HOW TO PROTECT ONESELF FROM QUISHING FRAUD?

Whether it's a message from the bank, a payment option at an electric charging station, or a parking ticket for illegal parking, these may appear as regular QR codes. Still, they are part of a fraudulent scheme called "quishing." Fraudsters use these fake QR codes to steal personal data and even money. Experts know how this scam operates, how to identify it, and how to safeguard yourself against it.

What Is Quishing and How Does It Work?

Quishing is a combination of "QR code" and "phishing". QR stands for "quick response". "Phishing" is a term formed by combining "password" and the English word "fishing." **In a figurative sense, quishing refers to attempting to obtain passwords using a QR code.** A QR code comprises tiny squares containing information, typically a website address. When scanned with a phone, it opens the referred website. However, the tricky part is that not all phones display the contents of the QR code before opening the destination website. Some devices redirect users directly to the website without showing the address first. Criminals exploit this by placing fraudulent QR codes that lead to fake websites, where they attempt to intercept sensitive data or initiate unauthorized money transfers.

Quishing Fraud in Everyday Life

Beware of fraudulent letters or bank emails asking you to update the app. These messages may contain a QR code that leads to a website run by criminals. Most virus scanners only recognize the code as an image, so the emails are classified as harmless and in your inbox. The real bank has nothing to do with these messages. These fake messages are not personalized and generally address the account holder.

Be cautious of manipulated QR codes on electric car charging stations. Criminals may place fake QR codes over the original ones to trick you into making payments for the charging process, leading you to their websites.

Another scam involves fake parking tickets with QR codes placed under the windshield wipers of parked cars. To avoid falling victim to this scam, drivers should have the parking ticket checked by the police before paying the supposed fine.

How Can You Protect Yourself from Quishing Fraud?

Remember to be cautious any time when scanning QR codes. Only scan them if you trust the source. If using a smartphone camera app, ensure it shows the website address before opening the page so you can verify it. **If you receive suspicious letters or emails with QR codes, research the sender before scanning the code.** It's best to contact the sender directly using their official contact details, not the ones provided in the letter or email.

Also, when using electric charging stations, check if the QR code is tampered with. If unsure, consider using alternative payment methods such as an app or a charging card.

Date: 2024-09-30

Article link:
https://www.tourism-review.com/travelers-need-to-be-aware-of-quishing-fraud-news14611