DE IBK

Tanácsok, tippek, ha baj van

Hogyan cselezhetjük ki a QR-kódos csalókat?

A QR (Quick Response) kódok sokoldalú felhasználhatóságuk miatt egyre elterjedtebbek az élet számos területén, azonban fontos tudnunk, hogy ezekkel különböző csalásokat is el lehet elkövetni. Bemutatunk néhány példát QR-kódos csalásra, és elmondjuk, hogy mire és miért érdemes odafigyelni, hogy elkerüljük azt, hogy áldozattá váljunk.

A QR-kód (Quick Response kód) egy kétdimenziós vonalkód. Nevét az angol Quick Response (=gyors válasz) rövidítéséből kapta, egyszerre utalva a gyors visszafejtési sebességre és a felhasználó által igényelt gyors reakcióra. Bármilyen irányból készülhet róla fénykép vagy szkennelt kép, nem kell törődni a kód helyes tájolásával. A kód megfejtésére, dekódolására szolgáló programok a három sarokban elhelyezett jellegzetes, minden QR-kódban azonos minta alapján el tudják dönteni, milyen irányban kell a kód pontjait értelmezni, feldolgozni, még akkor is, ha a kódbélyegről készült kép teljesen ferde.

*A QR-kódok alapvető problémája, hogy nem tudjuk ellenőrizni, hogy a beolvasásuk mit fog eredményezni, ezért megbízunk a készítőikben. Azt sem tudhatjuk, mi mindent tartalmaz egy QR-kód, még akkor sem, ha mi magunk készítjük el a sajátunkat. Emiatt a QR-kód nagyon könnyen kihasználható csalás elkövetésére, amit „**quishingnek**” (QR-code phishing) is neveznek.*

QR-kódos csalások

Voltak olyan esetek, hogy a csalók az utcán szólították meg az áldozatot, hogy gyorsan segítsenek rajtuk egy csekély összeg, például a parkolási díj vagy egy buszjegy kifizetésével. A pénzt egy QR-kód beolvasásával, és a fizetési adatok megadásával tudták volna elküldeni, azonban valójában egy csaló weboldal jelent meg, amin az áldozatok megadták a bankkártya adataikat, ami így a csalók birtokába jutott.

Vagy a csalók a parkoló automatákon egyszerűen átragasztották a QR-kódot egy „gyorsabb parkolási fizetést ígérő” weboldalra. Azok a parkolók, akik ezt beszkennelték, nem a pakolást rendezték, hanem a csalóknak utalták a pénzt.

Mit tehetünk az ellen, hogy QR kódos csalás áldozatává váljunk?

1. **Nézzük meg a QR-kód helyét!** Hol található a QR-kód? Egy jól ismert létesítményben van, vagy az utcán, ahol bárki hozzáférhet? Milyen anyagra nyomtatták? A nyilvános helyen (például egy buszmegállóban) lévő QR-kódokat könnyebb manipulálni, ezért mindig fokozott óvatossággal javasolt

beolvasni ezeket! A plakáton vagy táblán lévő QR-kód beolvasása előtt végezzünk gyors fizikai ellenőrzést, hogy megbizonyosodjunk arról, hogy a kódot nem ragasztották-e az eredeti képre!

2. **Az ördög a részletekben lakozik!** A QR-kód hitelességének ellenőrzéséhez figyeljük meg az apró részleteket! Például egy poszter, amely számos nyelvtani hibát tartalmaz valószínűleg nem lesz megbízható.
3. **Ellenőrizzük a QR kód tartalmát!** Mielőtt beolvasnánk a QR-kódot, győződjünk meg arról, hogy az hova is vezet! Apple eszközön, a kamera alkalmazásnál a jobb oldalon megjelenő ikonra koppintva megtekinthető a link. A Google Lens használatával a képernyő közepén feltünteti a hivatkozást.
4. **Ne osszunk meg érzékeny adatokat!** Egy QR-kód beolvasását követően soha ne osszuk meg személyes adatainkat, hacsak nem vagyunk teljesen biztosak a weboldal hitelességében.
5. A legtöbb bank mobil alkalmazásában, a „QR olvasás” funkcióval fizethetünk, valamint a “fizetési kérelmek”-kel létrehozhatunk QR-kódot. Az azonnali fizetési QR-kód beolvasását követően az átutalási megbízási űrlapon megjelenik a kedvezményezett neve, a kedvezményezett bankszámlaszáma és az átutalandó összeg forintban. **Azt fontos tudnunk, hogy a bankok nem ellenőrzik, hogy a kedvezményezett neve és a kedvezményezett számlaszáma összetartozik-e.** Hiába szerepel a kedvezményezett neve rovatban az általunk ismert szolgáltató neve, ha a kedvezményezett számlaszám a csalóé. **Amennyiben nem vagyunk biztosak a QR-kód valódiságában, ellenőrizzük azt a Magyar Nemzeti Bank erre a célra létrehozott weboldalán, ahol a fizetési kérelmek beolvasásával annak részleteit tekinthetjük meg!**