Anna Męzik
Absolwentka studiów I stopnia IPSiR UW

Rodzaje kradzieży tożsamości oraz przypadki kradzieży tożsamości w Polsce

Wstęp

Zjawisko podszywania się pod inną osobę jest obecne w historii i kulturze od starożytności. Historia biblijnego Jakuba, który przy pomocy matki - Rebeki, przebrał się za swojego starszego brata, aby to jemu ojciec udzieli błogosławieństwa i przekazał majątek jest najstarszym przypadkiem kradzieży tożsamości opisanym w literaturze1. Przez lata słynni szpiedzy posługujący się cudzą tożsamością, a także wybitni oszuści stali się bohaterami kultury popularnej. Wydaje się jednak że to przełom XX i XXI wieku, wraz z rozwojem technologii i postępującą globalizacją sprawił że kradzież tożsamości stała się przedmiotem reakcji prawnokarnych w najbardziej rozwiniętych państwach świata. W państwach takich jak Stany Zjednoczone powstały również wyspecjalizowane organizacje zajmujące się wspieraniem ofiar kradzieży tożsamości, oraz przeciwdziałaniem temu zjawisku. Problematyką kradzieży tożsamości zajęły się również organizacje broniące prawa do prywatności. Instytucje te wyodrębniły rozmaite rodzaje kradzieży tożsamości, kilka z nich omówię w tym artykule. Spróbuję również przybliżyć obraz tego zjawiska w Polsce, opisując przypadki kradzieży tożsamości na podstawie dostępnych publikacji.

Rodzaje kradzieży tożsamości

Przy omawianiu typów kradzieży tożsamości niezbędne wydaje się odwołanie do anglojęzycznych opracowań na temat tego zjawiska. Najwięcej publikacji na temat kradzieży tożsamości powstaje w Stanach Zjednoczonych, gdzie ofiarami tego procederu każdego roku staje się kilka milionów Amerykanów2. Powstają tam również rozmaite typologie kradzieży tożsamości, wyszczególnione ze względu na cel działania sprawcy lub specyficzną grupę ofiar. W opracowaniach wymienia się od kilku do kilkudziesięciu typów kradzieży tożsamości3. W artykule przedstawię kilka najczęściej pojawiających się w publikacjach. Część z nich wydaje się być specyficzna dla uwarunkowań kulturowych czy prawnych USA,

[1] *Jakub otrzymuje zdobyte podstępem błogosławieństwo,*[w:] *Pismo Święte Starego i Nowego Testamentu (Biblia Tysiąclecia),* wydanie 5,wydawnictwo Pallottium, Poznań 2000, Rdz 27, s.49-51.

[2] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 2013,s.4. http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf [dostęp 27.04.2014].

[3] Strona internetowa firmy zajmującej sprzedażą ubezpieczeń i ochroną danych http://www.identityfraud.com/partners/site/identity_theft_types.html [dostęp 27.04.2014].

ale uważam że przynajmniej w pewnym stopniu, w związku z postępem cywilizacyjnym, mogą mieć zastosowanie przy analizowaniu zjawiska w Polsce.

Najlepiej znanym konsumentom rodzajem kradzieży tożsamości jest finansowa kradzież tożsamości (financial identity theft) Wiąże się ona z wszelkim wykorzystaniem przez sprawcę cudzych danych osobowych w celach finansowych, takich jak wyłudzanie kredytów, korzystnie z kont bankowych ofiar do dokonywania transakcji, korzystania z kart kredytowych i bankomatowych ofiar, zakładanie nowych kont bankowych na dane ofiary i późniejsze wykorzystywanie ich do osiągnięcia korzyści majątkowych4.

Można wymienić dwa podstawowe rodzaje finansowej kradzieży tożsamości. Pierwszy z nich polega na tym, że sprawca wykorzystuje istniejące już rachunki bankowe ofiary i karty kredytowe lub bankomatowe ofiar. Najczęściej sprawca uzyskuje do nich dostęp poprzez kradzież dokumentów czy kart bankomatowych ofierze. Jeżeli ofiara zgłosi kradzież lub zagubienie dokumentów, proceder korzystania z jej rachunków nie trwa długo, gdyż najczęściej bank czy instytucja finansowa blokuje korzystanie rachunku lub karty. Ofiary ponoszą straty finansowe, ale są one niewielkie w porównaniu z drugim rodzajem finansowej kradzieży tożsamości, polegającej na założeniu przez sprawcę nowego rachunku bankowego na dane ofiary, której skradziono tożsamość. Wówczas proceder wykorzystywanie jej danych trwa o wiele dłużej - kilka miesięcy lub nawet lat, sprawcy często budują historię kredytową ofiary dokonując płatności z założonego fikcyjnego konta, zaciągając kredyty, a to wymaga czasu. Ofiara często nie uświadamia sobie że na jej dane zostało założone fikcyjne konto bankowe, póki nie spotka się z konsekwencjami dotyczącymi jej bezpośrednio, takimi jak wezwania do spłaty pożyczek, czy odmowa udzielenia kredytu. Konsekwencje w tym wypadku są bardziej dotkliwe dla ofiar, nie tylko ze względu na straty finansowe przez nie poniesione, ale również ze względu na czas konieczny do uporządkowania swojej historii kredytowej.

Finansowa kradzież tożsamości, nie jest najdotkliwszym z rodzajów kradzieży tożsamości, ponieważ także w interesie banków leży odzyskanie środków finansowych i zaufania obywateli. Ofiary innych rodzajów kradzieży tożsamości mogą odczuwać skutki finansowe i to najczęściej one dopiero uświadamiają im że ich dane osobowe zostały wykorzystane5.

Zdecydowanie bardziej dotkliwa dla ofiar jest medyczna kradzież tożsamości (medical identity theft). Polega ona na tym, że sprawca używa danych osobowych oraz dokumentów potwierdzających ubezpieczenie zdrowotne ofiary bez jej wiedzy i zgody do uzyskania świadczeń medycznych. Zdarza się fałszowanie dokumentacji medycznej ofiar w celu uzyskania środków finansowych na zabiegi medyczne. Sprawcami medycznej kradzieży tożsamości są lekarze, pielęgniarki, inni pracownicy służby zdrowia, a także przestępcy i coraz częściej organizacje przestępcze. Sprawcy posługują się różnymi modelami działania, jednak cechą wspólną dla medycznej kradzieży tożsamości jest to, że dane osobowe ofiar zostają wykorzystane bez ich wiedzy w celu uzyskania świadczeń medycznych6.

---

[4] Axton E. Betz, Whitney Walters, *Medical Identity Theft,* „Journal of Consumer Education", 29, 2012 s. 75. http://works.bepress.com/cgi/viewcontent.cgi?article=1004&context=axton_betz-hamilton [dostęp 27.04.2014].

[5] Strona internetowa na temat kradzieży tożsamości http://idtheft.about.com/od/identitytheft101/a/FinancialIDT.htm [dostęp 30.04.2014].

[6] Dixton Pam, *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You,* World Privacy Forum, 2006 s.2, 16, 36. http://www.worldprivacyforum.org/wp-

Zjawisko medycznej kradzieży tożsamości jest słabo zbadane. Niewielka jest również wiedza na jego temat wśród społeczeństwa. Według raportu Federalnej Komisji Handlu (Federal Trade Commission) z 2006 roku przypadki medycznej kradzieży tożsamości stanowiły w latach 2001-2006 co najmniej 250 000 wszystkich zgłoszonych w tym czasie przypadków kradzieży tożsamości w Stanach Zjednoczonych7.

Medyczna kradzież tożsamości jest trudna do wykrycia, gdyż ofiary często nie są świadome że ich tożsamość została wykorzystana do wyłudzenia usług medycznych. Rodzi to poważne konsekwencje. Ofiary mogą podobnie jak ofiary innych typów kradzieży tożsamości odczuwać konsekwencje finansowe takie jak: konieczność zapłaty za usługi medyczne z których nigdy nie korzystały czy niemożność uzyskania kredytu8.

Jednak bardziej niebezpieczne dla samych ofiar są skutki w postaci zmian w dokumentacji medycznej. Błędne informacje mogą zostać wprowadzone przez samych sprawców kradzieży tożsamości lub stanowić wtórne skutki kradzieży tożsamości. Zmiany w dokumentacji medycznej ofiar mogą pozostawać przez wiele lat nieodkryte. W związku z tym ofiary mogą otrzymać na podstawie sfałszowanej dokumentacji niewłaściwe leczenie, które może prowadzić do pogorszenia ich stanu zdrowia, a nawet śmierci. Inne konsekwencje dla ofiar to na przykład: niemożność podjęcia zatrudnienia ze względu na dolegliwości zdrowotne, które zostały wprowadzone do ich dokumentacji, a na które faktycznie nie cierpią czy trudności z uzyskaniem ubezpieczenia zdrowotnego. Ofiary medycznej kradzieży tożsamości nie otrzymują takiego wsparcia jak osoby, które dotknęła finansowa kradzież tożsamości ze strony instytucji czy organizacji pomagającym ofiarom przestępstw. Przestępstwo medycznej kradzieży tożsamości jest trudne do wykrycia, a ciemna liczba przypadków medycznej kradzieży tożsamości jest znaczna9.

Wykrycie medycznej kradzieży tożsamości utrudnia dodatkowo fakt, że jej sprawcami często są profesjonaliści zaznajomieni z funkcjonowaniem specjalistycznych baz danych pacjentów, co ułatwia im ukrycie fałszywej dokumentacji. Ponadto, Pam Dixton zauważa niebezpieczeństwo związane z tworzeniem ogólnokrajowych elektronicznych baz pacjentów. Bazy takie w założeniu mają zmniejszyć liczbę oszustw i poprawić jakość opieki zdrowotnej. Autorka zauważa przede wszystkim dwa problemy związane z wprowadzeniem w Stanach Zjednoczonych National Health Information Network - ogólnokrajowej elektronicznej bazy informacji o pacjentach. Po pierwsze jej zdaniem stworzenie takiej bazy umożliwi przestępcom łatwiejszy dostęp do danych ofiar, zwiększy także zakres informacji, do których potencjalni sprawcy mogą mieć dostęp. Usprawni to ich przekazywanie, które w formie elektronicznej zdecydowanie łatwiej jest transmitować. Po drugie, utworzenie elektronicznej bazy danych pacjentów może powielać istniejące obecnie błędy w dokumentacji medycznej, których pacjenci nie są świadomi i nie posiadają również możliwości ich naprawienia. W przywoływanym raporcie podkreślono, że problem wykorzystania nowoczesnych technologii w ochronie zdrowia nie musi być niekorzystny dla pacjentów. Nie należy jednak traktować

---

content/uploads/2007/11/wpf_medicalidtheft2006.pdf [dostęp 30.04.2014].

[7] Axton E. Betz, Whitney Walters, *Medical Identity Theft,* "Journal of Consumer Education", 29, 2012, s. 75. http://works.bepress.com/cgi/viewcontent.cgi?article=1004&context=axton_betz-hamilton [dostęp 30.04.2014].

[8] Dixton Pam, op. cit. s.5. http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf [dostęp 30.04.2014].

[9] Dixton Pam, *op. cit.,* s.6-8.http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf [dostęp30.04.2014].

elektronicznych baz danych jako rozwiązania wszystkich problemów. Ponadto samo zjawisko medycznej kradzieży tożsamości nie jest dobrze zbadane, a to dodatkowo utrudnia zapobieganie mu 10.

Wydaje się, że z podobnymi problemami będziemy musieli zmierzyć się w Polsce wraz z wdrażaniem systemu Elektronicznej Dokumentacji Medycznej 11.

Kolejną formą kradzieży tożsamości wyróżnioną w opracowaniach jest kradzież tożsamości dziecka (child identity theft). Została ona wyróżniona ze względu na specyficzną grupę ofiar jaką są dzieci. Najczęściej popełniana jest w celach finansowych, takich jak zaciągniecie kredytu na dane dziecka, dokonywanie zakupów. Zdarzają się również przypadki wyłudzania usług medycznych przy posłużeniu się danymi dzieci. Dzieci często padają ofiarą kradzieży tożsamości w Stanach Zjednoczonych z kilku przyczyn. Po pierwsze w Stanach Zjednoczonych nie funkcjonuje dokument tożsamości na poziomie federalnym. Do uwierzytelnienia danych czy założenia rachunku bankowego wykorzystuje się Numer Ubezpieczenia Społecznego (Social Security Number). Instytucje finansowe z reguły nie łączą numerów ubezpieczenia społecznego zamieszczonych we wnioskach o kredyt z datą urodzenia osoby o taki kredyt występującej. W rezultacie złodzieje tożsamości mogą korzystać z tożsamości dziecka przez wiele lat bez obawy że zostaną złapani. Kolejną przyczyną, dla której to dzieci są szczególnie narażone na kradzież tożsamości, jest brak historii kredytowej i nikłe prawdopodobieństwo tego że w ciągu najbliższych kilku lat dziecko będzie ubiegało się o kredyt. Ofiary kradzieży tożsamości są coraz młodsze. Według danych Identity Theft Resource Center liczba przypadków kradzieży tożsamości dzieci będzie wzrastać. Sprawcami kradzieży tożsamości dzieci są najczęściej ich rodzice, którzy używają tożsamości swych dzieci do zaciągania kredytów na przykład samochodowych, czy uzyskania kart kredytowych. Sprawcami kradzieży tożsamości dziecka mogą być również osoby niespokrewnione z ofiarą, ale posiadające dostęp do danych osobowych dzieci. Są to na przykład nauczyciele, inni pracownicy szkoły czy służby zdrowia. Wyróżnia się dwa rodzaje ofiar kradzieży tożsamości dziecka ze względu na wiek w którym to ofiara odkryła że jej tożsamość została skradziona. Pierwsze to pokrzywdzone dzieci (child victims). Są to osoby, które przy pomocy dorosłych najczęściej rodziców, odkrywają przed ukończeniem 18 roku życia że stały się ofiarami kradzieży tożsamości. Drugą grupę ofiar stanowią dorosłe ofiary (adlut/child victims), są to osoby, które już po osiągnięciu przez nie pełnoletniości dowiedziały się że ich tożsamość została skradziona gdy były dziećmi. Kradzież tożsamości wychodzi na jaw najczęściej gdy ubiegają się o kredyt, otrzymują odmowę udzielenia pożyczki ze względu na negatywną historię kredytową. Uświadamia im to, że ich dane zostały wykorzystane, gdy byli dziećmi. Ponieważ proceder wykorzystywania ich danych mógł trwać wiele lat, trudno jest im oczyścić historię kredytową, w związku z czym mają problemy z uzyskaniem kredytów12.

[10] Dixton Pam, *ibid.,* s.9-10. http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf [dostęp 30.04.2014].

[11] Obwieszczenie ministra zdrowia z dnia 6 czerwca 2013 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania, Dz. U. Z 2014. poz. 177.

[12] Bentz E. Axton, Gudmunson Clinton G.,Hong Gong- Soon, *The Recovery Experiences of Child Identity Theft Victims: Preliminary Results*, „Consumer Interests Annual",Volune 58, 2012 , brak numeracji stron http://www.consumerinterests.org/assets/docs/CIA/CIA2012/2012-49%20the%20recovery%20experience%20of%20child%20identity%20theft%20victims%20-%20preliminary%20results.pdf [dostęp 30.04.2014].

Kolejną formą kradzieży tożsamości jest kryminalna kradzież tożsamości (criminal identity theft, criminal record identity theft). Występuje ona gdy oszust podaje przedstawicielom organów ścigania dane osobowe innej osoby lub przedstawia im fałszywe dokumenty weryfikujące tożsamość, podczas dochodzenia lub zatrzymania. Najczęściej wykorzystanie cudzej tożsamości ma miejsce gdy sprawca kradzieży tożsamości dokona przestępstwa lub wykroczenia drogowego. Otrzymuje wówczas mandat na nazwisko ofiary. Osoba której danymi się posłużono nie często nie jest świadoma tego że jej tożsamość została skradziona. Dowiaduje się o tym gdy otrzymuje wezwanie do zapłaty mandatów lub podczas zatrzymania w trakcie rutynowej kontroli drogowej. Może nawet zostać aresztowana za przestępstwa których nie dokonała. Część sprawców jednak dłużej posługuje się skradzioną tożsamością, odbywa karę za dokonane przestępstwa. Do bazy danych osób skazanych trafiają jednak nie dane oszusta, a ofiary. Posługiwanie się skradzioną tożsamością przez oszusta może trwać wiele lat. Ofiara uświadamia sobie, że jej dane zostały skradzione dopiero, gdy ma na przykład problemy z zatrudnieniem, ze względu na wcześniejszą karalność. Proces oczyszczenia historii kryminalnej trwa bardzo długo. Często ofiary nie otrzymują wsparcia ze strony policji i sądów13.

Ciekawym i bardzo trudnym do wykrycia typem kradzieży tożsamości jest klonowanie i ukrywanie tożsamości (identity cloning and concealment). W takiej sytuacji złodziej tożsamości podszywa się pod kogoś innego w celu ukrycia swojej prawdziwej tożsamości. Takie zjawisko dotyczy na przykład nielegalnych imigrantów, osób ukrywających się przed wierzycielami, czy osób które chcą pozostać anonimowe z przyczyn osobistych14.

Wraz z rozwojem sieci internetowej pojawili się tzw. posers czyli osoby tworzące konta na portalach społecznościowych przy wykorzystaniu zdjęć i informacji dotyczących innych osób. Jeżeli sprawca tego typu kradzieży tożsamości jest w stanie zbudować odpowiednią historię do tożsamości, którą wykorzystuje przez długi czas może pozostać nie wykryty15. Zjawisko to dotyczy głównie podszywania się pod znane osoby, aktorów, piosenkarki, gwiazdy medialne16. Kradzież tożsamości na portalach społecznościowych wiąże się też z cyberprzemocą, chęcią ośmieszenia ofiary, na przykład poprzez umieszczanie kompromitujących treści w jej imieniu 17.

Coraz popularniejszym w ostatnim czasie typem kradzieży tożsamości jest syntetyczna kradzież tożsamości (synthetic identity theft). W tym wypadku sprawca wykorzystuje dane kilku osób lub również swoje własne do stworzenia tożsamości fikcyjnej tożsamości18.

---

[13] Strona organizacji pozarządowej działającej w USA działającej na rzecz poszanowania prawa do prywatności https://www.privacyrights.org/criminal-identity-theft-what-to-do-if-it-happens-to-you [dostęp 8.05.2013].

[14] Tate Charles ,*Identity Theft Terms - What Is Identity Cloning and Concealment*? http://EzineArticles.com/5447554 [dostęp 8.06.2014].

[15] *Call for Justice, LLC—United Way 2-1-1 Training Paper Session 12: Identity Theft and Work of the Minnesota Attorney General* s. 2. http://callforjustice.org/wp-content/uploads/2013/05/Training-Paper-Volume-12-Identity-Theft_For-Website.pdf [dostep 8.06.2014].

[16] Słownik internetowy języka potocznego http://www.urbandictionary.com/define.php?term=poser&defid=4066254 [dostęp 7.06.2014].

[17] Reznik, Maksim (2013) *Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation* Touro Law Review:Vol. 29: No. 2, Article 12, s.11-12 http://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12 [dostęp 8.06.2014].

[18] Internetowy słownik terminów związanych z prawem http://definitions.uslegal.com/s/synthetic-

Poza przybliżonymi przeze mnie w tej części pracy typami kradzieży tożsamości z pewnością można wymienić jeszcze wiele innych rodzajów kradzieży. Należy pamiętać, że kradzież tożsamości często jest tylko etapem działania sprawców innych przestępstw takich jak terroryzm, oszustwa czy szpiegostwo19.

Zjawisko kradzieży tożsamości w Polsce

Zjawisko kradzieży tożsamości w Polsce nie jest dobrze zbadane. Brak jest reprezentatywnych badań dotyczących jego skali. Również kryminalizacja i jej zakres budzi szereg wątpliwości wśród prawników. Nie oznacza to jednak że problem kradzieży tożsamości nie istniał przed 2011 rokiem, gdy w Kodeksie karnym stypizowano przestępstwo kradzieży tożsamości. W tym punkcie artykułu chciałabym omówić kilka mechanizmów i przypadków kradzieży tożsamości, które miały miejsce w Polsce.

Posługiwanie się skradzionymi lub sfałszowanymi dokumentami tożsamości było szczególnie popularną metodą działania sprawców, którzy próbowali wyłudzić kredyty lub założyć fikcyjną działalność gospodarczą w okresie transformacji ustrojowej w pierwszej połowie lat 90. XX wieku. Jedno z pierwszych doniesień medialnych mówiące o próbie wyłudzenia kredytu przy posłużeniu się cudzym dowodem osobistym pochodzi z 1995 roku. W Warszawie zatrzymano wówczas dwudziestoośmioletniego mężczyznę, który to usiłował wyłudzić pieniądze z banku PEKAO S. A., jego wspólnik zbiegł, jednak pozostawił w okienku kasowym dowód osobisty z cudzymi danymi. Dowód ten został rok wcześniej skradziony w Bielsku Podlaskim20. Próby wyłudzenia kredytów przy posługiwaniu się skradzionymi lub zagubionymi dokumentami stwierdzającymi tożsamość są nadal powszechne. Według 17 edycji raportu „InfoDOK raport o dokumentach" pomiędzy II kwartałem 2013 roku, a I kwartałem 2014 roku udaremniono 7190 prób wyłudzeń kredytów. Łączna kwota, na którą próbowano wyłudzić kredyty, wynosiła 495 818 429 zł21. Dane te dotyczą jedynie prób wyłudzeń, przy użyciu dokumentów figurujących w bazie Dokumenty Zastrzeżone prowadzonej przez Związek Banków Polskich na podstawie zgłoszeń właścicieli zagubionych lub skradzionych dokumentów w placówkach banków.

Poza próbami wyłudzenia kredytów skradziony dowód tożsamości może służyć także do wynajęcia mieszkania lub pokoju hotelowego w celu kradzieży wyposażenia lub uniknięcia opłat, kradzieży wypożyczonego samochodu lub innych przedmiotów22.

Jednym z przypadków w którym złodzieje tożsamości posłużyli się skradzionym dowodem osobistym do zawarcia umowy z operatorem sieci telefonii komórkowej był przypadek pani Katarzyny, nauczycielki akademickiej z Krakowa. Kobiecie pod koniec lat 90. XX wieku podczas pobytu nad morzem skradziono torebkę wraz z dokumentami i kartami kredytowymi. Ofiara zgłosiła kradzież na policję. Wyrobiła nowe dokumenty i na kilkanaście lat zapomniała o całej sprawie. W 2013 roku otrzymała wezwanie od firmy windykacyjnej

---

identity-theft [dostęp 8.05.2014].

[19] *Call for Justice, LLC—United Way 2-1-1 Training Paper Session 12: Identity Theft and Work of the Minnesota Attorney General* s. 1 http://callforjustice.org/wp-content/uploads/2013/05/Training-Paper-Volume-12-Identity-Theft_For-Website.pdf [dostęp 8.06.2014].

[20] Wójcik Jerzy Wojciech, *Oszustwa finansowe zagadnienia kryminologiczne i kryminalistyczne,* wydawnictwo JWW, Warszawa 2008, s.190-191.

[21] *Raport o dokumentach infoDOK I kwartał 2014 – 17,* Związek Banków Polskich,.s. 3.

[22] *Informator Jak zachować się w przypadku utraty dokumentów,* Związek Banków Polskich, Warszawa 2013.http://cpb.home.pl/dokumentyzastrzezone/materialy.informacyjne.i.multimedia/kdz.informator.110614.pdf [dostęp 8.06.2014].

nakazujące jej spłatę zadłużenia w wysokości ponad siedmiu tysięcy złotych za niezapłacone rachunki telekomunikacyjne. W 2004 roku osoba posługująca się skradzionym dowodem zawarła umowę z operatorem sieci telefonii komórkowej w jednym z miasteczek na Pomorzu, następnie przez kilka lat nie płaciła rachunków za rozmowy telefoniczne. Mimo przedstawienia przez krakowiankę pism policyjnych informujących o zgłoszeniu kradzieży dokumentów firma windykacyjna nadal wymagała od niej spłaty zadłużenia23.

Znane są również przypadki gdy sprawca posługuje się zagubionym lub skradzionym dowodem tożsamości w innym celu niż próba wyłudzenia kredytu czy dokonywania zakupów na konto ofiary. Taki proceder może trwać nawet kilka lat. Przykładem ilustrującym taki mechanizm działania sprawcy jest historia trzydziestosiedmioletniej mieszkanki Wrocławia. Kobieta w 2005 roku zgubiła dowód osobisty, zgłosiła sprawę w stosownym urzędzie i wrobiła nowy dokument. W 2011 roku chciała zagłosować w wyborach w swoim miejscu zamieszkania. W lokalu wyborczym okazało się jednak, że nie znajduje się na liście osób uprawnionych do głosowania we Wrocławiu, gdyż zgłosiła chęć głosowania w Zakopanem. Przedstawicielka komisji wyborczej zawiadomiła policję w Zakopanem, tam czterdziestotrzyletnia kobieta posługująca się zagubionym kilka lat wcześniej dowodem osobistym wrocławianki oddała głos w wyborach. Funkcjonariusze Powiatowej Komendy Policji w Zakopanem zbadali sprawę. Okazało się, że oszustka przez kilka lat posługiwała się dowodem osobistym, który zagubiła mieszkanka Wrocławia. Pracowała w Zakopanem jako pokojowa używając nazwiska ofiary, ponadto ukończyła kurs oraz korzystała z opieki zdrowotnej posługując się skradzioną tożsamością. Sprawczyni od 2005 roku była ścigana listem gończym za niespłacone alimenty. Według policji pomiędzy ofiarą, a sprawczynią kradzieży tożsamości istnieje pewne podobieństwo w wyglądzie24.

W 2013 roku policja stwierdziła 12088 przypadków posługiwania się dokumentem innej osoby25.

Przełom XX i XXI wieku to okres gwałtownego rozwoju sieci internetowej. Według danych Głównego Urzędu Statystycznego dostęp do Internetu w 2012 roku posiadało 70,5% gospodarstw domowych w Polsce26. Najpopularniejszą aktywnością wśród polskich internautów jest korzystanie z poczty elektronicznej, korzysta z niej 50,4% badanych. Drugie miejsce zajmuje używanie czatów, udział w forach dyskusyjnych oraz aktywność na portalach społecznościowych - Internetu w tym celu używa 42,9% respondentów. Wzrasta odsetek korzystających z usług bankowości elektronicznej oraz sprzedających towary lub usługi za pomocą sieci27.

---

23 Strona internetowa czasopisma regionalnego z małopolski „Dziennik Polski" http://www.dziennikpolski24.pl/artykul/3233662,scigani-za-przedawnione-i-fikcyjne-dlugi,2,id,t,sa.html [dostęp 9.05.2014].

24 Strona internetowa czasopisma regionalnego z małopolski „Dziennik Polski" http://www.dziennikpolski24.pl/artykul/3067314,przy-okazji-wyborow-zdemaskowali-kradziez-tozsamosci,id,t.html [dostęp 9.05.2014].

25 Strona internetowa polskiej Policji zawierająca statystyki postępowań wszczętych i przestępstw stwierdzonych, statystyka dotycząca przestępstwa z art. 275 k. k. http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-15/63998,Poslugiwanie-sie-dokumentem-innej-osoby-art.-275.html [dostęp 9.05.2014.].

26 Główny Urząd Statystyczny Urząd Statystyczny w Szczecinie Ośrodek Nauki, Techniki, Innowacji i Społeczeństwa Informacyjnego: *Społeczeństwo Informacyjne w Polsce,* Szczecin 2012, s. 9.

27 Główny Urząd Statystyczny Urząd Statystyczny w Szczecinie Ośrodek Nauki, Techniki, Innowacji i Społeczeństwa Informacyjnego: *Społeczeństwo Informacyjne w Polsce,* Szczecin 2012, s. 13.

Coraz większa aktywność użytkowników i wzrost liczby udostępnianych w Internecie informacji sprawia, że staje się on miejscem atrakcyjnym dla działalności oszustów i cyberprzestępców. Dodatkowym warunkiem sprzyjającym takiej działalności jest pozorna anonimowość w Internecie oraz niewielka wiedza na temat bezpieczeństwa udostępnianych danych wśród użytkowników sieci.

Ataki cyberprzestępców często rozpoczynają się od wysyłania wiadomości będących spamem, czyli niepożądaną korespondencją wysyłaną za pośrednictwem drogi mailowej28. Aby wiadomość zakwalifikować jako spam, musi ona spełniać trzy warunki. Po pierwsze, treść wiadomości musi mieć charakter masowy, wyklucza to wiadomości o charakterze prywatnym. Po drugie, odbiorca nie wyraził zgody na otrzymanie takiej wiadomości. Po trzecie, nadawca, w wyniku wysłania wiadomości może odnieść korzyści większe od odbiorcy. Sam spam nie jest niebezpieczny dla odbiorców, jego masowy charakter może jedynie zablokować przeciążone serwery pocztowe29.

Wysyłany spam może służyć kradzieży danych ofiar na przykład zachęcając do udziału w internetowych grach hazardowych30.

Popularnym i niebezpiecznym dla potencjalnych ofiar spamem, nie tylko ze względu na utratę środków finansowych, ale również z powodu możliwości utraty danych osobowych jest tak zwany szwindel nigeryjski, nazwa tego mechanizmu działania pochodzi od oszustwa zainicjowanego przez mafię nigeryjską. Obecnie takie wiadomości wysyłane są z niemal każdego państwa na świecie. W wiadomości do potencjalnej ofiary zgłasza się oszust informujący o tym, że może podjąć ogromną kwotę pieniędzy, jednak konieczny jest udział osoby postronnej niezwiązanej z zainteresowanym, ani jego krajem. W zamian za pomoc finansową na przykład na opłacenie prawników oszust oferuje udział w zysku od 5 do 25 procent. Gdy ofiara podejmie korespondencję z oszustem, w którymś z maili pojawia się prośba o podanie danych i dokonanie wpłaty trudnymi lub niemożliwymi do namierzenia metodami, takimi jak przekazy pieniężne Western Union. Autor na którego się powołuję analizował treść wiadomości, które otrzymał, wykorzystujące mechanizm szwindlu nigeryjskiego. Pojawiały się wśród nich informacje o wygranej na loteriach czy otrzymaniu niespodziewanych spadków31.

Za pośrednictwem spamu oszuści wysyłają też propozycje intratnej oferty pracy. Zachęceni odbiorcy przesyłają na wskazany adres mailowy swoje CV, numer konta bankowego oraz kopię dowodu osobistego. Zaczynają pracować online dla instytucji finansowej. Ich zadaniem jest przekazywanie pieniędzy, które otrzymują od firmy po odliczeniu prowizji, na wskazane konta bankowe za pośrednictwem trudnych do namierzenia metod, takich jak przekazy pieniężne Western Union. Zostają tak zwanymi mułami pieniężnymi (money mule). W rzeczywistości, pieniądze, które podejmuje na konto muł pieniężny, którego tożsamość skradziono, pochodzą z nielegalnej działalności, z kradzieży kart kredytowych, fałszywych banków i sklepów internetowych. Następuje proceder prania

[28] Internetowy słownik języka polskiego PWN .http://sjp.pwn.pl/slownik/2575920/spam [dostęp 9.05.2013].

[29] Tejderowski Tomasz, *Kradzież tożsamości, terroryzm informatyczny, cyberprzestępstwa, internet, telefon, facebook,* ENETEIA Wydawnictwo Psychologii i Kultury , Warszawa 2013, s, 103.

[30] Wójcik Jerzy Wojciech, *op. cit.* ,s. 352.

[31] Tejderowski Tomasz, *op. cit*. s. 114-117.

brudnych pieniędzy. Osoba, która została mułem pieniężnym jest łatwa do namierzenia, gdyż pieniądze pochodzące z przestępstw docierały na jej konto32.

Jedną z najpopularniejszych metod kradzieży tożsamości w internecie jest phishing[33].

W 2005 roku skazano pierwszych sprawców korzystających z techniki phishingu, którzy okradli klientów jednego z banków. W 2004 roku stworzyli oni fałszywą stronę internetową tego banku i skradli ofiarom ponad trzydzieści trzy tysiące złotych34. Podczas największej kradzieży przy użyciu phishingu w Polsce, łupem oszustów padł milion złotych, jednak w tym wypadku to nie same ofiary wprowadziły swoje dane na oszukańczej stronie internetowej. Hasła i kody dostępu zostały im skradzione przy użyciu specjalnego oprogramowania rozsyłanego drogą mailowa 35.

W styczniu 2010 roku hakerzy zaatakowali klientów polskiego Banku PKO BP. Wysłano do nich maile, w których w polu nadawcy wiadomości widniał dobrze podrobiony adres mailowy banku (sevice@pkobp.pl). Celem ataku było zdobycie haseł do kont internetowych klientów banku oraz danych kart bankomatowych i kredytowych36.

Ciekawy proceder wyłudzania pożyczek na dane ofiar za pomocą oszukańczych ofert pracy stał się popularny w 2012 roku. Na portalach ogłoszeniowych, sprawcy zamieszczali oferty pracy online, na przykład jako tester usług bankowych. Wszystkie sprawy związane z podjęciem zatrudnienia były prowadzone drogą mailową lub za pośrednictwem specjalnych formularzy. Oszuści nakazywali ofiarom podanie swoich danych osobowych, numeru PESEL oraz dokonania przelewu niewielkiej kwoty w wysokości 1 złotego lub 1 grosza w celu potwierdzenia danych do umowy, która miała zostać przesłana pocztą. Przelew musiał być wykonany z rachunku bankowego należącego do ofiary. W tym momencie kontakt z potencjalnym pracodawcą się urywa. Ofiary w większości nieświadome tego, że w Polsce można założyć rachunek bankowy, bez konieczności wizyty w oddziale banku, właśnie za pomocą przelewu potwierdzającego dane, były przekonane, że straciły jedynie niewielkie kwoty. Oszust prosząc o przelanie tej niewielkiej kwoty ofiarę, tak naprawdę zakłada fikcyjne konto w banku na jej dane. Następnie wykorzystuje je do zaciągania pożyczek w instytucjach finansowych udzielających ich drogą online. Sprawca otrzymuje pieniądze na konto, którego właścicielem jest ofiara oszustwa. O tym, że ich tożsamość została skradziona, ofiary przekonują się dopiero gdy to na ich adres przychodzą monity informujące o konieczności spłaty zadłużenia37. Ponadto oszust uzyskując raz dane ofiary, może mnożyć rachunki

---

[32] Strona internetowa opisująca mechanizmy oszustw internetowych http://www.oszustwsieci.pl/ph_kr_pr_podsumowanie.php [dostęp 9.05.2014].

[33] *Phishing*- metoda używana do wyłudzenia poufnych informacji od ofiar np. haseł dostępu, danych osobowych przy użyciu podstępu . Najczęściej polega na wysłaniu wiadomości e –mail do potencjalnej ofiary, w której sprawca podszywa się pod instytucję godną zaufania np. bank, której takie poufne dane są szybko potrzebne. http://pl.wikipedia.org/wiki/Phishing [dostęp 9.05.2014].

[34] Redakcja , *Polscy pisherzy oskarżeni,* „Dziennik Internautów”, za: Tejderowski Tomasz, *op. cit*., s.109.

[35] Krawczyk P., *Rekordowy phishing w Polsce- skradziony 1 milion złotych,* „Computer world” 11 maja 2005 za: Tejderowski Tomasz, *op. cit*., s. 109.

[36] Bielska Iwona, *Przestępstwa komputerowe i internetowe. Aspekty kryminologiczne i prawne,* [w:] Grażyna Kędzierska, Wiesław Pływaczewski (red.),*Kryminologia wobec współczesnych wyzwań cywilizacyjnych,* s.163.

[37] Magazyn internetowy na temat pożyczek pozabankowych http://loan-magazine.pl/oferta-pracy-w-domu-moze-skonczyc-sie-wyludzeniem-pozyczki-na-nasze-nazwisko/ [dostęp 9.05.2014];Historia ofiary opublikowana w serwisie poświęconym problemom związanym z sektorem usług http://piekielni.pl/45049#comment_461535 [dostęp 9.05.2014]; Serwis poświęcony zagrożeniom związanym z korzystaniem z nowoczesnych technologii http://niebezpiecznik.pl/post/jak-zostac-slupem-czyli-falszywe-oferty-

bankowe, które jej założył, dokonując autoryzacji danych wykonując przelew z poprzedniego rachunku[38]. Fikcyjnie założone konta mogą być sprzedawane osobom, które chcą na przykład ukryć swoje dochody przed komornikami czy urzędem skarbowym[39].

Kroki, aby zapobiec tego typu oszustwom podjął Związek Banków Polskich i Komisja Nadzoru Finansowego. Związek Banków Polskich zaleca między innymi, aby w bankach oferujących taką usługę wymagano w tytule przelewu jednoznacznej informacji, że przelew dokonuje aktywacji rachunku. Bank powinien również wysyłać przelew zwrotny, informujący o uwierzytelnieniu danych i założeniu konta. Jeden z największych polskich banków zrezygnował z możliwości zakładania rachunku bankowego, przy użyciu przelewu[40]. Komisja Nadzoru Finansowego w związku z procederem wyłudzania danych wystosowała specjalny komunikat, w którym zaleciła obywatelom szczególną ostrożność przy ujawnianiu swoich danych osobowych w internecie[41].

Przy użyciu skradzionej tożsamości oszuści dokonują również zakupów na raty za pośrednictwem sklepów internetowych. Przykładem takiego działania jest postępowanie rodziny N., która oszukała dziewięciu mieszkańców Opola. Sprawcy zdobywali personalia, numer dowodu osobistego, numer PESEL ofiary i wpisywali je w formularzu na stronie sklepu internetowego, w polu „adres" natomiast podawali swoje miejsce zamieszkania. Dokonywali w ten sposób zakupów na kredyt sprzętu elektronicznego i AGD. Zamówione towary trafiały pod ich adres, gdy otrzymywali monity wzywające do spłaty rat za sprzęt wyrzucali je. Ani bank, ani sklep, ani kurier nie zweryfikował danych podanych przez oszustów. Bank jedynie sprawdził czy numery dowodów podane w formularzu na podstawie którego sporządzono umowę nie figurują w bazie dokumentów zastrzeżonych zgodnie ze standardową procedurą. Dokumenty nie znajdowały się w bazie, nie stwierdzono więc przeszkód, aby udzielić kredytu. Dowód osobisty powinien sprawdzić kurier, który dostarczył sprzęt i umowę, najprawdopodobniej tego nie zrobił. Ofiary, o tym że zaciągnięto kredyty na zakup sprzętu posługując się ich danymi, dowiadywały się dopiero gdy komornik zajmował ich konta bankowe[42].

Oszuści działają nie tylko po to aby wyłudzić pieniądze czy towary lub usługi. Przykładem działania sprawcy, którego celem było wyrządzenie ofierze szkody osobistej jest sprawa młodej kobiety z Bielawy, która w 2007 roku, złożyła zawiadomienie na policję o włamaniu się na jej konta poczty e- mail, komunikatorów internetowych, oraz w serwisie aukcyjnym. Sprawca z przejętych kont wysyłał wiadomości o obraźliwej treści oraz ogłoszenia o charakterze erotycznym. Dodatkowo zmienił hasła dostępu do kont co uniemożliwiło ofierze normalne korzystanie z internetu. Po zbadaniu sprawy przez

---

pracy-testera-bankowosci/ [dostęp9.05.2014].

[38] Boczoń Wojciech *Lewych kont "na przelew" mogą być już tysiące,* tekst zamieszczony w serwisie bankier.pl na temat finansów http://www.bankier.pl/wiadomosc/Lewych-kont-na-przelew-moga-byc-juz-tysiace-2781522.html [dostęp 9.05.2014].

[39] Boczoń Wojciech *"Sprzedam anonimowe konto bankowe" - niebezpieczny biznes kwitnie w sieci,* serwis poświęcony usługom finansowym http://prnews.pl/hydepark/quotsprzedam-anonimowe-konto-bankowequot-niebezpieczny-biznes-kwitnie-w-sieci-6548579 [dostęp 9.05.2014].

[40] Artykuł w serwisie internetowym na temat finansów http://prnews.pl/hydepark/pko-bp-rezygnuje-z-kont-otwieranych-przelewem-zbp-ostrzega-inne-banki-3062428.html [dostęp 9.05.2014].

[41] *Komunikat w sprawie „phishingu" danych,* Komisja Nadzoru Finansowego, 13 listopada 2013.

[42] Żbikowska Izabela *Liczy się znaleźć jelenia,* 28.08.2013 strona internetowa Gazety Wyborczej http://wyborcza.pl/1,87648,14504996,Liczy_sie_znalezc_jelenia.html?as=1 [dostęp 9.05.2014]. oraz Żbikowska Izabela *Jak łatwo wrobić w kredyt* 28.08.2013 strona internetowa Gazety Wyborczej http://wyborcza.pl/1,76842,14505530,Jak_latwo_wrobic_w_kredyt.html [dostęp 9.05.2014].

policjantów z sekcji do walki z przestępczością gospodarczą okazało się, że sprawcami są dwie osoby: były chłopak ofiary i jego nowa partnerka. Przedstawiono im zarzuty utrudniania, niszczenia i zmiany dostępu do danych teleinformatycznych[43].

Wraz z rosnącą popularnością portali społecznościowych aktywność cyberprzestępców przeniosła się również tam. Uzyskanie danych osobowych jest dużo łatwiejsze, niż poprzez wysyłanie e-maili i tworzenie oszukańczych stron internetowych. Często nawet same ofiary upubliczniają wrażliwe dane.

Znając jedynie imię i nazwisko oraz miejsce zamieszkania potencjalnej ofiary, cyberprzestępca może uzyskać dostęp m. in. do jej zdjęć, informacji na temat jej wieku, miejsca pracy, przebiegu edukacji, poznać stan cywilny, a nawet numer telefonu. Dodatkowo analizując powiązania z innymi członkami portalu może określić na przykład czy dana osoba ma dzieci, gdzie wyjeżdża na wakacje, w jakich godzinach korzysta z internetu, jakie formy aktywności w czasie wolnym preferuje, jakie są jej upodobania muzyczne[44]. Tak zwane „ustawienia prywatności", czy też regulaminy korzystania z usług danego portalu są napisane językiem niezrozumiałym dla wielu użytkowników oraz często modyfikowane. Bardziej świadomi użytkownicy serwisów społecznościowych ukrywają poufne informacje na swój temat.

Obecnie portale społecznościowe służą również do rozprzestrzeniania szkodliwego oprogramowania. Przykładem takiego działania może być wirus koobface. Robak ten, rozsyłał użytkownikom facebooka prywatne wiadomości z zainfekowanych kont znajomych, w których informował o pojawieniu się nowego zdjęcia czy filmu na którym rzekomo znajdował się adresat wiadomości. Gdy kliknął on w zawarty w wiadomości odsyłacz do zdjęcia czy filmu, został poproszony o zaktualizowanie oprogramowania czy też instalację odpowiedniej wtyczki, aby wyświetlić udostępniony materiał. W rzeczywistości, aktualizacja oprogramowania to wirus. Komputer użytkownika zostaje zainfekowany i może być kontrolowany przez hakera. Zainfekowane komputery tworzą botnet, czyli sieć komputerów wykorzystywanych do wysyłania spamu lub atakowania serwerów. Powoduje to dalsze rozprzestrzenianie wirusów, o czym użytkownicy zainfekowanych kont często nie wiedzą. Nie są świadomi tego, że z ich konta wysyłany jest spam[45].

W 2013 roku pojawiła się kolejna fala ataków scamowych na popularnym w Polsce portalu społecznościowym. Scam jest to oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych[46]. Na portalu pojawia się szokująca informacja na przykład: „Tragiczny wypadek w centrum, dwie osoby nie żyją. 2013.09.20" aby spotęgować ciekawość potencjalnego odbiorcy informacja jest udostępniana przez kogoś ze znajomych użytkownika, z dodatkowym podpisem sugerującym, że wydarzenie miało miejsce w miejscowości, w której mieszka ów znajomy. Po kliknięciu w hiperłącze, ofiara zostaje przekierowana na fałszywą stronę internetową na przykład

[43] *IX Seminarium Naukowe Przestępczość teleinformatyczna Materiały poseminaryjne*, red. Kosiński Jerzy, Szafrański Jerzy ,Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2008, s. 272.

[44] Tejderowski Tomasz, *op. cit.,* s.149-150.

[45] Strony internetowe na temat bezpieczeństwa w sieci http://securelist.pl/analysis/6008,poradnik_bezpieczenstwa_dla_dzieci_i_rodzicow_portale_spolecznosciowe.html [dostęp: 24.11.2013]. oraz http://niebezpiecznik.pl/post/uwaga-wirus-na-facebooku/ [dostęp: 24.11.2013].

[46] Encyklopedia internetowa http://pl.wikipedia.org/wiki/Scam [dostęp: 24.11.2013].

wladomoscl.pl zamiast wiadomosci.pl. Strona nie służy oczywiście celom informacyjnym. Żadne zdjęcia, ani filmy nie wyświetlają się prawidłowo. Użytkownik jest proszony o podanie swego numeru telefonu oraz nazwy miejscowości w której mieszka, rzekomo w celu weryfikacji danych, bądź akceptacji polityki prywatności serwisu. W rzeczywistości zapisuje się na subskrypcję płatnych smsów, o czym jest informowany małym drukiem, w kolorze zbliżonym do barwy tła strony[47].

Poza oszustwami, których celem jest wyłudzenie od ofiar pieniędzy lub zdobycie poufnych informacji coraz częściej dochodzi do przejmowania kont ofiar na portalach społecznościowych lub tworzenia fikcyjnych kont istniejących osób i publikowania treści w ich imieniu[48].

W 2008 roku oszust złapany przez policjantów z wydziału przestępczości gospodarczej w Opolu, założył fikcyjny profil piosenkarki i aktorki Marii Peszek na portalu społecznościowym nasza-klasa.pl. Aby uwiarygodnić profil na bieżąco aktualizował zamieszczane informacje. Udostępniał zdjęcia i wywiady artystki. Pewnego dnia zamieścił list-apel, w którym to piosenkarka rzekomo zwraca się z prośbą do swoich fanów o wsparcie finansowe dla ciężko chorego chłopca. We wpisie podał numer konta na które należało dokonywać wpłat. Policjanci dzięki współpracy z administracją portalu ustalili, że twórcą fikcyjnego konta był dwudziestotrzyletni student jednej z opolskich uczelni [49].

Przestępcy wykorzystywali również mechanizm spoofing sms- umożliwiający zmianę numeru nadawcy wiadomości tekstowej za pomocą bramki sms. Jeżeli ofiara posiadała konto w serwisie społecznościowym połączone z jej numerem telefonu, a sprawca znał ten numer i wysłał wiadomość na numer dostępowy portalu za pomocą bramki sms umożliwiającej zmianę numeru nadawcy, to treść wiadomości została opublikowana w imieniu ofiary[50].

Wymienione przykłady oszustw na portalach społecznościowych z pewnością nie wyczerpują tematu kradzieży tożsamości – z wykorzystaniem tego coraz popularniejszego miejsca aktywności internautów. Serwery portali społecznościowych są coraz częstszym celem ataków cyberprzestępców[51].

Nowym problemem związanym z kradzieżą tożsamości w Internecie jest problem podszywania się pod osoby posługujące się w Internecie pseudonimami, na przykład bloggerów. W 2013 roku, oszustka podszywająca się pod bloggerkę posługującą się pseudonimem Odette Swan, wyłudzała produkty od firm kosmetycznych i ubrania. Założyła konto e-mail odetteswan@wp.pl, przy jego rejestracji posłużyła prawdziwym imieniem i nazwiskiem osoby, pod którą się podszywała. Ponadto, założyła konto na portalu społecznościowym, z którego to również kontaktowała się z firmami, od których chciała wyłudzić produkty[52].

---

[47] Serwis poświęcony zagrożeniom związanym z korzystaniem z nowoczesnych technologii http://niebezpiecznik.pl/post/uwaga-na-kolejny-scam-na-facebooku-tragiczny-wypadek-w-centrum-dwie-osoby-nie-zyja/ [dostęp: 24.11.2013].

[48] Reznik, Maksim, *op. cit.* s. 3.

[49] *IX Seminarium Naukowe Przestępczość teleinformatyczna Materiały poseminaryjne*, red. J. Kosiński, J. Szafrański, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2008, s. 264-265.

[50] Serwis poświęcony zagrożeniom związanym z korzystaniem z nowoczesnych technologii http://niebezpiecznik.pl/post/spoofing-sms-czyli-falszowanie-nadawcy-sms-a/ [dostęp 9.05.2014].

[51] Strona dla przedsiębiorców na temat internetu http://www.egospodarka.pl/43549,Ataki-na-portale-spolecznosciowe-czestsze,1,12,1.html [dostęp: 24.11.2013].

[52] Blog poświęcony oszustwom w sieci http://aferkowo-male.blogspot.com/2013/07/kradziez-tozsamosci-oszustwo-i-wyudzenia.html [dostęp 9.05.2014].

Opisane przeze mnie przypadki i mechanizmy kradzieży tożsamości w Polsce stanowią jedynie wstęp do poznania metod działania sprawców. Zjawisko kradzieży tożsamości wymaga dalszych badań, chociażby dlatego, aby zwiększyć wiedzę społeczeństwa na jego temat czy umożliwić pomoc ofiarom. Dogłębne poznanie zjawiska wymaga interdyscyplinarnej wiedzy z zakresu: prawa, ekonomii, informatyki i kryminologii. Wraz z postępem technicznym dane osobowe stają się niezwykle cennym dobrem.