



Bezpieczeństwo
bankowości internetowej

SKIMMING



I-BIS.PL

Taka sytuacja. Korzystasz z bankomatu – wszystko działa, jak powinno. Wypłacasz pieniądze, ale kilka dni później odkrywasz, że z Twojego konta zniknęły środki ... choć tym razem **to nie Ty je wypłaciłeś**. Jak to możliwe? Odpowiedź: **skimming**.

Co to jest skimming?

To metoda oszustwa, w której przestępcy instalują urządzenia na bankomatach lub terminalach płatniczych. Skimmer kopiuje dane z paska magnetycznego Twojej karty, a ukryta kamera lub fałszywa klawiatura zapisuje PIN. Z tymi danymi oszuści tworzą kopię Twojej karty i wypłacają Twoje pieniądze bez Twojej wiedzy.

Jak się chronić?

- Dokładnie sprawdzaj bankomat przed użyciem** – zwróć uwagę na nietypowe elementy, luźne klawiatury lub dziwnie wyglądające szczeliny na karty.
- Zasłaniaj klawiaturę podczas wpisywania PIN-u** – nawet jeśli wydaje się, że nikt nie patrzy.
- Korzystaj z płatności zbliżeniowych i wirtualnych kart** – zmniejszasz ryzyko kontaktu z fałszywym urządzeniem.
- Ustaw limity transakcji i włącz alerty SMS** – szybciej zareagujesz, gdy coś jest nie tak.

Co zrobić, jeśli padniesz ofiarą skimmingu?

- Natychmiast zablokuj kartę i skontaktuj się ze swoim bankiem.
- Zgłoś sprawę na policję, dostarczając wszelkie informacje, które mogą pomóc w dochodzeniu.
- Rozważ korzystanie z kart z funkcją chipową – trudniejsze do skopiowania niż te z paskiem magnetycznym.

Skimming działa po cichu, ale Ty możesz być krok przed oszustami. Zawsze sprawdzaj urządzenia, z których korzystasz, i chroń swoje dane. Bezpieczeństwo zaczyna się od czujności!

#Skimming #BezpieczeństwoKart #Bankomat #UważajNaOszustów #BezpiecznaBankowość #EBO #EBOeBankOnline #EBOMobilePRO