Mire kell figyelni, hogy elkerüljük a QR-kódos csalásokat?

Az utóbbi időben megszaporodtak azok a csalási formák, amely során a támadók QR-kód segítségével lopják el a potenciális áldozatok adatait, vagy akár a pénzüket. Az Azonnali Fizetési Rendszer (AFR2.0) továbbfejlesztésével a banki ügyfelek új fajta fizetési megoldásokkal találkozhatnak majd 2024-ben, miszerint minden pénzforgalmi szolgáltató köteles fizetési kérelmet fogadni és az egységes adatbeviteli szabványt (pl.: QR, NFC, deeplink) alkalmazni.

Hogyan használják a kiberbűnözők a QR-kódokat?

Az emberek nem tudják előre, hogy mi fog történi, ha beolvasnak egy QR-kódot, ezért kénytelenek megbízni annak készítőjében. Még akkor sem tudhatjuk, mi mindent tartalmaz egy QR-kód, ha mi magunk készítjük el a sajátunkat. Emiatt a QR-kód nagyon könnyen kihasználható csalás elkövetésére. A QR-kódos csalásként ismert visszaélés során a csalók károkozó QR (Quick Response) kódokat juttatnak el az áldozathoz.

A csalás valójában egy újabb adathalász módszer, amellyel a személyes adatokhoz, illetve bankszámla adatokhoz férnek hozzá. A QR-kódok kódolt adatokat tartalmaznak, és linkként, hivatkozásként működnek. A link „mögött" lehet egy hamis weboldal, amivel adatokat akarnak megszerezni tőlünk vagy le is töltődhet egy káros applikáció az eszközünkre. A csalók QR-kódokat helyeznek el hamis weboldalakon vagy matricákon, és különböző trükkökkel arra ösztönzik az embereket, hogy azokat olvassák be a telefonjaikkal. Nem ritka, hogy a támadók legitim felek munkájára és hírnevére támaszkodnak, és hivatalos plakátokon, posztereken vagy szórólapokon lévő törvényes QR-kódot a sajátjukra cserélik.

A kiberbűnözők által létrehozott QR-kód egy adathalász webhelyre mutat, ezek a hamis oldalak megtévesztésig hasonlítanak például egy online bank bejelentkezési oldalára vagy fizetési szolgáltatók bejelentkező oldalaira. Amennyiben az áldozatok ezen bejelentkeznek könnyen elveszíthetik pénzüket vagy érzékeny adataikat.

A Magyar Nemzeti Bank készített egy weboldalt, ahol a fizetési kérelmek beolvasásával annak részleteit tekinthetjük meg. (https://mnbqr.hu/)

Íme néhány tipp a QR-kódos csalások elkerüléséhez, amellyel megvédhetjük magunkat a kiberbűnözőktől:
Általánosságban véve, ugyanazok a tanácsok érvényesek a QR-kódos csalásra, mint az adathalászatra, hiszen mindkettő adathalászat.

- **A kétlépcsős azonosítás vagy ha lehetőség van rá, biometrikus azonosítás használata sok csalási formától megóvhat minket!**
- **Legyünk óvatosak, mielőtt eszközünkkel beolvasunk egy QR-kódot!**
- **A legtöbb QR-kód egy vagy több URL-t tartalmaz, amelyek beolvasáskor**
- **Figyeljünk a kód beolvasásakor megjelenő linkekre! Apple eszközön, a kamera alkalmazásnál a jobb oldalon megjelenő ikonra koppintva megtekinthető a link. A Google Lens használatával a képernyő közepén feltünteti a hivatkozást. felbukkannak a képernyő. Az URL biztonságának vizsgálatakor tudnunk kell, hogy mindenképp rendelkeznie kell a „https" protokollal a hivatkozás címének elején. A domain névnek meg kell egyeznie a QR-kódot hirdető márkával vagy cégnévvel. A webhelynek ugyanolyan tartalommal kell rendelkeznie, mint a plakáton hirdetett tartalmaknak. Ha a céloldalon egy bejelentkezési űrlap jelenik meg, amely közvetlenül kéri személyes vagy banki adatainkat, jelszavainkat, akkor semmiképp se adjuk meg ezeket, hanem azonnal zárjuk be az oldalt!**
- **Különösen akkor legyünk óvatosak, ha az URL-t lerövidítették, mert a QR-kódok esetében nincs kényszerítő ok arra, hogy bármilyen linket lerövidítsenek. Ehelyett használjon keresőmotort vagy hivatalos weboldalt!**
- **Óvjuk a telefonunkat víruskereső telepítésével! A víruskereső minden alkalommal értesítést küld, ha rosszindulatú QR-kódot olvas be, vagy egy URL-hez fér hozzá. Megkímélhet minket attól, hogy rosszindulatú programok kerüljenek az eszközünkre, különösen, ha véletlenül egy spam hivatkozásra kattintunk.**
- **Mérjük fel a QR-kód helyét! Hol található a QR-kód? Egy jól ismert létesítményben van, vagy az utcán, ahol bárki hozzáférhet? Milyen anyagra nyomtatták?**
- **A csalók hajlamosak QR-kód matricákat ragasztani egy meglévő QR-kód képhez, hogy becsapják áldozataikat. A nyilvános környezetben lévő QR-kódokat könnyebb manipulálni, ezért mindig legyünk fokozottan óvatosak, mielőtt beolvassuk ezeket! A plakáton vagy táblán lévő QR-kód beolvasása előtt végezzünk gyors fizikai ellenőrzést, hogy megbizonyosodjon arról, hogy a kódot nem ragasztották-e az eredeti képre!**
- **A QR-kód hitelességének ellenőrzéséhez figyeljük meg az apró részleteket! Például egy számos nyelvtani hibát és elrendezést tartalmazó poszter valószínűleg nem megbízható.**
- **Ne olvassuk be a nyilvánvalóan gyanús forrásból származó QR-kódokat!**
- **A QR-kódok értékes információkat, például e-jegyek számát is tartalmazhatják, ezért soha ne tegyünk közzé QR-kóddal ellátott dokumentumokat a közösségi médiában.**

További érdekes információk és elkerülendő példák találhatók a Nemzeti Kibervédelmi Intézet tájékoztató füzetében: https://nki.gov.hu/wp-content/uploads/2023/12/QR-kodos-csalasok.pdf

FORRÁS: KIBERPAJZS
https://kiberpajzs.hu/hirek/mire-kell-figyelni-hogy-elkeruljuk-a-qr-kodos-csalasokat-tippek-es-tanacsok

KiberPajzs
Védelem a pénzügyekben