31.05.2024

QR Phishing

QR codes enjoy huge popularity and are being used for various purposes. It is obvious this can also be abused, as shown by one PostFinance case which became public this week.

This week it was revealed fraudsters have been circulating deceptively realistic letters containing a QR code in the name of PostFinance. This QR code links to a phishing website with the aim to capture victims' log-in credentials for their e-banking facilities.

It is well known that e-mails or short messages such as texts or WhatsApp can be abused for QR phishing. It is a new method though that fraudsters pay postage and use high-quality letterheads.

Either way, care must be taken when scanning QR codes. Protect yourself by following these recommendations:

- Only use QR code scanners (apps) which show you the content of the code first and don't just process it straight away.
- After scanning a QR code, make sure to always check the **link destination (domain name)** before opening the destination page.
- Never enter your log-in information on any website you have accessed via a QR code.
- Only ever use QR codes in situations you consider standard or safe.
- To pay QR invoices, only use your financial institution's app.
- If you are concerned you have been scammed, alert your financial institution as soon as possible.

The PostFinance report can be found here (https://www.postfinance.ch/en/about-us/media/newsroom/phishing-letters.html) .

Copyright © 2024 – All rights reserved. Lucerne School of Information Technologies