Ekonomiczne Problemy Usług nr 123

ISSN: 1896-382X | www.wnus.edu.pl/pl/epu/
DOI: 10.18276/epu.2016.123-19 | strony: 203-211

MARIUSZ CZYŻAK
Urząd Komunikacji Elektronicznej

CYBERPRZESTĘPCZOŚĆ BANKOWA I ŚRODKI JEJ ZWALCZANIA

Streszczenie

Cyberprzestępczość bankowa to jedna z najgroźniejszych form współczesnej przestępczości. Należą do niej m.in. takie działania przestępcze, jak: phishing, skimming, hacking, spoofing czy sniffing. Zapobieganiu i zwalczaniu cyberprzestępstw bankowych służą rozwiązania organizacyjno-techniczne stosowane przez banki oraz regulacje prawnokarne skierowane przeciwko ich sprawcom.
Słowa kluczowe: cyberprzestępczość, bankowość elektroniczna.

Wprowadzenie

Jedną z najgroźniejszych form współczesnej przestępczości, uwarunkowaną środowiskiem działania przestępców i rodzajem stosowanej przez nich technologii, jest cyberprzestępczość. Pod pojęciem tym kryją się w najprostszym tego słowa znaczeniu czyny zabronione, które popełniane są w cyberprzestrzeni i z jej wykorzystaniem. Czym jest jednakże sama cyberprzestrzeń? W dokumencie „Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016" określa się ją jako „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami" (Rządowy program 2010, s. 6). Nie stanowi ona jednakże jedynie zbioru takich fizycznych składników, jak: systemy, sieci, oprogramowanie oraz przetwarzane w nich informacje, chociaż wskazywałyby na to niektóre jej definicje, w tym ta przywołana powyżej. Nie jest to także wyłącznie suma transakcji dokonywanych przez użytkowników Internetu, jakkolwiek sam Internet stanowi jej najistotniejszy element składowy. Cyberprzestrzeń to również koncepcja utworzenia równoległego środowiska będącego nowym wymiarem ludzkiej aktywności (Wasilewski 2013, s. 231–232). Współcześnie środowisko to wy-

korzystywane jest powszechnie do dokonywania operacji finansowych, przede wszystkim bankowych, stanowiąc przy tym nie tylko nową sferę obrotu gospodarczego, ale i obszar występowania nowych zjawisk patologicznych, w tym cyberprzestępczości. W dalszych rozważaniach przedstawione zostaną wybrane typy cyberprzestępstw towarzyszących bankowości elektronicznej oraz środki ich zwalczania.

1. Pojęcie bankowości elektronicznej

Pod pojęciem bankowości elektronicznej kryje się „forma usług świadczonych przez banki na rzecz klientów, polegająca na umożliwieniu dostępu do rachunku bankowego na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak komputer, telefon, bankomat, terminal, odbiorniki telewizji cyfrowej" (Górnisiewicz, Obczyński i Pstruś 2014, s. 30). Wyróżnić można trzy podstawowe rodzaje usług bankowości elektronicznej – bankowość terminalową, bankowość internetową i bankowość telefoniczną (Kwaśniewski, Leżoń, Szwajkowski i Woźniczka 2010, s. 6). Bankowość terminalowa, inaczej zwana również samoobsługową (ang. *selfbanking*), opiera się na wykorzystaniu urządzeń znajdujących się na zewnątrz banku, jak np. bankomaty i terminale POS (ang. *point of sale*) zlokalizowane głównie w punktach handlowych. Dostęp do bankowości internetowej możliwy jest natomiast za pośrednictwem standardowych urządzeń i oprogramowania i opiera się na komunikacji za pośrednictwem portalu internetowego właściwego banku. Dzięki niej posiadacz rachunku bankowego korzysta z takich funkcji, jak udostępnienie przez bank informacji o rachunku, czy też przekazanie bankowi poleceń rozliczeniowych (Iwański 2014, s. 50). Do cech bankowości internetowej należą z kolei: brak konieczności bezpośredniego kontaktu klienta z bankiem, wysoki poziom funkcjonalności serwisów bankowych (w tym dostępność wszystkich standardowych usług oferowanych w placówce banku), całodobowy dostęp do usług bankowych, możliwość jednoczesnej i automatycznej obsługi znacznej liczby klientów w czasie rzeczywistym, należyty poziom bezpieczeństwa transakcji i środków klienta przy zachowaniu przez niego wymaganych zasad bezpieczeństwa, brak ograniczeń terytorialnych w zakresie dostępu do rachunku bankowego oraz niższe koszty realizacji transakcji i obsługi klienta (Kwaśniewski, Leżoń, Szwajkowski i Woźniczka 2010, s. 24–25). Bankowość telefoniczna polega natomiast na wykorzystaniu telefonu do komunikacji klienta usług bankowych z bankiem. Bankowość telefoniczna stacjonarna obejmuje możliwość skorzystania z usług call center (dwustronna komunikacja głosowa z operatorem banku) oraz usług Interactive Voice Response (automatyczny serwis telefoniczny banku pozwalający na dokonywanie transakcji bankowych za pomocą doboru określonej sekwencji znaków na klawiaturze telefonu klienta w reakcji na komunikaty

głosowe generowane przez serwis). W ramach bankowości mobilnej klienci usług bankowych korzystać mogą z kolei z usług typu: SMS Banking (wykorzystywanie krótkich informacji tekstowych do otrzymywania wiadomości z banku i zlecania określonych operacji bankowych), WAP (Wireless Application Protocol – korzystanie z bankowości internetowej za pomocą wyświetlacza telefonu i innych urządzeń przenośnych) oraz SIM Toolkit (Subscriber Identity Module Application Toolkit – wykonywanie operacji bankowych za pomocą zainstalowanej na standardowej karcie SIM aplikacji bankowej przesyłanej drogą elektroniczną) (Kwaśniewski, Leżoń, Szwajkowski i Woźniczka 2010, s. 38–42).

2. Cyberprzestępstwa bankowe

Część spośród zachowań przestępczych towarzyszących bankowości elektronicznej powiązana jest z bezpieczeństwem transakcji dokonywanych za pomocą kart płatniczych. Jednym z nich jest skimming, który polega na bezprawnym skopiowaniu zawartości paska magnetycznego karty bankowej (np. płatniczej bądź kredytowej) służącym wytworzeniu duplikatu karty w postaci tzw. „białej karty" lub oryginalnej karty uzyskanej w banku w drodze przestępstwa. Kopia karty wykorzystywana jest analogicznie jak karta oryginalna i obciąża rachunek bankowy właściciela tej ostatniej. Karty podlegają kopiowaniu w punktach, w których dokonać można transakcji drogą elektroniczną z wykorzystaniem karty bankowej. Karty kopiowane są zwykle przez specjalne czytniki umieszczane w samoobsługowych terminalach płatniczych lub bankomatach, zaś numery PIN pozyskiwane są przez przestępców za pomocą znajdujących się na tych urządzeniach kamer bądź specjalnych nakładek na klawiaturę (Mikołajczyk 2014, s. 104 i n.). Wspomnieć należy w tym miejscu również o zagrożeniach związanych z utratą kart bezstykowych, których użycie polega na zbliżeniu karty do terminala bez obowiązku potwierdzania transakcji dokonywanej za pomocą karty podpisem lub kodem PIN. Związane one są bowiem nie tylko z możliwym dokonywaniem transakcji o wartości nie przekraczającej kwoty 50 zł przez osoby, które nielegalnie stały się posiadaczami karty, ale z wykorzystaniem przez przestępców przenośnych czytników pozwalających na nielegalne pozyskiwanie danych z kart zbliżeniowych (Kwaśniewski, Leżoń, Szwajkowski i Woźniczka 2010, s. 19 i n).

Phishing jest kolejnym działaniem przestępczym polegającym na zdalnym wyłudzeniu informacji służących autoryzacji. Przybierać ono może postać: e-maila wysyłanego rzekomo w imieniu banku, zawierającego prośbę o podanie loginu i haseł dostępu, przekserowania klienta usług bankowych do fikcyjnej strony www imitującej graficznie stronę banku i kontrolowanej przez przestępcę, jak również telefonu do klienta banku z fałszywą informacją pochodzącą rzekomo od pracownika banku z prośbą o podanie loginu i hasła (Kwaśniewski, Leżoń, Szwajkowski

i Woźniczka 2010, s. 6). Nie można zapominać również o, powiązanym z hackingiem, szkodliwym oprogramowaniu określanym mianem crimeware, które jest instalowane potajemnie na komputerze klienta usług bankowych i zwykle stanowi jedną z wielu odmian trojana. Niektóre spośród nich służą rejestrowaniu uderzeń klawiszy (tzw. keyloggery), inne z kolei wykonują zrzut ekranu, gdy użytkownik korzysta z serwisu bankowego, bądź też pozwalają hakerom uzyskać zdalny dostęp do komputera osoby będącej klientem usług bankowych świadczonych za pomocą elektronicznego kanału dostępu. Wszystkie one służą jednak w rzeczywistości pozyskiwaniu przez cyberprzestępców poufnych informacji (m.in. haseł i numerów PIN) w celu nielegalnego pozyskiwania środków finansowych zgromadzonych na rachunkach bankowych (Crimeware, www.pandasecurity.com 2015).

Wspomnieć należy również o innych typach działań przestępczych towarzyszących korzystaniu z elektronicznego kanału dostępu do usług bankowych, takich jak np. tzw. sniffing, czy spoofing. Ten pierwszy to przechwytywanie przez nieuprawnione osoby danych przesyłanych w sieciach lokalnych oraz w sieciach WiFi. Przestępcy wykorzystują w tym przypadku dedykowane programy komputerowe (tzw. sniffery), których zadaniem jest odbiór i analiza danych pozyskiwanych z sieci. Śledząc dane dotyczące transakcji finansowych dokonywanych za pośrednictwem Internetu, uzyskać mogą m.in. dane dostępowe do kont internetowych, a następnie użyć ich do rozporządzania środkami finansowymi zgromadzonymi na określonym rachunku bankowym. Ten drugi oznacza zaś podszywanie się pod inny element systemu informatycznego (np. komputer innego użytkownika systemu) celem wykorzystania go jako narzędzia do przeprowadzenia ataku na określoną stronę internetową (Górniszewski, Obczyński i Pstruś 2014, s. 35–36).

3. Zwalczanie cyberprzestępczości bankowej

Po pobieżnym przedstawieniu wybranych form cyberprzestępczości bankowej poświęcić wypada wreszcie nieco miejsca zagadnieniu zwalczania cyberprzestępczości bankowej, zarówno o charakterze prewencyjnym, jak i represyjnym. Z jednej strony zatem instrumentom służącym jej zapobieganiu, z drugiej zaś tym, które stanowią reakcję państwa na zjawiska patologiczne tego rodzaju. W tym pierwszym przypadku odnieść się należy przede wszystkim do rozwiązań organizacyjno-technicznych stosowanych przez banki, w tym drugim odwołać się wypada natomiast do regulacji o charakterze prawnokarnym, na gruncie których poddano penalizacji szczególnie groźne zachowania godzące w bankowość elektroniczną.

Warto w tym miejscu wobec tego zwrócić uwagę na aktywność Komisji Nadzoru Finansowego (dalej: KNF) w obszarze bezpieczeństwa systemów teleinformatycznych wykorzystywanych w bankowości. Zgodnie z art. 137 ustawy z 29 sierpnia 1997 r. Prawo bankowe (Tekst jednolity DzU z 2015 r., poz. 128, ze zm.), może

ona „wydawać rekomendacje dotyczące dobrych praktyk ostrożnego i stabilnego zarządzania bankami". Rekomendacja „D" KNF dotyczy zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Zawarta w niej szczegółowa rekomendacja nr 16 odnosi się do obszaru „Zarządzanie elektronicznymi kanałami dostępu". W myśl jej postanowień „Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwa danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów". Wybór stosowanej przez bank metodologii potwierdzania tożsamości klientów korzystających z elektronicznych kanałów dostępu poprzedzony powinien zostać systematyczną analizą ryzyka towarzyszącego używaniu tego rodzaju kanałów. Powinna ona obejmować, obok możliwości transakcyjnych oferowanych przez określony kanał i łatwość korzystania przez klienta z poszczególnych metod potwierdzania tożsamości, również rozpoznane techniki ataków. Bank zobligowany jest udostępniać swoim klientom kanał komunikacyjny (np. telefoniczny bądź elektroniczny), za pomocą którego mogliby oni informować bank o zidentyfikowanych zdarzeniach związanych z bezpieczeństwem elektronicznych kanałów dostępu, w tym m.in. o atakach przybierających postać phishingu. Niezwykle istotnym aspektem przeciwdziałania cyberprzestępczości bankowej jest również edukacja klientów banków, która pozwoliłaby na zrozumienie przez nich istoty zagrożeń towarzyszących korzystaniu z elektronicznych kanałów dostępu. Odbywa się ona w szczególności za pośrednictwem komunikatów umieszczanych na stronach bankowości elektronicznej, ulotek informacyjnych, czy też przesyłanych do klientów wiadomości e-mail (Komisja Nadzoru Finansowego 2013, s. 48–50). Przed atakiem phishingowym uchronić może klienta usług bankowych świadczonych drogą elektroniczną przestrzeganie kilku podstawowych zasad, w szczególności zaś: ostrożne traktowanie przesłanych drogą e-mailową wiadomości żądających podania osobistych informacji, powstrzymanie się od wypełniania formularzy przesłanych drogą e-mailową żądających podania tego rodzaju danych i wprowadzanie takich danych wyłącznie za pośrednictwem bezpiecznej strony internetowej, każdorazowe informowanie banku o podejrzanych incydentach towarzyszących korzystaniu z bankowości elektronicznej, zaniechanie otwierania stron internetowych przy użyciu odsyłaczy zawartych w wiadomościach e-mail, regularne sprawdzanie stanu kont bankowych, czy też używanie najnowszych wersji przeglądarek internetowych (www.kaspersky.pl).

Kolejnym zasługującym na przywołanie szczegółowym zaleceniem zawartym w Rekomendacji „D" KNF, o której należy wspomnieć, jest wskazówka dotycząca obszaru „Zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego". Wymaga ona bowiem od banku posiadania sformalizowanych zasad zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinforma-

tycznego, obejmujących ich „identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn". Zasady postępowania z incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego określać powinny m.in.: metody i zakres zbierania informacji o incydentach, sposób przeprowadzania analiz ich wpływu na środowisko teleinformatyczne, zasady kategoryzacji i priorytetyzacji incydentów oraz wykrywania zależności pomiędzy nimi, które pozwolą w konsekwencji zidentyfikować lub usunąć przyczyny incydentów powiązanych ze sobą, sposób gromadzenia i zabezpieczania dowodów związanych z incydentami, które mogłyby być wykorzystane w potencjalnych postępowaniach sądowych, itp. (Komisja Nadzoru Finansowego 2013, s. 57).

Zachowania cyberprzestępców towarzyszące bankowości elektronicznej podlegają penalizacji na gruncie przepisów ustawy z dnia 6 czerwca 1997 r. Kodeks karny (dalej: kk), wypełniając w głównej mierze znamiona przestępstw przeciwko: wolności (art. 190 § 2 kk), informacji (art. 267 kk, art. 268 kk i art. 268a kk), czy też przeciwko mieniu (art. 286 § 1 kk i art. 287 § 1 kk). Przywołać w tym miejscu należy treść tychże przepisów. I tak na gruncie art. 267 kk grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 podlega m.in. nieuprawnione uzyskanie dostępu do informacji nieprzeznaczonej dla sprawcy, polegające w szczególności na podłączeniu się do sieci telekomunikacyjnej lub przełamaniu albo ominięciu elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Tej samej karze podlega nieuprawnione uzyskanie dostępu do całości lub części systemu informatycznego, a także zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem, w celu uzyskania informacji, do której sprawca nie jest uprawniony. Wspomnieć wypada także o przestępstwach komputerowych skierowanych przeciwko nienaruszalności i dostępności informacji (art. 268 i 268a kk). Dodać przy tym trzeba, że znacząca część przywołanych powyżej działań przestępczych prowadzi zwykle do tzw. fraudów bankowych (Staszczyk 2015, s. 44). Stanowią one zatem zwykle również przestępstwo oszustwa (art. 286 § 1 kk), polegające m.in. na doprowadzeniu innej osoby do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu, w celu osiągnięcia korzyści majątkowej, i podlegające karze pozbawienia wolności od 6 miesięcy do lat 8. Typem przestępstwa przeciwko mieniu jest również przestępstwo tzw. oszustwa komputerowego. Zgodnie z dyspozycją art. 287 § 1 kk karze pozbawienia wolności od 3 miesięcy do lat 5 podlega ten, „kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych". Nie można przy tym zapominać również o tym, że na podstawie art. 190a § 2 kk karze pozbawienia wolności do lat 3 podlega podszywanie

się pod inną osobę, a także wykorzystywanie jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej.

Pamiętać trzeba, że odpowiedzialność karna towarzysząca zjawiskom patologicznym w cyberprzestrzeni i stanowiące jej istotę zagrożenie sankcjami karnymi za poszczególne zachowania cyberprzestępców stanowi instrument przeciwdziałania przestępczości, zarówno o charakterze prewencyjnym, jak i represyjnym. Niemniej jednak samo ściganie sprawców przestępstw popełnianych w cyberprzestrzeni napotyka na szereg problemów, związanych chociażby z pozyskaniem dowodów czy też identyfikacją samych sprawców, którzy „działają" w cyberprzestrzeni i stąd też są trudni do wykrycia.

Podsumowanie

Korzystanie z różnych usług bankowości elektronicznej stało się w ostatnich latach czymś naturalnym. Według danych Związku Banków Polskich na koniec września 2015 r. liczba umów klientów indywidualnych, umożliwiających dostęp do usług bankowości internetowej, przekroczyła 30 mln, przy czym w samym III kwartale odnotowano przyrost rachunków tego rodzaju na poziomie 8,34%. Przybyło zatem w tym okresie 2,3 mln umów bankowości internetowej. Liczba klientów aktywnych (dokonujących co najmniej jednej operacji miesięcznie) wyniosła 14,64 mln, tj. ponad 550 tys. (3,96%) więcej niż w poprzednim kwartale tego roku. Całkowity przyrost aktywnych indywidualnych klientów bankowości internetowej w ujęciu rocznym wyniósł natomiast ponad 2 mln (NetB@nk 2015, s. 5). Korzystanie z usług bankowych, ze swej natury związane z towarzyszącym im obrotem środkami finansowymi, narażone jest na ataki o charakterze przestępczym. Co za tym idzie, w ostatnich latach daje się również zauważyć wzrost liczby przestępstw bankowych, w tym i tych popełnianych w cyberprzestrzeni. Zgodnie z danymi Komendy Głównej Policji w okresie styczeń–wrzesień 2015 r. odnotowano m.in. 4119 przestępstw o charakterze oszustwa bankowego, wobec 2512 przestępstw tego rodzaju w całym roku 2014. Spośród nich 713 czynów zabronionych określono mianem przestępstw związanych z bankowością internetową (w roku 2014 – 585), w tym 73 uznano za phishing, a 118 jako skimming (Boczoń 2015). Wobec skali operacji dokonywanych drogą elektroniczną przez klientów usług bankowych znaczącym problemem wydaje się jednak tzw. „ciemna liczba" tego rodzaju przestępstw, tj. tych nie ujętych w statystykach kryminalnych na skutek niewykrycia. Z uwagi na postępujący rozwój technologii informatycznych oraz towarzyszące temu procesowi – rozwój gospodarczy i nieodwracalne zmiany zachowań społecznych nie jest ani celowe, ani nie wydaje się możliwe ograniczenie skali wykorzystania elektronicznych kanałów dostępu do usług bankowych. Mając jednak na uwadze zarówno trudność w wykrywaniu cyberprzestępstw bankowych, jak rów-

nież w ściganiu ich sprawców, a także nieustanne doskonalenie przez nich metod przestępczego działania, za skuteczniejsze uznać należy jednakże nie narzędzia prawnokarne, ale te instrumenty zwalczania przestępczości, których istotą jest edukacja klientów elektronicznych usług bankowych oraz stosowanie właściwych rozwiązań organizacyjno-technicznych przez sektor bankowy. Służą one bowiem podniesieniu poziomu bezpieczeństwa usług świadczonych drogą elektroniczną, a tym samym utrudniają cyberprzestępcom skuteczne podejmowanie działań przestępczych.

Literatura

1. Boczoń W., *Coraz więcej przestępstw w bankowości. Oto dane Komendy Głównej Policji*, www.bankier.pl [dostęp 8.01.2016].
2. *Crimeware: the silent epidemic. Malware evolves to focus on obtaining financial returns*, www.pandasecurity.com [dostęp 8.01.2016].
3. Górnisiewicz M., Obczyński R., Pstruś M. (2014), *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną. Poradnik klienta usług finansowych*, Komisja Nadzoru Finansowego, Warszawa.
4. Iwański W. (2014), *Umowa rachunku bankowego objętego bankowością internetową z punktu widzenia nowej regulacji usług płatniczych*, Warszawa.
5. Kwaśniewski P., Leżoń K., Szwajkowska G., Woźniczka F. (2010), *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa.
6. Komisja Nadzoru Finansowego (2013), *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i środowiska teleinformatycznego w bankach*, Warszawa.
7. Mikołajczyk K. (2014), *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 10.
8. NetB@nk (2015), *Raport: bankowość internetowa i płatności bezgotówkowe, III kwartał 2015 r.*, zbp.pl [dostęp 8.01.2016].
9. Phishing, www.kaspersky.pl [dostęp 8.01.2016].
10. *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* (2010), Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa.
11. Staszczyk M. (2015), *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, „Finanse i Prawo Finansowe", nr 1.
12. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (DzU nr 88, poz. 553, ze zm.).
13. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (tekst jednolity DzU z 2015 r., poz. 128, ze zm.).

14. Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

BANKING CYBERCRIME AND COUNTERACTING MEASURES

Summary

Cybercrime in the banking sector is one of the most dangerous form of the contemporary crimes. It includes inter alia criminal actions such as: phishing, skimming, hacking, spoofing and sniffing. To prevent or combat cybercrimes in the banking sector banks' organizational and technical solutions or rules of criminal law against cybercrime perpetrators are used.
Keywords: cybercrime, electronic banking.

Translated by Mariusz Czyżak