TEAL
ALWAYS CHALLENGING IT

Wie schütze ich mich vor Quishing

Quishing / QR Phishing ist eine raffinierte Form des Online-Betrugs, bei dem Cyberkriminelle gefälschte QR-Codes verwenden, um Nutzer auf schädliche Websites oder bösartige Anwendungen zu leiten. In der heutigen vernetzten Welt sind QR-Codes fast überall zu finden. Das Scannen eines manipulierten Codes kann dazu führen, dass persönliche Informationen gestohlen oder Malware auf das Gerät geladen wird.

1. QR-Code-Scanner überprüfen

Installieren Sie QR-Code-Scanner nur aus **vertrauenswürdigen App-Stores (falls nicht bereits im Smartphone integriert)**. Lesen Sie die Bewertungen und achten Sie auf regelmäßige Aktualisierungen, um keine Sicherheitsupdates zu verpassen. **Vermeiden Sie unsichere Apps, um potenzielle Risiken zu minimieren.**

2. Aufmerksamkeit beim Scannen

Seien Sie wachsam, wenn Sie QR-Codes scannen und prüfen Sie die Herkunft. Achten Sie darauf, dass Ihr **Smartphone keine unbekannten oder unerwarteten Aktionen ausführt**, die auf einen potenziellen Angriff hinweisen könnten.

3. Überprüfung der Ziel-URL

Bevor Sie auf eine Website weitergeleitet werden, überprüfen Sie die URL sorgfältig.

Die Verwendung von v**erdächtigen Zeichen oder ungewöhnlichen Domainnamen / -endungen** kann vor betrügerischen Seiten schützen.

4. Aktivieren von Zwei-Faktor-Authentifizierung (2FA)

Erhöhen Sie Ihre digitale Sicherheit, indem Sie zusätzlich zu Passwörtern eine zweite Authentifizierungsebene aktivieren.

2FA ist ein effektiver Schutzschild gegen unautorisierte Zugriffe und sichert Ihre Online-Konten.

Quishing-Fazit

Während Cyberangriffe in rasantem Tempo zunehmen, gehört QR-Code-Phishing zu den noch recht neuartigen, aber höchst effektiven Angriffstaktiken.

Dabei setzen Angreifende auf die Tatsache, dass viele Personen noch nicht mit QR-Codes vertraut sind, während andere bereits so daran gewöhnt sind, dass sie diese oft scannen, ohne sie zu hinterfragen oder die damit verbundenen Risiken zu kennen.