

Tylko w jeden dzień, w gorączce „Czarnego Piątku” w 2019 r., Polacy wydali ponad 121 mln zł na same zakupy ratalne, co oznacza ponad dwukrotnie (206%) większą wartość sprzedaży kredytów ratalnych w stosunku do średniej udzielanej w pozostałe dni robocze w listopadzie 2019 r. W tym roku, choć święto zakupowe przypada na 27 listopada, to specjalne oferty i rozliczne zniżki kuszą już od kilku tygodni. Sprzedawcy aktywnie przekierowują naszą uwagę na przeceny ze sklepów stacjonarnych do internetowych, mając na względzie wprowadzone w Polsce od 7 listopada ograniczenia w funkcjonowaniu galerii handlowych. Obserwacje potwierdzają, że jeszcze łatwiej jest poddać się wyprzedażom i okazjom, przeglądając Internet bez celu. Jak nie wpaść w pułapkę pochopnych decyzji, żłudnych obniżek, a przede wszystkim, jak uchronić się przed wyłudzeniem kredytu na skradzione dane?

Niezmienne, apetyt Polaków na rabaty i promocje specjalne z roku na rok owocuje wzrostem liczby i wartości udzielanych kredytów ratalnych w stosunku do pozostałych dni w listopadzie. A to wszystko z powodu szaleństwa wyprzedaży – zakupowego święta, które wzorem ze Stanów Zjednoczonych, ugruntowało swoją pozycję także w kalendarzu konsumpcyjnym Polaków. Polowanie na okazje cenowe to domena zarówno kobiet, jak i mężczyzn. Nie zawsze jednak w ślad za zakupem, idzie realna potrzeba czy konkretny cel. Często, kierowani impulsem, narażamy się na nieprzemyślane wydatki, a ciężar spłaty nadmiarowych kosztów pozostaje z nami miesiącami.

Zakupowy szal potwierdzają również statystyki BIK o sprzedaży ratalnej

Sprzedaż kredytów ratalnych w „Black Friday” już od kilku lat wyraźnie zaznacza się na listopadowych wykresach opracowywanych w BIK. W 2018 r. liczba udzielonych kredytów ratalnych w weekendy listopadowe wzrosła o ponad 36% w stosunku do średniej z pozostałych weekendów w roku 2018, a w 2019 r. ten wzrost przekroczył 50%.

W piątkowe szaleństwo, które w 2019 r. wypadło 29 listopada, znów liczba udzielonych kredytów ratalnych poszybowała w górę. Banki udzieliły 32,2 tys. kredytów ratalnych na łączną kwotę 121,4 mln zł, co oznacza, że tylko w ten jeden dzień podwoiła się wartość sprzedaży, a liczba kredytów była ponad 2,5-krotnie wyższa w stosunku do średniej w pozostałe listopadowe dni robocze.

Średnia kwota kredytu ratalnego przyznanego w „Czarny Piątek” 2019 r. wyniosła 3.769 zł i była wyższa o 1,8% niż rok wcześniej, w 2018 r.

BlackFriday raty w górę

Jak kupować mądrze?

W tym roku, ze względu na obostrzenia związane z pandemią koronawirusa, wiele sklepów ruszyło z ofertami specjalnymi już na początku listopada. Sprzedawcy kuszą, jak mogą i zachęcają do zakupów online, bezpiecznych dla naszego zdrowia. Ważne, by w tym szale kupowania nie zapomnieć także o bezpieczeństwie swojego portfela. Dlatego zanim ruszymy na zakupy i wydamy ciężko zarobione pieniądze, warto przeczytać informacje o interesującym nas produkcie, sprawdzić bieżące ceny, zweryfikować wiarygodność sprzedawcy. Pośpiech może okazać się złym doradcą, a okazja zakupu w dobrej cenie – pozorną. Należy wziąć pod uwagę dopłaty, np. koszty dostawy – nie zawsze da się ich uniknąć, ponieważ niektóre e-sklepy wymagają minimalnej wartości zamówienia.

Idealem jest wyjście od potrzeb, kupowanie z wcześniej spisanej listy zakupów i ustalonym limitem

swojego budżetu. Warto jeszcze „wypożyczyć się” w odrobinę dystansu – pamiętać, że nie ma nic za darmo, a duże rabaty niekoniecznie oznaczają faktyczne oszczędności.

Nierzadko zdarza się, że ulegamy presji czasu, przyciągnięci ofertą godzinową albo „darmowym” prezentem przy każdym zakupie. To już tylko o krok od pochopnego kliknięcia, które nierzadko prowadzi do utraty danych. Na podobne działania, zwłaszcza na brak należytej uwagi, obliczone są ataki większości hakerów internetowych, tzw. cyberprzestępców. Dla nich polem do łowienia okazji, nie tylko w „black weeks”, są wszelkie sytuacje, w których udostępniamy nasze dane osobowe, takie jak: imię i nazwisko, adres, numer dowodu osobistego, PESEL i data urodzin. Każdy z nas może paść ofiarą kradzieży naszych cennych danych, które przez złodziei tożsamości mogą zostać użyte, m.in. do wyłudzenia kredytu czy pożyczek zarówno na osobę fizyczną, jak i na firmę.

Listopadowe polowanie na okazje i super przeceny będzie przyjemnością, gdy nie stracimy głowy. Należy nie tylko unikać pułapki nadmiernych wydatków w wyniku pochopnych decyzji, ale przede wszystkim zadbać o ochronę swoich danych. Warto wyrobić sobie nawyk ostrożnego kupowania i dokonywania transakcji płatniczych w internecie, by uchronić się przed wyłudzeniem i kradzieżą naszych danych oraz korzystać ze sprawdzonych rozwiązań ochronnych, jak Alerty BIK.

Uniwersalne porady eksperckie na bezpieczne e-zakupy

Aż 94 procent osób przyznało, że korzysta z Internetu przynajmniej raz dziennie. Ze względu na przeniesienie do Internetu znacznej części transakcji zakupowych, a tym samym większości transakcji finansowych, należy zdawać sobie sprawę ze sprytu przestępców internetowych. Scenariusze hakerów bazują nie tylko na technologii, ale nadal przede wszystkim wykorzystują ludzką naiwność. Złodzieje czyhają na błędy, jakie popełniamy z powodu szybkości, automatyzmu postępowania lub zwykłego braku świadomości, jak można chronić swoje dane.

Korzystając z internetu, powinniśmy wyznawać zasadę, że im mniej danych podamy, tym lepiej. Ze szczególną ostrożnością podchodzimy do wszelkich formularzy, w których wymagane jest podanie danych osobowych, numeru pesel, telefonu czy adresu.

- Robiąc zakupy warto zadać sobie pytanie, czy podawanie tzw. wrażliwych danych jest potrzebne. Czy nasz PESEL albo numer naszego dowodu są faktycznie niezbędne tej drugiej stronie do sprzedania nam jakiegoś produktu czy usługi? - wskazuje Andrzej Karpiński, szef ds. bezpieczeństwa w BIK i dodaje, że niezależnie w jakim okresie kupujemy, należy przestrzegać naczelnej zasady, by nikomu nie podawać swoich haseł i loginów do naszych kont.

- Trzeba także pamiętać, by tworzyć silne hasła. Dobre hasło nie może zawierać ciągu cyfr 1-6, dat urodzenia czy danych oczywistych, jak imiona rodziców, które złodzieje sprytnie mogą wykorzystać. Ważne jest także regularne zmienianie haseł, a także wyrobienie nawyku instalowania ich na naszych smartfonach. Jak wynika z badań opinii BIK, co 5-ty Polak nie ma ustawionych haseł na swoich telefonach, a to przecież obecnie nasze główne centrum dowodzenia – tłumaczy Karpiński.

Oszust niekoniecznie potrzebuje wejść w posiadanie dowodu osobistego osoby, na którą planuje zaciągnąć kredyt lub pożyczkę. Przestępcy oczywiście nadal mogą fizycznie ukraść dokument, więc należy chronić tzw. plastik. Coraz częściej jednak do kradzieży danych osobowych dochodzi w wyniku stosowania różnego rodzaju metod socjotechnicznych, wykorzystujących ludzkie słabości. Złym doradcą

będą także pośpiech, rutyna i emocje.

- Złodzieje nie próżnują nawet w okresie pandemii, kiedy niemal każdy coś zamawiał z doręczeniem do domu, wykorzystali tzw. metodę scammingu. To oszustwo polegające na wzbudzeniu zaufania ofiary, aby zdobyć dane do wyłudzenia pieniędzy. Oszuści, podszywając się pod firmy kurierskie, wysyłali sms z treścią informującą o konieczności dopłaty niewielkiej kwoty w celu poprawnego zrealizowania zamawianej paczki. Łatwo można było ulec fałszywej wiadomości. Wystarczyło kliknięcie w podany link, przenoszący niczego nieświadomą ofiarę na fałszywą stronę firmy kurierskiej w celu podania danych złodziejowi. To może wydawać się nieprawdopodobne, ale ten proceder, obliczony na efekt skali, niestety działa – mówi Joanna Charlińska, dyrektor ds. sprzedaży detalicznej w BIK.

Zamawiając produkty czy usługi zdalnie, musimy zachowywać szczególną ostrożność, gdzie pozostawiamy swoje dane, dokładnie czytać adresy stron, z których korzystamy, nie klikać pochopnie w linki, podsuwane zarówno w mailach, jak i w wiadomościach sms. Zawsze należy kierować się zdrowym rozsądkiem i zasadą ograniczonego zaufania.

Warto pielęgnować dobre nawyki, świadomie i ostrożnie dokonywać transakcji w sieci, są jednak zdarzenia, na które nie mamy wpływu, jak np. wycieki danych z instytucji, sytuacje, takie jak powyżej, w których tracimy czujność i po prostu ulegniemy socjotechnikom hakerów. Dlatego najlepszym rozwiązaniem we wszystkich sytuacjach, w których niepokoi nas o bezpieczeństwo naszych danych osobowych, jest działanie przed szkodą, czyli posiadanie aktywnej ochrony przed wyłudzeniem.

Źródło: ip