credentials

Countermeasures and Best Practices

- Technical Defenses
  - Technical methods for defending against QR code-based attacks include cryptographic techniques such as digital signatures and public-key infrastructure, which authenticate QR codes and confirm their authenticity and integrity

[4] Nidhi Nigam and Rajat Bhandari. Performance analysis of QR Phishing detection approaches. Journal of Information Systems Engineering and Management, 10(33s), 2025.

Countermeasures and Best Practices

- Technical Defenses
  - Technical methods for defending against QR code-based attacks include cryptographic techniques such as digital signatures and public-key infrastructure, which authenticate QR codes and confirm their authenticity and integrity
- Organizational Measures
  - Public awareness campaigns as well as security training will enable people to realize the dangers of malicious use of the technology through QR codes as well as the need not to trust them blindly [4]

[4] Nidhi Nigam and Rajat Bhandari. Performance analysis of QR Phishing detection approaches. Journal of Information Systems Engineering and Management, 10(33s), 2025.

User Best Practices

Good scanning practices represent an important defense mechanism. Users should not scan QR codes from unfamiliar or unreliable sources, utilize safe scanner software that offers preview functions and warnings, and exercise caution if QR codes ask for credentials, payments, or downloads

Future Improvements and Secure QR Code Designs

- Improving resistance to attacks related to manipulated QR code attacks will remain a challenge. But, it is important to ensure, through both technical and educational means, trust in QR code systems is maintained

References

- Godwin Awuah Amoah and J. B. Hayfron-Acquah. QR Code Security: Mitigating the issue of quishing (QR Code Phishing). International Journal of Computer Applications, 184(33), 2022.
- Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. QR Code Security. In Proceedings of the Workshop on Trustworthy Ubiquitous Computing (TwUC), Paris, France, 2010.
- Marvin Kowalewski, Leona Lassak, Markus Durmuth, and Theodor Schnitzler. Scanned and scammed: Insecurity by obsqrity? measuring user susceptibility and awareness of QR code-based attacks. In Proceedings of the 34th USENIX Security Symposium (USENIX Security 25), Seattle, WA, USA, August 2025. USENIX Association.
- Nidhi Nigam and Rajat Bhandari. Performance analysis of QR Phishing detection approaches. Journal of Information Systems Engineering and Management, 10(33s), 2025.

- Thank you for your attention!