

QR-Code-Betrug

© 2026: luise Oranienburg - Lizenz CC BY-NC



Beispiel eines ehrlichen QR-Codes



Dies ist ein „guter“ QR-Code. Er enthält genau die Adresse, welche darunter steht. Wird dieser Code mit dem Smartphone gescannt, zeigt der Browser die erwartete Webseite an.

<https://luise-oranienburg.de>

Beispiel eines betrügerischen QR-Codes



Dies ist ein „böser“ QR-Code. Er enthält eine völlig andere Adresse, als darunter steht. Wird dieser Code mit dem Smartphone gescannt, zeigt der Browser eine fremde Webseite an.

<https://luise-oranienburg.de> ¹

¹ Der QR-Code ist gefälscht und enthält stattdessen die Web-Adresse <https://luise-oranienburg.de.scandemo.hwn.de/?im-himmel-ist-jahrmarkt>

QR-Code-Betrug

© 2026: luise Oranienburg - Lizenz CC BY-NC



Das Problem

QR-Codes finden sich inzwischen überall: im Internet, am Parkscheinautomaten, am Bahnhof und auf Rechnungen. Sie vereinfachen das Leben gewaltig, da lästiges Abtippen und Tippfehler wegfallen.

QR-Codes sind aber auch ein Sicherheitsrisiko. Vor allem, wenn sie mit der Android-Kamera gescannt werden.

Warum ist das so ...

- Die Webseite, welche unter dem QR-Code steht, ist oft eine andere als die Webseite, welche durch den QR-Code aufgerufen wird.
- Man sieht den vollständigen QR-Code meist erst, wenn die Kamera die Seite geöffnet hat. Dann ist aber der Schaden meist schon geschehen.
- Oft enthalten Webseiten verschlüsselte Kurzadressen (sog. Short URLs). Diese Kurzadressen lassen sich nicht überprüfen und können sowohl zur Überwachung als auch zu bösartigen Webseiten (sog. Malware) umleiten.

Die Lösung

- Jede gescannte URL vor dem Aufruf prüfen.
- Spezielle QR-App verwenden. ²
- Keine abgekürzten Web-Adressen aufrufen. Niemals!

² Wir empfehlen QR-Scanner von SECUSO