Bitdefender

Quishing – niebezpieczne kody QR

25.01.2024

Czy skanujesz kody QR, aby sprawdzić menu restauracji, parkometry, otrzymać kupon rabatowy, połączyć się z firmową siecią Wi-Fi lub dowiedzieć się więcej o miejscu historycznym? Kody QR są wszędzie i stały się częścią naszego codziennego życia. Czasami jednak nie są one tym, czym myślisz, że są. Federalna Komisja Handlu (FTC) ostrzega, że oszuści ukrywają szkodliwe linki w kodach QR i wykorzystują je w atakach phishingowych, co jest taktyką znaną jako quishing.

Co to jest Quishing i jak działa?

Phishing jest metodą oszustwa, przybierającą różne formy w zależności od trendów cyfrowych. Atak ten ma na celu oszukanie ludzi w dowolny sposób w celu ujawnienia poufnych informacji, takich jak nazwy użytkowników, hasła i dane karty kredytowej, które można następnie wykorzystać do dalszych działań przestępczych.

Biorąc pod uwagę popularność kodów QR i, co ważniejsze, tendencję do

ich skanowania bez kwestionowania ich przeznaczenia, kody QR stały się doskonałymi narzędziami dla oszustów.

Manipulując kodami QR, oszuści kierują osoby na fałszywą stronę internetową, która wygląda na wiarygodną. Jeśli zalogujesz się na tej fałszywej stronie, oszuści mogą ukraść wszelkie wprowadzone przez Ciebie informacje.

Alternatywnie kod QR może zainstalować złośliwe oprogramowanie, które po cichu zbiera Twoje informacje, zanim jeszcze zdasz sobie z tego sprawę.

Krótka historia kodów QR

Kody QR, zwane także kodami szybkiej odpowiedzi, zostały wynalezione przez Masahiro Harę, pracownika japońskiej firmy motoryzacyjnej Denso Waves, w 1994 roku.

Firma stanęła przed wyzwaniami związanymi z tradycyjnymi kodami kreskowymi, wymagającymi maksymalnie 10 znaków na jednym produkcie. Takie podejście doprowadziło do opóźnień w produkcji, ponieważ skanery miały trudności z odczytaniem ich z jednego kierunku.

Masahiro Hara znalazł inspirację dla kodów QR podczas gry Go. Uświadomił sobie, że podobny system oparty na siatce, jak plansza do gry GO, może przechowywać więcej informacji w jednym kodzie i być odczytywany z wielu kierunków, kątów i odległości.

Popularność kodów QR nastąpiła w 2020 r., kiedy wybuchła pandemia, i wszyscy unikali kontaktu fizycznego.

Quishing – przykłady?

Oto różne scenariusze, w których możesz napotkać złośliwy kod QR:

· E-maile i wiadomości: cyberprzestępcy często wysyłają kody QR za pośrednictwem e-maili lub wiadomości, udając, że pochodzą z legalnych źródeł, takich jak znane firmy lub marki.

· Fałszywe promocje: wiele zwodniczych kodów QR prowadzi do przekonania, że otrzymasz zniżkę lub ofertę specjalną.

· Przestrzeń fizyczna: fałszywe kody QR strategicznie umieszczone w przestrzeni publicznej, na plakatach, a nawet na opakowaniach produktów.

Strategie oszustów mające na celu nakłonienie Cię do zeskanowania ich złośliwych kodów QR:

Cyberprzestępcy mogą wykazać się dużą kreatywnością, stosując różne przebiegłe taktyki, aby nakłonić Cię do zeskanowania ich fałszywych kodów QR, począwszy od zakrywania własnych legalnych kodów QR po wysyłanie przekonujących e-maili i wiadomości.

Oto kilka sposobów, w jakie próbują Cię oszukać:

Przestępcy mogą podszywać się pod firmę kurierską i mówić, że nie mogli dostarczyć Twojej paczki, więc proszą Cię o skontaktowanie się z nimi w celu zmiany terminu. Następnie udają, że jest problem z Twoim kontem i nalegają, abyś potwierdził swoje dane. Później kłamią na temat wykrycia podejrzanej aktywności na Twoim koncie i namawiają Cię do zmiany hasła. Ich przesłania wywołują poczucie pilności. Chcą tylko, żebyś zeskanował ich kod.

Jak się chronić przed quishingiem?

„Jeśli chcesz sprawdzić, czy dany kod QR jest niebezpieczny to, użyj Bitdefender Scamio, czyli bezpłatnego narzędzia antyphishingowego. Możesz z nim rozmawiać na Messengerze lub w przeglądarce. Jeśli napotkasz podejrzany kod QR, to przeskanuj go za pomocą Scamio i poczekaj, aż narzędzie go przeanalizuje i wskaże czy dany kod QR jest złośliwy, czy nie” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Inne opcje:

- Sprawdź adres URL przed jego otwarciem. Jeśli wygląda na znajomy adres URL, upewnij się, że nie jest sfałszowany, sprawdzając, czy nie ma błędów ortograficznych lub zamienionych liter.

- Nie skanuj kodu QR w wiadomości e-mail lub SMS, której się nie spodziewałeś. Jeśli chcesz sprawdzić, czy wiadomość jest wiarygodna, skontaktuj się z firmą telefonicznie lub za

pośrednictwem strony internetowej.

- Chroń swój telefon i konta. Korzystaj z odpowiedniego oprogramowania antywirusowego na swoich urządzeniach i chroń swoje konta internetowe za pomocą silnych haseł oraz uwierzytelniania wieloskładnikowego.

- Jeśli zeskanujesz fałszywy kod QR, zmień hasła do kont, do których mogłeś dać dostęp oszustom, i monitoruj swoje konta.

Źródło: https://bitdefender.pl/quishing-niebezpieczne-kody-qr/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 25.01.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz

EDR i XDR.