

Uważaj na oszustwa z wykorzystaniem kodu QR

Przestępcy coraz częściej wykorzystują kody QR do kradzieży danych osobowych, infekowania urządzeń złośliwym oprogramowaniem czy dokonywania nieautoryzowanych transakcji. Zjawisko to ma już nawet swoją nazwę, jest to tzw. quishing.

Przestępstwo przy użyciu kodu QR polega na spreparowaniu kodu QR, który po zeskanowaniu przekierowuje nas na fałszywe strony internetowe lub inicjuje pobieranie złośliwego oprogramowania. Są one wyjątkowo skuteczne, gdyż nie widzimy zawartości kodu QR przed jego zeskanowaniem.

Najczęstsze oszustwa z użyciem QR kodu:

- płatność za parkowanie – kody QR umieszczone na parkometrach w przestrzeni publicznej są łatwym celem dla oszustów. Podmieniony kod może przekierować użytkownika na fałszywą stronę płatności. Ludzie często śpiesząc się nie weryfikują poprawności linku.
- przyjmowanie paczek, których nie zamawialiśmy- oszuści na nasz adres nadają paczki, których w rzeczywistości nie zamawialiśmy. Ich odbiór wiąże się z zeskanowaniem kodu QR oraz podaniem danych osobowych, danych karty, hasła lub PIN-u.
- fałszywe mandaty - za wycieraczką samochodu można znaleźć wezwanie do zapłaty za rzekome wykroczenie drogowe, wraz z kodem QR „do szybkiej płatności”. Zeskanowanie takiego kodu może skutkować utratą pieniędzy i udostępnieniem danych przestępcom.
- fałszywe kupony- oszuści tworzą fałszywe kupony przy użyciu generatora kodów QR. Następnie wysyłają je SMS-em, mailem lub rozdają ulotki na ulicach, wraz z instrukcją dotyczącą ich użycia. Zeskanowanie kodu grozi utratą danych lub zainfekowaniem urządzenia.

Jak rozpoznać, że kod QR jest fałszywy?

- Sprawdź, czy kod nie nosi śladów podmiany lub manipulacji np. jest naklejony na innym kodzie
- Sprawdzaj adres URL używając podglądu linku z kodem QR (prawidłowe łącze powinno zaczynać się od https:// lub mieć symbol kłódki na początku adresu)
- Oceń, skąd pochodzi wiadomość zawierająca kod - czy adres e-mail wygląda profesjonalnie, nie zawiera błędów językowych, czy logo i nazwa marki są poprawne

Zasady bezpieczeństwa - co warto zapamiętać:

- Policja lub Straż Miejska nigdy nie przesyła mandatów z kodem QR - wręczane są one osobiście;
- nie skanuj kodu QR, jeśli nie masz wiedzy do czego on Cię zaprowadzi;
- znane marki i sklepy internetowe zazwyczaj nie wysyłają kodów QR;
- wiadomość z kodem QR od nieznanego nadawcy jest podejrzana;
- nie odbieraj przesyłek, których się nie spodziewasz;
- nigdy nie podawaj poufnych danych nieznanemu osobie;
- używaj aplikacji do skanowania kodów QR, które posiadają funkcję podglądu adresu URL;
- nie działaj pod presją czasu - oszuści często próbują ją wywołać;
- regularnie aktualizuj oprogramowanie antywirusowe.

Zawsze bądź ostrożny! Jeśli przez nieuwagę zeskanowałeś kod QR chcąc np. opłacić fałszywy mandat lub udostępniłeś swoje dane, jak najszybciej skontaktuj się z bankiem w celu zablokowania transakcji i dostępu do rachunku. Zgłoś również sprawę na policję.