

Uważaj na fałszywe QR kody

Przestępcy coraz częściej wykorzystują **QR kody** czyli **quishing** do kradzieży danych osobowych, dokonywania nieautoryzowanych transakcji oraz infekowania urządzeń złośliwym oprogramowaniem.

Atak polega na spreparowaniu kodów QR, które po zeskanowaniu przekierowują nas na fałszywe strony internetowe lub inicjują pobieranie złośliwego oprogramowania. Swoją skuteczność zawdzięcza faktowi, że nie widzimy zawartości QR kodu przed jego zeskanowaniem.

Najczęstsze oszustwa z wykorzystaniem QR kodów:

- dokonywanie płatności za parkowanie - parkomaty znajdują się w miejscach publicznych dzięki czemu oszuści mają łatwy dostęp do manipulacji przy kodach. Dodatkowo ludzie korzystający z parkingów zazwyczaj śpieszą się w miejsce docelowe i nie weryfikują poprawności kodów;
- fałszywe mandaty - oszuści wystawiają fałszywe wezwania do zapłaty za interwencję służb, dotyczącą złamania przepisów ruchu drogowego i umieszczają np. za wycieraczką auta. Kod QR umożliwia szybką zapłatę za mandat, a w rzeczywistości prowadzi do utraty środków i udostępnienia danych;
- przyjmowanie paczek, których nie zamawialiśmy - oszuści nadają przesyłki, które nie były przez Ciebie zamawiane. Często ich odbiór wiąże się z zeskanowaniem kodu QR oraz podaniem danych osobowych, danych karty kredytowej, hasła lub PINu;
- fałszywe kupony - przestępcy tworzą fałszywe kupony przy użyciu generatora kodów QR. Następnie rozsyłają je SMSem lub e-mailem wraz z instrukcją dotyczącą skanowania kodu przy kasie. Zeskanowanie kodu grozi utratą danych karty kredytowej lub zainfekowaniem urządzenia.

Jak rozpoznać fałszywy QR Kod:

- zwróć uwagę na stan fizyczny kodu i potencjalne oznaki manipulacji,
- sprawdź adres URL używając podglądu linka z kodem QR (prawidłowe łącze powinno zaczynać się od „https://” lub mieć symbol kłódki na początku adresu URL),
- dokładnie sprawdź adres, z którego został przesłany QR kod (logo, gramatyka, nazwa marki w adresie e-mail).

Pamiętaj:

- Funkcjonariusze Policji wystawiają mandaty osobiście;
- Wiadomość z QR kodem od nieznanego nadawcy jest podejrzana;
- Nie skanuj kodów QR jeśli nie wiesz do czego służą;
- Większość znanych marek unika wysyłania kodów QR;
- Nie odbieraj przesyłek, których się nie spodziewasz;
- Nie podawaj poufnych informacji osobie nieznanej;

- Używaj aplikacji do skanowania kodów QR z funkcją podglądu adresu URL;
- Nie działaj pod presją czasu;
- Regularnie aktualizuj oprogramowanie antywirusowe.

Bądź ostrożny! Jeżeli przez nieuwagę opłaciłeś 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.