Skimming, phishing i inne wyłudzenia

data aktualizacji: 2024.03.11

Karta paliwowa to jedno z podstawowych narzędzi, którym kierowcy firm transportowych posługują się na co dzień. I podobnie jak kredytowa czy debetowa, narażona jest na ataki ze strony złodziei. Częstą formą jest po prostu włamanie się do kabiny kierowcy i fizyczna kradzież lub podmiana karty, ale przestępcy coraz częściej używają bardziej wyrafinowanych metod. Jedną z nich jest skimming.

Karta paliwowa umożliwia wygodne płacenie za paliwo, bez stania w kolejce do kasy i bez konieczności noszenia przy sobie gotówki, a do tego ułatwia zarządzanie wydatkami w firmie i ich kontrolę. Nic więc dziwnego, że stała się tak powszechna. Według raportu GlobalData, rynek kart paliwowych w Polsce już w 2020 roku został wyceniony na blisko 5 mln euro, a w latach 2021-2024 prognozuje się średnioroczne tempo wzrostu na poziomie ponad 11 proc. CAGR . Niestety, oprócz szeregu korzyści karta paliwowa niesie też za sobą pewne niebezpieczeństwa, a jednym z najpoważniejszych jest tzw. skimming. Wraz ze wzrostem liczby użytkowników kart paliwowych może rosnąć liczba przestępstw skimmingowych, dlatego warto już teraz dowiedzieć się, jak się przed nimi ustrzec. Jak to zrobić?

Karta paliwowa, podobnie jak kredytowa czy debetowa, narażona jest na ataki ze strony złodziei. Częstą formą jest po prostu włamanie się do kabiny kierowcy i fizyczna kradzież lub podmiana karty, ale przestępcy coraz częściej używają bardziej wyrafinowanych metod. Jedną z nich jest skimming. Polega on na montowaniu na terminalach płatniczych tzw. skimmerów, czyli urządzeń, które kopiują paski magnetyczne znajdujące się na karcie i sczytują kody PIN. Dzięki temu możliwe jest wyrobienie identycznej karty, którą następnie przestępcy dokonują płatności za paliwo, oczywiście obciążając przy tym konto faktycznego właściciela karty.

Niebezpieczeństwem, które czyha na właścicieli cyfrowych kart paliwowych, jest także phishing. To nic innego, jak wyłudzanie danych poprzez fałszywe SMS-y bądź e-maile, w których przestępcy podszywają się pod emitenta karty, próbując skłonić jej posiadacza do kliknięcia w link i zalogowania się na swoje konto. Oczywiście pod linkiem znajduje się fałszywa strona, dlatego wpisane dane błyskawicznie dostają się w ręce przestępców. Wielu fraudów na kartach paliwowych dokonują niestety również sami kierowcy. Mowa tutaj o przypadkach, w których sprzedają oni kartę, dobrowolnie przekazują ją do skopiowania albo wykorzystują do celów prywatnych. Są to jednak przypadki fraudów wewnętrznych, nad którymi firma musi zapanować sama poprzez odpowiedni dobór pracowników i wewnętrzne zabezpieczenia.

- Niestety nieautoryzowane transakcje paliwowe są dość powszechnym zjawiskiem, dlatego dostawcy kart paliwowych powinni stawiać na pierwszym miejscu bezpieczeństwo takich operacji. Zdecydowanie przewagę na rynku zyskują ci, którzy dostarczają coraz to skuteczniejszych rozwiązań antyfraudowych. Jest to niezwykle istotna kwestia, biorąc pod uwagę fakt, że paliwo jest jednym z największych kosztów prowadzenia firmy transportowej, stanowiącym nawet do 40 proc. wszystkich wydatków przedsiębiorstwa. Jego kradzież może narazić firmę na poważne straty finansowe - komentuje Tomasz Czyż, główny ekspert ds. rozwiązań technologicznych, Inelo z Grupy Eurowag.

Skala strat trudna do określenia

Niestety trudno określić dokładną skalę tego procederu, ponieważ ani policja ani same firmy transportowe nie udostępniają statystyk na ten temat. Niemniej jednak, można się domyślać, że jest ona duża i przynosi firmom niemałe straty. Potwierdzają to chociażby pojedyncze przypadki takich oszustw, które są nagłaśniane. Przykładowo, w 2018 roku pewien mieszkaniec Gubina dopuścił się skimmingu kart paliwowych i pozyskał dzięki temu ponad 94 tysiące litrów paliwa, co naraziło właściciela firmy transportowej na straty w wysokości ponad 405 tysięcy złotych . Nie dalej jak w 2022 roku szerokim echem w mediach odbił się też przypadek transgranicznego, zorganizowanego oszustwa polegającego na podrabianiu kart paliwowych między innymi w Rumunii, Bułgarii, Austrii i Belgii. W samej Rumunii sprawa dotyczyła łącznie 83 firm przewozowych. Zatrzymano wówczas 11 osób podejrzanych o zaangażowanie w ten proceder, którzy dokonali kradzieży paliwa na kwotę co najmniej 420 tysięcy euro .

Jak zabezpieczyć kartę flotową przed duplikacją?

W obliczu wspomnianego problemu, właściciele firm transportowych często zastanawiają się, co można zrobić, aby zabezpieczyć firmową kartę paliwową przed skimmingiem. Oczywiście ważna jest ostrożność. Warto przeszkolić kierowców, aby przed włożeniem karty do czytnika zwracali uwagę, czy nie ma na nim widocznych śladów ingerencji, na przykład w postaci zerwanej plomby. Dobrze też, żeby wybierali dystrybutory znajdujące się w dobrze widocznych miejscach, a najlepiej dystrybutory monitorowane. Warto jednak rozważyć też wdrożenie bardziej konkretnych zabezpieczeń.

Co prawda nie wymyślono jeszcze sposobu na udaremnienie pracy samych skimmerów, ponieważ technologia tworzenia kart paliwowych ciągle zakłada, że muszą być wyposażone w paski magnetyczne, które są możliwe do skopiowania. Walka z oszustami toczy się jednak na dalszym etapie. Mowa o rozwiązaniach, dzięki którym przestępcy mimo wyrobienia identycznej karty i posiadania numeru PIN nie będą mogli wykorzystać jej do płacenia za paliwo. To zarówno proste rozwiązania, oparte na możliwości ustawienia dziennych limitów płatności kartą, jak i bardziej zaawansowane, bazujące na dwustopniowym odblokowywaniu karty albo na porównywaniu lokalizacji.

- W naszym przypadku jest to telematyka EVA z funkcją Fuel Guard, która działa w oparciu o sieć

satelitów. Cały mechanizm jest prosty - system weryfikuje, czy karta paliwowa używana jest w tej samej lokalizacji, w której znajduje się pojazd. Jeżeli występuje niezgodność, karta jest blokowana, a firma transportowa natychmiastowo otrzymuje powiadomienie o tej sytuacji. Nie ma możliwości, aby doszło tutaj do pomyłki, bo mapa aktualizowana jest co 2 sekundy, więc informacja o lokalizacji ciężarówki zawsze jest precyzyjna - tłumaczy Julian Michański, Manager ds. operacyjnych i zaopatrzenia z Grupy Eurowag.

Innym rozwiązaniem zabezpieczającym, w dodatku zupełnie bezpłatnym, jest Card Lock. Działa ono na zasadzie dodatkowej warstwy uwierzytelniania, którą użytkownik ma możliwość wybrać sam. Przykładowo, karta może być aktywowana dopiero po wpisaniu kodu z SMSa, który przychodzi na telefon kierowcy podczas próby zapłacenia kartą paliwową. Rozwiązanie to działa jednak jedynie z kartami wspomnianego dostawcy. Są to karty używane przez wiele firm transportowych w Polsce i akceptowane na stacjach partnerskich w całej Europie. Można także posługiwać się nimi w punktach własnych Eurowag - tzw. Truck Parkach. To prężnie rozrastająca się sieć, która pod koniec stycznia 2024 poszerzyła się o kolejną stację - w Okmianach.

Bezdotykowe, cyfrowe płatności za paliwo mogą pomóc

Skoro karta paliwowa narażona jest na skimming i fizyczną kradzież, sposobem na uniknięcie ryzyka może być też rezygnacja z tego fizycznego elementu na rzecz płatności mobilnych. Istnieje bowiem wiele aplikacji, które mogą pełnić taką samą funkcję, jak karta i są jej dobrą alternatywą, umożliwiając kierowcy wygodne płacenie za paliwo z poziomu smartfona czy tableta.

- Jedną z bezpłatnych aplikacji tego typu jest właśnie Eurowag Pay. Dzięki niej kierowca nie musi już nosić przy sobie plastikowej karty ani zapamiętywać wielu kodów PIN - wystarczy znać jeden PIN, który obowiązuje nawet w razie zmiany pojazdów. Jeżeli telefon zostanie skradziony albo zwyczajnie się rozładuje i kierowca nie będzie miał, jak uruchomić aplikacji istnieje możliwość awaryjnej zdalnej obsługi i wówczas płatności za tankowanie może dokonać dyspozytor. Aplikacja została też dodatkowo zabezpieczona na okoliczność oszustwa. Polega to na tym, że blokuje zakupy, jeżeli użytkownik, który obsługuje telefon znajduje się w odległości większej niż 100 metrów od dystrybutora - wyjaśnia Julian Michański.

Podsumowując, karta paliwowa to wygodne rozwiązanie, które pozwala oszczędzać czas, a wielokrotnie i pieniądze z racji specjalnych zniżek przyznawanych posiadaczom tych instrumentów płatniczych. Pozwala także łatwiej kontrolować wydatki na paliwo i zwiększa bezpieczeństwo, ponieważ kierowca nie musi mieć przy sobie gotówki, którą łatwo ukraść lub zgubić. Warto jednak zachować czujność i korzystać z rozwiązań, które chronią dane z karty przed dostaniem się w niepowołane ręce.

Fot. Inelo