



Warszawa, 28.01.2026 r.

INFORMACJA PRASOWA

.....

Smartfon – start ścieżki zakupowej i cel cyberoszustów

Smartfon stał się dziś głównym narzędziem zakupów online — potwierdza to 82 proc. użytkowników. Przez telefon kupujemy szybko i wygodnie, ale także bardziej impulsywnie, np. pod wpływem SMS-ów o „niepowtarzalnej okazji”. Na naszą ufność i natychmiastową reakcję coraz częściej liczą oszuści, którzy podszywają się pod znane mechanizmy sprzedażowe i próbują przechwycić nasze personalne dane. Takie ryzyko dostrzegło w 2025 roku 61 proc. kupujących - wskazuje Raport Antyfraudowy BIK. To sygnał ostrzegawczy dla dynamicznie rozwijającego się w Polsce handlu mobilnego. Tym bardziej, że wielu konsumentów nie chroni właściwie swoich telefonów i coraz częściej daje się nabrać na oferty fikcyjnych sklepów internetowych.

Najważniejsze wnioski z Raportu Antyfraudowego BIK:

- Rośnie skala ataków na urządzenia mobilne. Co czwarty użytkownik (27 proc.) zmierzył się z próbą przejęcia swojego smartfona przez oszustów, aż 4 na 10 spotkało się z próbą phishingu, a 22 proc. z tego typu atakiem poprzez komunikatory internetowe.
- Popularnym motywem działań przestępczych są się fikcyjne sklepy internetowe, a odsetek poniesionych z tego tytułu strat finansowych wynosi już 43 proc. i niemal dwukrotnie przewyższa poziom strat związanych z wyłudzeniami „na fałszywe inwestycje”.
- Co szósty ankietowany przyznał, że w ogóle nie stosuje żadnej blokady ekranu telefonu. Niecała połowa (47 proc.) użytkowników deklaruje, że korzysta z funkcji automatycznych aktualizacji w smartfonach, podczas gdy 5 proc. w ogóle nie aktualizuje oprogramowania.
- Najczęściej wykorzystywanymi zabezpieczeniami smartfonów pozostają: kod PIN (40 proc.), odcisk palca (36 proc.) lub hasło (22 proc.).

Zakupy internetowe stały się dziś tak naturalną częścią codzienności, jak te robione w tradycyjnym sklepie. Coraz częściej nasz wirtualny koszyk zapełniamy nie przez ekran komputera, ale za pomocą smartfona. Telefon, w którym mamy dziś mnóstwo informacji, przejął rolę podstawowego narzędzia zakupowego.

Mobilny handel, czyli m-commerce, to już nie nisza, ale kluczowy kanał sprzedaży, który generuje dziesiątki miliardów złotych rocznie. Wartość sektora e-commerce w Polsce wg szacowanych danych może do 2028 roku osiągnąć 192 mld zł, z czego za połowę będą odpowiadać zakupy za pośrednictwem urządzeń mobilnych. Nic zatem dziwnego, że tak dynamicznie rozwijający się rynek przyciąga nie tylko biznes, ale i oszustów.

Fałszywe e-sklepy, SMS-y, powiadomienia

Ekran telefonu komórkowego to dziś początek ścieżki zakupowej. Widać to szczególnie wśród najmłodszych grup konsumentów – osoby poniżej 25 roku życia kupują prawie wyłącznie za pośrednictwem telefonu. Dla wielu stał się on naturalnym kanałem zakupów, także tych nieplanowanych. Decyzje podejmowane na ekranie telefonu zapadają bowiem spontanicznie, niejednokrotnie pod wpływem SMS-a czy tzw. powiadomienia push z okazją „tu i teraz”. Coraz częściej ich nadawcą nie jest jednak ulubiona marka czy sklep, ale podszywający się pod nie oszust. Potwierdza to Raport Antyfraudowy BIK 2025, zgodnie z którym niepokojąco rośnie liczba prób wyłudzeń za pośrednictwem urządzeń mobilnych. W ubiegłym roku aż 40 proc. ankietowanych spotkało się z próbą oszustwa przez SMS, a 22 proc. z podobnym zdarzeniem w komunikatorze internetowym, takim jak Messenger czy WhatsApp.

– *Najczęściej mamy do czynienia w phishingiem, czyli podszywaniem się pod zaufane instytucje w celu wyłudzenia danych, do czego przestępcy wykorzystują m.in. nasze smartfony. Popularną formą oszustwa stają się też fałszywe sklepy internetowe, oferujące atrakcyjne produkty w niskich cenach. Po dokonaniu płatności klient nie otrzymuje zamówienia, a kontakt ze „sklepem” się urywa. O skuteczności tego działania może świadczyć fakt, że odsetek poniesionych z tego tytułu strat finansowych wynosi już 43 proc. i niemal dwukrotnie przewyższa poziom strat związanych z wyłudzeniami „na fałszywe inwestycje”. Ofiarą kradzieży danych może paść każdy, najczęściej są to osoby, które nieświadomie odpowiedzą np. na wiadomość o rzekomo nieudanej płatności mobilnej i pobiorą groźne oprogramowanie. W takim wypadku kluczowe jest, by natychmiast zastrzec PESEL, ale też sprawdzić historię kredytową i pomyśleć nad rozwiązaniem, takim jak Alerty BIK – tłumaczy Karol Głogowski, Dyrektor IT Usług Antyfraudowych, BIK S.A.*

Niezabezpieczony telefon jest jak otwarta kieszeń

Przestępcy specjalizujący się w obszarze handlu mobilnego stają się coraz bardziej niebezpieczni dzięki stosowaniu zaawansowanych technologii oraz socjotechnik. Niestety zdarza się, że oszustwa i kradzieże ułatwiają nieświadomie nawet ich ofiary. Głównie chodzi o tych użytkowników smartfonów, którzy ich odpowiednio nie chronią. Dane dotyczące zabezpieczenia smartfonów są alarmujące. Co szósta osoba przyznaje (16 proc.), że w ogóle nie stosuje żadnej blokady ekranu telefonu.

Do najczęściej wykorzystywanych zabezpieczeń smartfonów należą kod PIN (40 proc.), odcisk palca (36 proc.) lub hasło (22 proc.). Jednocześnie, tylko niecała połowa respondentów deklaruje, że korzysta z funkcji automatycznych aktualizacji oprogramowania w smartfonach, podczas gdy 5 proc. zaniedbuje to całkowicie.

– *Bieżące aktualizowanie systemu, programów i aplikacji to jedna z podstawowych form ochrony urządzeń mobilnych, podobnie jak stosowanie antywirusa. Dzięki nim udaje się ograniczyć ryzyko wykradzenia danych oraz ewentualne straty finansowe. Tymczasem dla niemal 60 proc. badanych, najlepszym sposobem ochrony telefonu jest unikanie otwierania wiadomości i załączników od nieznanych nadawców. Zdecydowanie skuteczniejsze będą proaktywne formy ochrony przed kradzieżą, np. ostrzeżenia przed autoryzowaniem transakcji noszących znamiona oszustwa. Takie rozwiązanie oferują Alerty BIK, w ramach których poszliśmy jeszcze dalej, umożliwiając klientom możliwość monitorowania, czy ich dane nie trafiły do darknetu – mówi Karol Głogowski, Dyrektor IT Usług Antyfraudowych, BIK S.A.*

Kradzież pieniędzy z naszych smartfonowych portfeli często zaczyna się od oszustwa i wykradzenia danych, dlatego należy wciąż pracować nad edukacją i zwiększaniem świadomości klientów w zakresie cyberbezpieczeństwa. O tym, jak jest to ważne, nie tylko dla konsumentów, ale i całego sektora e-commerce mogą świadczyć dane z raportu Gemiusa - 17 proc. z nas nie kupuje on-line z obawy o bezpieczeństwo płatności. Także tych mobilnych.

Źródła:

Raport antyfraudowy BIK, 2025 dostępny jest na <https://rozwiązania-antyfraudowe.bik.pl/pl/raporty>

Raport „E-commerce w Polsce 2025”, Gemius

Raport “E-commerce w Polsce: konkurencja i rosnące oczekiwania napędzają rozwój”, Strategy&

Biuro Informacji Kredytowej S.A. wspiera bezpieczeństwo instytucji finansowych i ich klientów, udostępniając bezpieczny system wymiany informacji kredytowych i gospodarczych oraz nowatorskie rozwiązania antyfraudowe. Jako jedyne biuro kredytowe w Polsce, poprzez internetowy portal www.bik.pl oraz aplikację mobilną [Mój BIK](#), umożliwia klientom indywidualnym monitorowanie własnej historii kredytowej, a dzięki [Alertom BIK](#) ostrzega przed każdą próbą wyłudzenia kredytu. Sektorowe rozwiązania antyfraudowe w portfolio BIK to: Platforma Antyfraudowa BIK, Platforma Blockchain, Platforma Cyber Fraud Detection, Platforma Weryfikacji Behawioralnej. Najnowsze rozwiązanie - Platforma ESG BIK, to nowy standard wymiany i raportowania danych. BIK gromadzi i udostępnia dane o historii kredytowej klientów indywidualnych i przedsiębiorców z całego rynku kredytowego, oraz dane z obszaru pożyczek pozabankowych. BIK gromadzi i udostępnia dane o historii kredytowej klientów indywidualnych i przedsiębiorców z całego rynku kredytowego, oraz dane z obszaru pożyczek pozabankowych. Baza BIK zawiera informacje o 444 mln rachunków należących do 25,5 mln klientów indywidualnych oraz 6,6 mln rachunków należących do 2,2 mln przedsiębiorców. BIK posiada najwyższe kompetencje w zakresie [Analiz rynkowych](#) i nowoczesnych technologii. Łączy cechy nowoczesnej firmy technologicznej z atrybutami instytucji zaufania publicznego. Od kilkunastu lat BIK jest aktywnym członkiem międzynarodowego Stowarzyszenia ACCIS.

Kontakt dla mediów:

Aleksandra Stankiewicz-Billewicz

Biuro prasowe BIK

kom.: + 48 512 164 131

aleksandra.stankiewicz-billewicz@bik.pl