The Hidden Dangers of QR Codes

Understanding the Mobile Security Risks and What to Do About Them

ZIMPERIUM®

Executive Summary

QR (quick-response) codes are popping up all over, including in restaurants, transit centers, advertisements, and more. While QR codes offer convenience and speed, they can also introduce risk. The reality is that enterprising cybercriminals are exploiting QR codes in a number of ways, exposing the sensitive assets of employees and organizations alike. This white paper introduces the risks posed by QR usage and examines how enterprise security teams can protect employees from these threats.

Introduction

Recent years have ushered in the rise of the mobile-first business. Mobile apps and devices have become integral in a broad array of customer and employee services, and play an increasingly vital role in how business gets done.

For the mobile-first business, QR codes represent an increasingly common part of the landscape. First created back in the 1990s, QR codes went mainstream during the pandemic, offering a convenient, contactless way to access information, conduct transactions, and more. Further, QR code usage is expected to continue to skyrocket; between 2022 and 2025, the number of QR code users in the US is projected to grow by 16 million.

QR codes are widely used by a range of organizations, including manufacturers, restaurants, hotels, retailers, media outlets, and healthcare providers. Adopting QR codes has helped businesses improve social engagement, increase sales, and streamline operations. For users, QR codes offer seamless convenience and simplicity.

5.3 billion coupons were redeemed in 2019.

52% of all restaurants in the US have implemented QR code menus.

Contactless payments in the US have surged 150% since 2019.

Digital business card market is projected to reach $242.3 million by 2027.

Login with QR Code

Scan this QR Code to log in instantly.

From a mobile device's camera app, the user views a code and can click on a link that automatically appears. In this way, users can gain direct access to websites and social media accounts, add a new contact, or compose an email or text message. QR codes can also be used to connect to a wireless network and as an alternative to password-based authentication. QRLs, which stands for quick-response code logins, enable individuals to use their mobile phones to view a QR code that features login credentials and use those credentials to gain access to protected resources.

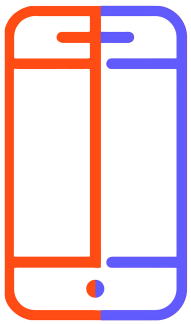
Beyond Convenience

For all the benefits QR codes provide, they also pose security risks for enterprise users and mobile-first businesses. Malicious actors are often looking at new attack vectors, while using QR codes to access sensitive information and credentials is the latest attack trend. Malicious QR codes can appear anywhere, whether at a shopping center, billboard, parking meter, bus stop, on T.V, or virtually any public location. These codes can also be distributed electronically, including in digital ads, websites, and emails.

With a large number of enterprises employing a bring-your-own-device policy, it is no surprise that 28% of employee-owned devices are the most common targets for attacks. Using personal devices for work can significantly blur the lines and could pose security risks.

Whether at a bus terminal or café, employees typically assume QR codes and associated links are legitimate. Cybercriminals can, and do, exploit this trust.

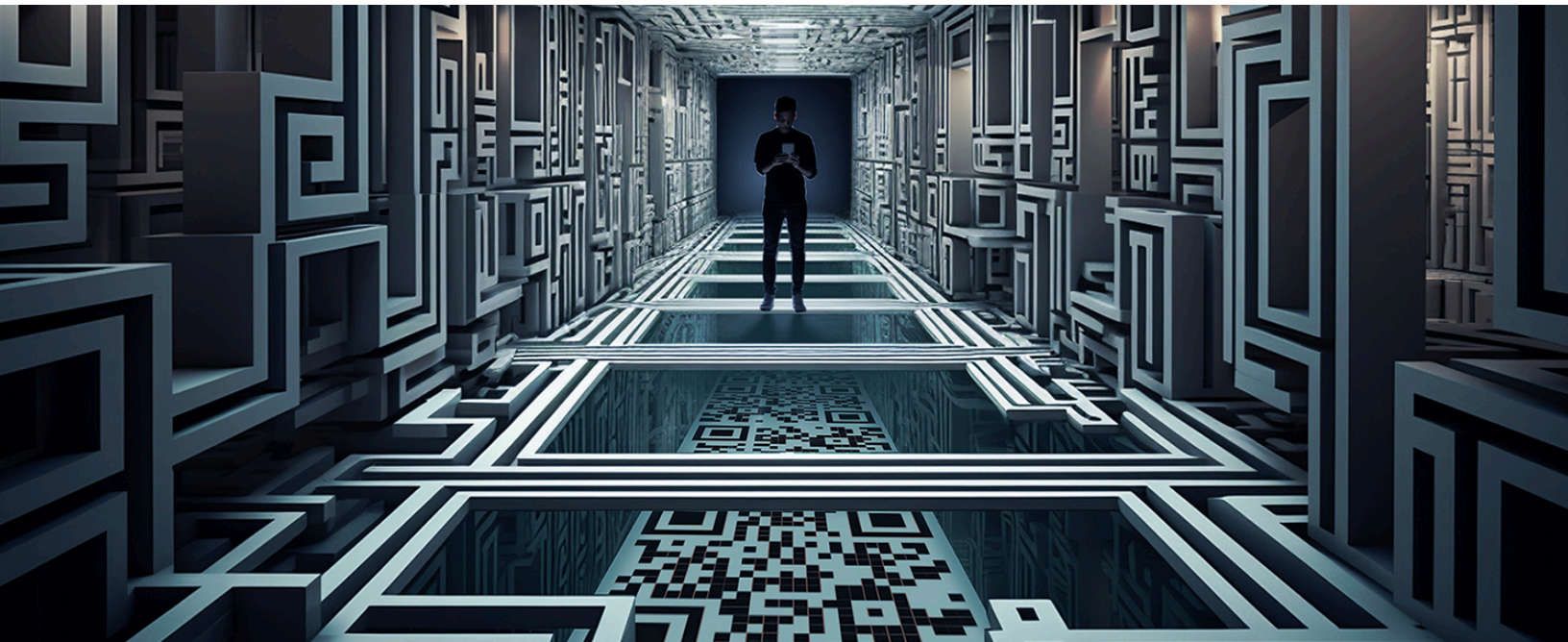
78%
use work devices for personal activities



72%
use personal devices for work activities

Fundamentally, just by looking at a QR code or link, it can be difficult to detect a potential compromise on a device due to the shortened QR code links. Similar to phishing, mobile phones and employees are particularly susceptible to QR code attacks. First, most devices lack the phishing and malware protections that many laptop and desktop computers have. Second, their smaller form factorsmake spotting malicious URLs or sites more difficult.

Consequently, consumers—and the enterprises they work for—are at risk. If employee devices are compromised, corporate credentials and assets may be exposed.



The Rise of QR Code Attacks

Guarding Against Quishing

QR codes present links, and these links can direct and redirect users to a phishing site. Through a phishing site, criminals can dupe an unsuspecting user into divulging login credentials, personally identifiable information (PII), and financial details, such as credit card numbers.

This new form of QR-code-based phishing, sometimes referred to as "quishing", continues to grow more prevalent. Attackers can send QR codes via email or post them in public spaces. These QR codes are often accompanied by a call to action, such as a request for account verification or some other inquiry. These tactics often endeavor to instill some sense of urgency, such as notifying users that they are about to be locked out of an account or a payment was denied. Ultimately, users are tricked into providing confidential information.

QR Code-Based Malware & Cybersecurity Risks

QR codes can also be a way for cybercriminals to spread malware and perpetrate attacks. As outlined in an FBI bulletin, "Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information."

The Deception of QRL Jacking

Malicious actors can create a duplicate of a QR code and have it link to a deceptive login page, a practice referred to as "QRL jacking." They also have the ability to manipulate QR codes through techniques like dimming specific sections or subtly distorting square dots within the code. By altering the code in this way, attackers can circumvent the original functionality and direct users to a site of their choosing.

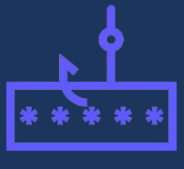
Through QRL jacking, malicious actors can redirect users to a fake login page, where they trick users into divulging credentials and other sensitive details. In addition, they can intercept a user's QR code login session to gain access to credentials. They can also employ a malware-infected app to scan a QR code.

POPULAR SCAMS

Phishing Scams
Drive users to malicious websites

Distribute Malware
Automatically download malware

Payment Fraud
Replace legitimate QR codes



Credential Theft
Request users to log in or reset passwords

Real-World Example

Cases of QR-code-based attacks have continued to increase. One prominent example occurred in San Antonio, Texas, where fake QR codes were detected on parking meters. San Antonio police explained that "People attempting to pay for parking... may have been directed to a fraudulent website and submitted payment to a fraudulent vendor."

Recently, a major energy company was hit with a phishing campaign that used QR codes to bypass email security. The attack began with an email that claimed its recipients must update their Microsoft O365 account settings within 2-3 days. The attackers used QR codes embedded in the attachment to bypass security tools that scan messages for unknown and malicious links.

Keeping Employees Cybersafe

Often, QR-code-based attacks have a social engineering component. Therefore, it is vital for security teams to educate employees on the threats posed by malicious QR codes and to provide guidance on minimizing their exposure. In many cases, simply avoiding QR codes isn't an option. However, it's vital to ensure employees minimize their use and, to the extent possible, only use them in controlled, trusted environments.

80%
of phishing sites target mobile devices
(Zimperium)

2X
Social Engineering Incidents Doubled
(2023 Verizon DBIR)

54%
% of devices which a phishing link was clicked, on a personal device
(2023 Verizon MSI)

How Zimperium Can Help

Zimperium Mobile Threat Defense (MTD) is a privacy-first application that provides comprehensive mobile device security for enterprises. It is designed to provide security teams with mobile vulnerability risk assessments, valuable insights into the risk of mobile applications and threat protection to managed and BYO devices from advanced persistent threats across device, network, phishing, and app risks.

With MTD, security teams can protect users' mobile devices against QR code scams. Zimperium's MTD enables employees to scan a QR code, identify if the corresponding URL links to a malicious or phishing site, and issue a warning. The solution can secure devices even if they're not connected to the network by delivering on-device dynamic detection.

ZIMPERIUM®

Contact Us to Learn More

As the use of QR codes continues to grow increasingly common, so do the associated threats. Zimperium MTD solutions enable security teams to establish robust safeguards that prevent QR-code-based attacks from exposing employees or corporate assets. To learn more, be sure to contact us. https://www.zimperium.com/contact-us/.