Oszustwo na kod QR: nowa plaga cyberprzestępców

Kategoria: Styl życia
Opublikowano: wtorek, 09, wrzesień 2025 09:42
Ewelina Kocemba

Cyberprzestępcy do kradzieży danych osobowych wykorzystują już nie tylko fałszywe linki, ale także kody QR. Co więcej, działają zarówno w świecie online, jak i offline. Umieszczają podrobione piktogramy w wiadomościach e-mail, SMS-ach, załącznikach z plikami PDF, czy na parkomatach bądź tabliczkach przy szlakach turystycznych.

Tego typu oszustwo doczekało się nawet własnej nazwy - quishing. Nic dziwnego, ponieważ z danych firmy Check Point Software wynika, że w latach 2021-2024 ataki phishingowe oparte o kody QR wzrosły o 900 proc.

Cyberprzestępcy są wyjątkowo sprytni, ponieważ przed tego typu oszustwem szczególnie trudno się uchronić. Aż 83 proc. Polaków deklaruje, że nie otwiera podejrzanych linków i załączników. Nieco częściej kobiety (85 proc.) niż mężczyźni (80 proc.) – wynika z badania przeprowadzonego na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów. Niestety, często kody QR są w stanie ominąć filtry antyspamowe, ponieważ dla systemów pocztowych są jedynie grafiką. Oznacza to, że nie da się ich automatycznie odczytać i przeanalizować, tak jak tradycyjnych odnośników do stron internetowych. W związku z tym zagrożenie kradzieży danych osobowych jest bardzo poważne.

Ponadto cyberprzestępcy umieszczają również fałszywe kody QR w treści SMS-ów tworząc pozory wiarygodności. Podszywają się pod firmy kurierskie, platformy sprzedażowe czy instytucje państwowe, pod pretekstem odbioru paczki, nagrody lub zapłaty mandatu. Niestety, Polacy przyznają, że najczęściej mieli do czynienia z wyłudzeniem danych osobowych lub jego próbą poprzez e-mail (47 proc.) lub SMS (40 proc.).

To nie paczka, to pułapka

Metoda działania oszustów jest zaskakująco prosta i paradoksalnie właśnie dlatego tak skuteczna. Zamiast wysyłać klasyczny link tekstowy, podszywają się pod znane marki i instytucje, zamieszczając kod QR prowadzący do fałszywej strony logowania lub formularza płatności. W ostatnich miesiącach szczególnie często wykorzystują do tego popularne platformy sprzedażowe, takie jak Allegro czy OLX. Wystarczy krótka wiadomość z informacją o sprzedaży przedmiotu i prośbą o potwierdzenie odbioru środków, by niczego niepodejrzewający użytkownik zeskanował kod. W rzeczywistości trafia on na stronę phishingową, gdzie przestępcy próbują wyłudzić dane osobowe.

- Z pozoru niewinny kod QR może być początkiem bardzo poważnych kłopotów. Po zeskanowaniu przez nas piktogramu oszuści są w stanie przejąć dane logowania do bankowości internetowej, numer karty płatniczej czy inne wrażliwe informacje. W efekcie możemy nie tylko stracić wszystkie pieniądze z konta, ale też narazić się na ryzyko kradzieży danych osobowych, w tym PESEL-u, wraz z próbami zaciągnięcia kredytu lub pożyczki na nasze nazwisko – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Oszustwo za szybą

Jednak oszustwa z wykorzystaniem kodów QR nie ograniczają się tylko do Internetu, a coraz częściej przenoszą się również do codziennego życia. We Wrocławiu zgłoszono przypadki fałszywych naklejek z piktogramami umieszczanych na parkomatach, które wyglądały jak oficjalna metoda płatności, a w rzeczywistości prowadziły do stron wyłudzających dane karty.

Oszuści stosują również inne formy podszywania się pod instytucje publiczne. Znane są przypadki, gdzie

kierowcy znajdowali za wycieraczkami samochodów kartki łudząco przypominające mandaty, opatrzone logotypami policji lub Krajowej Administracji Skarbowej. Zawierały one kod QR, który po zeskanowaniu kierował na fałszywą stronę płatności. Innym niepokojącym przykładem są tabliczki z piktogramami rozwieszane w lasach, m.in. w rejonie Wałbrzycha. Leśnicy oficjalnie apelują, aby ich nie skanować, ponieważ mogą prowadzić do złośliwych stron lub służyć do wyłudzania danych osobowych.

Lepiej sprawdź, zanim zeskanujesz

Niestety, ataki z wykorzystaniem kodów QR są skuteczne, bo opierają się na prostym mechanizmie: ofiara nie widzi, co skanuje. W przeciwieństwie do tradycyjnego linku, zawartość piktogramu nie jest widoczna od razu, a dopiero po zeskanowaniu okazuje się, do jakiej strony internetowej nas przekieruje. To wystarczy, by wiele osób działało impulsywnie, zwłaszcza gdy wiadomość sugeruje pilną potrzebę zapłaty, odbioru nagrody czy uniknięcia mandatu.

- Do kodów QR, podobnie jak do podejrzanych linków, trzeba mieć ograniczone zaufanie. Jeśli adres odnośnika do strony jest nietypowy, skrócony, zawiera literówki lub wygląda inaczej niż oficjalna domena znanej firmy czy instytucji państwowej, to powinien być to dla nas sygnał ostrzegawczy. Nie należy też skanować przypadkowych piktogramów umieszczonych w miejscach publicznych, na plakatach, ulotkach czy w mailach od niezweryfikowanych nadawców. Pod żadnym pozorem nie można również podawać danych logowania, PESEL-u czy numeru karty płatniczej po zeskanowaniu kodu QR z nieznanego źródła – przestrzega Bartłomiej Drozd.

Aby dodatkowo zwiększyć bezpieczeństwo, warto upewnić się, dokąd prowadzi piktogram. W tym celu możemy najpierw zrobić zdjęcie lub zrzut ekranu, a następnie sprawdzić zawartość kodu QR za pomocą darmowych serwisów online. Tego typu narzędzia pozwalają wyświetlić pełny adres URL zakodowany w grafice, zanim zdecydujemy się otworzyć link prowadzący do strony.

Ponadto należy też unikać korzystania ze standardowych skanerów kodów QR umieszczonych w aparacie smartfonów. Lepszym rozwiązaniem są aplikacje mobilne, które również umożliwiają zapoznanie się z pełnym adresem URL linku przed jego otwarciem.

Źródło: IP