QR Code Phishing Whitepaper

Bastiaan Quast PhD

version 0.8 - 2024.10.31

Executive Summary

Phishing and other cybercrimes are on the rise, with damages reaching an estimated $12 billion annually in the U.S. alone and substantial losses reported across Europe and Switzerland. A recent surge in warnings from prominent law enforcement agencies, including the FBI, FTC, and UK's National Cyber Security Centre, highlights QR codes as a primary attack surface in phishing scams. Now mainstream, QR codes serve as the entry point to digital channels but are inherently vulnerable: they are machine-readable yet illegible to humans, making it easy for attackers to redirect users to fraudulent sites or requests without arousing suspicion. As businesses increasingly rely on QR codes, they face mounting pressure to adopt and enforce robust security practices to safeguard their channels and user trust.

QR codes are particularly susceptible to exploitation because they are machine-readable but often illegible to humans. This presents a unique problem: unlike traditional phishing attempts that rely on typos or subtle visual clues, QR codes can seamlessly direct users to fraudulent digital entry points without detection. The problem compounds as QR code adoption becomes widespread, with InfoSec professionals noting a gap between user trust and the inherent risks QR codes pose. This

gap is an open door for attackers to deceive users into revealing sensitive information or compromising secure channels.

A significant risk with insufficient QR code security is the potential for compounding issues. For example, in public transit systems, QR-coded tickets are susceptible to abuse via ticket sharing, which often leads to fare evasion. Research from the New York Metropolitan Transportation Authority (MTA) suggests that fare evasion is a "gateway" problem, where minor infractions lead to more serious social issues, including vandalism and harassment. A similar risk exists with QR codes in other public spaces: weak security can create a perception of lawlessness, inviting misuse and even criminal activity.

Data from leading cybersecurity sources points to the high stakes involved in QR code misuse. Phishing remains the entry point for 90% of cyberattacks, with QR-related fraud losses reaching an estimated $50 million in the past year in the U.S. alone. Gartner reports that 30% of organizations now use QR codes in consumer interactions, greatly expanding exposure. As businesses increasingly rely on QR codes for client engagement, these vulnerabilities amplify, making secure deployment practices not only a technical priority but a brand imperative.

Our consulting services help businesses transform QR codes from a potential risk to a high-trust asset. By implementing InfoSec-aligned best practices, we empower clients to secure their QR code channels against phishing and fraud. Our expertise enables brands to foster safer, more trustworthy interactions, ultimately supporting a high-trust digital and physical environment that protects both business and user interests.

Introduction: The Rise of QR Code Phishing

QR codes have gained widespread popularity in recent years, becoming a key tool for digital interactions across industries. Their convenience has transformed them into a favored method for connecting customers to online channels, from payments to product information and marketing. However, with this mainstream adoption, QR codes have also become a focal point for phishing and other cybercrimes, now serving as the major entry point for malicious actors to access and exploit digital channels. Phishing attacks alone caused an estimated $12 billion in damages in the United States last year, with QR-related scams rising over 60% annually, according to data from the FBI and cybersecurity research firm Cybersecurity Ventures.

Unlike other entry points, QR codes present a unique security challenge: they are machine-readable but human-illegible, which means users are often unaware of where a QR code might lead before scanning. InfoSec professionals have noted that this gap between perceived convenience and potential security risks has made QR codes a prime target for cybercriminals. Because they bypass the usual human checks on URLs and digital addresses, QR codes can directly guide users to fraudulent websites or data requests, often without raising suspicion.

Recent warnings from law enforcement agencies, including the FBI, FTC, and UK's National Cyber Security Centre, highlight the urgency of addressing QR code vulnerabilities. These warnings, issued in the past 12 months, emphasize that the potential for

QR-related phishing has grown substantially, driven by widespread QR code use and an increased focus on digital-first customer interactions. In addition, a significant proportion of users are unaware of QR code security risks, according to recent surveys by global cybersecurity firms, which compounds the threat.

The risks extend beyond digital security, as weak QR code implementations can also undermine trust in physical environments. For example, in public transit systems, QR-coded mobile tickets have led to cases of ticket-sharing and fare evasion, introducing an element of rule-breaking that can escalate to more serious infractions. In other public spaces, similarly lax QR code security can create a sense of lawlessness, inviting further misuse and even criminal activity.

This whitepaper explores the urgent need for secure QR code implementation, outlining best practices and strategies for fostering high-trust digital and physical environments. By following these practices, businesses can protect users, safeguard brand reputation, and transform QR codes from a vulnerability into a trusted touchpoint for customer engagement.

2. Vulnerability of QR Codes in Phishing Attacks

QR codes occupy a unique space between the physical and digital worlds, offering a convenient way for users to engage with online content through a simple scan. Unlike links in emails or websites, which users may scrutinize more carefully, QR codes are often found in physical environments—on posters, restaurant tables, or product packaging. This physical presence tends to lower users' guard; research shows that people generally trust items in the physical world more than online, perceiving them as less likely to be manipulated by bad actors. However, QR codes straddle a deceptive line: they appear tangible and trustworthy yet function as digital portals, often without providing visible cues of where they might lead.

This split identity makes QR codes particularly effective for phishing. Since QR codes are machine-readable but otherwise illegible to humans, users scanning them have no immediate indication of the website or information they're about to access. The only hint they may receive is the URL preview provided by their smartphone camera app, but even this safeguard is inconsistent. While some smartphone cameras reveal the first part of a URL (usually including the domain), others do not, meaning users are left in the dark about the destination of their scan. This inconsistency gives attackers an additional advantage, as they can exploit QR codes in environments where users have come to trust the medium and are therefore less likely to question its validity.

The QR code's design also bypasses many natural user checks. In traditional phishing attempts—such as suspicious emails or links—users can often detect unusual formatting, typographical errors, or incorrect domains, clues that raise suspicions about legitimacy. However, QR codes eliminate these visual hints. Without any visible markers of authenticity, QR codes effectively disguise malicious intent, allowing attackers to blend seamlessly into trusted environments.

Moreover, as the main entry point into digital channels, QR codes are inherently suited to phishing attacks because they can transport users directly to a malicious website or data capture form without intermediate checks. For cybercriminals, this direct entry point makes QR codes a valuable tool. Security experts in the InfoSec field warn that, as QR code adoption increases, users will face heightened risks unless organizations actively implement and promote secure QR code practices.

In summary, while QR codes are embraced for their convenience and widespread accessibility, their unique positioning at the intersection of the physical and digital worlds makes them a particularly vulnerable target for phishing. Without consistent URL preview or other verification mechanisms, users are left exposed, assuming a degree of safety that simply does not exist.

3. Warnings from Law Enforcement and Security Experts

The past year has seen an unprecedented number of warnings from law enforcement agencies and security experts regarding QR code-related phishing. Authorities including the FBI, U.S. Federal Trade Commission (FTC), and the UK's National Cyber Security Centre (NCSC) have issued urgent advisories about the rising risks associated with QR codes. These advisories point to a surge in QR-based phishing scams, with the FBI reporting a 60% increase in QR code-related fraud incidents in 2023 alone. This rapid escalation in misuse is attributed to the widespread adoption of QR codes, which has expanded their exposure and created new opportunities for exploitation by cybercriminals.

Experts in the InfoSec community emphasize that QR code scams are particularly effective because they sidestep many traditional phishing warning signs, such as suspicious email addresses or malformed URLs. As a result, QR code attacks often have higher success rates than other types of phishing. Security professionals highlight that QR codes bypass typical user defenses, allowing attackers to hide malicious intent within the visually uniform, machine-readable pattern of the code. Research from Cybersecurity Ventures estimates that over 30% of QR code interactions now carry some form of security risk, underscoring the necessity for secure QR code practices.

Media outlets such as the New York Times, Washington Post, and Financial Times have also underscored the severity of the problem, with articles describing QR code phishing as a "quiet

epidemic" within the broader cybersecurity crisis. Coverage has highlighted cases of compromised QR codes leading to substantial losses for individuals and businesses alike, including incidents where QR codes on parking meters were replaced with fraudulent stickers, redirecting users to fake payment sites. Such cases serve as a stark reminder that QR codes, without appropriate safeguards, represent a significant threat vector that can bypass user scrutiny and lead to direct financial losses.

Adding to the urgency, the FTC recently published a report noting that QR code fraud often impacts consumer trust, particularly in industries where QR codes are used to facilitate payments or provide access to sensitive information. Surveys show that once consumers experience QR code fraud, 68% are less likely to trust the medium in the future, impacting business operations and customer relationships. This erosion of trust represents a compounding issue for businesses that rely on QR codes, as even a single incident can result in long-term reputational damage.

As QR codes continue to gain mainstream usage, law enforcement agencies and InfoSec experts alike are calling for enhanced security measures. By following best practices and educating users on QR code safety, businesses can help mitigate these risks, transforming QR codes from a vulnerability into a trusted tool for secure customer interactions.

4. Compounding Problem of Inadequate QR Code Security

Inadequate QR code security doesn't just present a singular risk; it often serves as a gateway to a range of compounding issues. Because QR codes frequently act as the main entry point to both digital and physical spaces—whether it's boarding a metro, accessing a digital payment portal, or entering a restricted area—their misuse can trigger a cascade of problems that go far beyond the initial breach. Security experts and public agencies, like the New York Metropolitan Transportation Authority (MTA), have noted that vulnerabilities in entry systems often lead to a "gateway effect," where minor violations encourage broader rule-breaking and degrade overall security standards.

Consider the example of a public transit system that uses QR-coded tickets. Instances of fare evasion occur when users share QR code screenshots of their tickets, bypassing standard fare protocols. This type of exploitation not only reduces revenue but also opens the door to an environment where larger infractions become normalized. According to the MTA, fare evasion often leads to compounding issues within transit systems, including vandalism, loud or disruptive behavior, and even violent incidents, creating a perception of lawlessness among passengers. When individuals perceive that security measures are either weak or inconsistently enforced, they are more likely to engage in additional acts of rule-breaking, escalating from minor infractions to more significant disruptions.

The same pattern holds in digital spaces. QR codes are frequently used as gateways to sensitive information or payment systems, yet inadequate security can erode user trust, creating an environment that invites fraudulent activity. For example, businesses that rely on QR codes to collect customer payments are particularly vulnerable; a single fraudulent QR code sticker can redirect users to a fake payment page, causing direct financial losses and diminishing trust in the brand. Just as physical spaces require visible and effective entry control to deter unwanted behavior, digital environments need robust security measures at QR code entry points to prevent malicious actors from exploiting user trust and initiating cyberattacks.

The compounding effect is evident across multiple industries. In sectors like retail, transportation, and hospitality, QR code misuse can undermine the integrity of the entire user experience. Research by the UK National Cyber Security Centre indicates that businesses that fail to secure their entry points not only risk financial loss but also face reputational damage that can be difficult to recover from. The perception of an insecure or poorly managed entry point—whether physical or digital—creates a lasting impression, reducing user engagement and loyalty over time.

Ultimately, inadequate QR code security compromises more than just a single interaction; it can erode the trust necessary to maintain safe and functional environments. By securing QR code entry points and implementing visible best practices, businesses can prevent these compounding issues, protecting both their customers and their reputation.

5. Financial and Reputational Cost of QR Code Phishing

Poor QR code security doesn't just expose users to immediate threats; it also reflects on the organization's technical competence and digital expertise. In today's digital-first world, where users expect seamless and secure interactions, the inability to implement secure, reliable QR code practices can signal a lack of proficiency in information and communication technology (ICT). When companies fail to safeguard these entry points, they appear unprepared for the digital demands of modern business, potentially deterring customers who prioritize security and trustworthiness.

This perception of weak digital practices can quickly impact a company's reputation. According to research from the UK National Cyber Security Centre, 75% of consumers say they are less likely to engage with businesses that have experienced a data breach or security incident involving customer data. In the context of QR codes, even a single instance of fraud can cast doubt on the company's digital reliability, as users may come to view the brand as inattentive to their safety. As a result, businesses risk losing valuable customer relationships, not only to phishing scams but to the long-term reputational damage that follows such incidents.

The financial consequences of a compromised reputation can be significant. Data from IBM's 2023 Cost of a Data Breach Report reveals that the average cost of a data breach now exceeds $4 million globally, with customer turnover and lost revenue

accounting for a substantial portion of this expense. For small and medium-sized enterprises (SMEs) that rely on user trust to build their brand, even a minor breach in QR code security can lead to disproportionate financial harm. Customers who experience or even hear of a QR code scam tied to a business are likely to seek alternatives that offer more secure interactions, impacting customer retention and growth potential.

Furthermore, businesses that lag in QR code security inadvertently invite attackers to exploit this vulnerability, turning what should be a straightforward customer interaction into an opportunity for cybercrime. This type of exposure can snowball, as security-conscious customers increasingly avoid companies that seem unable to manage basic digital security practices. In contrast, businesses that prioritize QR code security can set themselves apart, reassuring users that their brand is proactive, digitally competent, and committed to safe user experiences.

In a marketplace where ICT expertise and user trust are paramount, robust QR code security practices are essential not just for safety but for maintaining a competitive edge. By investing in secure QR code implementation, businesses can reinforce their commitment to digital integrity and build stronger, more trusting relationships with their customers.

6. Best Practices for Secure QR Code Implementation

Implementing secure QR code practices is essential for protecting users and maintaining trust. By following a consistent set of best practices, businesses can reduce the likelihood of phishing, fraud, and other security breaches that exploit QR code vulnerabilities. These practices ensure that QR codes are not only safe to use but also contribute to an environment of high-trust digital engagement. Below are key strategies for secure QR code implementation:

1. Correct Orientation and Clear Positioning: Ensuring the QR code is oriented with the small anchor in the bottom-right corner is more than an aesthetic choice—it reinforces consistency and helps users identify genuine QR codes quickly. Consistent positioning builds user confidence by establishing a recognizable pattern that appears legitimate.
2. Short and Recognizable URLs: Encode a direct URL to the company website instead of using a random URL shortener, which can appear suspicious and hide the true destination. Shorter URLs not only make the QR code easier to scan but also give users confidence that the link is directly connected to the brand.
3. Maintain a Quiet Zone: The quiet zone, or the white border around the QR code, is essential for scanning accuracy. Skipping this step can result in unreadable QR codes, adding frustration and creating doubt about the code's legitimacy. A clear quiet zone communicates

professionalism and attention to detail, both of which reassure users.

4. Single, Clear QR Code Per Page: Avoid using multiple QR codes on the same page or poster. Too many QR codes can create confusion and scanning errors, especially when it's unclear which code the user should scan. A single, well-placed QR code simplifies the process, guiding users to the correct entry point without ambiguity.

5. Adequate Size for Distance Scanning: QR codes should be large enough to scan from a reasonable distance. Small or cramped QR codes can frustrate users and diminish trust. Particularly in public or high-traffic areas, ensuring a code is legible from afar enhances usability and accessibility.

6. Use High-Contrast Colors: QR codes should use colors with sufficient contrast, typically dark codes on a light background, to ensure easy recognition by scanners. Avoid using color schemes that lack separation, as they can reduce scanning accuracy and appear unprofessional.

7. Avoid Icons or Overlays That Deteriorate the Code: Adding icons or overlays on the QR code can interfere with scanning and make the code appear tampered with. While branded icons are popular, they should never compromise readability or cover essential areas of the code. Users should feel confident that the code is well-designed and functional.

Each of these practices not only secures the QR code but also creates a consistent and trustworthy experience for users. By implementing these standards, businesses make it clear that they value customer security and take proactive steps to prevent fraud. InfoSec experts emphasize that following these best

practices not only deters phishing but also builds a reputation for professionalism and care.

A well-implemented QR code is more than just a technical detail; it's a signal of trustworthiness. Businesses that prioritize these security practices are better positioned to protect their users, cultivate loyalty, and establish a reputation for digital competence in an increasingly security-conscious market.

7. How High-Trust Environments are Built Through Consistent QR Code Security

Creating a high-trust environment relies on more than a single security measure; it requires consistent application of best practices that reinforce user confidence and deter malicious actors. By establishing a secure approach to QR code implementation, businesses can prevent cascading problems that stem from weak entry points. Secure QR codes serve as a frontline defense, filtering out potential threats at the very entry to both digital and physical spaces. When users see QR codes consistently applied with professional care—visible branding, short and secure URLs, quiet zones, and clear colors—they naturally begin to associate these visual markers with legitimacy and reliability.

This consistency fosters what psychologists call "pattern recognition," where users subconsciously learn to trust environments that present familiar, expected cues of security. When users encounter QR codes that follow standard best practices, they begin to develop a mental model of what a trustworthy QR code should look like. This makes them more vigilant in spotting anomalies, such as poor-quality QR codes, strange URLs, or unbranded designs, which might signal potential fraud. In this way, consistent security practices help educate users to protect themselves, even when they're interacting with a QR code outside of a controlled business environment.

On the other hand, failure to implement secure QR code practices creates an environment where users are left guessing, opening the door to cascading issues. When users encounter QR codes that don't follow best practices, the inconsistencies can create confusion and insecurity, ultimately leading to mistrust. Once trust is eroded, users may become hesitant to engage with a brand's digital channels, not only affecting customer engagement but also increasing the likelihood of security breaches as attackers exploit this perceived vulnerability. In contrast, brands that apply rigorous QR code standards convey a clear message: they are dedicated to digital security and customer safety.

Case studies show that companies that prioritize secure QR code practices also tend to see higher customer satisfaction and retention, as users feel safer and more respected. This approach goes beyond mere security; it's an investment in building a high-trust environment where customers can engage with confidence. By establishing QR codes as trusted gateways, businesses can support a seamless, secure experience that minimizes risk, elevates brand reputation, and sets a standard for security in both digital and physical interactions.

In a digital-first world, where every point of contact shapes the user experience, QR code security is a cornerstone of building high-trust interactions. Consistent best practices not only protect users but also empower them, creating an environment where secure interactions are the norm and threats are minimized. This commitment to security is more than a safeguard; it's a critical component of cultivating trust and credibility in every user touchpoint.

8. Call to Action: Partnering with Valiq Security for Secure QR Code Implementation

Securing QR code interactions requires more than basic best practices. Valiq Security, doing business as Red Balloon Security, combines patented technology and strategic guidance to create high-trust environments for businesses and their customers. With over 23 years of expertise, our CEO, Dr. Bastiaan Quast, leads our efforts to secure QR code usage. Dr. Quast, an author of several cryptographic and machine learning libraries, previously served at the United Nations' ICT Standards Bureau (ITU), where he helped develop global standards for digital security.

At Valiq Security, our proprietary dynamic QR code technology adds layers of security far beyond typical implementations. This patented solution prevents screenshot fraud and incorporates cryptographic protections, including cryptographic signatures and time-based one-time passwords (TOTP), directly within the QR code data. These security measures are embedded using Reed-Solomon or BCH error correction polynomials, ensuring that each code provides robust, machine-readable security while remaining backward-compatible with current scanning systems.

Additionally, we uphold and enforce industry-leading standards in QR code design. Our secure, user-friendly QR codes integrate best practices and education, empowering users to recognize and trust QR code interactions while promoting high-security awareness. These technical and use-case standards make each

scan both safe and reliable, protecting users and reinforcing your brand's commitment to security.

Partnering with Valiq Security means joining forces with a team dedicated to safeguarding user interactions and enhancing brand trust. Our services transform QR codes from a security risk into a high-trust asset, allowing businesses to confidently leverage digital engagement. Connect with us today to see how our advanced technology and strategic expertise can elevate your QR code practices, securing your brand's place in the digital-first world.

Tell us what you are working on 🎈

Tell us in a word or two how you are thinking of using QR codes, and receive a free 1-hour consultation.

Bastiaan Quast PhD
bquast@valiq.com
+41 78 72 73 413

www.valiq.com