Nr 3(96) 2024 Bezpieczny Bank

DOI: 10.26354/bb.3.3.96.2024

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Skimming jako zagrożenie dla bezpieczeństwa bankowości mobilnej

Streszczenie

Przedmiot i cel pracy: Celem pracy jest analiza problemu skimmingu, czyli nielegalnego pozyskiwania danych z kart płatniczych, oraz przedstawienie metod zapobiegania temu zjawisku. Skimming stanowi istotne zagrożenie dla użytkowników kart płatniczych i instytucji finansowych, pomimo wprowadzenia nowoczesnych technologii zabezpieczających, jak np. czipy EMV.

Materiały i metody: Przeprowadzono przegląd literatury dotyczącej skimmingu na podstawie baz danych Web of Science i Scopus oraz wykorzystano narzędzie bibliometrix do analizy 70 publikacji. Dodatkowo zidentyfikowano główne metody skimmingu i zapobiegania na podstawie dostępnych raportów oraz badania rozwoju urządzeń wykrywających skimmery.

Wyniki: Zidentyfikowano różne typy urządzeń skimmingowych, w tym: zewnętrzne, wewnętrzne, *deep-insert* oraz EMV shimmer, a także przedstawiono ich ewolucję. Analiza wskazuje, że wprowadzenie zaawansowanych technologii zabezpieczeń nie wyeliminowało problemu, a oszuści znajdują nowe sposoby obejścia tych mechanizmów. Przedstawiono również skuteczne środki zapobiegania, takie jak urządzenia do wykrywania skimmerów oraz nowoczesne technologie zabezpieczeń bankomatów.

Wnioski: Skimming pozostaje istotnym zagrożeniem, wymagającym nieustannego rozwoju technologii zabezpieczeń oraz edukacji użytkowników. Banki i instytucje finansowe powinny inwestować w zaawansowane systemy ochrony oraz prowadzić kampanie edukacyjne, aby minimalizować ryzyko przestępstw finansowych. Współpraca technologii i świadomości użytkowników jest kluczowa dla skutecznej walki z tego typu oszustwami.

Słowa kluczowe: skimming, oszustwo kartowe, karty płatnicze

Kody JEL: L86

* Patryk Król – Uniwersytet Ekonomiczny w Poznaniu, Katedra Pieniądza i Bankowości.

Skimming as a threat to mobile banking security

Abstract

Subject and purpose of the study: The aim of this paper is to analyse the problem of skimming, i.e. the illegal extraction of payment card data, and to present methods to prevent this phenomenon. Skimming poses a significant threat to payment card users and financial institutions, despite the introduction of modern security technologies such as EMV chips.

Materials and methods: A literature review on skimming was conducted using the Web of Science and Scopus databases and the bibliometrix tool was used to analyse 70 publications. In addition, the main methods of skimming and prevention were identified from available reports and a survey of the development of skimmer detection devices.

Results: Different types of skimming devices were identified, including external, internal, deep-insert and EMV shimmer, and their evolution was presented. The analysis shows that the introduction of advanced security technologies has not eliminated the problem, and fraudsters are finding new ways to circumvent these mechanisms. Effective prevention measures such as skimmer detection devices and modern ATM security technologies are also presented.

Conclusions: Skimming remains a significant threat, requiring continuous development of security technologies and user education. Banks and financial institutions should invest in advanced security systems and educational campaigns to minimise the risk of financial crime. The collaboration of technology and user awareness is crucial to effectively combat this type of fraud.

Keywords: skimming, card fraud, payments card

JEL Codes: L86

Wstęp

Każda nowo wprowadzona metoda płatności, choć z założenia ma na celu ułatwienie i przyspieszenie transakcji finansowych, niesie ze sobą również nowe wyzwania w zakresie bezpieczeństwa. Współczesny świat finansów jest nierozerwalnie związany z nowoczesnymi technologiami, które umożliwiają szybkie, wygodne i bezpieczne dokonywanie płatności, zarówno w świecie rzeczywistym, jak i cyfrowym. Jednak każda innowacja finansowa staje się jednocześnie polem do nadużyć ze strony przestępców, którzy nieustannie poszukują luk w zabezpieczeniach oraz nowych sposobów na przejęcie środków pieniężnych. Nie inaczej jest w przypadku kart płatniczych, które od lat stanowią fundament systemów płatności na całym świecie, w tym w Polsce, gdzie ich popularność nieustannie rośnie.

Karty płatnicze – zarówno kredytowe, jak i debetowe – stały się powszechnie akceptowanym i uznanym środkiem płatniczym, zastępującym gotówkę w coraz większej liczbie transakcji. Ta wygoda użytkowania przyciąga jednak nie tylko konsumentów, ale również osoby o nieuczciwych intencjach, które rozwijają coraz bardziej zaawansowane techniki oszustw. Jedną z najbardziej rozpowszechnionych form nadużyć związanych z kartami płatniczymi jest skimming, który polega na niele-

galnym pozyskiwaniu danych z kart kredytowych i debetowych. Jak wskazują Bhatla, Prabhu, Dua (2003), oszustwa tego typu stanowią istotne zagrożenie zarówno dla posiadaczy kart, jak i dla instytucji finansowych, które muszą stale inwestować w poprawę swoich systemów zabezpieczeń, aby zapobiec potencjalnym stratom.

Skimming początkowo koncentrował się na wykorzystaniu paska magnetycznego znajdującego się na kartach płatniczych do kopiowania znajdujących się tam informacji. Z czasem jednak, wraz z postępem technologicznym, metody te ewoluowały i objęły również karty wyposażone w czipy, które miały stanowić bezpieczniejszą alternatywę dla tradycyjnych kart magnetycznych. Mimo wprowadzenia zaawansowanych zabezpieczeń, takich jak czipy EMV, przestępcy znaleźli sposoby na obejście tych mechanizmów, co sprawia, że zarówno użytkownicy kart, jak i banki muszą zachować szczególną ostrożność (niebezpiecznik.pl 2015a).

Banki oraz inne instytucje finansowe, które korzystają z szerokiej sieci bankomatów, mają naturalny interes w zapewnieniu jak najwyższego poziomu bezpieczeństwa transakcji dokonywanych za ich pośrednictwem. Automatyzacja transakcji za pomocą kart płatniczych pozwala instytucjom finansowym na znaczne ograniczenie kosztów operacyjnych, zwłaszcza związanych z obsługą kasową w oddziałach. Wymusza to jednak konieczność inwestowania w zaawansowane technologie zabezpieczeń, aby zapobiec ewentualnym stratom wynikającym z oszustw, takich jak skimming (Brush, Dangol, O'Brien 2012). Dlatego banki stale rozwijają swoje systemy ochrony, starając się przeciwdziałać zagrożeniom, które ewoluują równie szybko, co sama technologia płatnicza.

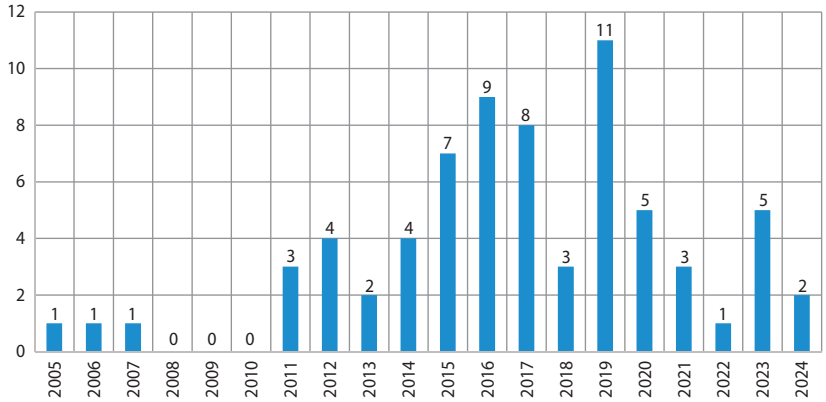
W rezultacie, zrozumienie mechanizmów działania takich oszustw oraz środków zaradczych staje się kluczowe zarówno dla instytucji finansowych, jak i dla użytkowników kart, którzy muszą być świadomi potencjalnych zagrożeń związanych z korzystaniem z nowoczesnych form płatności.

1. Przegląd literatury

Przy użyciu narzędzia bibliometrix (Aria, Cuccurullo 2017) przeprowadzono analizę 70 publikacji pochodzących z bazy Web of Science oraz Scopus, związanych ze skimmingiem. Pierwsze publikacje dotyczące skimmingu w tychże bazach odnotowano w 2005 roku. W swojej pracy Walsh (2005) skupił się na wprowadzanych wówczas kart z czipem, jako bezpieczniejszej, odpornej na skimming alternatywy wobec kart z paskiem magnetycznym. Biorąc pod uwagę, że pojawienie się skimmerów dostosowanych do kart czipowych odnotowano w 2015 roku (niebezpiecznik.pl 2015b), wnioski z pracy Walsha wydają się słuszne, lecz powinny skłaniać nas ku ciągłemu poszukiwaniu nowych rozwiązań oraz udoskonalaniu już istniejących.

Jak możemy zauważyć na rysunku 1, szczyt publikacji dotyczących skimmingu przypadł na latach 2015–2019, co może być związane z pojawieniem się nowych metod skimmingu (EMV Shimmer).

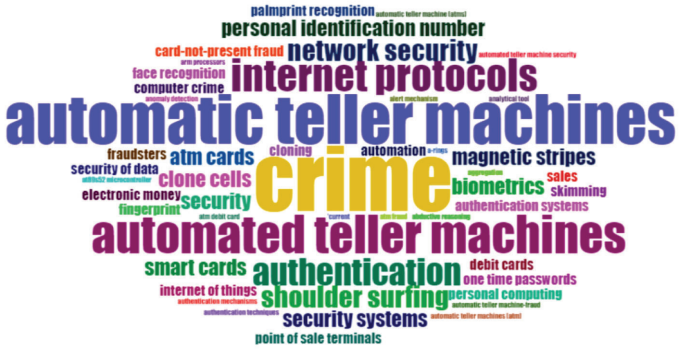
Rysunek 1. Liczba publikacji dotyczących skimmingu w bazach Web of Science i Scopus



Źródło: opracowanie własne, na podstawie danych Web of Science, Scopus sporządzone z pomocą narzędzia bibliometrix.

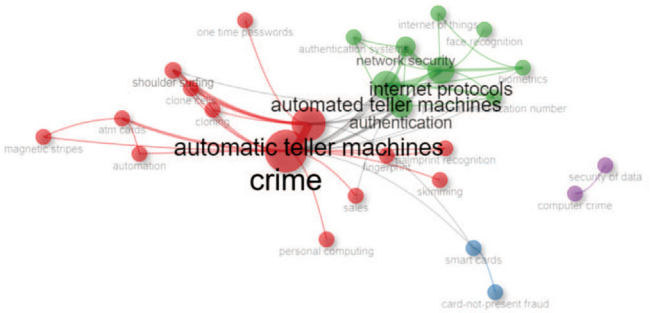
Najczęściej cytowanymi publikacjami były materiały pokonferencyjne z konferencji prowadzonych przez IEEE (Instytut Inżynierów Elektryków i Elektroników), w tym książka Bond, Choundary, Murdoch, Skorobogatov i Anderson (2014), dotycząca klonowania kart płatniczych z czipem (EMV), która została zacytowana 171 razy, w tym 48 przez czasopisma z baz Scopus i Web of Science. Drugą najbardziej cytowaną (48 cytowań Google Scholar, 13 cytowań WoS i Scopus), choć wyraźnie mniej od poprzedniczki, była publikacja Khan, Hasan i Xu (2015), która również pochodziła z konferencji IEEE. Autorzy proponowali w niej nowe narzędzie (SEPIA) do autoryzacji płatności w bankomatach.

Rysunek 2. Najczęstsze słowa kluczowe w artykułach WoS i Scopus dotyczących skimmingu



Źródło: opracowanie własne na podstawie bibliometrix.

Rysunek 3. Główne obszary badań nad skimmingiem



Źródło: opracowanie własne przy wykorzystaniu narzędzia bibliometrix.

Jak możemy zauważyć na rysunku 3, głównym tematem odnoszącym się do procederu skimmingu są bankomaty (ATM, automatic teller machines), a także ujęcie skimmingu jako przestępstwa. Jako tematy drugorzędne możemy wyróżnić tematy powiązane z bezpieczeństwem i zabezpieczeniami (*internet protocols*, *authentication*, *security of data*, *smart cards*).

2. Metody skimmingu

Jak zauważają Scaife, Peeters, Traynor (2018), skimmery, czyli urządzenia służące do nielegalnego pozyskiwania danych z kart płatniczych, można podzielić na kilka typów, w zależności od ich fizycznej budowy oraz metody odczytu danych na:

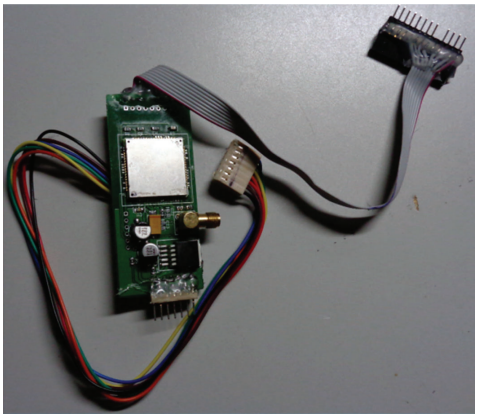
Zewnętrzne (Overlay) – zamontowane na urządzeniu płatniczym, najczęściej zakrywające wlot od urządzenia, lub będące nakładką na klawiaturę numeryczną.

Rysunek 4. Przykład urządzenia typu overlay

Źródło: Komenda Stołeczna Policji (2015).

Wewnętrzne (Internal) – zamontowane wewnątrz urządzenia płatniczego, zamontowanie ich wymaga dostępu do wnętrza urządzenia płatniczego.

Rysunek 5. Przykład urządzenia typu internal



Źródło: krebsonsecurity.com (2017).

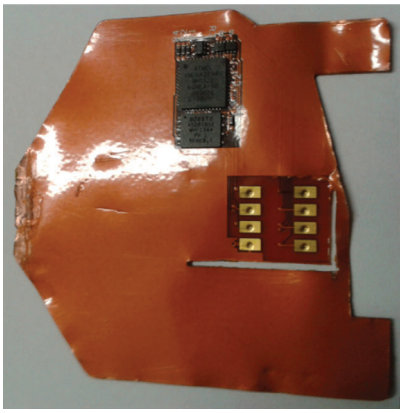
Deep-instert – do tej grupy możemy zaklasyfikować urządzenia umieszczane we wnętrzu urządzenia płatniczego, do której dostęp można uzyskać od zewnętrz urządzenia, najczęściej są to „wkładki" do slotu na karty płatnicze.

Rysunek 6. Przykład urządzenia typu deep-instert

Źródło: krebsonsecurity.com (2022).

EMV Shimmer – to urządzenia podobne do urządzeń deep-instert, potrafiące odczytać dane czipu płatniczego,

Rysunek 7. Przykład urządzenia typu EMV Shimmer



Źródło: Niebezpiecznik.pl (2015b).

Wiretap – to urządzenia podłączane od zewnątrz, najczęściej do kabla Ethernet bankomatu, umożliwiające przechwycenie danych przesyłanych z bankomatu (atak *man-in-the-middle*).

Opitek (2017) wyróżnia trzy etapy realizacji przestępstwa skimmingu:

1. Skopiowanie danych z paska magnetycznego i rejestracja numeru PIN.
2. Produkcja fałszywej karty i identyfikacja przypisanego jej PINu.
3. Realizacja transakcji przy użyciu fałszywych kart.

Obecnie dane mogą być zarejestrowane nie tylko z paska magnetycznego, ale również czipu karty kredytowej.

3. Główne metody zapobiegania skimmingowi

Jedną z metod zapobiegania oszustw z użyciem skimmera jest wykorzystanie specjalistycznych urządzeń. Pierwszym tego typu urządzeniem był „Skim Reaper" (urządzenie działające na tej samej zasadzie widoczne jest na rysunku 8), opracowany przez badaczy University of Florida (Nolen Scaife i Christian Peeters), przy współpracy z nowojorską policją (NYPD) (Scaife, Peeters, Traynor 2018). Urządzenie pierwotnie składało się z mikrokontrolera i „karty pomiarowej", a działa na zasadzie wykrywania skoków napięcia powstających w wyniku kontaktu paska magnetycznego z głowicą czytnika (Maj 2018). W przypadku prawidłowo działającego bankomatu powinna zostać wykryta jedna głowica, natomiast gdy system wykryje powyżej jednej głowicy oznacza to obecność skimmera w bankomacie.

Możliwe do kupienia są urządzenia do użytku komercyjnego, jak „Skim Scan" (rysunek 8), oraz „Skim Swipe" (rysunek 9).

Rysunek 8. Urządzenie „Skim Scan"

Źródło: Amazon.com (n.d.).

Rysunek 9. Urządzenie „Skim Swipe"

Źródło: Amazon.com (n.d.).

4. Propozycje działań banków

Konieczna jest edukacja w zakresie bezpieczeństwa transakcji klientów instytucji finansowych. Banki powinny informować klientów o potencjalnych zagrożeniach. Jest to ważne nie tylko z perspektywy klienta, dla którego utrata środków pieniężnych zgromadzonych na koncie może być traumatycznym przeżyciem (Bruhn 2015), ale również z perspektywy instytucji finansowej, która najprawdopodobniej będzie zobowiązana zwrócić oszukanemu klientowi pieniądze z własnych środków. Jeżeli bowiem klient nie dopuścił się rażącego niedbalstwa (np. dopuścił się „tylko" niedbalstwa lub został oszukany przy zachowaniu środków ostrożności) bank jest zobowiązany zwrócić pieniądze ofierze przestępstwa (Sąd Rejonowy dla Warszawy-Mokotowa w Warszawie 2017).

W zapobieganiu i utrudnianiu praktyki skimmerskich wartościową praktyką jest umieszczanie na bankomacie lub w jego otoczeniu zdjęcia wzorcowego danego modelu bankomatu. Pozwala to klientowi na upewnienie się, że do bankomatu nie zostały

doczepione urządzenia skimmerskie typu overlay. Warto przy tym zadbać, aby w przypadku wyświetlania komunikatu na ekranie bankomatu był on dostosowany do wyglądu modelu bankomatu, na którym jest wyświetlany (Niebezpiecznik.pl 2018).

Innym sposobem przeciwdziałania skimmingowi jest ochrona fizyczna. Na uwagę zasługują tutaj takie rozwiązania jak ActivEdge (firma Diebold Nixdorf), polegające na odczytywaniu karty włożonej do bankomatu dłuższą krawędzią, a nie krótszą krawędzią, jak w przypadku tradycyjnych bankomatów. Z kolei firma Level IO oferuje nakładki na terminale sklepowe, co ma stanowić zabezpieczenie przed skimmerami typu overlay. Amerykańska sieć sklepów Taget sprzedaje natomiast plastikowe wkładki, którymi można przetestować gniazdo terminala na karty bankowe. Jeżeli urządzenie można włożyć w całości, oznacza to, że jest bezpieczne. Należy również rozważyć instalowanie w bankomatach ruchomych (zasłanianych) urządzeń wejściowych (klawiatury PIN, wlotu na kartę etc.), co uniemożliwiłoby instalację części skimmerów. Aktywowanie urządzeń mogłoby następować zbliżeniowo (po przyłożeniu karty) lub stopniowo (np. klawiatura PIN byłaby udostępniana po włożenia karty i wpisaniu kodu PIN). Potencjalnym zabezpieczeniem mogłoby być również wyposażenie bankomatów w gniazdo USB do odczytu kluczy U2F lub autoryzacja za pomocą biometrii.

5. Prawne aspekty skimmingu

Janowicz i Klepacz (2002) definiują skimming jako nielegalną operację, polegającą na skopiowaniu zawartości paska magnetycznego podczas transakcji dokonywanej przez prawowitego właściciela karty. Z kolei Mikołajczyk (2014) definiuje skimming jako bezprawne skopiowanie informacji paska magnetycznego, umieszczonego na karcie płatniczej, oraz przechwycenie przypisanego do niej kodu PIN, bez wiedzy i woli użytkownika karty, w celu wykorzystania duplikatu służącego do obciążenia rachunku bankowego posiadacza. Gadecki (2023) z kolei zauważa, że takie czynności jak przybycie sprawcy na miejsce przestępstwa, zamontowanie urządzenia kopiującego zapis paska magnetycznego, nagrywanie kombinacji klawiszy wybieranych na klawiaturze bankomatu podczas wybierania numeru PIN są czynnościami przygotowawczymi do przestępstwa skimmingu, a nie usiłowaniem przestępstwa jako takim.

W zależności od kwalifikacji karnej czynu skimming może być zakwalifikowany zarówno jako:

1. Podrobienie innego środka płatniczego (art. 310 § 1 k.k.) – za co grozi kara do 25 lat pozbawienia wolności.
2. Kradzież informacji zakodowanej w pasku magnetycznym karty (art. 267 § 1 k.k.) – za co grozi kara do 2 lat pozbawienia wolności.
3. Kradzież pieniędzy z konta przypisanego do danej karty (art. 278 § 1 k.k.) – za co grozi kara do 5 lat pozbawienia wolności.

Podsumowanie

W dobie szybkiego rozwoju technologii płatniczych, jak karty płatnicze czy transakcje bezgotówkowe, zagrożenia związane z oszustwami, w tym skimmingiem, stają się coraz bardziej powszechne i zaawansowane. Skimming, polegający na nielegalnym kopiowaniu danych z kart płatniczych, nieustannie ewoluuje, co stawia zarówno instytucje finansowe, jak i użytkowników, w obliczu nowych wyzwań. Pomimo wprowadzenia zaawansowanych środków zabezpieczeń, jak czipy EMV, przestępcy wciąż znajdują sposoby na obejście tych technologii, rozwijając coraz bardziej wyrafinowane metody pozyskiwania danych.

W związku z tym konieczne jest nieustanne doskonalenie systemów ochrony i inwestowanie w nowoczesne technologie zabezpieczające, jak detektory skimmerów, lepsze zabezpieczenia fizyczne bankomatów oraz innowacyjne rozwiązania technologiczne, które zmniejszają ryzyko ataku. Ochrona przed skimmingiem nie powinna ograniczać się jedynie do technologii, ale także obejmować edukację użytkowników, którzy muszą być świadomi zagrożeń i stosować zasady bezpiecznego korzystania z kart płatniczych.

Instytucje finansowe mają obowiązek nie tylko inwestować w zabezpieczenia, ale również prowadzić działania prewencyjne, które pomogą klientom unikać niebezpieczeństw. Z kolei dla użytkowników kluczowe jest świadome korzystanie z nowoczesnych form płatności, regularne monitorowanie swoich kont oraz unikanie transakcji w podejrzanych miejscach.

Podsumowując, walka z oszustwami finansowymi, jak skimming, wymaga stałej współpracy między instytucjami finansowymi, producentami technologii i użytkownikami. Tylko poprzez wspólne działania, w tym wdrażanie coraz bardziej zaawansowanych zabezpieczeń oraz edukację społeczeństwa, możliwe jest zminimalizowanie ryzyka utraty środków i skuteczne przeciwdziałanie przestępczości finansowej.

Bibliografia

Amazon.com (n.d.), Skim Scan detects hidden card skimmers in ATMs, fuel dispensers and more. Pobrano z: https://www.amazon.com/Instantly-detects-Hidden-Skimmers-terminals/dp/B085R98GGH (dostęp: 12.09.2024).

Aria M., Cuccurullo C. (2017), bibliometrix: *An R-tool for comprehensive science mapping analysis*, „Journal of Informetrics", 11(4), pp. 959–975, Elsevier.

Bhatla T.P., Prabhu V., Dua A. (2003), *Understanding credit card frauds*, „Cards business review", 1(6).

Bond M., Choudary O., Murdoch S.J., Skorobogatov S., Anderson R. (2014), *Czip and Skim: cloning EMV cards with the pre-play attack*, [w:] *2014 IEEE Symposium on Security and Privacy* (pp. 49–64), IEEE.

Bruhn A.G. (2015), *Personal and social impacts of significant financial loss*, „Australian Journal of Management", 40(3).

Brush T.H., Dangol R., O'Brien J.P. (2012), *Customer capabilities, switching costs, and bank performance*, „Strategic Management Journal", 33(13).

Gadecki B. (2023), *Kodeks karny. Część szczególna. Art*, 252–316.

Janowicz R., Klepacz R. (2002), *Pieniądz elektroniczny na świecie, istota i zastosowanie elektronicznej portmonetki*, Warszawa.

Khan R., Hasan R., Xu, J. (2015), SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices, [w:] 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (pp. 41–50). IEEE.

Komenda Stołeczna Policji (2015), *„Skimmer" wpadł przy banku*. Pobrano z: https://ksp.policja.gov.pl/pl/dzialania/aktualnosci/34119,Skimmer-wpadl-przy-banku.html (dostęp: 25.08.2024).

Krebsonsecurity.com-(2017),*GasPumpSkimmerSendsCardDataViaText.*Pobranoz:https://krebsonsecurity.com/2017/07/gas-pump-skimmer-sends-card-data-via-text/ (dostęp: 25.08.2024).

Krebs B. (2022), *Say hello to crazy thin 'deep insert' ATM skimmers. Krebs on Security*, https://krebsonsecurity.com/2022/09/say-hello-to-crazy-thin-deep-insert-atm-skimmers/

Maj M. (2018), *Oto wykrywacz skimmerów. Szkoda, że nie jest masowo produkowany*. Pobrano z: https://niebezpiecznik.pl/post/oto-wykrywacz-skimmerow-szkoda-ze-nie-jest-masowo-produkowany/ (dostęp: 25.08.2024).

Mikołajczyk K. (2014), *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 10(6).

Niebezpiecznik.pl (2015a), *Pierwszy skimmer na karty czipowe*. Pobrano z: https://niebezpiecznik.pl/post/pierwszy-skimmer-na-karty-czipowe/ (dostęp: 24.08.2024).

Niebezpiecznik.pl (2015b), Pierwszy skimmer na karty czipowe. Pobrano z: https://niebezpiecznik.pl/post/pierwszy-skimmer-na-karty-czipowe/ (dostęp: 25.08.2024).

Niebezpiecznik.pl (2018), ** Skimmer czy nie? Czyli ciekawy komunikat od BZWBK*. Pobrano z: https://niebezpiecznik.pl/post/skimmer-czy-nie-czyli-ciekawy-komunikat-od-bzwbk/ (dostęp: 7.09.2024).

Opitek P. (2017), *Skimming aspekty kryminalistyczne Cyberprzestępczość w bankowości elektronicznej*, CH Beck, Warszawa.

Sąd Rejonowy dla Warszawy-Mokotowa w Warszawie, 27 września 2017, XVI C 169/19 (Polska), https://orzeczenia.mokotow.sr.gov.pl/details/$N/154505200008003_XVI_C_002019_2016_Uz_2017-09-27_001

Scaife N., Peeters C., Traynor P. (2018), *Fear the reaper: Characterization and fast detection of card skimmers*, [w:] 27th USENIX Security Symposium (USENIX Security 18).

Walsh N. (2005), *ATM fraud prompts card rethink?*, Card Technology Today, 17(2), 10.