Bitdefender

Uważaj na 6 oszustw związanych z parkowaniem

14.06.2024

Wkrótce rozpocznie się sezon wakacyjny, co może sprzyjać pewnemu nieoczywistemu rodzajowi cyberoszustwa, o którym większość użytkowników sieci nie wie, czyli oszustwach związanych z wyłudzaniem danych i pieniędzy za pomocą aplikacji do uiszczania opłat za parkowanie samochodu. Jak zauważają eksperci do spraw cyberbezpieczeństwa z Bitdefender, to coraz powszechniejsze niebezpieczeństwo i warto się z nim zapoznać, szczególnie jeśli planujemy wakacyjną podróż samochodem za granicę.

Oszustwa związane z parkowaniem

Cyberprzestępcy coraz częściej wykorzystują technologię do nakłonienia niczego niepodejrzewających kierowców do zapłacenia im pieniędzy za parkowanie. Oszuści mogą na przykład zrobić fałszywe bilety i zostawić je na przedniej szybie samochodu z prośbą o dokonanie płatności online lub za pośrednictwem PayPal.

W innych przypadkach udostępniają fałszywe kody QR, które przekierowują właścicieli samochodów do fałszywej witryny płatniczej lub wysyłają e-maile z informacją, że użytkownik musi zapłacić za zaległy bilet parkingowy.

Jeśli internauta postąpi zgodnie z instrukcjami zawartymi w którejkolwiek wersji oszustwa, zapłaci karę, która nie została na niego nałożona, lub będzie mieć wrażenie, że naprawdę zapłacił za parking, w efekcie czego otrzyma mandat. Warto także zauważyć, że takie oszustwa często mają także na celu wyłudzenie danych, które zostaną wpisane w fałszywym formularzu.

Ostrzeżenie dla kierowców związane z gwałtownym wzrostem liczby oszustw związanych z parkowaniem za pomocą kodów QR

Zespół Bitdefender przygotował krótki przewodnik, który pomoże Ci zrozumieć, jak działają oszustwa związane z parkowaniem, rozpoznać te najczęstsze i uchronić się przed staniem się ich ofiarą.

6 najczęściej zgłaszanych oszustw parkingowych, o których powinieneś wiedzieć

Fałszywe bilety parkingowe za przednią szybę

Oszuści wykorzystujący zaawansowane, przenośne drukarki do tworzenia fałszywych biletów parkingowych. Umieszczają je na samochodach, namawiając niczego niepodejrzewających kierowców do płacenia kar w Internecie lub za pośrednictwem usług takich jak PayPal.

Niektóre fałszywe bilety zawierają nawet kod QR, który przenosi ofiary na stronę zawierającą nieuczciwą płatność. Jeśli zastosujesz się do tych instrukcji, zapłacisz grzywnę, której nie jesteś winien, a oszuści mogą ukraść Twoje dane osobowe.

2. Fałszywi pracownicy parkingu

W tym rodzaju oszustwa fałszywy pracownik kieruje Cię na pobliski parking. Płacisz za miejsce parkingowe i otrzymujesz rachunek płatności jako dowód zakupu. Jednak po powrocie do samochodu odkryjesz, że osoba, która skierowała Cię do parkingu, była oszustem, która zabrała Twoje pieniądze i zniknęła, zostawiając Twój samochód zaparkowany nielegalnie. Prawdziwy właściciel działki może odholować twój samochód, lub nałożyć na Ciebie karę finansową.

3. Fałszywe kody QR

Oszuści umieszczają fałszywe naklejki z kodem QR na parkometrach lub innych oznakowaniach parkingowych. Niczego niepodejrzewający kierowcy skanują te kody, myśląc, że są legalne i dokonują płatności na rzecz oszustów. Te fałszywe kody QR mogą mieć postać naklejek umieszczonych na prawdziwych kodach, co utrudnia wykrycie oszustwa na pierwszy rzut oka.

4. Oszustwa SMS-owe

Oszuści wykorzystują wiadomości tekstowe, taktykę zwaną

smishingiem, aby oszukać swoje ofiary i przekonania ich, że mają zaległy bilet parkingowy wymagający natychmiastowej zapłaty. Wiadomości te często zawierają link do fałszywej strony płatniczej. Na przykład potencjalna ofiara może otrzymać wiadomość o treści: „Twój niezapłacony bilet parkingowy wymaga dzisiaj rozpatrzenia. Zapłać go do godziny …".

Należy pamiętać, że za bilety parkingowe nie można płacić SMS-em, a legalne władze nie będą prosić o płatność w ten sposób. Zawsze należy zachować ostrożność w przypadku podejrzanie wyglądających wiadomości tekstowych i unikać klikania jakichkolwiek łączy lub podawania danych osobowych, takich jak hasła.

5. Fałszywe E-maile i phishingowe strony internetowe

Innym powszechnym oszustwem są fałszywe e-maile, które wydają się pochodzić od lokalnych władz odpowiedzialnych za parkowanie i zwierają informacje, że masz niezapłacony bilet parkingowy. Fałszywe bilety e-mail mogą zawierać łącza do zdjęć, opcji płatności i procedury odwoławczej. Nie należy klikać tych linków, ponieważ mogą one zawierać złośliwe oprogramowanie.

Oszuści często tworzą także fałszywe witryny internetowe, które żądają informacji finansowych. Jeśli witryna internetowa wydaje się w jakikolwiek sposób podejrzana, unikaj jej używania. Bardzo ważne jest sprawdzenie adresu URL witryny, aby potwierdzić, że jest to legalna aplikacja, z której zamierzałeś korzystać. Na przykład, jeśli korzystasz z „ParkMobile", a adres URL ma postać https://park-space.xyz, może to

być fałszywy link. Prawidłowy adres URL aplikacji internetowej ParkMobile powinien zawsze zaczynać się od app.parkmobile.io. Jeśli masz jakiekolwiek wątpliwości, zamknij przeglądarkę i uzyskaj bezpośredni dostęp do aplikacji lub strony internetowej dotyczącej parkowania.

6. Fałszywe oszustwa związane z aplikacjami parkingowymi

Oszuści tworzą fałszywe aplikacje parkingowe imitujące te legalne. Mogą wysyłać linki do pobierania pocztą elektroniczną lub kierować potencjalne ofiary do witryn stron trzecich. Te fałszywe aplikacje mogą wykraść informacje o płatnościach lub zainstalować złośliwe oprogramowanie na Twoim urządzeniu.

Jak uchronić się przed oszustwami parkingowymi?

Aby nie paść ofiarą oszustw związanych z parkowaniem, wykonaj następujące kroki:

Zweryfikuj bilet: sprawdź, czy na bilecie znajduje się oficjalne logo i dane kontaktowe organu upoważnionego do pobierania opłat za parkowanie. W razie wątpliwości skontaktuj się bezpośrednio z oficjalną organizacją, korzystając z informacji z jego oficjalnej strony internetowej.

Uważaj na e-maile i SMS-y: Wszelkie niechciane wiadomości dotyczące mandatów za parkowanie traktuj podejrzliwie. Unikaj klikania linków i podawania danych osobowych. Zamiast tego odwiedź oficjalną stronę internetową władz odpowiedzialnych za parkowanie, aby zweryfikować

wszelkie roszczenia.

Korzystaj z oficjalnych aplikacji: pobieraj aplikacje parkingowe wyłącznie z oficjalnych sklepów z aplikacjami lub ze strony internetowej władz odpowiedzialnych za parkowanie. Zachowaj ostrożność w przypadku witryn stron trzecich lub łączy do pobierania wysyłanych e-mailem. Jeśli to możliwe, za parkowanie i mandaty płać kartą płatniczą. Ułatwi to kwestionowanie fałszywych opłat, jeśli zostaniesz oszukany.

Monitoruj swoje finanse: Regularnie przeglądaj wyciągi z konta bankowego i karty kredytowej pod kątem nieautoryzowanych transakcji.

Zgłaszaj oszustwa: Jeśli doświadczysz oszustwa, zgłoś je na lokalnej policji. Twój raport pomoże ostrzec innych przed oszustwami związanymi z parkowaniem.

„Jeśli planujesz zagraniczną podróż samochodem, pamiętaj, aby zabezpieczyć swój smartfon za pomocą skutecznego programu antywirusowego z modułem antyphishingowym. W ten sposób uchronisz się przed skutkami oszustw związanych z parkowaniem, które wykorzystują phishing i złośliwe oprogramowanie, ponieważ antywirus zablokuje niebezpieczne strony Internetowe oraz fałszywe aplikacje” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/uwazaj-na-6-oszustw-zwiazanych-z-parkowaniem/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 14.06.2024
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.