CTI Jelentés

QR-kódos csalások

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

KiberPajzs
Védelem a pénzügyekben

Tartalomjegyzék

A QR-kódos csalások

A Nemzeti Kibervédelmi Intézet új csalási formára szeretné felhívni a figyelmet. 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 újfajta fizetési megoldásokkal találkozhatnak.

2024. április 1-től minden pénzforgalmi szolgáltató köteles fizetési kérelmet fogadni.

***A quishing** (vagy kvishing) **phishing és a QR kombinációjából alkotott kifejezés**, azonban a közérthetőség érdekében jelen tájékoztatóban végig QR-kódos csalásként hivatkozunk majd erre. **Ennek 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.** Amennyiben már a készülékünkön van a káros app, azzal hozzáférhetnek akár egy Wi-Fi hálózathoz, GPS koordinátákhoz, vCardhoz, közösségi profilhoz, de akár fizetési kérelemhez is.*

***vCard**: az elektronikus névjegykártyák fájlformátum szabványa. A vCardok csatolhatók e-mail üzenetekhez, elküldhetők a multimédiás üzenetküldő szolgáltatáson keresztül, a világhálón, azonnali üzenetküldéssel, NFC-vel vagy QR-kóddal.*

TUDTAD?

Mik azok a QR-kódok?

A QR-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.

Néhány példa a gyakoribb QR-kódokból:

Klasszikus QR-kód

Ez a Denso Wave által az 1990-es években létrehozott QR-kód eredeti változata. Könnyen felismerhető a bal alsó, bal felső és jobb felső sarkában található három keresőmintáról.

rMQR kód

Helytakarékos, négyszögletes formában jelenik meg, ezáltal keskeny munkadarabokhoz is használható. Az akár 361 numerikus karakter tárolására képes, valamint a rMQR Code nagy kapacitást és kompakt méretet is kínál. Ugyanaz a gyors szkennelés, mint a hagyományos QR-kód esetében, a torzítás észlelésére szolgáló modulok olvasásával valósul meg.

Nemzeti Kibervédelmi Intézet weboldalára mutató rMQR kód

Frame QR-kód

Ennek a típusnak van egy középső területe, amelyben képet lehet elhelyezni. Mivel a keret alakja és színe rugalmasan változtatható, a kódnak sokféle alkalmazása van.

A névjegykártyákra és katalógusokra nyomtatott FrameQR a cég fényképével a weboldalára vezeti az ügyfelet. A QR-kód a hamisítás ellen hologrammal kombinálható.

Kibertámadás! podcast

Aztec kód

nki.gov.hu

Bár a QR-kódhoz hasonlóan néz ki, a Welch Allyn által kifejlesztett azték kód csak egy keresőmintát tartalmaz, pontosan középen.

Maxi kód

Ezt a fajta QR-kódot az Egyesült Államok postája használja. Abban hasonlít az azték kódhoz, hogy a keresőmintát középre helyezi, de négyzetek helyett méhsejtmintát használ.

nki.gov.hu

PDF417

A furcsa nevű PDF417-et 1991-ben találta fel Ynjiun Wang a Symbol Technologies cégtől, és három évvel megelőzte a QR-kódot. Úgy néz ki, mint egy QR-kód és egy vonalkód keveréke, és könnyen felismerhető a téglalap alakjáról.

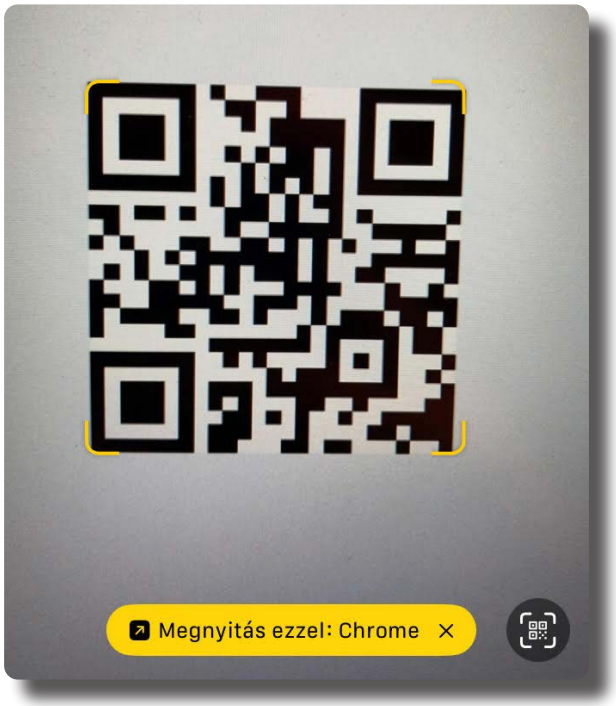
Nemzeti Kibervédelmi Intézet weboldalára mutató PDF417 kód

vCard QR-kód

Virtuális névjegykártyaként működik, és lehetővé teszi kapcsolati adatok megosztását mobileszközökön. A QR-kód tartalmazza az elérhetőségeket, például nevet, telefonszámot, e-mail címet stb. A felhasználók beolvashatják a vCard QR-kódot, megkapják az adatokat, és elmenthetik készülékükre a névjegyet.

Hogyan működnek?

A QR-kódok beolvasásához nem szükséges alkalmazást telepítenünk, használhatjuk a telefon gyári kameráját, ehhez csak rá kell irányítani a kamerát a kódra. Az okostelefon automatikusan felajánlja a link megnyitását, amely lehet URL vagy egy alkalmazás letöltése.



A Nemzeti Kibervédelmi Intézet weblapjának megnyitása Android Google Lens kamera alkalmazással

A Nemzeti Kibervédelmi Intézet weblapjának megnyitása iOS kamera alkalmazással

QR-kód generálásra rengeteg ingyenes eszköz létezik. Egyes alkalmazások képesek QR-kódokat létrehozni, hogy bizonyos információkat adjanak bárkinek, aki beolvassa őket.

A QR-kódokkal egyre több helyen találkozhatunk, helyezhetnek el ilyen kódokat egy parkban, egy történelmileg fontos fa vagy emlékmű tábláján, a park hivatalos alkalmazásával történő beolvasással elindítható egy vezetett túra, vagy egyszerűen megnyitja a park weboldalán található leírást.

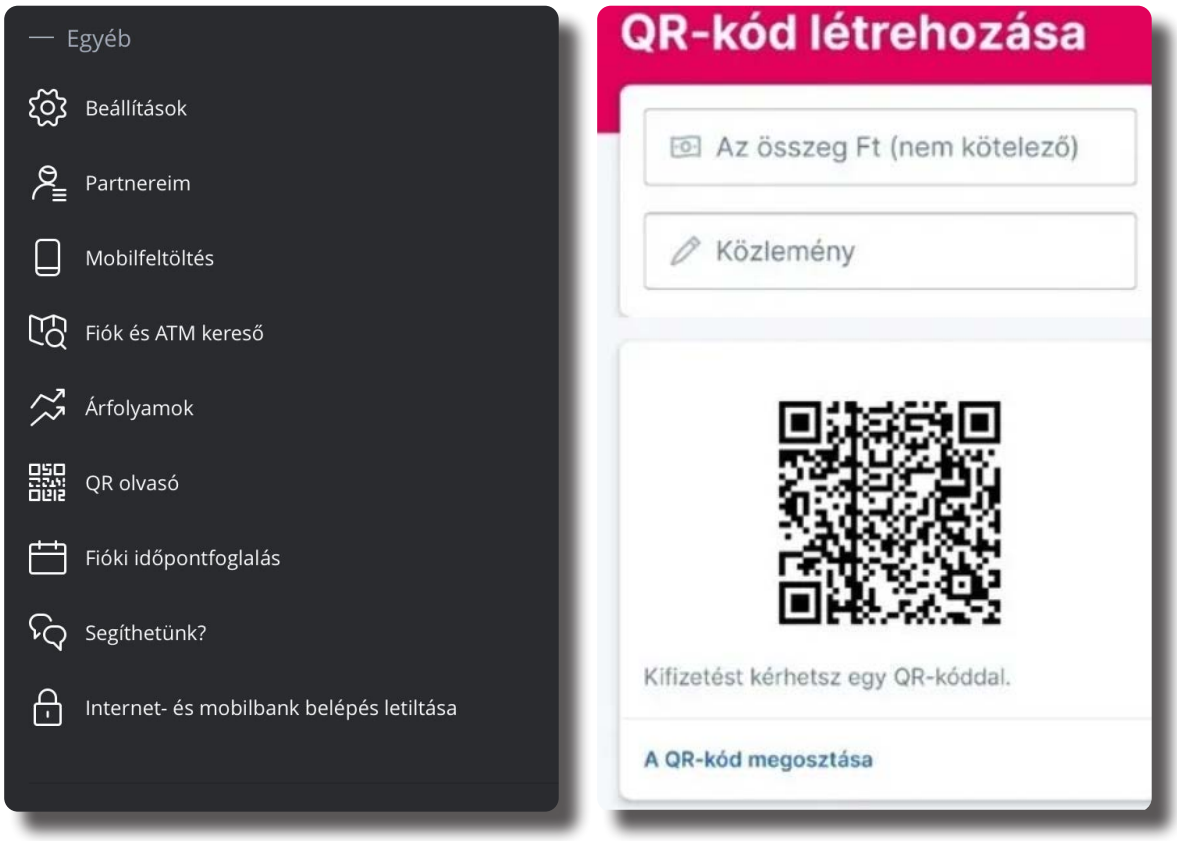
A QR-kódban tárolt adatok tartalmazhatnak weboldal URL-címeket, telefonszámokat vagy akár 4000 karakternyi szöveget. Ezen kívül tárolhatnak még:

- **Közvetlen hivatkozást** egy alkalmazás letöltéséhez az Apple App Store-ból vagy a Google Play-ből.

- **Személyes fiókok hitelesítését és bejelentkezési adatok ellenőrzését** Microsoft Authenticator vagy Google Hitelesítő alkalmazás használatával.

- **Wi-Fi elérést** a titkosítási adatok, például SSID, jelszó és titkosítási típus tárolásával.

- A legtöbb bank mobilalkalmazásában, a „QR olvasás" funkcióval fizethetünk, valamint a "fizetési kérelmekkel" létrehozhatunk QR-kódot. 2024. szeptember 1-től a hazai pénzügyi mobilalkalmazások mindegyikének kötelezően tudnia kell kezelni a QR-kódos fizetést.



QR kód olvasása az OTP alkalmazásában,
valamint fizetési kérelem létrehozása az Erste George alkalmazásában

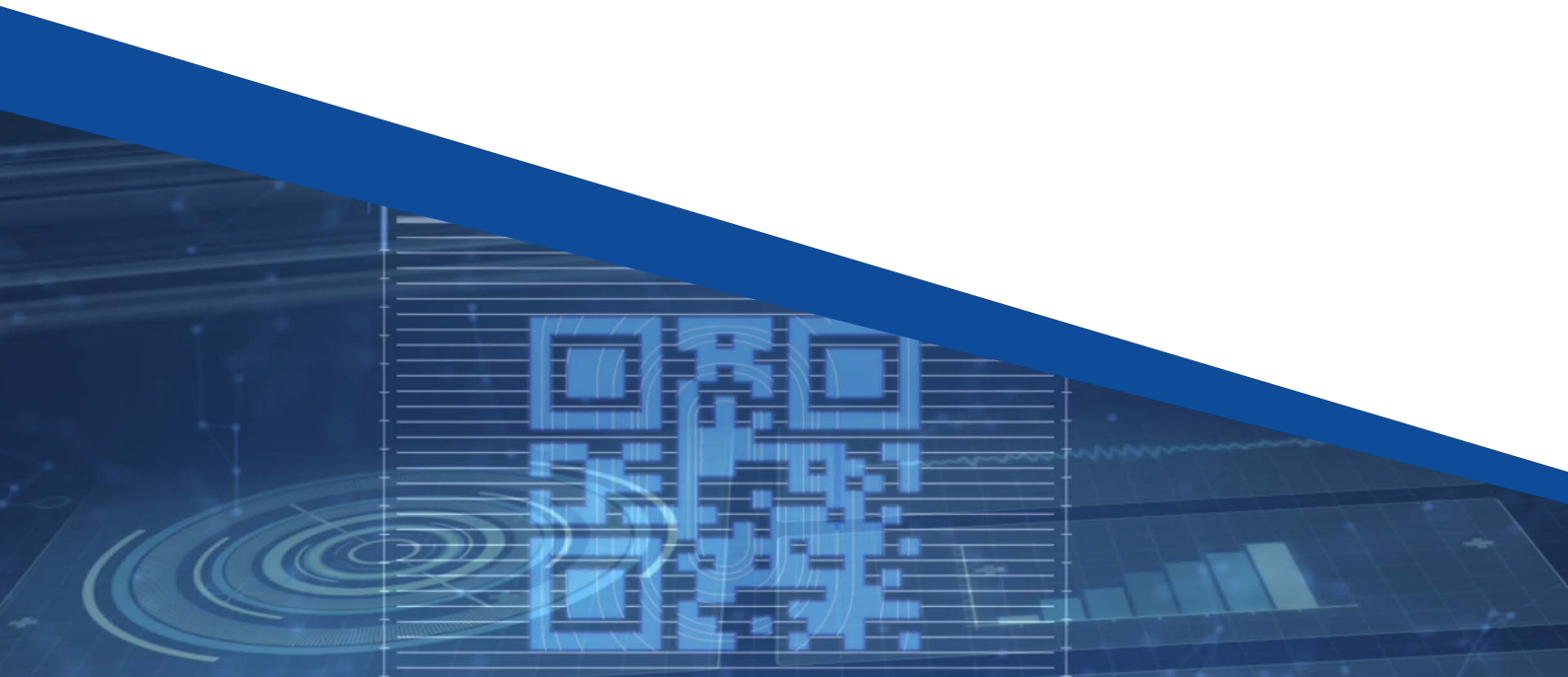
- ..és még sok minden mást. Például egy QR Memories nevű **brit cég még sírkövekre is készít QR-kódokat**, amelyek segítségével az emberek a kódot beolvasva többet olvashatnak az elhunyt személy életéről *(ez lehet akár gyászjelentés vagy hírek az elhalálozottal kapcsolatban)*.

Hogyan használják a kiberbűnözők a QR-kódokat?

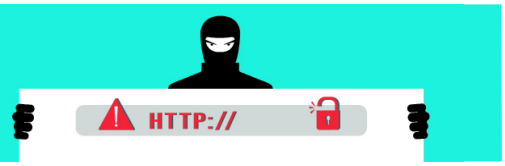
Az emberek nem tudják előre, hogy mi fog történi, ha beolvasnak egy QR-kódot, ezért kénytelenek megbízni annak készítőjében.

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.

A QR-kódok rendkívül hasznosak és elterjedtek lettek a digitalizált világunkban, de a csalók már megtalálták a módját, hogy ezeket károkozásra használják. Ehhez általában elég rávenniük az áldozatot, hogy a készülékén beolvasson egy káros tartalomra mutató QR-kódot.



Adathalász hamis weboldalak



A csalók QR-kódokat helyeznek el hamis weboldalakon vagy matricákon, és különböző trükkökkel – *amelyekre lentebb konkrét példákat is bemutatunk* – arra ösztönzik az embereket, hogy azokat olvassák be a telefonjaikkal. 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 támadók gyakran URL shortenereket használnak, akárcsak az adathalász e-maileknél. Ez jelentősen megnehezíti a hamisítvány felismerését, amikor az okostelefon megerősítést kér.

URL-shortener vagy linkrövidítő:
egy olyan eszköz, amely a hosszú hivatkozásokat sokkal rövidebb hosszúságúvá alakítja, csökkentve ezzel karakterszámát.
A két link ugyanoda fog mutatni, csak megjelenésre,formára különböznek.
(Pl: bit.ly, tinyurl, c9)

TUDTAD?

Papír alapon

A csalást tartalmazó QR-kódot úgy terjesztik, hogy papírra vagy matricára nyomtatják.

Nem ritka, hogy a támadók legitim felek munkájára és hírnevére támaszkodnak, és hivatalos plakátokon, posztereken vagy szórólapokon lévő törvényes QR-kódot a sajátjukra cserélik.

Az Amerikai Egyesült Államokbeli Texasban a csalók több száz parkoló automatán egyszerűen átragasztották a QR-kódot, mely így egy másik, gyorsabb parkolási fizetést ígérő weboldalra vitt, így nem a pakolást rendezte az ügyfél, hanem a csalóknak utalt pénz. Emellett természetesen parkolási bírság vagy akár a jármű elvontatása is társult a kár mellé.

Találkoztak olyan parkolási csalással is, ahol a bűnözők gyorsabb vagy olcsóbb fizetési lehetőséget ígértek a kiragasztott QR-kód segítségével letölthető alkalmazással. A felhasználóknak az app letöltése után meg kellett adniuk bankkártya adataikat, ami a bűnözők kezébe került.

Social Engineering

Hollandiában jegyeztek fel olyan eseteket, amikor embereket idegenek kértek meg az utcán, hogy segítsenek rajtuk egy kisebb értékű kifizetéssel, például a parkolás díjának befizetésével, vagy buszjegy vásárlásával. A pénzt pedig egy QR-kód beolvasásával, és a fizetési adatok megadásával tudták volna elküldeni, azonban a bankkártya adataikat lopták el.

A QR-kódokkal való csalás nem korlátozódik a kiberbűnözőkre. Ausztráliában társadalmi aktivisták is elkezdték használni a QR-kódok helyettesítését ötleteik terjesztésére. A COVID járvány alatt letartóztattak egy férfit, aki a COVID-19 központok bejelentkezési tábláin lévő QR-kódokat lecserélte a sajátjára, ami egy oltásellenes weboldalra vezetett.

Egy QR-kód beolvasásával hozzáadhatóak az elérhetőségi adatok egy névjegykártyáról. A csalók például "Bank" néven új kontaktot adhatnak a címjegyzékéhez, hogy hitelessé tegyék a csaló telefonhívást.

TUDTAD?

Előfordult olyan csalási forma is, amikor a bank nevében, ügyintézői megkeresésnek álcázva hívták fel az áldozatot. A telefonhívás során közölték az „ügyféllel", hogy egy vagy több nagyobb összegű átutalást kezdeményeztek a hívott fél bankszámlájáról. Majd a hívás során a csalók egy QR-kódot küldtek ki, utasítva, hogy olvassa azt be. A beszélgetéssel lefoglalták az áldozatot. A QR-kód beolvasásával hozzáférést adott a csalóknak a banki adataihoz.

E-mail

Nem csak a nyilvános helyeken található QR-kódok nem megbízhatóak. A csalók és a hackerek közvetlenül az e-mail fiókunkra is küldhetnek ilyeneket, vagy az erre a célra létrehozott weboldalakon vagy a közösségi médiában is megoszthatnak ilyen QR-kódot. Az online hirdetésekben jelennek meg QR-kódok, amelyek azt ígérik, hogy különleges ajánlatokhoz vagy termékekhez vezetnek.

Azonban a QR-kódok általában egy rosszindulatú weboldalra irányítják az embereket, vagy akár káros kódot is letöltenek a készülékekre. Sok esetben a Google Play és az App Store logóját is mellé rakják, hogy a bizalmat megteremtse.

Célzott adathalászat (spear phishing)

A csalók képekbe ágyazott QR-kódokat is használnak, hogy megkerüljék a biztonsági eszközök vizsgálatát rosszindulatú hivatkozások után, így az adathalász üzenetek nagyobb valószínűséggel jutnak el a célpont postaládájába. Ezek a csaló e-mailek általában PNG vagy PDF mellékleteket tartalmaznak, amelyekben QR-kód volt megtalálható. Több olyan esetről is tudunk, amikor a csaló e-mailek egy sürgős Microsoft 365 fiókfrissítésre hivatkoztak.

A csalók a címzettektől azt kérték, hogy szkenneljék be, és hajtsák végre a fiókfrissítést 2-3 napon belül. A hitelesítő adatok megadásával a felhasználó elveszítette a fiókját.


Microsoft

Multi-Factor Authentication.

[redacted], you are mandeted to update and enable **2FA** Security on your account as of **6/2/2023**. to mitigate theft and help protect your account. **Quickly scan above QR Code with your phone camera.**

Review security requirements within **72 hours of the received date** by going to View account in the Security Center.

Forrás: cofense.com

Google hirdetések

A South China Morning Post cikke arról számolt be, hogy nőtt a népszerű WhatsApp kommunikációs eszközzel kapcsolatos rosszindulatú weboldalak száma, amelyet rosszindulatú Google hirdetések segítségével terjesztenek. A cikk szerint ezek a hirdetések tavaly átlagosan havi 300 000 dolláros veszteséget okoztak.

A hirdetés egy hiteles kinézetű, a WhatsApp webes változatához hasonló weboldalra vezet. A WhatsApp mobilalkalmazás mellett létezik számítógépekre telepíthető asztali alkalmazás verziója is. A csatlakoztatni kívánt készüléken, a WhatsApp for Windows alkalmazás megnyitását követően, egy QR-kód fog megjelenni, amelyet be kell olvasni a már bejelentkezett telefonnal. Így a QR-kód szkennelése és az új eszköz engedélyezése után a WhatsApp használható a PC-n vagy Mac-en. A probléma az, hogy a szkennelt QR-kód egy olyan rosszindulatú oldalhoz köthető, amelynek semmi köze a WhatsApphoz. Ebben az esetben nem a felhasználó eszköze került hozzáadásra a WhatsApp fiókhoz, hanem a csalóé.

A csaló weboldalra mutató keresési eredmény.

Rosszindulatú alkalmazások

Hasonló sémák becsaphatják a felhasználókat az alkalmazások letöltési hibáival, például úgy, hogy a tervezett játék vagy program rosszindulatú szoftvereket tölt le. Ezen a ponton a határ a csillagos ég; a rosszindulatú szoftverek ellophatják a jelszavakat, rosszindulatú üzeneteket küldhetnek a kapcsolattartóknak és még sok más módon okozhatnak kárt.

Wi-Fi hálózati csalások

Csalók olyan QR-kódokat osztanak meg, amelyekkel látszólagosan ingyenes Wi-Fi-hez lehet csatlakozni. Amikor az emberek beolvassák ezeket a kódokat, a támadók hozzáférnek az eszközökhöz, és megfigyelhetik az online tevékenységeket.

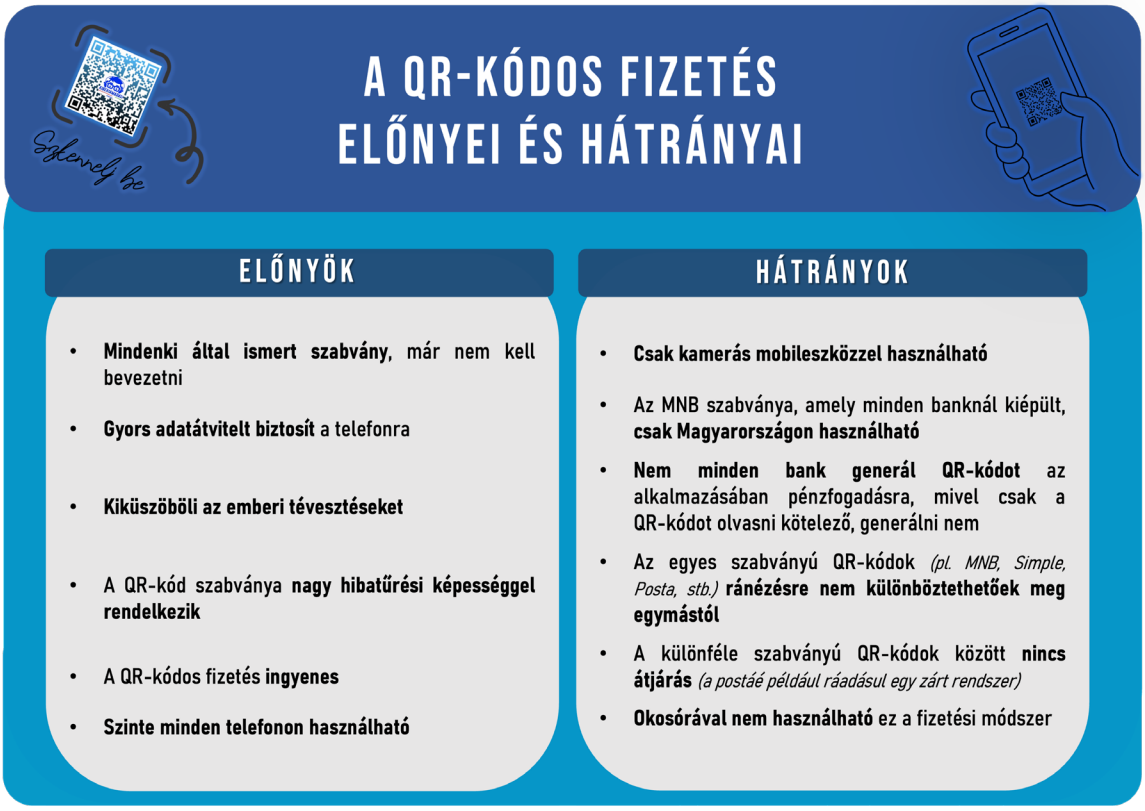
Ransomware terjesztés

A támadók QR-kódokat helyezhetnek el például hamis alkalmazásokon keresztül, amelyeket az emberek letölthetnek. Ezek az alkalmazások ransomware-t tartalmazhatnak, amely zárolja az eszközt, és váltságdíjat követel a feloldáshoz.

További lehetséges QR-kódolt parancsok

A weboldalakra való hivatkozáson túl a QR-kód tartalmazhat bizonyos műveletek elvégzésére vonatkozó parancsokat is. Ezek a többek között lehetnek:

- Kapcsolat hozzáadása
- Kimenő hívás kezdeményezése
- E-mail szerkesztése, címzett és a tárgysor kitöltés
- Szöveges üzenet küldése
- Megoszthatja a tartózkodási helyét egy alkalmazással
- Közösségi média fiók létrehozása
- Naptári esemény ütemezése
- Egy preferált Wi-Fi hálózat hozzáadása a hitelesítő adatokkal az automatikus csatlakozáshoz



Mint a fentiekből is látszik, a QR-kódok felhasználási területe igen széles, azonban pont ez ad a csalóknak lehetőséget új visszaélések kitalálásához.

A Magyar Nemzeti Bank készített egy weboldalt, ahol a fizetési kérelmek beolvasásával annak részleteit tekinthetjük meg.

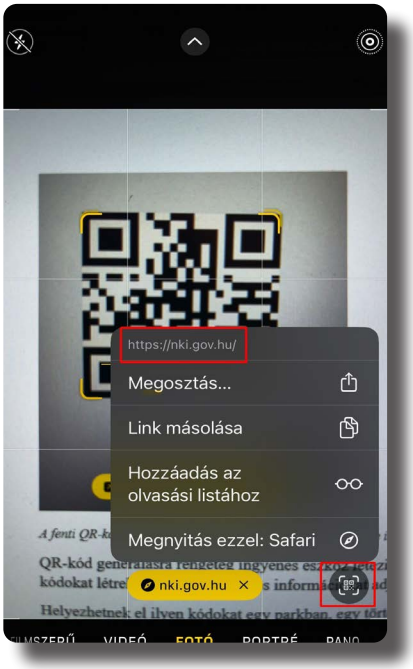
Íme néhány további tipp a QR-kódos csalások elkerüléséhez, amellyel megvédhetjük magunkat a kiberbűnözőktől:

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!

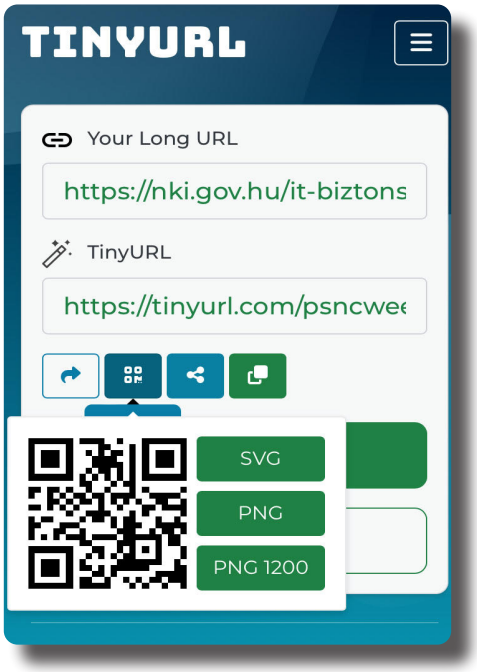
- **Legyünk óvatosak, mielőtt eszközünkkel beolvasunk egy QR-kódot!**

- A legtöbb QR-kód egy vagy több URL-t tartalmaz, amelyek beolvasáskor felbukkannak a képernyőn.
  Mindig ellenőrizzük a linkeket, mielőtt rákattintunk!
  Egy QR-kód azonban csak körülményesen ad módot erre.



- **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.

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.

- **A QR-kód hitelességének ellenőrzéséhez figyeljük meg az apró részleteket!** Például egy számos nyelvtani hibát és elrendezést tartalmazó poszter valószínűleg nem megbízható.

- 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!
- **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!**

Fontos, hogy tisztában legyünk alap szinten a QR-kódok működésével, mert így tudunk felkészülni az ilyen módon elkövetett csalásokra.

- **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?

Összefoglalás

- Fontos előírás az egységes adatbeviteli szabvány (QR, NFC, deeplink) alkalmazása és a fizetési kérelem fogadásának biztosítása.
- Megújult az azonnali fizetési tranzakciók indítására alkalmas QR-kód szabvány.
- Az Azonnali fizetési rendszerben teljesülő tranzakciók 10 millió forintos értékhatárát 20 millió forintra emelték.
- Az intézkedéscsomag többi részét 2024. szeptember 1-ig kell az érintetteknek teljesíteni.
- Folyamatban van az azonnali fizetést népszerűsítő egységes arculati elemek kidolgozása.
- A Magyar Nemzeti Bank készül egy edukációs kampánnyal is.
- Kidolgozás alatt van az Azonnali fizetéshez kapcsolódó speciális visszatérítési mechanizmus.
- A Magyar Nemzeti Bank vizsgálja a központi üzleti modell szükségességét.
- A pénzügyi tranzakciós illeték mentessége kiterjesztésre került az egységes adatbeviteli megoldás útján benyújtott vagy a fizetési kérelemmel kezdeményezett azonnali átutalási megbízások esetében.
- Kidolgozás alatt van a Magyar Nemzeti Bank 2030-ig terjedő pénzforgalmi stratégiája.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023