Potrzeby i możliwości badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon

Mgr Ewa Gidel-Stefaniec – KA im. A. F. Modrzewskiego w Krakowie

Ur. 09 sierpnia 1989 roku w Jędrzejowie. W 2007 – 2012 studia prawnicze na Katolickim Uniwersytecie Lubelskim im. Jana Pawła II w Lublinie, WZPiNoG w Stalowej Woli. Obecnie seminarzystka seminarium doktorskiego z prawa na Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. W 2012-2013 studia podyplomowe z Kryminalistyki na Wyższej Szkole Ekonomii i Prawa im. prof. Edwarda Lipińskiego w Kielcach, 2013 - kurs pedagogiczny dla czynnych zawodowo nauczycieli. Swoje zainteresowania z kryminalistyki rozwija poprzez systematyczny udział w seminariach i konferencjach naukowych.

WPROWADZENIE

Obecny postęp rozwoju bankowości telefonicznej w Polsce jest oparty na dostępnych zaawansowanych urządzeniach telefonicznych, które łączą zwykłe funkcje telefonu z wieloma innymi funkcjami, w tym usługi finansowe. Telefon komórkowy coraz częściej wykorzystywany do identyfikacji właściciela. Pojawiły sie usługi pozwalające regulować płatności za pomocą telefonu[1]. Bankowość komórkowa to jeden z elementów współczesnej bankowości elektronicznej. Jest to usługa, która „polega na wykorzystaniu telefonu do obustronnej komunikacji klienta z bankiem, wykorzystująca telefony komórkowe oraz inne urządzenia przenośne”[2]. W bankowości komórkowej wykorzystywane są systemy SIM Toolkit. SIM Toolkit (Subscriber Identity Module Application Toolkit) jest „technologią, umożliwiającą wykonywanie operacji bankowych poprzez zainstalowanie na standardowej karcie SIM telefonu komórkowego specjalnie przygotowanej aplikacji bankowej przesyłanej drogą bezprzewodową”[3]. Coraz popularniejsze stają się też płatności zbliżeniowe. Operatorzy T-Mobile i Orange wprowadzili do swojej oferty telefony, które pozwalają na dokonywanie płatności zbliżeniowych oraz transferu pieniędzy pomiędzy telefonami. Te możliwości sprawiają, że pojawiło się zjawisko zdalnego okradania użytkownika płatności telefonicznych. Artykuł ma na celu zbadanie potrzeb i możliwości badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon w kryminalistyce.

I. ISTOTA PRZESTĘPSTW W PŁATNOŚCIACH ELEKTRONICZNYCH PRZEZ TELEFON/SMARTFON

Rozwiązania techniczne w bankowości komórkowej bazują na szerokiej współpracy banków z operatorami sieci komór-

[1] Z. Jakubowski, *Wybrane aspekty ochrony tożsamości elektronicznej*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 60.

[2] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010, s. 38.

[3] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości* …, dz. cyt., s. 42.

kowych, a dostarczona przez bank aplikacja umożliwia realizację różnych zleceń bankowych. Warunkiem korzystania z tego typu usługi jest „posiadanie tzw. inteligentnych telefonów (smartphonów), w tym urządzenia działające pod kontrolą systemów Symbian, Windows CE, Android i iPhone OS”[4].

Usługa obejmuje liczne produkty bankowe, w których kontakt banku z klientem następuje za pomocą tzw. smartphonów. Smartphony to urządzenia wielofunkcyjne, łączące funkcje zwykłego telefonu komórkowego (wykonywanie połączeń, SMS) z minikomputerem. Aplikacje do smartphonów są bardzo zaawansowane i opierają się o zaawansowane systemy operacyjne i aplikacje. Banki od lat dają możliwość korzystania klientom z usług bankowości telefonicznej. Stworzyły aplikacje na smartphony, które umożliwiają dokonywanie standardowych usług i operacji płatniczych takich jak:[5]

– informacje ogólne - stan rachunku, przelewy, pytanie o limity kredytowe,
– prowadzenie transakcji - przelewy, zlecenia stałe, zamawianie czeków,
– pytania o specjalistyczne informacje o produktach - warunki zawierania transakcji,
– składanie wniosków kredytowych i otwieranie lokat pieniężnych,
– funkcje płatnicze – wirtualne karty oraz płatności zbliżeniowe.

Procedura zawarcia transakcji bankowych poprzez platformy elektroniczne jest dość szczegółowo określona. Jednak można wskazać na kilka dróg, kiedy to może dojść do działań przestępczych. Może to być:[6]

1. kradzież telefonu poprzez przywłaszczenie (art. 278 k.k.)[7], w tym rzeczy będące współwłasnością. Sprawca dokonuje zaboru po to, aby włączyć cudzą rzecz do swojego majątku i postępować z nią jak właściciel (tzn. zużywając, darowując, sprzedając itp.). Pozbawienie pokrzywdzonego władztwa nad telefonem może posłużyć do podjęcia pieniędzy z rachunku pokrzywdzonego, czy to wirtualnego (skarbonka, mobilny portfel NCF), co może stanowić odrębne przestępstwo.
2. kradzież z włamaniem stanowi kwalifikowany typ wszystkich odmian kradzieży określonych w art. 278 k.k. - ma miejsce wtedy, gdy:
   – jej sprawca zabiera mienie w celu przywłaszczenia w następstwie usunięcia przeszkody materialnej, będącej częścią konstrukcji pomieszczenia zamkniętego lub specjalnym zamknięciem tego pomieszczenia utrudniającym dostęp do jego wnętrza,[8].

[4] E. Gidel-Stefaniec, *Zagrożenia przestępstwem w płatnościach elektronicznych przez telefon/smartfon*, Wydawnictwo Wyższej Szkoły Handlowej, Kielce 2013, tom 1, s. 163.

[5] Wojciechowska-Filipek S., *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, s. 53.

[6] Zob. E. Gidel-Stefaniec, *Zagrożenia przestępstwem w płatnościach elektronicznych przez telefon/smartfon*, Wydawnictwo Wyższej Szkoły Handlowej, Kielce 2013, tom 1, s. 163-168; J.W. Wójcik, Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne, Wydawnictwo JWW, Warszawa 2008, s. 381.

[7] Por. Pływaczewski E., Guzik - Makaruk E., *Przestępstwa przeciwko mieniu,* [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Lexis Nexis, Warszawa 2012, s. 1164-1165; M. Szwarczyk, A. Michalska-Warias, T. Bojarski, J. Piórkowska-Flieger, *Kodeks karny. Komentarz*, Lexis Nexis, Warszawa 2012, s. 742.

[8] Wytyczne wymiaru sprawiedliwości i praktyki sądowej SN z 25 czerwca 1980 r. w sprawie odpowiedzialności karnej za przestępstwa określone w art. 208, VII KZP 48/78, Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa 1980, nr 8, poz. 65.

– sposób pokonania przeszkody materialnej, broniącej dostępu do mienia, jest obojętny dla bytu tego przestępstwa,[9]
– pokonanie, przez zniszczenie (uszkodzenie) przeszkody w postaci ogrodzenia zabezpieczającego mienie, dokonane w celu zaboru cudzego mienia,[10]

3. kradzież w wyniku rozboju (art. 280 k.k.), używając przemocy, grożąc natychmiastowym użyciem takiej przemocy albo doprowadzając człowieka do stanu nieprzytomności lub bezbronności[11].
4. kradzież rozbójnicza (281 k.k.) - polega na dokonaniu kradzieży z zastosowaniem przemocy bądź jej groźby w celu utrzymania się w posiadaniu zabranej rzeczy[12].
5. wprowadzenie nielegalnego oprogramowania na telefon, który przechwytuje dane o transakcjach, loginie, haśle i innych danych na różnych etapach dokonywania transakcji – wirusa[13]. Jest to oszustwo (art. 286 § 1 k.k.), które polega na osiągnięciu korzyści majątkowej, doprowadzania innej osoby do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania[14].
6. złamanie zabezpieczeń transferu danych, dzięki czemu można dowolnie manipulować danymi. Jest to oszustwo komputerowe (art. 287 k.k.), czyli działanie w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, które wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwanie albo wprowadzanie nowych zapisów danych informatycznych[15].

II. SKALA PROBLEMU

Co chwilę w prasie i telewizji przestrzega się przed grupami przestępczymi, które tworzą i rozpowszechniają oprogramowanie, które przechwytuje loginy i hasła do internetowych kont bankowych. Wskazuje się, że obecne rozwiązania, np. mobilny portfel NCF oraz tzw. mikropłatnosci, mogą być dokonywane przez przestępców mogą po-

[9] Wyrok z 15 sierpnia 1986 r., I KR 212/85, OSNKW 1986, nr 11-12, poz. 97.

[10] Postanowienie SN z 24 czerwca 2010 r., V KK 388/09, Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa 2010, nr 9, poz. 82.

[11] Zob. E. Pływaczewski, E. Guzik - Makaruk, *Przestępstwa przeciwko mieniu*, dz. cyt., s. 1167, Wyrok SN z 12 stycznia 2011 r., III KK 230/10, Biuletyn Prawa Karnego 2011, nr 6, poz. 9. Wyrok SA w Białymstoku z 17 stycznia 1995 r., II AKr 207/94, Orzecznictwo Sądów Apelacji Białostockiej 1995, nr 1, poz. 10.

[12] Zob. M. Szwarczyk, A. Michalska-Warias, T. Bojarski, J. Piórkowska-Flieger, *Kodeks karny. Komentarz*, dz. cyt., s. 748; A. Marek, *Kodeks karny*, Wolters Kluwer, Warszawa 2010, s. 509.

[13] Zob. *Trojan CITADEL atakuje PC – Trojan ZITMO infekuje telefony komórkowe*, Rada Bankowości Elektronicznej, Związek Banków Polskich http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci [2.11.2013]

[14] Zob. Wyrok SA w Katowicach z 17 sierpnia 2000 r., II AKa 168/00, Orzecznictwo Sądów Apelacyjnych 2001, nr 7-8, poz. 51, s. 53; Wyrok SN z 29 marca 2011 r., III KK 321/10, Biuletyn Prawa Karnego 2011, nr 9. E. Pływaczewski, E. Guzik - Makaruk, *Przestępstwa przeciwko mieniu,* dz. cyt., s. 1172. J. Skorupka, *Wady oświadczenia woli w wybranych przestępstwach gospodarczych*, Przegląd Sądowy 2000, nr 4, s. 38

[15] Zob. M. Szwarczyk, A. Michalska-Warias, Bojarski T., Piórkowska-Flieger J., *Kodeks karny. Komentarz*, dz. cyt., s. 764, Kardas P., *Oszustwo* komputerowe w kodeksie karnym, Przegląd Sądowy 2000, nr 11 – 12, s. 43; A. Marek, Kodeks karny, dz. cyt., s. 519; M. Kalitowski, *Przestępstwa przeciwko ochronie informacji* [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Lexis Nexis, Warszawa 2012, s. 1141.

Table I. The number and the shift of crimes related to mobile phones. (Liczba i zmiana przestępstw dotyczących telefonów komórkowych)

Years (Lata)	Stealing some else's property (Kradzież cudzej rzeczy)	Burglary (Kradzież z włamaniem)	Robbery (Przestępstwa rozbójnicze)	Fraud (Oszustwo)	Total (Ogółem)
	liczba wykrytych przestępstw				
2005	53 110	6 394	15 809	5 522	87 124
2006	46 012	4 315	12 581	5 148	75 097
2007	37 314	3 076	9 187	5 394	62 363
2008	32 303	2 554	8 149	4 600	55 931
2009	29 133	2 543	6 986	5 198	52 569
2010	26 172	2 215	5 657	5 906	49 304
2011	23 553	1 946	4 688	6 761	46 257
2012	24 643	1 699	4 116	5 677	46 585
2012:2008 shift Zmiana 2012:2008	**-23,7**	**-33,5**	**-49,5**	**23,4**	**-16,7**
2012:2005 shift Zmiana 2012:2005	**-53,6**	**-73,4**	**-74,0**	**2,8**	**-46,5**

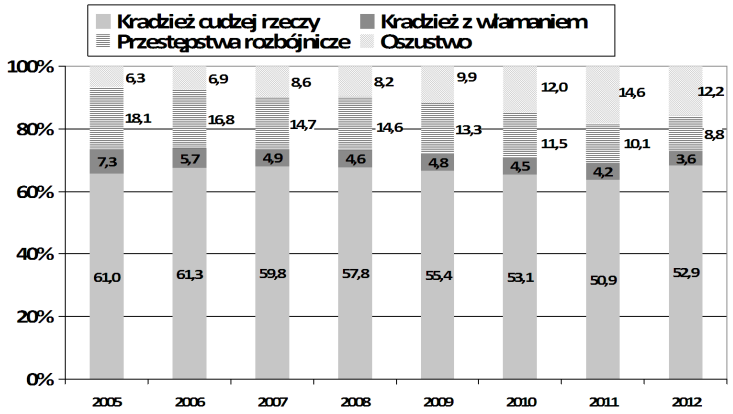
Źródło: opracowanie własne na podstawie: Przestępstwa dotyczące telefonów komórkowych, http://statystyka.policja.pl/st/informacje/87763,Przestepstwa-dotyczace-telefonow-komorkowych.html [10.11.2013]

wodować duże szkody. Transakcje są małe, jednak ich dokonywanie na dużą skalę może zachwiać bezpieczeństwem i wiarygodnością współczesnych systemów płatności.

Obecne dane Policji wskazują na określone przestępstwa związane z przejęciem i oszustwem (tabela I).

Dane wskazują, że ogólna liczba przestępstw dotyczących telefonów komórkowych spadła od 2005 roku o blisko połowę (o 46,5%), a kradzieże z włamaniem i przestępstwa rozbójnicze obniżyły się o około 74%. Jednak od 2008 roku rośnie liczba oszustw (o 23,4%).

Figure 1. The structure of the mobile phones related crimes. (Struktura przestępstw dotyczących telefonów komórkowych)



Źródło: opracowanie własne na podstawie: Przestępstwa dotyczące telefonów komórkowych, http://statystyka.policja.pl/st/informacje/87763,Przestepstwa-dotyczace-telefonow-komorkowych.html [10.11.2013]

Przestępstwa oszustwa (rys. 1) podwoiły swój udział w ogóle przestępstw dotyczących telefonów komórkowych. W tej grupie należy upatrywać czynów, związanych z przestępstwami w płatnościach elektronicznych przez telefon/smartphon. Jednak nie ma oficjalnych statystyk w tym zakresie. Jednak zarówno w prasie krajowej jak i zagranicznej wskazuje się na występowanie problemu kradzieży danych ze smartphonów. Doniesienia te wskazują na elektroniczne kradzieże kieszonkowe, gdzie przestępca z czytnikiem kart lub smartphonem może odczytać informacje na temat kart zbliżeniowych i popełnienia oszustwa[16]. W polskiej telewizji TVN pokazał na przykładzie eksperymentu, że karty płatnicze można skanować za pomocą telefonu. Karta z funkcją PayPass (Mastercard) bądź payWave (Visa) jest bardzo wygodnym sposobem na transakcje do 50 zł, ale również niebezpiecznym. Okazuje się bowiem, że istnieje możliwość zeskanowania takiej karty kredytowej bądź płatniczej za pomocą smartfona, którym potem można dokonać płatności w tej samej technologii. Wystarczy odpowiednia aplikacja na system operacyjny smartphonu, aby przybliżając urządzenie do karty kredytowej czy płatniczej wyposażonej w odpowiedni chip, pozyskać dane potrzebne do tego, aby płacić na konto osoby okradzionej[17]. Oficjalnie MSW oraz Komenda Główna Policji twierdzą, że do tej pory nie było żadnych zgłoszeń dotyczących kradzieży danych z kart płatniczych poprzez wykorzystanie telefonów komórkowych. Jednak problem skanowania kart jest znany od kilku lat[18], ale nie pozostaje bez echa - zarówno w środowisku ludzi projektujących technologie po stronie organizacji kart płatniczych, jak również po drugiej stronie, czyli tych, którzy próbują przełamać te zabezpieczenia. Mimo zaawansowanej technologii zabezpieczającej obecnie pozyskanie danych z kart czy innych spartphonów nie jest zbyt dużym problemem. Wydaje się, że problem jest mały, gdyż transakcje wymagające użycia telefonu czy płacenia cudzą kartą bezstykową nie są zbyt popularne[19].

III. POTRZEBY BADANIA ŚLADÓW PRZESTĘPSTW W PŁATNOŚCIACH ELEKTRONICZNYCH PRZEZ TELEFON/ SMARTPHON

Potrzeby badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon wynikają z dwóch zasadniczych przesłanek. Jedna wynika z potrzeby nadążania za aktywnością przestępców. Już teraz w literaturze kryminalistycznej wskazuje się na zaniedbania tzw. „nowinek kryminalistycznych" należących do zakresu pokrewnych nauk sądowych. H. Kołecki podkreśla, że cały czas zaniedbuje się wciąż nierozwiązane lub kontrowersyjne (i wymagające od lat dalszych badań) zagadnienia z zakresu klasycznej problematyki kryminalistycznej oraz całkowicie pomija się (lub podejmuje się rzadko) nowe problemy, zagadnienia

[16] *Should I be concerned about security of contactless payment cards?* http://www.cba.ca/en/consumer-information/42-safeguarding-your-money/622-contactless-payment-card-security-an-faq[10.11.2013]

[17] *Złodzieje mogą skanować dane telefonem* , http://www.tvn24.pl/wiadomosci-z-kraju,3/niebezpieczne-karty-zblizeniowe-zlodzieje-moga-skanowac-dane-telefonem,364859.html [10.11.2013]

[18] Por. niebezpiecznik.pl [10.11.2013]

[19] *Złodzieje mogą skanować dane telefonem* , http://www.tvn24.pl/wiadomosci-z-kraju,3/niebezpieczne-karty-zblizeniowe-zlodzieje-moga-skanowac-dane-telefonem,364859.html [10.11.2013]

czy kwestie stwarzane przez nową „rzeczywistość przestępczą”[20].

Zagadnienie potrzeb badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon jest konieczne w kontekście ustalenia całego mechanizmu przestępstwa (taktyki popełniania przestępstw gospodarczych - ujęcie od strony sprawcy), czy taktyki zwalczania (przeciwdziałania) przestępstw gospodarczych (ujęcie od strony organów ścigania). Ponadto konieczne jest wskazanie środków technicznych stosowanych przez sprawców przy popełnianiu przestępstw gospodarczych oraz przez organy ścigania przy zwalczaniu przestępstw gospodarczych.

Druga kwestia potrzeby badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon dotyczy wzmacniania wiedzy an temat efektywnosci systemów uwierzytelniania użytkowników. Aby informacja mogła zostać wykorzystana w procesach biznesowych, musi posiadać kilka podstawowych cech, takich jak: autentyczność, integralność i poufność. Brak którejkolwiek z tych cech powoduje, że informacja nie może być wykorzystana do prowadzenia działań biznesowych[21].

Z kwestią uwierzytelniania wiąże się też problem kreowania tożsamości w celu dokonywania przestępstw i prania pieniędzy poprzez systemy płatności. W przypadku korzystania z poczty elektronicznej, usług płatniczych, forum, korzysta się w telefonach, podobnie, jak w komputerach, z formularzy rejestracyjnych. Podczas wypełniania takiego formularza rejestracyjnego powstaje zapis, który może być odwzorowaniem wykreowanej tożsamości i może nie mieć żadnej przydatności dla organów ścigania ze względu na niemającą odwzorowania w rzeczywistości tożsamość. Podczas kreowania tożsamości w ramach rejestracji, podaje się imię, nazwisko, adres zamieszkania, wiek, numer telefonu, zainteresowania, adres poczty elektronicznej, kraj pochodzenia. Po wypełnieniu pól wskazanymi danymi kreujemy naszą tożsamość, która zaczyna „istnieć” w Internecie. Jednak dane, które ją tworzą, nie są prawdziwe lub są skradzione np. z innego telefonu. Obecnie rozwijają się metody działania sprawców, sposoby organizowania grup zajmujących się pozyskiwaniem i transferem pieniędzy. Przestępcy nie tylko kreują tożsamości, ale przy okazji przejmowania telefonów uzyskują często hasła dostępowe do kont e-mail, kont bankowych, kont w usługach płatniczych czy kont na portalach aukcyjnych, dokonując tym samym kradzieży tożsamości wykreowanych przez właścicieli przejętych komputerów[22].

IV. MOŻLIWOŚCI BADANIA ŚLADÓW PRZESTĘPSTW W PŁATNOŚCIACH ELEKTRONICZNYCH PRZEZ TELEFON/ SMARTPHON

W praktyce kryminalistycznej w Polsce brakuje procedur badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon. Na pierwsze

[20] H. Kołecki, *Niektóre zaniedbane obszary badawcze współczesnej kryminalistyki w Polsce*, [w:] T. Widła (red.), *Obszary badawcze współczesnej kryminalistyki*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2011, s. 63.

[21] Z. Jakubowski, *Wybrane aspekty ochrony tożsamości elektronicznej*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 51.

[22] K. Zawadzki, *Kreowanie tożsamości w celu dokonywania przestępstw i prania pieniędzy poprzez systemy płatności w Internecie*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 266.

zagrożenia związane z używaniem telefonów komórkowych wskazywano w publikacjach zagranicznych[23], jednak nie dotyczyły one przestępstw w płatnościach elektronicznych przez telefon/smartphon. Do tej pory nie wypracowano jednolitego standardu w tym zakresie. jednak technologia współczesnych smartphonów ma swoje odzwierciedlenie w rozwoju komputerów. Miniaturyzacja sprawiła, że powstały najpierw przenośne komputery a potem telefony wyposażono w pamięci, kamery, wi-fi. Stworzono też oprogramowanie, która pozwala na szerokie wykorzystanie telefonów zarówno do pracy, rozrywki jak i realizacji np. płatności.

Centralne Labolatorium Kryminalistyczne posiada specjalne jednostki zajmujące się ujawnianiem śladów przestępstw komputerowych. Mimo pewnych podobieństw do spartphonów jednak nie wypracowano odrębnych procedur i metod badania pod kątem przestępstw w płatnościach elektronicznych przez telefon/smartphon.

Można jednak niektóre techniki dotyczące ujawniania śladów w komputerach przenieść do ujawniania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon. Jednak aby zastosować określone techniki trzeba znać techniczne ograniczenia popełnienia przestępstwa kradzieży danych z telefonu i oszustwa.

Płatności bezstykowe są osadzone w wielu warstw bezpieczeństwa. Te funkcje zabezpieczeń obejmują:[24]

– Krótki zasięg - karty bezstykowe mogą działać tylko blisko detalicznego terminala, który utrudnia przestępcom dostęp do informacji z daleka.
– Szyfrowanie - podczas transakcji telefon i terminal porozumiewają się ze sobą, wykonują kontrolę bezpieczeństwa i przekazują unikalny kod szyfrowania, który wygasa po zakończeniu transakcji. Jeśli ktoś był w stanie uzyskać dane z karty czy telefonu, nie będzie w stanie wykorzystać uzyskanego kodu szyfrowania wielokrotnie, ponieważ po dokonaniu transakcji wygasły.
– Ograniczone informacje - informacje przekazywane podczas bezdotykowej transakcji są bardzo ograniczone i obejmują takie rzeczy jak preferencje języka, numer karty i kodowanie. Inne dane, jak nazwa klienta, numer konta bankowego i trzycyfrowy kod bezpieczeństwa nie są przesyłane podczas transakcji bezstykowych.
– Niskie limity transakcyjne - karty bezstykowe na ogół mają niskie limity transakcyjne - zwykle około 50 zł - i każdy większy zakup będzie wymagać podania kodu PIN. Jeśli telefon został ukradziony lub przechwycone dane, zapobiega to dużym zakupom.
– Zero odpowiedzialności - Visa, MasterCard i Interac w swojej polityce nie ponoszą odpowiedzialności dla posiadaczy debetowych, kredytowych i kart. W przypadku nadużyć finansowych, nie ponoszą one odpowiedzialności i poszkodowana osoba nie może otrzymać zwrotu pieniędzy.

[23] Zob. A.M. Marshall, B.C. Tompsett, *Silicon Pathology*?, Science & Justice, Volume 44, Issue 1, January 2004, s 43-50; E. Philips, *Mobile phone – friend or foe*? Science & Justice, Volume 42, Issue 4, October 2002, s. 225-229.

[24] *Should I be concerned about security of contactless payment cards*? http://www.cba.ca/en/consumer-information/42-safeguarding-your-money/622-contactless-payment-card-security-an-faq [10.11.2013]

Jednak telefony służą też do dokonywania następujących operacji bankowych:[25]

– wypłat z bankomatu bez karty (procedura: uruchomienie aplikacji → generowanie kodu → wpisanie kodu w bankomacie → wypłata),
– płatność kartą bez użycia terminala (procedura: podanie karty sprzedawcy → sprzedawca skanuje kartę przez smartfon → podpis na ekranie telefonu → transakcja zapłacona),
– przelewy pomiędzy telefonami (procedura: uruchomienie aplikacji na dwóch urządzeniach → połączenie telefonów, np. przez Wi-Fi → wpisanie kwoty → realizacja, np. przez stuknięcie <oferta CITI HANDLOWY> → przelew zrealizowany),
– mobilny portfel NCF, który umożliwia realizację płatności przez kilka wirtualnych kart (procedura: wybranie karty na urządzeniu → przyłożenie karty do czytnika → zapłacone),
– zapłata za rachunki bez wpisywania danych (procedura: uruchomienie aplikacji → zeskanowanie kodu lub zrobienie zdjęcia → weryfikacja danych → zatwierdzenie → transakcja wykonana).

Można wskazać na pewne procedury postępowania z dowodami elektronicznymi, zgodne z zasadami informatyki śledczej. Wymagają one od organów ścigania właściwego poszukiwania, rozpoznania i ochrony dowodów pochodzących z urządzeń elektronicznych, w tym smartphonów, zgodnie z obowiązującymi przepisami prawnymi, dobrymi praktykami i innymi wytycznymi. Stosowane techniki muszą być dopasowane do technologii zastosowanej w danym telefonie. Właściwe przygotowanie powinno, już na etapie rozpoznania, zakładać znajomość odpowiedzi na poniższe pytania:[26]

– Czy jest sens zabezpieczania (analizy) telefonów/smartphonów?
– Czy zamiast telefonów wystarczy zabezpieczyć dane?

Metody badania telefonów, które posłużyły do kradzieży danych lub zostały skradzione i wykorzystano je do oszustwa można podzielić na dwie grupy.

Pierwsza bada same urządzenie lub urządzenia. Szczególne znaczenia ma to w przypadku, gdy są przedmiotem wykonawczym przestępstwa. Najbardziej właściwe postępowanie to:[27]

– opisz lub sfotografuj wszystkie informacje z wyświetlacza,
– następnie odłącz od źródła zasilania, odłącz kable z urządzenia,
– odłącz zasilanie przed transportem, zabierz ładowarkę, jeśli jest dostępna.
– zidentyfikuj i zabezpiecz nośniki (karty pamięci) przez zmianę pozycji przełącznika zapisu w pozycję „locked", w celu zabezpieczenia przed przypadkowym nadpisaniem.
– pamiętaj, że w niektórych modelach opóźnienia w przeprowadzaniu ekspertyzy mogą skutkować utratą informacji z powodu rozładowania baterii,
– wraz z urządzeniem zabezpiecz wszelkie instrukcje odnoszące się do niego wraz z kablami zasilającymi i innymi urządzeniami powiązanymi[28].

[25] Por. *Polska bankowość mobilna - infografika przygotowana przez Organizatorów plebiscytu Złoty Bankier*, http://www.payu.pl/aktualnosci/polska-bankowosc-mobilna-infografika-przygotowana-przez-organizatorow-plebiscytu-zloty [2.07.2013]

[26] P. Krejza, *Najlepsze praktyki zabezpieczania elektronicznego materiału dowodowego,* w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 133.

[27] P. Krejza, *Najlepsze praktyki* …, dz. cyt., s. 137.

[28] P. Krejza, *Najlepsze praktyki* …, dz. cyt., s. 138.

– jeśli urządzenie jest wyłączone, nie włączaj go, gdyż włączenie urządzenia zmienia zapisane w nim informacje,, a opóźnienie w przeprowadzeniu ekspertyzy może skutkować utratą informacji;
– wyłączenie może powodować konieczność ustalenia PUK od operatora,
– włączony telefon nadal odbiera połączenia i wiadomości SMS (może to powodować nadpisanie skasowanych informacji),
– jeśli bateria zostanie wyczerpana postaraj się o zapewnienie zasilania,
– aby przeanalizować dane z telefonu, niezbędne mogą być kody PIN łub PUK. Jeśli nie uzyskano ich od podejrzanego, można zwrócić się do dostawcy usług. Może on zostać zidentyfikowany poprzez numer ICC wydrukowany na karcie SIM.
– zapakuj telefon co najmniej w folię ochronną, a najlepiej do kartonika z etykietą „ostrożnie".

Oprócz powyższych procedur mogą mieć zastosowanie metody daktyloskopijne, badania DNA czy zapachów, które pozostawili przestępcy.

Druga analizuje dane zawarte w telefonie i innych urządzeniach, które zanotowały transakcje płatnicze. Podstawą jest tu zabezpieczenie dowodów. Moment zabezpieczania dowodów elektronicznych opiera się na problemie uwierzytelnienia w sposób niepozostawiający wątpliwości, że zostały one uzyskane z danego urządzenia, w określonym miejscu i czasie. W zależności od sprawy, może to wymagać różnego podejścia. Na przykład w przypadku zdarzeń związanych z Internetem istotne mogą być wszelkiego typu logi, odwiedzane strony WWW, adresy e-mail, nazwy użytkowników, serwery, urządzenia peryferyjne, czy również nośniki kopii zapasowych. Zasady informatyki śledczej, w ramach przygotowania zabezpieczenia danych elektronicznych w tym z telefonów, zakładają wzięcie pod uwagę następujących elementów:[29]

– jeśli telefon działa i jest podłączony do internetu możliwa jest ingerencja osób trzecich i na przykład wymazanie istotnych danych,
– nośniki, jakie należy brać pod uwagę, na przykład niektóre informacje mogą być przechowywane nie w kluczowych systemach, tylko na pamięciach przenośnych (na przykład breloczki z pamięciami USB czy kart pamięci),
– podejrzany nie musi być właścicielem urządzeń lub nośników. Informacje mogą być przechowywane na „wspólnych" dla wielu podmiotów serwerach, np. w „chmurze",
– przechowywane w systemach telefonów informacje są często chronione prawami administracyjnymi, których podejrzany może nie posiadać,
– w systemie mogą być przechowywane informacje prawnie chronione, na przykład tajemnica radcowska,
– informacje mogą być zabezpieczone za pomocą haseł, kluczy szyfrowych, kluczy fizycznych i innych urządzeń z kontrolą dostępu,
– informację można szybko usunąć, również poprzez sieć komputerową,
– czas zabezpieczania jest tym dłuższy, im więcej jest danych.

Potencjalne dowody pochodzące z danych telefonu komórkowego/smartphonu obejmują książkę telefoniczną, wiadomości SMS, połączenia przychodzące i wychodzące, nazwiska i inne dane kontaktowe, zdjęcia, dane logowania do różnych usług, odzyskane informacje[30].

[29] P. Krejza, *Najlepsze praktyki* …, dz. cyt., s. 134.
[30] P. Krejza, *Najlepsze praktyki* …, dz. cyt., s. 136.

Obecne telefony posiadają aparaty cyfrowe, kamery, sprzęt audio, który rejestruje liczne dane w różnym formacie. Można je też edytować i zmieniać. Aparaty, kamery oraz sprzęt audio mogą działać zarówno niezależnie, jak i w sieci, być wykorzystywane w warunkach domowych oraz biznesowych. Mogą zawierać obrazy, również dokumenty i archiwa. Niektóre urządzenia mogą być bardzo zaawansowane i przechowywać wiele informacji.

Istotne dane mogą zawierać zainstalowane w smartphonach satelitarne systemy nawigacyjne. Potencjalne dowody to zapamiętane dane, tekst, obrazy (mapy), trasy, zaznaczone miejsca, ramy czasowe podróży. W tym zakresie można zastosować operacje opisane wcześniej. Jeśli to możliwe zabezpieczyc należy ponadto wszelkie instrukcje do GPS kable zasilające i inne urządzenia powiązane.

Odrębne metody badania mogą dotyczyć nośników danych. Nośniki danych służą do przechowywania informacji pochodzących z urządzeń elektronicznych. Na rynku istnieje wiele różnego typu nośników informacji. W telefonach wykorzystywane są zewnętrzne lub wymienne pamięci. Nośniki należy przechowywać z dala od magnesów i radioodbiorników oraz chronić przed szkodliwym wpływem środowiska: ciepłem, zimnem, brudem[31].

Zaletą stosowania powyższej procedury jest bezdyskusyjne obronienie wiarygodności pozyskanego w ten sposób materiału w sądzie. Cechy takie, jak autentyczność, wierność oraz integralność są tu bezsprzecznie zachowane, w każdej chwili istnieje możliwość sporządzenia kolejnej kopii binarnej zabezpieczonego nośnika i kopia ta będzie tożsama z oryginałem. Oznacza to, że sumy kontrolne, będące wartościami funkcji skrótu na całym obrazie kopii binarnej, wskażą zawsze taką samą wartość. Jest to gwarancją, że materiał dowodowy nie został zmanipulowany[32].

Niestety, metoda ta ma ograniczenia, o których warto wspomnieć. Głównym ograniczeniem podejścia tradycyjnego jest to, że podczas wyłączenia telefonu traci się bezpowrotnie dużą część informacji, z których można pozyskać materiał dowodowy. Powodem takiego stanu rzeczy jest technologia budowy pamięci operacyjnej RAM. Układy scalone pamięci przechowują informacje jedynie wówczas, gdy są. zasilane napięciem o odpowiedniej wartości. Z chwilą wyłączenia telefonu traci się wszystkie informacje zawarte w pamięci operacyjnej. Informacje, które utracimy, to między innymi:

- informacje o uruchomionych programach i procesach,
- informacje o działających usługach systemowych, otwartych plikach, —- informacje o załogowanych użytkownikach zdalnych,
- informacje o otwartych portach sieciowych, połączeniach,
- zawartość schowka systemowego i inne.

Ponieważ niektóre programy np. wirusy uruchamiają się i rezydują jedynie w pamięci RAM, często właśnie informacje pozyskane z uruchomionego telefonu są tymi najbardziej interesującymi dla biegłych[33].

Nowe podejście do zabezpieczenia uruchomionych komputerów Live Forensics

[31] P. Krejza, Najlepsze praktyki …, dz. cyt., s. 139.

[32] M. Jastrzębski, M. Kędziora, *Procesowe zabezpieczanie i analiza uruchomionych komputerów — dostępne narzędzia*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 141.

[33] M. Jastrzębski, M. Kędziora, *Procesowe zabezpieczanie* …, dz. cyt., s. 142.

może mieć zastosowanie do telefonów. Charakteryzuje się zmianami w procedurze procesowego pozyskania danych komputerowych. Pierwszą czynnością biegłego jest wykonanie snapshotu, czyli pozyskanie pamięci operacyjnej RAM oraz informacji ulotnych, czyli takich, które bezpowrotnie stracimy po wyłączeniu telefonu[34].

Działania sprawców przestępstw komputerowych często wzbudzają frustrację u osób, które mają za zadanie znaleźć na zabezpieczonych nośnikach danych ślady potwierdzające przypuszczenie o ich winie. Działania te określane mianem antiforensics lub counterforensics powodują, że ślady:

– nie pozostają na nośniku (np. korzystanie z bezdyskowych systemów operacyjnych),
– mogą zostać całkowicie zniszczone (np. wymazywanie dysku lub destrukcja fizyczna),
– mogą zostać ukryte (np. szyfrowanie sprzętowe woluminów plików, steganografia).

Możliwe jest takie zmodyfikowanie danych, aby biegły badający nośniki musiał włożyć bardzo dużo pracy w ich odtworzenie. Do tych działań zaliczyć należy: [35]

– modyfikację systemu plików,
– modyfikację formatu plików,
– modyfikację oprogramowania (np. systemu operacyjnego),
– modyfikację logów i dzienników,
– wykrywanie działania programów forensic,
– wykorzystywanie podatności programów forensic,
– wykrywanie zmiany środowiska (np. wirtualizacji),
– generowanie kolizji funkcji skrótu.

PODSUMOWANIE

Zakres potrzeb badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon jest szeroki i wynika z praktycznego przeciwdziałania przestępstwom w rzeczywistości. Szczególnie chodzi o ustalenie zakresu i trybu dowodzenia przestępstw dokonywanych przez telefon/smartphone albo wręcz o wyprzedzanie działań przestępców, zanim szkody dla gospodarki i obywateli będą ogromne.

Można wskazać na kilka dróg, kiedy to może dojść do działań przestępczych. Może to być kradzież urządzenia i jego wykorzystanie, wprowadzenie nielegalnego oprogramowania na telefon, który przechwytuje dane o transakcjach, loginie, haśle i innych danych na różnych etapach dokonywani transakcji. Wprowadzanie na szerszą skalę bankowości komórkowej wymaga zarówno wiedzy technicznej jak prawnej. Dzięki temu można stworzyć wytyczne dla samego operatora, jak i wypracować nowe mechanizmy prawne, które zabezpieczą użytkowników bankowości komórkowej przed przestępcami.

Konieczne są zatem szersze badania mające na celu określenie metodyki popełniania przestępstw gospodarczych w zakresie płatności elektronicznych przez telefon/smartphon — ujęcie od strony sprawcy (algorytm efektywnego postępowania sprawcy), a także metodyki zwalczania przestępstw gospodarczych - ujęcie od strony organów ścigania (algorytm efektywnych działań rozpoznawczo-zapobiegawczo-wykrywczo-dowodowych organów ścigania).

[34] M. Jastrzębski, M. Kędziora, Procesowe zabezpieczanie …, dz. cyt., s. 143.

[35] J. Kosiński, *Wybrane działania antiforensics*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2009, s. 177.

STRESZCZENIE

Celem artykułu jest zbadanie potrzeb i możliwości badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon w kryminalistyce. W pracy wykorzystano dwie metody badawcze. Pierwsza odnosi się do danych statystycznych z zakresu przestępstw dotyczących telefonów/smartphonów i obejmuje metody statystyki opisowej. Druga to analiza procedur możliwych do zastosowania do badania telefonów/smartphonów pod kątem uzyskiwania dowodów przestępstw. Badania statystyczne wskazały, że problem kradzieży telefonów się zmniejsza, jednak rośnie liczba przestępstw oszustwa. W tej grupie należy upatrywać czynów, związanych z przestępstwami w płatnościach elektronicznych przez telefon/smartphon. Jednak nie ma obecnie oficjalnych statystyk w tym zakresie. W praktyce kryminalistycznej w Polsce brakuje procedur badania śladów przestępstw w płatnościach elektronicznych przez telefon/smartphon. Jednak technologia współczesnych smartphonów ma swoje odzwierciedlenie w rozwoju komputerów i w pracy wykazano słuszność zastosowania wybranych technik badania śladów w komputerach. Analizy metod badania śladów wskazały, że powinno się stworzyć już teraz normy mające na celu określenie metodyki popełniania przestępstw gospodarczych w zakresie płatności elektronicznych przez telefon/smartphon — ujęcie od strony sprawcy (algorytm efektywnego postępowania sprawcy), a także metodyki zwalczania przestępstw gospodarczych - ujęcie od strony organów ścigania (algorytm efektywnych działań rozpoznawczo-zapobiegawczo-wykrywczo-dowodowych organów ścigania).

SUMMARY

The requirements and possibilities of examining the traces of crimes in the electronic payments by phone / smartphone.

The aim of the article is to examine the requirements and possibilities of examining the traces of crimes in electronic payment by phone / smartphone in crime detection. In the report two scientific methods were used. The first one is connected with the statistical data of the crimes related to the phones / smartphones and it includes descriptive statistics methods. The other one is the analysis of the procedures which can be used with checking the phones / smartphones in order to trace the evidence of the crime. The statistical research showed that the number of stolen phones is getting smaller, however the rate of the fraud is increasing. In this group we can also find the electronic payment crimes with the use of smartphones. At the moment there are no official statistical data on this problem. In the Polish criminal practice there is no procedure of tracing the electronic payment crimes with the use of phone / smartphone. The technology of modern smartphones is an indication of the development of computers and in the report it was pointed out that the selected methods of tracing crimes in computers are useful. The analyses of the methods of tracing the crime indicated that the standards of the methodology of economic crimes in terms of electronic payment with the use of phone / smartphone are to be settled - the perpetrator approach (the algorithm of the effective beahaviour of the perpetrator),

as well as, the methodology of fighting with economic crimes – the law enforcement approach (the algorithm of effective recognitive-preventive-tracing-evidential measures of law enforcement)

BIBLIOGRAFIA

Akty prawne:

Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U. Nr 88, poz. 553, z późn. zm.)

Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz.U. 1997 Nr 89, poz. 555 z późn. zm.)

Orzecznictwo:

Postanowienie SN z 24 czerwca 2010 r., V KK 388/09, Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa 2010, nr 9, poz. 82.

Wyrok SA w Białymstoku z 17 stycznia 1995 r., II AKr 207/94, Orzecznictwo Sądów Apelacji Białostockiej 1995, nr 1, poz. 10.

Wyrok SA w Katowicach z 17 sierpnia 2000 r., II AKa 168/00, Orzecznictwo Sądów Apelacyjnych 2001, nr 7-8, poz. 51, s. 53.

Wyrok SN z 12 stycznia 2011 r., III KK 230/10, Biuletyn Prawa Karnego 2011, nr 6, poz. 9.

Wyrok SN z 29 marca 2011 r., III KK 321/10, Biuletyn Prawa Karnego 2011, nr 9.

Wyrok z 15 sierpnia 1986 r., I KR 212/85, OSNKW 1986, nr 11-12, poz. 97.

Wytyczne wymiaru sprawiedliwości i praktyki sądowej SN z 25 czerwca 1980 r. w sprawie odpowiedzialności karnej za przestępstwa określone w art. 208, VII KZP 48/78, Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa 1980, nr 8, poz. 65.

Literatura:

Gidel-Stefaniec E., Zagrożenia przestępstwem w płatnościach elektronicznych przez telefon/smartfon, Wydawnictwo Wyższej Szkoły Handlowej, Kielce 2013, tom 1.

Jakubowski Z., Wybrane aspekty ochrony tożsamości elektronicznej, [w:] Przestępczość teleinformatyczna, J. Kosiński (red.), Wyższa Szkoła Policji, Szczytno 2009.

Jastrzębski M., Kędziora M., Procesowe zabezpieczanie i analiza uruchomionych komputerów — dostępne narzędzia, [w:] Przestępczość teleinformatyczna, J. Kosiński (red.), Wyższa Szkoła Policji, Szczytno 2009.

Kalitowski M., Przestępstwa przeciwko ochronie informacji [w:] Kodeks karny. Komentarz, M. Filar (red.), Lexis Nexis, Warszawa 2012.

Kardas P., Oszustwo komputerowe w kodeksie karnym, Przegląd Sądowy 2000, 11 – 12, 43-45.

Kołecki H., Niektóre zaniedbane obszary badawcze współczesnej kryminalistyki w Polsce, [w:] Obszary badawcze współczesnej kryminalistyki, T. Widła (red.), Wydawnictwo Uniwersytetu Śląskiego, Katowice 2011.

Kosiński J., Wybrane działania antiforensics, [w:] Przestępczość teleinformatyczna, J. Kosiński (red.), Wyższa Szkoła Policji, Szczytno 2009.

Krejza P., Najlepsze praktyki zabezpieczania elektronicznego materiału dowodowego, [w:] Przestępczość teleinformatyczna, J. Kosiński (red.), Wyższa Szkoła Policji, Szczytno 2009.

Marek A., Kodeks karny, Wolters Kluwer, Warszawa 2010.

Marshall A.M., Tompsett B.C., Silicon Pathology?, Science & Justice 2004, Vol. 44, Issue 1, 43-50.

Philips E., Mobile phone – friend or foe? Science & Justice 2002, Vol. 42, Issue 4.

Pływaczewski E., Guzik - Makaruk E., Przestępstwa przeciwko mieniu, [w:] Kodeks karny. Komentarz, M. Filar (red.), Lexis Nexis, Warszawa 2012.

Skorupka J., Wady oświadczenia woli w wybranych przestępstwach gospodarczych, Przegląd Sądowy 2000, 4, 38.

Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F., Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia, Urząd Komisji Nadzoru Finansowego, Warszawa 2010.

Szwarczyk M., Michalska-Warias A., Bojarski T., Piórkowska-Flieger J., Kodeks karny. Komentarz, Lexis Nexis, Warszawa 2012.

Wojciechowska-Filipek S., Technologia informacyjna w usługach bankowości elektronicznej, Difin, Warszawa 2010.

Wójcik J.W., Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne, Wydawnictwo JWW, Warszawa 2008.

Zawadzki K., Kreowanie tożsamości w celu dokonywania przestępstw i prania pieniędzy poprzez systemy płatności w Internecie, [w:] Przestępczość teleinformatyczna, J. Kosiński (red.), Wyższa Szkoła Policji, Szczytno 2009.

Netografia:

niebezpiecznik.pl [10.11.2013]

Polska bankowość mobilna - infografika przygotowana przez Organizatorów plebiscytu Złoty Bankier, http://www.payu.pl/aktualnosci/polska-bankowosc-mobilna-infografika-przygotowana-przez-organizatorow-plebiscytu-zloty [2.07.2013]

Przestępstwa dotyczące telefonów komórkowych, http://statystyka.policja.pl/st/informacje/87763,Przestepstwa-dotyczace-telefonow-komorkowych.html [10.11.2013]

Should I be concerned about security of contactless payment cards? http://www.cba.ca/en/consumer-information/42-safeguarding-your-money/622-contactless-payment-card-security-an-faq[10.11.2013]

Trojan CITADEL atakuje PC – Trojan ZITMO infekuje telefony komórkowe, Rada Bankowości Elektronicznej, Związek Banków Polskich http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci [2.11.2013]

Złodzieje mogą skanować dane telefonem , http://www.tvn24.pl/wiadomosci-z-kraju,3/niebezpieczne-karty-zblizeniowe-zlodzieje-moga-skanowac-dane-telefonem,364859.html [10.11.2013]

Wychowanie dziecka to nie miła zabawa, a zadanie, w które trzeba włożyć wysiłek bezsennych nocy, kapitał ciężkich przeżyć i wiele myśli…

(JK)