

Uwaga na skimmerów! Eksperci KNF radzą, jak bezpiecznie wypłacać z bankomatów

W październiku Sąd Apelacyjny w Białymstoku skazał trzech obywateli Łotwy na kary od 2,5 roku do 6 lat więzienia i grzywny za udział w tzw. skimmingu. Przestępcy podrabiali karty płatnicze i wypłacili prawie 500 tys. zł.

Czy w ogóle możliwa jest ochrona przez tzw. skimmerami? Banki montują różne zabezpieczenia na bankomaty, ale ważna jest też czujność samych klientów - przyznają eksperci Komisji Nadzoru Finansowego.

Wraz ze wzrostem popularności bankowości elektronicznej, rośnie też liczba zagrożeń przestępczością elektroniczną. Każdego dnia klienci banków wypłacają pieniądze z bankomatów. Rzadko myślimy o tym, że któregoś dnia, po takiej transakcji, z naszego konta mogą zniknąć środki.

Czym jest skimming?

Najogólniej skimming to przestępstwa polegające na zakładaniu na bankomatach urządzeń do nielegalnego zbierania informacji z karty płatniczej, np. miniaturowej kamery i czytnika kart, których zadaniem jest odczytanie informacji związanych z kartą płatniczą, tj. numeru PIN oraz skopiowanie danych z paska magnetycznego.

- *Co do zasady nie zawsze korzystając z bankomatu możemy zorientować się, że ktoś go „ulepszył” na swoje potrzeby* - przyznają eksperci Komisji Nadzoru Finansowego w specjalnym raporcie pt. „Bezpieczeństwo finansowe w bankowości elektronicznej - przestępstwa finansowe związane z bankowością elektroniczną”.

- *Aby skutecznie sczytać zawartość karty, przestępcy instalują nakładkę na otwór, w który wsuwamy kartę. Tym sposobem skanują całą zawartość paska magnetycznego, którą następnie mogą nagrać na dowolny kawałek plastiku z paskiem magnetycznym lub przesłać elektronicznie do swoich kolegów w dowolnej części świata, aby oni to zrobili* - czytamy w raporcie.

Jak podkreślają autorzy raportu, „skimming najczęściej dotyka bankomaty w dobrych lokalizacjach turystycznych, nie zlokalizowane w oddziałach bankowych, do których jest swobodny dostęp, i z którego korzysta dużo ludzi.

- *Nikogo wtedy nie dziwią ślady zużycia na bankomacie, które mogłyby wskazywać na jakąś podejrzaną działalność, ani fakt, że ciągle w okolicach bankomatu znajdują się ludzie* - czytamy w raporcie.

Jak działają skimmerzy?

Sprawa skazanych w październiku br. przez Sąd Apelacyjny w Białymstoku Łotyszów pokazuje, że w Polsce działają zorganizowane grupy przestępcze, które zajmują się

skimmingiem. Skazani Łotysze w 2013 roku, kilkakrotnie przyjeżdżając do Polski, na bankomatach m.in. w Białymstoku, Bielsku Podlaskim, Ełku, Suwałkach, Giżycku i Piszcu montowali specjalne czytniki oraz kamery do nagrywania kodów PIN z oryginalnych kart płatniczych w czasie, gdy właściciele owych kart wypłacali pieniądze.

- *Na podstawie pozyskanych danych wytwarzano następnie fałszywe karty płatnicze i wykorzystywano je oraz przyporządkowano im kody PIN do dokonywania nieautoryzowanych wypłat pieniędzy z rachunków bankowych* - poinformował Sąd Apelacyjny w Białymstoku.

Działalność ta była prowadzona w formie zorganizowanej grupy przestępczej, na czele której stał obywatel Łotwy Siergiej F. oraz nieustalone osoby z Bułgarii, którym członkowie grupy, w tym troje oskarżonych Łotyszy, przekazywali za pośrednictwem poczty elektronicznej albo osobiście dane skopiowanych pasków magnetycznych oraz pliki video zawierające nagrania kodów PIN.

Wypłaty pieniędzy z użyciem podrobionych kart, których dane w przestępczy sposób oskarżeni zdobyli na terenie Polski, dokonywano na terenie Tajlandii, Dominikany, USA, Hiszpanii, Łotwy oraz innych państw i dotyczyło to mienia znacznej wartości. W sumie wypłacono prawie 500 tys. zł, drugie tyle usiłowano wypłacić.

„Zęby”, moduł EMV i chipy dla ochrony

Banki starają się chronić swoich klientów przed skimmerami. Przykładowo, mechanizmem zabezpieczającym jest to, że karta po włożeniu do bankomatu jednocześnie wibruje utrudniając tym samym sczytanie danych z paska przez urządzenie zamontowane na bankomacie. Dodatkowo, banki często montują „zęby” bądź inne plastikowe wypustki wokół otworu na kartę, aby uniemożliwić zamontowanie tam tzw. skimmera.

Ochronę przed pozyskiwaniem przez przestępców danych stanowią też wbudowane chipy w karty bankomatowe. „Wiadomość, że karta posiada chip jest zapisana na pasku magnetycznym karty. Bankomat czyta tę informację i inicjuje tzw. moduł EMV, który porozumiewa się z chipem na karcie” - tłumaczą eksperci KNF. Kiedy więc na ekranie bankomatu wyświetla się komunikat o możliwym wydłużonym czasie oczekiwania na przeprowadzenie danej operacji, to nie należy się niecierpliwić. Raczej to dla klienta dobra informacja, że karta ma taki moduł EMV.

Po zeskimowaniu karty z chipem przestępcy nie mogą jej użyć w bankomacie, który obsługuje moduł EMV, a takich jest w Polsce większość, jeśli nie wszystkie. - Taki bankomat odczyta informacje o tym, że karta ma chip, poszuka go na zeskimowanej karcie i oczywiście nie znajdzie i nieprzeprowadzi transakcji - wyjaśniają eksperci KNF.

Są jednak kraje, w których technologia EMV nie działa tak dobrze albo w ogóle np. Ameryka Południowa czy USA. Tam komunikat o chipie z paska magnetycznego karty

nie będzie zinterpretowany przez bankomat, a przestępcy mając zawartość paska magnetycznego karty i numer PIN bez przeszkód dokonają wypłaty.

- Oczywiście banki chronią siebie i swoich klientów przed tym rodzajem przestępstw i bardzo często takie wypłaty blokują przed ich dokonaniem. Nie zawsze jednak pojedyncze transakcje uda się wychwycić, dlatego niezbędna jest czujność - zalecają eksperci Komisji Nadzoru Finansowego.

Uważaj, zachowaj czujność

Przede wszystkim, aby się chronić, eksperci nie zalecają korzystania z bankomatów, które nie są umiejscowione w oddziałach banków.

- Jeśli musimy skorzystać z bankomatu poza oddziałem, należy sprawdzić czy żadne jego części nie wyglądają „dziwnie”, „jakby doklejone”, „nadmiernie wystające” i niezintegrowane z całym bankomatem - radzą eksperci KNF.

Jeśli klawiatura sprężynuje przy wprowadzaniu PINu albo nawet odkleja się, należy transakcję przerwać. W razie jakichkolwiek wątpliwości lepiej skorzystać z innego bankomatu, a swoje podejrzenia zgłosić na infolinii banku.

Za: www.kurier.pap.pl

<http://kurier.pap.pl/depesza/158245/Uwaga-na-skimmerow-Eksperci-KNF-radza--jak-bezpiecznie-wyplacac-z-bankomatow>



[Powrót na stronę główną](#)

[Powrót do listy aktualności](#)