# A ONE-SQUARE TRAP: QUISHING AND THE FINANCIAL CRIME PERSPECTIVE

## I. The Widespread Use of QR Codes and the Expanding Risk Landscape

In recent years, QR codes have been widely used in many areas of daily life, ranging from reviewing restaurant menus and completing payment transactions to providing quick access to websites and facilitating information sharing. Their ease of scanning through mobile devices and the rapid access they provide to users have significantly increased the accessibility and frequency of this technology. However, the fact that the content to which QR codes direct users cannot always be clearly and transparently reviewed prior to scanning gives rise to certain security and data privacy risks. Scanning a QR code encountered in a physical or digital environment may, without the user's awareness, result in redirection to a malicious website or prompt the user to disclose personal information.

The increasing use of QR codes in financial transaction based contexts such as payment processes, promotional campaigns, and account verification has transformed this technology from merely an access tool into a potential vector for financial abuse. In this context, "*quishing*," a specific form of phishing carried out through QR codes, stands out as a financial crime capable of triggering fraud and unauthorized transaction risks through the compromise of personal and financial data.


## II. Understanding Quishing and Its Operational Mechanism

The term "quishing" is derived from the combination of "QR" (*Quick Response*) and "phishing" and refers to the redirection of users to malicious content through fake or subsequently altered QR codes. In this type of attack, threat actors encourage users to scan a QR code that appears legitimate and trustworthy, and subsequently redirect them to fraudulent login pages, files containing malicious software, or fake payment interfaces.

From a technical perspective, QR codes are divided into two categories: static and dynamic. In static QR codes, the embedded content remains fixed, whereas in dynamic QR codes, the redirected content can be updated without altering the visual structure of the code. While this flexibility offers advantages for legitimate use, the fact that dynamic QR codes operate through a background redirection address allows the underlying content to be converted into a malicious source without any visible change to the code itself. This constitutes one of the key factors that makes the detection of quishing attacks more difficult.

## III. The Operational Process of "*Quishing*" Attacks and Detection Indicators

"*Quishing*" attacks are based on creating the perception that the user is interacting with a harmless or necessary QR code. Attackers may generate QR codes that contain links redirecting users to fraudulent login pages imitating well known websites, fake payment processes, or files containing malicious software. These QR codes may be placed in physical environments or transmitted as visual elements through email or messaging channels. The delivery of a QR code in visual format may make it more difficult for certain security filters to directly analyze the underlying link.

From a detection perspective, certain indicators may raise suspicion, including QR codes placed in public areas that appear to have been affixed later or that seem inconsistent with the surface on which they are displayed, campaign or payment redirections from unclear sources, messages from unexpected senders that create a sense of urgency, suspicious pages requesting authentication or payment information after scanning, domain names that do not correspond to the institution they claim to represent, and unexpected file download requests.

The fact that QR codes are visually highly similar and that the redirection address cannot be clearly reviewed by the user prior to scanning constitutes one of the key factors that makes the risk more difficult to identify at the initial stage.

## IV. The Role of "*Quishing*" in the Financial Crime Ecosystem

"*Quishing*" is not merely a cybersecurity vulnerability but also functions as a practical tool that may be used in the commission of financial crimes. Authentication credentials, card data, or account access information obtained through fraudulent login pages may facilitate activities that result in direct financial loss, including fraud, account takeover, and unauthorized payment transactions. In particular, scenarios built around payment processes or themes such as delivery notifications, promotional campaigns, and account security are designed to target moments when users are more inclined to engage in financial transactions.

The widespread and legitimate use of QR codes in both physical and digital environments renders this method an effective redirection vector for social engineering based financial crimes. The redirection infrastructure concealed behind a visually trustworthy QR code may facilitate the generation of criminal proceeds or the compromise of financial data. In this respect, as digital payment habits continue to increase and mobile devices assume a central role in financial transactions, quishing is emerging as an increasingly visible risk within the financial crime landscape.

To mitigate these risks, individuals should approach QR codes encountered in public spaces with caution, carefully examine the link to which they are redirected after scanning, verify the legitimacy of the website before entering any personal or financial information, and, where possible, manually type the relevant address into their browser. In addition, implementing basic security measures such as keeping devices updated and enabling multi factor authentication can further help reduce exposure to risk.