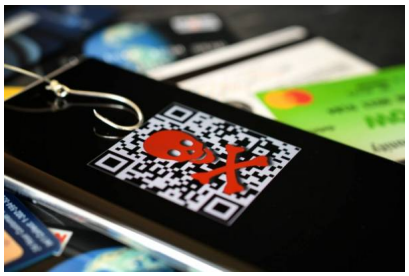
# QUISHING: TRAVELERS NEED TO BE CAREFUL WHEN SCANNING QR CODES



Since the COVID-19 pandemic, QR codes have become essential to everyday consumer life. Unfortunately, criminals have also taken notice and are attempting to profit quickly by creating fake QR codes and websites.

Drivers, in particular, need to be cautious, as this fraud—quishing—often occurs at electric car charging stations or parking machines.

**Quishing: How It Works**

In the first step, criminals create a website that mimics an official site, such as those belonging to a city or a charging station operator.

In the second step**, the fraudsters generate a QR code that links to this fake website.** They then print the QR code and attach it to public parking meters and charging stations for electric vehicles or place it over the legitimate QR codes.

When consumers scan the QR code and enter their personal information—such as when paying a bill—they inadvertently send their money or data directly to the fraudsters.

**Where Can You Encounter the QR Code Scam?**

Quishing primarily occurs in public spaces where QR codes streamline consumer processes, such as making payments. Examples include parking meters, e-charging stations, train stations, bus stops, bike rental stations, or even counterfeit parking tickets placed on windshields.

Fraud attempts related to quishing have been reported throughout Europe, meaning that business travelers may encounter these scams in any country they visit.

**How to Stay Protected from QR Code Fraud?**

Be cautious with public QR codes: QR codes found on flyers, posters, or other public spaces can be easily tampered with or replaced. Only scan them if you trust the source.

Consider alternatives: If possible, directly type in the URL instead of using a QR code. Check links carefully; many QR scanner apps display the URL before opening it.

Watch for suspicious domains or spelling errors.

If you're unsure, do not interact**. If you are doubtful about a website, close it immediately, and do not enter any personal information or bank details.**

Take action in case of fraud: If you notice a suspicious transaction, immediately block your credit card, request a chargeback from your bank, and notify the police and the service provider.

Date: 2025-01-20

Article link: https://www.tourism-review.com/tourists-face-quishing-the-qr-code-scam-news14761