OUCH! 2024. január

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

QR-kódok

Áttekintés

Biztos többünkben felvetődött már, vajon mit jelentenek a pontokból vagy sávokból álló „QR-kódoknak” nevezett kis négyzetek? Valószínűleg mindnyájan találkoztunk már velük különféle weboldalakon, plakátokon, mobiljegyként felhasználva vagy akár az éttermek asztalain. Hogyan is működnek és van-e okunk aggódni egyes kockázati tényezők miatt? Járjunk utána.

SANS OUCH webhelyére mutató QR-kód.

Hogyan működnek a QR kódok?

A QR-kód a „Quick-Response kód”, vagyis a gyors válaszkód rövidítése, ami egy géppel olvasható, általában fekete-fehér négyzetekből álló szimbólum. (Lehet másszínű is, még akár háttérképet is tartalmazhat.) Ezek a négyzetek könnyen létrehozhatóak QR-kód generátorral, és különféle információkat rejthetünk el bennük, mint például egy webhelyre mutató hivatkozást, e-mail címet, vagy bármilyen egyéb adatot. Gondoljunk a QR-kódra úgy, mint egy sokoldalú vonalkódra. A legtöbb telefon kamerája képes felismerni és dekódolni a mögött elrejtett információt. Más szóval, amikor egy QR-kódra irányítjuk telefonunk kameráját, az beolvassa a kódot és megkérdez minket, hogy el akarjuk-e érni a mögötte lévő információkat, például meg akarjuk-e nyitni a webhelyre mutató hivatkozást.

Mi ebben a veszélyes?

Mivel nekünk, embereknek nehezen értelmezhető egy csupán négyzetekből álló QR-kód, a kiberbűnözők ezt kihasználva, könnyen rosszindulatú információkat rejthetnek el mögéjük. Előfordulhat például, hogy olyan csaló weboldalra irányít minket a kód, ahol megpróbálják megszerezni személyes, és banki adatainkat, jelszavainkat, vagy akár kártékony programot is telepíthetünk így eszközünkre. Ezen felül a QR-kódok további lépéseket is végrehajthatnak a telefonunkon, például új névjegyet adhatnak hozzá kontaktjainkhoz vagy e-mailt küldhetnek a nevünkben. Fontos kiemelni, hogy a QR-kód önmagában nem jelent veszélyt, viszont az általa végrehajtott cselekvés igen.

Tegyük fel, hogy egy reptéren várakozunk éppen, és meglátunk egy számunkra érdekes terméket reklámozó plakátot. A poszteren van egy QR-kód, amin keresztül bővebb információkat kaphatunk a termékről. Amit viszont nem veszünk észre, hogy az eredeti QR-kódra valaki ráragasztott egy másik kódot. Amikor ránézünk a plakátra természetesen nem gyanakszunk, megbízunk benne, nem is vesszük észre, hogy már nem az eredeti QR-kód van rajta. Beolvassuk a kódot, hogy több információt kapjunk a kedvelt termékről, majd egy csaló oldalon találjuk magunkat, ahol a bűnözők célpontjaivá válunk.

Mit tehetünk a biztonságunk érdekében?

- Legyünk óvatosak mielőtt beszkenneljük a kódot. Először is kérdezzük meg magunktól: Megbízhatok a forrásban? Bízom a plakátban, az étteremben, vagy az adott weboldalban, ahol megtaláltam a QR-kódot? Ha valaki egy QR-kóddal ellátott szórólapot hagy a kocsinkon az megbízhatónak számít?
- Mikor beolvassuk a QR-kódot, a készülékünk minden esetben megkérdezi tőlünk, hogy végrehajtsa-e a kód tartalmához kapcsolódó tevékenységet. Tehát például, ha a QR-kód mögött egy weboldal linkje van, akkor a telefonunk megkérdezi, hogy meg akarjuk-e látogatni az adott oldalt. Mindig szánjunk egy kis időt a link vizsgálatára, és győződjünk meg arról, hogy az valóban biztonságos oldalra fog irányítani.
- Gondoskodjunk készülékünk rendszeres frissítéséről, ellenőrizzük, hogy a legújabb operációs rendszer fut-e rajta. Ezzel garantálva, hogy a legújabb biztonsági funkciókkal rendelkezünk. Ennek a legegyszerűbb módja, ha engedélyezzük az automatikus frissítések telepítését a készülékünkön.
- Ahhoz, hogy dekódolni tudjuk a QR-kódokat, nincs szükségünk speciális mobilalkalmazásokra, egyszerűen használjuk a telefonunk kameráját. Amennyiben egy webhely speciális QR-kód szkennelő alkalmazás letöltését kéri, legyünk résen, előfordulhat, hogy átverés.
- Mindig gondoljuk meg kétszer mielőtt bizalmas vagy személyes adatokat továbbítunk egy olyan webhelynek, amelyet nyilvánosan elérhető QR-kóddal értünk el.

Összességében a QR-kódok használata rendkívül kényelmes módja a információátadásnak. A fentebb említett néhány egyszerű lépés betartásával pedig biztonságosan tudjuk ezeket használni.

A szerzőről

A több, mint 27 éves tapasztalattal rendelkező Abdulmajeed AlAbdulhadi, IT/OT rendszerekkel foglalkozó tanácsadó. CISA (Certified Information System Auditor) és CISM (Certified Information Security Manager) tanúsítványokkal rendelkezik.

Források

Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing
Mobileszközök biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)