Kod QR równie niebezpieczny jak fałszywy link

Kategoria: Styl życia
Opublikowano: czwartek, 07, marzec 2024 12:19
Joanna Gryboś-Chechelska

70 proc. Polaków powyżej 18 r.ż. skanowało kod QR, a 64 proc. z nich robi to regularnie. Są one coraz popularniejsze, używa się ich m.in. do płatności online. Ten fakt wykorzystują również cyberprzestępcy, którzy za pomocą takich fałszywych piktogramów wyłudzają dane osobowe, uzyskują dostęp do kart płatniczych czy bankowości internetowej, albo infekują telefon złośliwym oprogramowaniem – ostrzegają eksperci serwisu ChronPESEL.pl.

Polacy najczęściej skanują kody QR w sklepach i drogeriach (38 proc.), na stronach internetowych (37 proc.) i w środkach transportu (26 proc.) – wynika z badania HX Study, zleconego przez agencję Starcom, we współpracy z ekspertami NextTechNow oraz firmami AMS i Hashting. Nie uszło to uwadze cyberprzestępców, którzy zaczęli tworzyć podrobione piktogramy przekierowujące nieświadome zagrożenia osoby do fałszywych stron internetowych. Zjawisko stało się na tyle powszechne, że zyskało własną nazwę – quishing. W Polsce znane są już przypadki wykorzystania quishingu np. do wyłudzania danych poprzez umieszczenie podrobionych naklejek z kodami QR na parkomatach.

Skanowanie w miejscach publicznych to ryzyko

Kody QR to kwadratowe obrazy z szeregiem czarno-białych wzorów, które są umieszczane w Internecie, gazetach, broszurach lub na plakatach. Umożliwiają zapisanie dużej ilości danych na małej powierzchni. Zeskanowanie tego rodzaju znaku graficznego pozwala przejść bezpośrednio na stronę internetową czy do aplikacji, co znacznie oszczędza nasz czas. Za ich pomocą właściciele smartfonów mogą m.in. realizować płatności online, skasować bilet komunikacji miejskiej czy przeglądać menu restauracji. Dla co drugiego Polaka najistotniejszym powodem wykorzystywania kodów QR jest szybkość dostępu do informacji (51 proc.). Następnie główną przyczyną jest możliwość uzyskania zniżek lub rabatów (45 proc.), dostęp do dodatkowych informacji (31 proc.), a także brak konieczności dotykania ekranu lub ulotki (27 proc.).

Skanowanie kodów QR w sklepie czy restauracji jest raczej bezpieczne, ale w miejscach publicznych musimy zachować szczególną ostrożność, ponieważ nie mamy pewności, że cyberprzestępcy ich nie podmienią. Oszuści mogą np. umieścić fałszywe naklejki na parkomatach czy plakatach na przystanku. W ten sposób można zamaskować niebezpieczne linki, a następnie przy dokonywaniu przez nas płatności przekierować np. na łudząco przypominającą prawdziwą stronę banku.

Kierowcy i turyści na celowniku cyberprzestępców

Cyberprzestępcy za pomocą quishingu mogą np. zaatakować kierowców płacących za parkowanie. W ubiegłym roku na niektórych parkomatach w Krakowie umieszczono fałszywe kody QR, które umożliwiły oszustom przechwycenie danych z kart płatniczych. Wykorzystana do wyłudzenia strona internetowa bardzo przypominała witrynę Zarządu Dróg Miasta Krakowa. W efekcie część kierowców straciła pieniądze.

– Zapłacić za parkowanie czy bilet wstępu po zeskanowaniu kodu QR można w wielu parkach narodowych, np. kierowcy mogą skorzystać z tej opcji przy wejściu do Tatrzańskiego Parku Narodowego czy Karkonoskiego Parku Narodowego. Jednak tablice z piktogramami często stoją w odludnych miejscach, gdzie oszuści bardzo łatwo mogą je podmienić. Tymczasem przez cały rok tymi szlakami wędruje tysiące turystów, którzy mogą być poważnie narażeni na quishing – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Wyłudzenie danych do kart płatniczych podczas wnoszenia opłat za parkowanie to nie jedyny pomysł cyberprzestępców. W ubiegłym roku mieszkańcy Warszawy znajdowali za wycieraczkami swoich

samochodów mandaty z kodami QR. Po zeskanowaniu kierowca był przekierowywany na fałszywą stronę, na której mógł pozostawić własne dane. W ten sposób oszuści mogą nie tylko uzyskać dostęp do loginów płatniczych, lecz także imienia, nazwiska, numeru PESEL lub dowodu osobistego, które można wykorzystać np. do zaciągnięcia kredytu. Kolejnym zagrożeniem może być zainfekowanie smartfona złośliwym oprogramowaniem. Wówczas przestępcy zyskują dostęp do wielu zgromadzonych na nich danych.

Liczba wyłudzeń błyskawicznie rośnie

W pierwszych dziewięciu miesiącach 2023 r. w Wielkiej Brytanii odnotowano ponad 400 cyberprzestępstw przy użyciu fałszywych kodów QR. To o około 300 więcej w porównaniu do 2020 r. – wynika z danych organizacji Action Fraud udostępnionych stacji BBC. Mimo że w Polsce nie prowadzi się osobnych statystyk dla przestępstw z wykorzystaniem quishingu, problem jest bez wątpienia bardzo poważny, skoro przed tym zagrożeniem ostrzega Ministerstwo Cyfryzacji, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Komisji Nadzoru Finansowego (CSIRT KNF) czy Zespół Szybkiego Reagowania na Incydenty Komputerowe (CERT).

Ponadto najczęściej dowiadujemy się o oszustwie z opóźnieniem. Wyjątkiem jest oczywiście sytuacja, gdy z konta bankowego znikają pieniądze. Ale gdy przestępcy przejmą nasze dane osobowe pozostawione na fałszywym formularzu albo zainfekują złośliwym oprogramowaniem smartfona, to często ich ofiary mogą nie skojarzyć negatywnych skutków takich działań z zeskanowaniem fałszywego piktogramu, np. na parkingu w czasie ferii zimowych. Kiedy więc mamy do czynienia z kodem QR umieszczonym w miejscu publicznym, lepiej wejść na stronę internetową usługodawcy i zapłacić za jej pośrednictwem. W taki sposób można bezpiecznie kupować bilety wstępu do parków narodowych.

– Należy pamiętać, że kody QR to również linki i zeskanowanie znaku graficznego może być tak samo niebezpieczne jak otwarcie odnośnika otrzymanego mailem czy SMS-em. Każdy może nakleić fałszywy piktogram na parkomat, plakat na przystanku czy sklepową lub restauracyjną witrynę. Warto więc wyłączyć w smartfonie opcję automatycznego skanowania kodów QR bądź samodzielnie wpisać adres strony w przeglądarkę i upewnić się, że cyberprzestępcy nie podmienili podobnie wyglądających liter. Należy również bardzo ostrożnie podawać dane osobowe lub loginy do bankowości internetowej, szczególnie podczas dokonywania płatności. Czerwona lampka powinna się nam także zapalić, jeśli po zeskanowaniu znaku jesteśmy proszeni o pobranie pliku, aplikacji lub aktualizacji – wyjaśnia Bartłomiej Drozd.

Źródło: IP