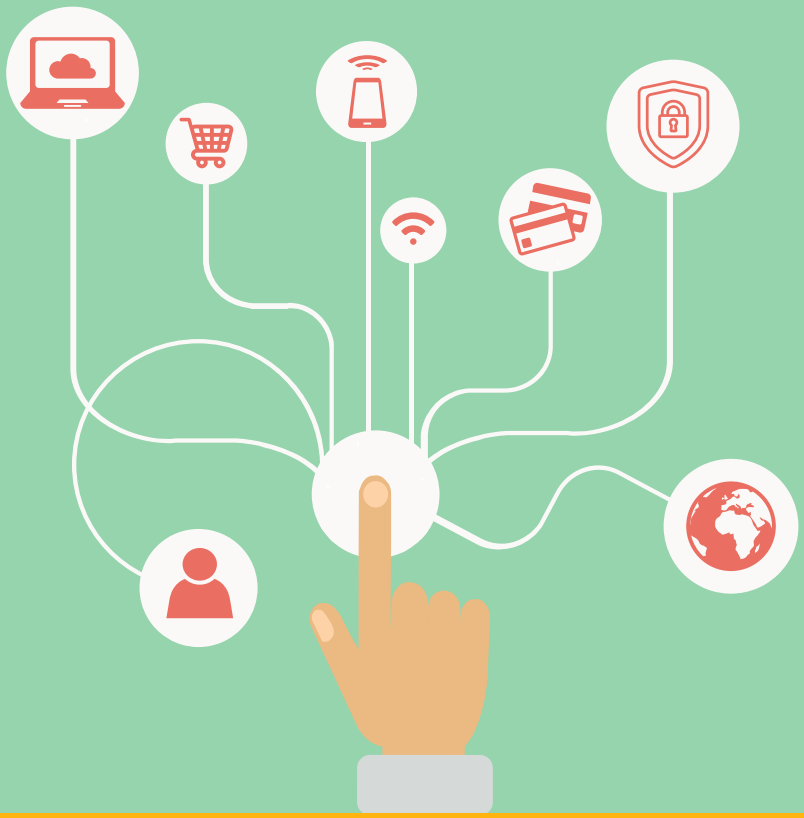
Maciej Krzysztoszek

KNF
KOMISJA
NADZORU
FINANSOWEGO



Bankowość elektroniczna w teorii i praktyce

Materiały edukacyjne dla środowiska szkolnego

MATERIAŁY EDUKACYJNE
DLA ŚRODOWISKA SZKOLNEGO

Maciej Krzysztoszek

BANKOWOŚĆ ELEKTRONICZNA W TEORII I PRAKTYCE

Warszawa 2017

KNF | KOMISJA NADZORU FINANSOWEGO

Publikacja została wydana nakładem Komisji Nadzoru Finansowego

Pl. Powstańców Warszawy 1
00-030 Warszawa
www.knf.gov.pl

Warszawa 2017
Wydanie I

ISBN 978-83-63380-11-3

Nakład: 3000 szt.

Przygotowanie do druku i druk:
EXPOL P. Rybiński, J. Dąbek, sp.j.

SPIS TREŚCI

WSTĘP

Bankowość elektroniczna, w tym bankowość mobilna, jest dziś jednym z najszybciej rozwijających się segmentów rynku finansowego. Powszechność dostępu za pośrednictwem Internetu, funkcjonalność oraz intuicyjność dostarczanych rozwiązań sprawia, że coraz chętniej korzystamy z tego kanału bankowego. Banki prześcigają się w dostarczaniu kolejnych udogodnień technologicznych, a mnogość i atrakcyjność oferowanych rozwiązań usypia nieco czujność obecnych i potencjalnych użytkowników. Tymczasem trzeba mieć świadomość, że wraz z rozwojem tych usług rosną także zagrożenia po stronie osób z nich korzystających. Cyberprzestępcy chętnie korzystają z nowych metod, by skutecznie przeprowadzić swój cyberatak. Grupą szczególnie narażoną na takie działania są użytkownicy bankowości elektronicznej, którzy nie są w stanie tak silnie zabezpieczyć swoich komputerów, jak czynią to banki.

Decyzja o wydaniu publikacji na temat bankowości elektronicznej, skierowanej do środowiska szkolnego, została podjęta z uwagi na pilną potrzebę edukacji w tym zakresie. Jej odbiorcami są młodzi ludzie, którzy już w tym okresie życia wchodzą na rynek finansowy: zakładają swoje pierwsze rachunki bankowe, otrzymują pierwsze karty płatnicze i zyskują pełnoprawny dostęp do oferty bankowej. To przede wszystkim tej grupie nowych klientów bankowość elektroniczna może wydawać się szczególnie atrakcyjna. Przyzwyczajeni są już bowiem do możliwości wykonywania większości czynności bez wychodzenia z domu, począwszy od otwarcia rachunku, przez wykonywanie operacji przelewów, po instalowanie aplikacji służących do płatności zbliżeniowych. Także często zawierają pierwsze umowy z instytucjami na rynku finansowym. Trzeba bowiem mieć na uwadze, że stając się pełnoprawnym posiadaczem rachunku, zyskuje się nie tylko prawa, ale też obowiązki. Jednym z nich jest obowiązek zachowania bezpieczeństwa w korzystaniu z bankowości elektronicznej.

Niniejsza publikacja została podzielona na trzy części. W ujęciu teoretycznym autor zwięźle przedstawia dynamiczny rozwój bankowości elektronicznej oraz zwraca uwagę na najważniejsze prawa i obowiązki wynikające z zawartych umów między bankami a klientami. Drugie ujęcie to próba spojrzenia na bankowość elektroniczną w sposób praktyczny. Autor stara się przedstawić najczęstsze zagrożenia wynikające z korzystania z usług elektronicznych i wska-

zuje na proste działania, które mogą zwiększyć bezpieczeństwo środków, którymi użytkownicy dysponują za pośrednictwem bankowości elektronicznej. Trzecia część to tzw. *case studies*, czyli konkretne przykłady działań w sieci i pytania problemowe, które mają zweryfikować wiedzę na temat bankowości elektronicznej. Materiał rekomenduje się do wykorzystywania w edukacji z obszaru finansów osobistych na lekcjach przedmiotów obejmujących zagadnienia z zakresu rynku finansowego.

UJĘCIE TEORETYCZNE

1. BANKOWOŚĆ ELEKTRONICZNA WCZORAJ I DZIŚ – DYNAMIKA ZMIAN

Boom na stacjonarne placówki bankowe polski sektor bankowy ma już za sobą. Dziś tradycyjne oddziały są stopniowo wypierane przez usługi, jakie banki oferują w Internecie i na urządzeniach mobilnych, ale jeszcze 20 lat temu bankowy świat wyglądał zupełnie inaczej.

Pierwsze usługi bankowości elektronicznej w Polsce zostały zaoferowane na początku lat 90-tych i przybrały one wówczas formę bankomatów. Była to tzw. bankowość terminalowa, która oferowała możliwość posługiwania się kartami płatniczymi. Jednocześnie, wraz ze zmianami w polskim sektorze bankowym i jego dynamicznym rozwojem, banki rozwijały obsługę klientów poprzez infolinie, gdzie w rozmowie z pracownikiem banku składano dyspozycje. Pod koniec lat 90-tych uruchomiono pierwszy bankowy serwis internetowy, a w 2000 roku powstał pierwszy bank internetowy. Od tego czasu w ciągu kolejnych czterech lat liczba użytkowników bankowości internetowej wzrosła aż 47 razy[1], a okres pierwszej dekady XXI wieku można określić mianem najbardziej dynamicznego rozwoju usług bankowości elektronicznej.

Dziś struktura bankowości elektronicznej jest dużo bardziej złożona. Za sprawą popularności tego kanału klienci otrzymują szereg możliwości korzystania ze swojego konta i produktów bankowych bez odwiedzania placówki. Obszarem,

[1] M. Polasik, *Rozwój bankowości elektronicznej w Polsce – w świetle badań ankietowych*, Bank i kredyt, sierpień 2005, s. 60.

w którym obserwuje się intensywny rozwój jest m.in. bankowość mobilna. Zaprojektowane na smartfony i tablety aplikacje mobilne sprawiają, że cały bank pozostaje w zasięgu urządzenia mobilnego. Możemy z niego wykonywać przelewy, zapłacić za zakupy, sprawdzić, gdzie jest najbliższy bankomat albo placówka banku, a nawet wykonać tzw. fotoprzelew. Rosnące zainteresowanie tym sposobem komunikacji z bankiem potwierdzają dane. Z raportu PRNews.pl wynika, że na koniec 2015 roku liczba użytkowników bankowości mobilnej przekroczyła 5,7 mln, co oznacza, że w ciągu roku przybyło aż 2,3 mln użytkowników tego kanału[2].

2. WIRTUALNA RZECZYWISTOŚĆ W GRANICACH PRAWA

Mimo że Internet oferuje szereg możliwości, z których możemy korzystać na co dzień, nie jest to świat niczym nieograniczony. Tak jak codzienne funkcjonowanie państwa jest uregulowane poprzez instytucje i przepisy prawa, tak również przestrzeń wirtualna podlega regułom, w granicach których możemy się poruszać. Podobnie jest na rynku finansowym, na którym klienci przechowują swoje pieniądze.

Bankowość elektroniczna nie jest uregulowana w przepisach prawa. W aktualnym stanie prawnym nie istnieje właściwa definicja tego pojęcia. Przyjmuje się natomiast, że poprzez bankowość elektroniczną należy rozumieć dostęp do zgromadzonych na rachunku bankowym środków finansowych i towarzyszących im usług za pośrednictwem urządzeń elektronicznych, w tym stacjonarnych i mobilnych. Wobec powyższego najczęściej stosuje się przepisy ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (tj. Dz.U. z 2016 r. poz. 1988 ze zm.), zwanej dalej „ustawą Prawo bankowe", które regulują działalność banków, oraz ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (tj. Dz.U. z 2016 r. poz. 1572 ze zm.), zwanej dalej „ustawą o usługach płatniczych", które w bardziej szczegółowy sposób odnoszą się do relacji między bankiem a klientem. Dla klientów jednak najistotniejsze są postanowienia zawarte w umowie. One bowiem regulują prawa i obowiązki obu stron umowy.

[2] Źródło: http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iv-kw-2015-6552323.html, data dostępu: 30 marca 2016 r.

2.1. Prawa i obowiązki po stronie banku i klienta

Jak zostało wspomniane wcześniej, ustawa Prawo bankowe dosyć ogólnie odnosi się do relacji między bankiem a klientem w kontekście bezpieczeństwa gromadzonych na rachunku środków. Zgodnie z art. 50. ust. 1 ustawy Prawo bankowe, *posiadacz rachunku bankowego dysponuje swobodnie środkami pieniężnymi zgromadzonymi na rachunku. W umowie z bankiem mogą być zawarte postanowienia ograniczające swobodę dysponowania tymi środkami*. Właściwy obowiązek zachowania bezpieczeństwa określa ust. 2 ww. artykułu ustawy: *bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych*.

Do zachowania bezpieczeństwa zobowiązuje banki także Komisja Nadzoru Finansowego, bowiem jednym z celów nadzoru jest *zapewnienie bezpieczeństwa środków pieniężnych gromadzonych na rachunkach bankowych* (art. 133 ust. 1 ustawy Prawo bankowe). Dlatego Komisja Nadzoru Finansowego, jako państwowy organ nadzorczy, wydaje bankom rekomendacje odnoszące się do poszczególnych obszarów ich działalności. Rekomendacje te mają na celu określenie oczekiwań nadzoru co do praktyk stosowanych przez banki. W zakresie bezpieczeństwa sieci teleinformatycznych KNF skierowała do banków dwie istotne rekomendacje. Pierwsza to Rekomendacja D z 2013 roku dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach[3]. Zastąpiła ona poprzednią rekomendację wydaną w tym zakresie w 2002 roku[4]. KNF określa w niej swoje oczekiwania względem banków co do działań odnoszących się m.in. do strategii i organizacji obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz zarządzania bezpieczeństwem środowiska teleinformatycznego. Treść rekomendacji dostępna jest na stronie internetowej KNF: www.knf.gov.pl. Drugi dokument odnoszący się do bezpieczeństwa w bankowości to Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje

[3] Dz. Urz. KNF z 2013 r., poz. 5;
Rekomendacja D stanowi załącznik do uchwały Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

[4] Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki wydana przez Komisję Nadzoru Bankowego w formie uchwały z dnia 11 grudnia 2002 r.

płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, która została wydana w listopadzie 2015 roku[5]. Dotyka ona przede wszystkim istoty ryzyk związanych z płatnościami internetowymi. Szczególny nacisk został położony na bezpieczeństwo danych służących do autoryzacji (potwierdzania) operacji wykonywanych w bankowości elektronicznej oraz bezpieczeństwo kart płatniczych wydawanych przez banki.

W wymiarze bardziej praktycznym relacje pomiędzy klientem a bankiem reguluje ustawa o usługach płatniczych. Z uwagi na tematykę niniejszej publikacji warto zwrócić uwagę na zapisy dotyczące korzystania z instrumentów płatniczych, jakimi są powszechnie używane karty płatnicze. Zgodnie z art. 42. ust. 1. Ustawy o usługach płatniczych, *użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany:*
1) korzystać z instrumentu płatniczego zgodnie z umową ramową oraz
2) zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.

Jak wynika z powyższego, ustawa o usługach płatniczych wskazuje umowę jako dokument szczegółowo regulujący prawa i obowiązki obu stron. Nakłada na klienta także obowiązek niezwłocznego poinformowania banku w przypadku utraty lub wykorzystania karty bez zgody jej posiadacza. Jest to o tyle istotne, że ust. 2 art. 42 jednoznacznie wskazuje, że użytkownik *podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym*. Jeśli zatem użytkownik nie zastosuje się do przepisów ustawy, bank – w wyniku zdarzenia utraty środków na rachunku – może rozpatrzyć reklamację negatywnie.

W takich przypadkach kluczowe są okoliczności, w jakich doszło do kradzieży środków, czyli do nieuprawnionego (bez naszej zgody) posłużenia się kartą.

[5] Dz. Urz. KNF z 2015 r., poz. 56;
Rekomendacja stanowi załącznik do uchwały Nr 584/2015 Komisji Nadzoru Finansowego z dnia 17 listopada 2015 r. w sprawie wydania Rekomendacji dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe.

Artykuł 45. ust. 1. ustawy o usługach płatniczych nakłada na bank obowiązek udowodnienia, *że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo*. Ponadto w ust. 2 ustawodawca wskazuje, że to bank jest *obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42*.

Dlatego istotne jest, by zawsze, gdy dojdzie do zdarzenia, w wyniku którego z rachunku bankowego znikną środki bez zgody klienta, niezwłocznie ten fakt zgłosić do banku. Banki zawsze indywidualnie badają okoliczności, w jakich doszło do ewentualnego przestępstwa i na tej podstawie podejmują decyzje o przywróceniu środków na rachunek klienta lub nieuznania reklamacji w przypadku, gdy klient sam nie dochował podstawowych zasad bezpieczeństwa.

UJĘCIE PRAKTYCZNE

3. BANKOWOŚĆ ELEKTRONICZNA NA CO DZIEŃ – WYGODA CZY RYZYKO?

Korzystanie z bankowości elektronicznej jest bardzo wygodne i oszczędza jej użytkownikom wiele czasu. Trzeba jednak mieć świadomość, że czynności, które wykonujemy w panelu bankowym przez Internet, nie zawsze nas prowadzą do zamierzonego celu. Zdarzyć się może, że środki, które chcemy przelać operatorowi komórkowemu za abonament lub za zakup biletów na koncert, trafią do zupełnie innego adresata, często nie z naszej winy – bądź też w wyniku niezachowania należytej staranności. Okazuje się bowiem, że w wielu przypadkach użytkownicy nie mają świadomości, że mogli stać się ofiarami cyberprzestępstwa.

Z badań, które przeprowadził ośrodek TNS Polska na zlecenie Komisji Nadzoru Finansowego wynika, że ponad 90 proc. użytkowników bankowości elek-

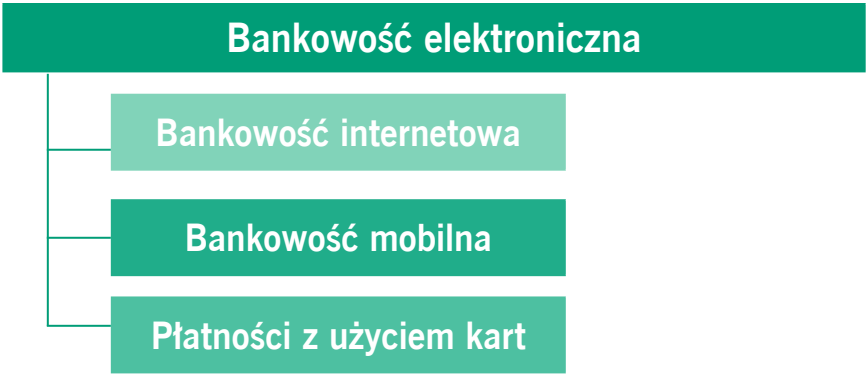
tronicznej nigdy nie spotkało się bezpośrednio z cyberatakiem[6]. Z pozoru taki wynik może zadowalać. W rzeczywistości jednak może okazać się, że część z nas nie ma świadomości, że taki atak (lub próba ataku) został przeprowadzony. Owo przeświadczenie przekłada się na poczucie bezpieczeństwa w korzystaniu z bankowości elektronicznej. Będąc przekonanym, że nie grozi nam żadne ryzyko, nie jesteśmy już tak czujni i nie wykonujemy prostych czynności, które mogłyby zwiększyć poziom bezpieczeństwa naszych środków w bankowości elektronicznej lub wyeliminować potencjalne próby dokonania cyberataku. A te mają miejsce i w kolejnych latach będzie ich przybywać. Tak jak bowiem w latach 90-tych w większym stopniu byliśmy narażeni na działalność kieszonkowców na ulicy lub w środkach komunikacji miejskiej, tak dziś jesteśmy narażeni na podobnych kieszonkowców, ale w wirtualnym świecie.

Cyberataki mają dwojaki charakter. Jeden strumień działań cyberprzestępców jest ukierunkowany na infrastrukturę banków, czyli na ich serwery i szeroko pojęte systemy teleinformatyczne. Banki są zobowiązane przepisami prawa i rekomendacjami Komisji Nadzoru Finansowego do utrzymywania poziomu bezpieczeństwa swojej infrastruktury na odpowiednio wysokim poziomie. Nikt jednak nie może w pełni zagwarantować bezpieczeństwa naszych środków, ponieważ wraz z rozwojem technologii zmieniają się także metody, którymi posługują się cyberprzestępcy. Na tego typu działania klienci banków nie mają większego wpływu, dlatego w przypadkach, gdy tracimy środki finansowe w wyniku ataku na infrastrukturę bankową, co do zasady reklamacje są uwzględniane. Musimy jednak zdawać sobie sprawę, że istnieje jeszcze drugi strumień cyberataków, który ukierunkowany jest na infrastrukturę klientów, czyli na nasze komputery i urządzenia przenośne. Te ataki zwykle są skuteczniejsze, ponieważ nam, jako klientom, trudniej jest zabezpieczyć tego rodzaju sprzęt elektroniczny w stopniu, w jakim robią to banki. Dlatego istotne jest, by wykonywać proste czynności, które mogą ograniczyć ryzyko dokonania cyberataku, a w konsekwencji zwiększyć bezpieczeństwo naszych środków finansowych.

Zanim jednak poznamy sposoby zabezpieczania się przed cyberatakami, na następnych stronach prześledzimy różnego rodzaju metody działań cyberprzestępców w podziale na trzy obszary.

[6] Źródło: https://www.knf.gov.pl/Images/KNF_badanie_14012016_tcm75-44164.pdf, data dostępu: 2 marca 2016 r.

4. GŁÓWNE OBSZARY BANKOWOŚCI ELEKTRONICZNEJ



Rys. 1. Główne obszary bankowości elektronicznej
Źródło: opracowanie własne

Głównym obszarem bankowości elektronicznej jest **bankowość internetowa**, przez którą należy rozumieć kanał elektroniczny, z którego użytkownicy korzystają przy użyciu komputera lub urządzenia mobilnego. Powszechność wykorzystania komputerów w bankowości elektronicznej potwierdzają badania Komisji Nadzoru Finansowego. Aż 79 proc. jej użytkowników deklaruje, że korzysta z komputera przenośnego (laptopa), a 28 proc. z komputera stacjonarnego[7].

Częścią bankowości elektronicznej jest także **bankowość mobilna**. W tym kanale użytkownicy dokonują operacji bankowych z wykorzystaniem aplikacji zainstalowanych w urządzeniach mobilnych. Około 21 proc. badanych deklaruje, że w bankowości elektronicznej korzysta ze smartfona, a 5 proc. wskazuje na tablet[8].

Obszarem, który uzupełnia ww. rodzaje bankowości elektronicznej są **płatności z użyciem kart**, których formy mnożą się i rozwijają niezwykle dynamicznie. Jedną z tych form są płatności zbliżeniowe z wykorzystaniem technologii

[7] Źródło: https://www.knf.gov.pl/Images/KNF_badanie_14012016_tcm75-44164.pdf, data dostępu: 2 marca 2016 r.
[8] Ibidem.

NFC (ang. Near Field Communication – Komunikacja Bliskiego Zasięgu), która umożliwia dokonywanie płatności do określonej kwoty bez podawania numeru PIN. Realizacja płatności zbliżeniowych nie jest ograniczona jedynie do transakcji płatniczych dokonywanych przy użyciu kart płatniczych, lecz znajduje również zastosowanie w bankowości mobilnej opartej na wykorzystaniu urządzeń mobilnych, w szczególności takich jak telefony komórkowe. Realizacja transakcji odbywa się wówczas za pośrednictwem aplikacji zainstalowanej w pamięci telefonu komórkowego, komunikującej się z tzw. bezpiecznym elementem zawierającym dane karty płatniczej klienta.

Jednak wszystkie możliwości korzystania z bankowości elektronicznej są obarczone pewnymi ryzykami, które zostały scharakteryzowane poniżej. Warto jednak pamiętać, że wymienione poniżej opisy mają charakter przykładowy, ponieważ wraz z rozwojem bankowości elektronicznej stale pojawiają się nowe typy zagrożeń.

BANKOWOŚĆ INTERNETOWA	
Phishing danych	To jedna z popularniejszych metod przeprowadzania cyberataku. Polega na pozyskaniu (przechwyceniu) danych osobowych lub danych do logowania do panelu bankowego, które następnie będą wykorzystane w celu dokonania operacji płatniczej w serwisie transakcyjnym lub skorzystania z produktu bankowego, posługując się naszą tożsamością (np. zaciągnięcie zobowiązania w formie pożyczki lub kredytu).
Pośrednictwo podmiotów trzecich	Odrębnym przypadkiem wyłudzania danych osobowych jest dokonywanie płatności za zakupy przez Internet z wykorzystaniem pośrednika, który nie przekierowuje klienta do panelu bankowego, w którym wykonuje się przelew, ale pozostawia użytkownika w swoim interfejsie, jednocześnie gromadząc jego dane do logowania w banku i wykonując operację przelewu we własnym zakresie. Takie działanie jest rozumiane jako udostępnienie danych do logowania osobom trzecim, w konsekwencji czego bank może rozpatrzyć negatywnie ewentualną reklamację.

Złośliwe oprogramowanie

Cyberprzestępca może zainfekować komputer poprzez korespondencję e-mail, podając się za bank i przesyłając zawirusowany załącznik lub załączając w korespondencji link, który przekierowuje użytkownika do fałszywej strony internetowej. W ten sposób instaluje złośliwe oprogramowanie, które następnie przechwytuje dane do logowania w panelu bankowym lub zmienia parametry operacji wykonywanych przez użytkowników, np. podmieniając cyfry w numerach rachunków przy ich kopiowaniu w okienku przelewu. **Uwaga! Złośliwe oprogramowanie nie zawsze uaktywnia się tuż po instalacji, czasem następuje to nawet po kilku tygodniach.**

Oszustwa przy zakupach przez Internet

Wraz ze wzrostem zainteresowania zakupami internetowymi zwiększa się częstotliwość przypadków oszustw, które zdarzają się w tym obszarze. Najczęściej dochodzi do nich poprzez ograniczenie przez nieuczciwego sprzedawcę metod płatności jedynie do formy przelewu bankowego. Wówczas sprzedawca przekazuje fałszywy numer rachunku do opłaty za zakupiony towar, a kupujący dowiaduje się o oszustwie z kilkudniowym opóźnieniem, gdy przedmiot zakupu nie zostaje dostarczony.

Oszustwa nigeryjskie

To metoda, którą dość łatwo można rozpoznać z uwagi na automatyczny charakter generowania korespondencji z użytkownikiem. Użytkownik otrzymuje wiadomość e-mail, której treść przypomina automatyczne tłumaczenie z języka obcego (nieskładna pisownia w jęz. polskim) i w której cyberprzestępca prosi o podanie danych niezbędnych do dokonania przelewu środków finansowych, np. w zamian za towar lub usługę (może to nosić znamiona prania pieniędzy) albo prosi o przelanie środków na numer rachunku osoby pochodzącej z odległego kraju, najczęściej afrykańskiego. Tego typu korespondencję dość często można otrzymać po wystawieniu przedmiotu na aukcji internetowej, ponieważ złośliwy robot automatycznie rozsyła ją do wielu użytkowników, którzy z takich platform korzystają.

Przejęcie kontroli nad urządzeniem	Z uwagi na dynamicznie rosnącą liczbę użytkowników bankowości mobilnej, korzystających z sieci Internet, coraz częściej można spotkać się z próbą przejęcia kontroli nad urządzeniem mobilnym, np. telefonem lub tabletem. Odbywa się to np. poprzez wysłanie drogą SMS lub e-mail odnośnika do strony internetowej, z której przeglądarka pobiera złośliwe oprogramowanie. Wirus przejmuje wówczas dane dostępowe do aplikacji służącej do logowania do panelu bankowego oraz uzyskuje kontrolę nad otrzymywanymi wiadomościami SMS, w których bank przesyła kod autoryzujący transakcję. Taka wiadomość bez wiedzy użytkownika może zostać przekierowana na inny numer rachunku. Dlatego ważne jest, by korzystając z bankowości elektronicznej, wykonywać przelewy na innym urządzeniu niż to, na które przesyłany jest kod autoryzujący transakcję.

BANKOWOŚĆ MOBILNA

Utrata urządzenia mobilnego	Jeśli w telefonie użytkownik ma zainstalowaną aplikację do bankowości elektronicznej, to jego utrata może być tak samo dotkliwa, jak utrata portfela z kartami płatniczymi. Dlatego ważne jest, by nie zapisywać haseł dostępowych do aplikacji mobilnych w notatnikach i innych aplikacjach. Jeśli już dojdzie do utraty urządzenia z nienależytym zabezpieczeniem aplikacji do bankowości elektronicznej, należy niezwłocznie o tym fakcie poinformować bank.
Nieuprawniona wymiana danych między urządzeniami	Technologia NFC, która umożliwia wymianę danych między urządzeniami wyposażonymi w specjalne chipy elektroniczne, może służyć do przechwycenia danych w nieuprawniony sposób przez osoby trzecie. Odbywa się to poprzez odczyt danych w technologii NFC przy użyciu specjalnego urządzenia znajdującego się w pobliżu lub w wyniku przechwycenia sygnału przepływającego między urządzeniami przez inne urządzenie. W takich sytuacjach haker może przechwycić sygnał między telefonem a czytnikiem kart płatniczych lub między dwoma telefonami i w ten sposób uzyskać dostęp do danych z karty kredytowej.

Kradzież danych przez skanowanie tagów NFC	Kradzież danych w technologii NFC może odbyć się też poprzez skanowanie tzw. tagów, czyli chipów umieszczanych w miejscach publicznych, np. na ulicznych wystawach, zapewniających szybki dostęp do pożądanej informacji. Niektóre tagi mogą być przeprogramowane przez hakera, przez co po zeskanowaniu kodu cyberprzestępca może pozyskać dane z telefonu lub zainstalować na nim złośliwe oprogramowanie, przejmując tym samym kontrolę nad urządzeniem.
PŁATNOŚCI Z UŻYCIEM KART	
Skimming	To innymi słowy kopiowanie kart płatniczych. To ryzyko najczęściej towarzyszy wypłacaniu pieniędzy z bankomatów. Przestępcy montują na bankomacie przy otworze na karty specjalną nakładkę, która skanuje zawartość paska magnetycznego karty, a następnie dane te umieszczają na innej karcie lub plastiku z paskiem magnetycznym, niejednokrotnie nawet w innej części świata, ponieważ dane te można przekazać drogą elektroniczną. Poza nakładką przy otworze instalowana jest też nakładka na klawiaturze, która umożliwia odczytanie numeru PIN.
Odczyt danych z karty zbliżeniowej	Posługując się kartą z funkcją zbliżeniową, trzeba mieć świadomość ryzyka, jakie niesie za sobą zdalny odczyt danych z karty za pośrednictwem specjalnego interfejsu zbliżeniowego. Jest to proces zbliżony do skimmingu, w tym przypadku jednak przestępca poprzez instalację fałszywej nakładki zbliżeniowej nie kopiuje karty, ale pobiera z niej dane, które następnie mogą mu posłużyć do wykonania płatności przez Internet.

Nieuprawnione wykorzystanie karty zbliżeniowej

Posługiwanie się kartą płatniczą z funkcją zbliżeniową jest bezpieczniejsze niż sczytywanie danych z paska magnetycznego lub chipa na karcie w terminalu, ponieważ zachowujemy cały czas kontakt z kartą (czasem zdarza się, że sprzedawca bierze kartę, by włożyć ją do terminala, a my na chwilę tracimy ją z oczu). Trzeba jednak mieć świadomość, że utrata karty (kradzież kieszonkowa) może skutkować w bardzo szybkim czasie stratą nawet kilkuset złotych, ponieważ płatności zbliżeniowe do kwoty 50 zł zazwyczaj nie wymagają potwierdzenia numerem PIN. Dopiero następna w kolejności operacja, np. piąta, takiego potwierdzenia wymaga. To szczególnie istotne w przypadkach kradzieży zbliżeniowych, nawet gdy nie rozstajemy się z naszą kartą. Przestępcy bowiem mogą wejść w posiadanie terminali, które sczytują dane z karty na odległość. W ten sposób, jadąc środkiem komunikacji miejskiej i trzymając kartę np. w kieszeni, wystarczy, że przestępca zbliży niepostrzeżenie urządzenie do naszej kieszeni i pobierze tym samym środki z karty do wysokości kwoty, która nie wymaga potwierdzenia kodem PIN.

Wyłudzenie danych z kart kredytowych

Karty kredytowe często służą użytkownikom bankowości elektronicznej do wykonywania płatności za zakupy w Internecie. Kluczową daną na karcie kredytowej jest tzw. kod CVC lub CVV, czyli trzycyfrowy numer zabezpieczający, który jest elementem weryfikującym transakcję za pomocą karty. Jeśli ten kod zostanie utracony, a dodatkowo użytkownik poda numer karty kredytowej i datę jej ważności, osoba posiadająca te dane będzie mogła posłużyć się kartą, nawet nie będąc w jej fizycznym posiadaniu. Dlatego istotne jest, by nikomu tych danych nie udostępniać, także przez telefon. Jeśli bank lub sprzedawca kiedykolwiek poprosi nas przez telefon o te dane, to możemy mieć pewność, że mamy do czynienia z przestępcą.

5. BEZPIECZEŃSTWO W SIECI – ZADBAJ O NIE W KILKU KROKACH

Korzystając z bankowości elektronicznej trzeba mieć świadomość, że nie da się wyeliminować w pełni wszystkich wyżej opisanych ryzyk. Można jednak wykonać szereg prostych czynności, które mogą zwiększyć bezpieczeństwo w korzystaniu z tego kanału bankowego.

Trzeba pamiętać, że bezpieczeństwo środków finansowych gromadzonych na rachunkach bankowych zależy także od nas. Jak o nie zadbać?

- **Nie udostępniaj nikomu loginu i hasła do systemu bankowości elektronicznej. Nie zapisuj loginu i hasła na dysku komputera, dysku sieciowym, w pamięci telefonu komórkowego lub karty SIM, ani w żaden inny sposób.** Utrata tak ważnych danych dostępowych do rachunku bankowego może skutkować odmową uwzględnienia reklamacji przez bank w przypadku utraty środków finansowych.

- **Cyklicznie zmieniaj hasło do logowania w systemie bankowości elektronicznej.** Cyberprzestępca nie zawsze włamuje się na rachunek z chwilą przejęcia hasła. Zmieniając je co kilka tygodni, możesz zminimalizować ryzyko cyberataku. Przy tworzeniu hasła pamiętaj, by było odpowiednio długie, składające się z wielkich i małych liter, cyfr i znaków specjalnych. Unikaj skojarzeń z imieniem, nazwiskiem, miejscem zamieszkania lub datą urodzenia.

- **Nie otwieraj podejrzanych linków do stron internetowych w otrzymanych wiadomościach e-mail i SMS.** Mogą one przekierować Cię do fałszywego serwisu bankowego, łudząco przypominającego stronę internetową Twojego banku lub też spowodować zainstalowanie złośliwego oprogramowania na komputerze, lub urządzeniu mobilnym.

- **Zainstaluj i aktualizuj oprogramowanie antywirusowe, które może uchronić komputer i urządzenia mobilne przed wirusami oraz oprogramowaniem szpiegującym.** Pamiętaj, by oprogramowanie pochodziło z legalnego i zaufanego źródła. To ważne, zwłaszcza gdy dojdzie już do

cyberataku. Bank może wziąć te okoliczności pod uwagę przy uwzględnianiu ewentualnej reklamacji.

- **Na bieżąco aktualizuj system operacyjny oraz przeglądarkę internetową w komputerze lub telefonie, a także cyklicznie skanuj każde urządzenie programem antywirusowym.** Złośliwe oprogramowanie często uaktywnia się po jakimś czasie od zainfekowania sprzętu. Skanując urządzenie, możesz uchronić komputer lub urządzenie mobilne przed uaktywnieniem się wirusa.

- **W trakcie logowania upewnij się, czy zostałeś przekierowany do właściwej witryny, zapewniającej połączenie zabezpieczone kryptograficznie.** Adres internetowy widoczny w oknie przeglądarki powinien zaczynać się od „https://www...", a w oknie przeglądarki powinna pojawić się ikona zamkniętej kłódki.

- **Cyklicznie sprawdzaj, czy numery rachunków bankowych w przelewach zdefiniowanych nie uległy podmianie.** Na początku możesz nie mieć świadomości, że wykonujesz przelew środków na zupełnie inne konto. Zwykle dowiadujesz się o tym z chwilą, gdy przychodzi informacja o zaległości w zapłacie.

- **Nie kopiuj numerów rachunków bankowych do przelewów na zasadzie operacji** kopiuj-wklej**.** Złośliwe oprogramowanie może podmienić kilka cyfr, co spowoduje wykonanie przelewu na inny rachunek. Najbezpieczniej jest, gdy wpisujesz numer rachunku samodzielnie i dokładnie go weryfikujesz przy potwierdzeniu wykonania operacji.

- **Przed potwierdzeniem transakcji dla pewności zawsze weryfikuj zgodność numeru konta, na które przelewasz środki pieniężne, z numerem odbiorcy.** Bank nie ma obowiązku weryfikacji numeru rachunku z danymi jego właściciela.

- **Na bieżąco przeglądaj historię rachunku i operacji na każdej karcie płatniczej pod kątem podejrzanych transakcji.** Możesz nie mieć świadomości, że ktoś przelewa z Twojego konta drobne kwoty, których na

co dzień nie zauważasz. Jeżeli jest to możliwe, to włącz powiadomienia SMS o każdej wykonywanej transakcji.

- **Ustal odpowiednie do Twoich potrzeb limity operacji dla przelewów i kart płatniczych.** Zbyt wysokie limity ułatwiają przestępcom wyprowadzanie znacznych środków z rachunku.

- **Weryfikuj kody SMS.** Pamiętaj, żeby przed potwierdzeniem operacji dokładnie przeczytać wiadomość z kodem i upewnić się, czy kwota operacji i numer rachunku odbiorcy są zgodne ze zleceniem przelewu.

- **Nie korzystaj z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń, np. publicznej sieci WiFi.** Atak za ich pośrednictwem jest znacznie bardziej prawdopodobny niż w przypadku prywatnych sieci.

- **Korzystaj z własnego sprzętu i nie udostępniaj go osobom trzecim.** Logując się do swojego konta bankowego unikaj także korzystania z obcego sprzętu lub z komputerów dostępnych publicznie. Jeśli musisz przekazać urządzenia np. do serwisu, wyloguj się ze wszystkich aplikacji służących do obsługi bankowości elektronicznej. Pamiętaj, by usunąć SMS-y od banku i historię przeglądarki, która może zawierać informacje poufne.

- **Dbaj o „higienę" swoich zachowań w Internecie.** Nie odwiedzaj niezaufanych stron i nie ściągaj programów z nieznanych źródeł. Rejestrując się w różnych serwisach, nigdy nie stosuj tych samych danych uwierzytelniających, których używasz do swojego konta bankowego.

Jeżeli zaobserwujesz nietypowe lub podejrzane działania, niezwłocznie zgłoś ten fakt do banku, z którego usług korzystasz w ramach bankowości elektronicznej.

PRZYKŁADY

6. ANALIZA WYBRANYCH ZAGROŻEŃ NA PODSTAWIE OPISANYCH PRZYPADKÓW

Przykład 1.
Wystawiłeś przedmiot na aukcji internetowej. Kilka godzin później otrzymujesz wiadomość e-mail o poniższej treści (pisownia oryginalna):
„Zaplace 2400+300 zl kosztów wysylki poprzez EMS Pocztex. Proszesprawdzic tutaj koszty wysylki: (http://www.pocztex.pl/ems/cennik/) do Londyny w Wielkiej Brytanii . Proszezakonczyc aukcje na allegro i podeslac do mnie pelne dane bankowe do wykonania przelewu. Potrzebuje:
Numer Konta:
Nazwa banku:
Numer Telefonu:
Przelew wykonam jak najszybciej. Czekam na szybka odpowiedz.
pozdrawiam serdecznie"

To tzw. oszustwo nigeryjskie. Przestępca kontaktuje się z daną osobą w celu przetransferowania środków finansowych na wskazany w odpowiedzi numer rachunku lub dokonania próby zainfekowania komputera wirusem. Numer rachunku będzie potrzebny przestępcy do przejęcia kontroli nad rachunkiem bankowym, a numer telefonu do ewentualnego przechwycenia kodu autoryzującego transakcję. Na tego typu wiadomości nie należy odpisywać, a w określonych przypadkach warto je zgłaszać na policję.

Przykład 2.
Przeglądasz ogłoszenia o pracę. Na jednym z portali znajdujesz informację o rekrutacji osób do pracy zdalnej. Wymagane jest tylko posiadanie rachunku bankowego, ponieważ praca związana będzie z wykonywaniem przelewów. W odpowiedzi na ogłoszenie należy wysłać swoje CV z danymi osobowymi i numerem dowodu osobistego, a najlepiej z jego skanem. Po dwóch dniach potencjalny przyszły pracodawca informuje o zakwalifikowaniu się do kolejnego etapu rekrutacji, ale, z uwagi na konieczność potwierdzenia posiadania rachunku bankowego, prosi o wykonanie przelewu o wartości 1 zł na

wskazany numer rachunku. Po kilku dniach kandydat jest informowany, że proces rekrutacji zakończył się i, niestety, zdecydowano się na innego kandydata. Po upływie trzech miesięcy dostajesz wezwanie do zapłaty z tytułu niespłaconej w terminie raty kredytu. Problem polega na tym, że nie brałeś żadnego kredytu.

To klasyczny przykład tzw. phishingu danych. Cyberprzestępca pod pozorem oferty pracy wyłudza dane osobowe (dane z CV i skan dowodu osobistego), na podstawie których zakłada przez Internet rachunek bankowy. Ponieważ bank wymaga potwierdzenia danych osobowych w formie przelewu o wartości 1 zł, cyberprzestępca prosi o wykonanie przelewu na nowo założony rachunek. W ten sposób nieświadomie potwierdza się własnymi danymi założenie rachunku. Przestępca dysponując takim rachunkiem bankowym, może zaciągnąć zobowiązanie w banku lub złożyć wniosek o wydanie karty kredytowej.

Dodatkowe informacje znajdują się w następujących materiałach edukacyjnych, dostępnych pod adresem www.knf.gov.pl:

- *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, M. Górnisiewicz, R. Obczyński, M. Pstruś, publikacja edukacyjna wydana nakładem KNF w 2014 r.,
- *Scenariusze lekcji z zakresu rynku finansowego z zadaniami matematycznymi i logicznymi z odpowiedziami dla szkół gimnazjalnych i ponadgimnazjalnych*, praca zbiorowa, publikacja edukacyjna wydana nakładem KNF w 2015 r.,
- *Scenariusze lekcji z zakresu rynku finansowego dla szkół podstawowych i ponadgimnazjalnych*, A. Cichy, E. Kęsik, W. Wyszyński, publikacja edukacyjna wydana nakładem KNF w 2015 r.,
- *Użytkowanie kart płatniczych – prawa, obowiązki, bezpieczeństwo*, K. Wójcicka,
- *Karty płatnicze w Polsce*, K. Wójcicka,
- *Bezpieczne bankowanie cz. 1 – wybór oferty rachunku, kredytu, karty*, E. Kotowicz,
- *Bezpieczne bankowanie cz. 2 – bezpieczeństwo w bankowości elektronicznej i internetowej, bezpieczne korzystanie z bankomatu*, E. Kotowicz,
- *Jaką kartę chcesz mieć w portfelu?*, A. Cichy, E. Kęsik.

7. TEST WIEDZY

Przeczytaj uważnie pytania i wybierz tylko jedną spośród zaproponowanych odpowiedzi.

1. Który dokument szczegółowo reguluje relacje między bankiem a klientem?

a) ustawa Prawo bankowe,
b) umowa zawarta między stronami,
c) ustawa o usługach płatniczych.

2. Wyłudzanie danych osobowych celem kradzieży środków na rachunku lub wygenerowania zadłużenia to:

a) oszustwo nigeryjskie,
b) skimming,
c) phishing danych.

3. Pierwszym przejawem bankowości elektronicznej w Polsce były:

a) konta internetowe,
b) bankomaty,
c) infolinie bankowe.

4. Jak zminimalizować ryzyko przeprowadzenia cyberataku?

a) cyklicznie zmieniać bank,
b) cyklicznie zmieniać komputer,
c) cyklicznie zmieniać hasło do panelu bankowego.

5. Przy wykonywaniu przelewów przez Internet można zwiększyć bezpieczeństwo poprzez:

a) wykorzystanie dwóch różnych urządzeń: na jednym wykonywany jest przelew, na drugim autoryzacja,
b) wykonanie kilku przelewów o mniejszych sumach, zamiast jednego na dużą kwotę,
c) anulowanie opcji potwierdzania transakcji w formie SMS.

6. W przypadku utraty karty płatniczej należy w pierwszej kolejności:
a) zgłosić się na policję,
b) niezwłocznie zawiadomić o tym fakcie bank,
c) dokończyć zakupy, karta jest zabezpieczona kodem PIN.

7. Jak należy zachować się, jeśli pracownik banku prosi przez telefon o podanie hasła do bankowości internetowej?
a) udostępnić dane, w końcu to pracownik banku,
b) udostępnić dane, ale tylko poprzez e-mail, żeby został po tym ślad,
c) rozłączyć się, bo bank nigdy o te dane nie poprosi.

8. Jak najbezpieczniej wykonać przelew w bankowości internetowej?
a) kopiując numer rachunku do formularza,
b) wpisując ręcznie numer rachunku odbiorcy,
c) korzystając z przelewu zdefiniowanego.

Odpowiedzi:
1. b) / 2. c) / 3. b) / 4. c) / 5. a) / 6. b) / 7. c) / 8. b)

SŁOWNIK POJĘĆ

Autoryzacja – zgoda na wykonanie działania. Jej celem jest weryfikacja woli posiadacza rachunku co do wykonania danej operacji w bankowości elektronicznej. Autoryzacja może mieć formę np. wpisania kodu PIN lub hasła z listy haseł jednorazowych lub z otrzymanej wiadomości SMS.

Bank – instytucja pośrednicząca w obiegu pieniądza, utworzona zgodnie z przepisami ustaw, działająca na podstawie zezwoleń uprawniających do wykonywania czynności bankowych, wydanych w formie decyzji administracyjnych przez organ nadzoru.

Bankowość elektroniczna – kanał elektroniczny w bankowości, z którego użytkownicy korzystają przy użyciu urządzeń elektronicznych, np. telefonu, komputera, bankomatu lub karty płatniczej. Najpopularniejszą formą bankowości elektronicznej jest bankowość internetowa, umożliwiająca wykonywanie czynności bankowych przez Internet.

Cyberatak (cyberprzestępstwo) – forma przestępstwa w bankowości elektronicznej, mająca na celu kradzież środków finansowych z rachunku. Przestępstw tych dokonuje się z wykorzystaniem urządzeń elektronicznych i/lub poprzez uzyskanie danych dostępowych do rachunku bankowego w Internecie.

Dane uwierzytelniające – dane służące do identyfikacji użytkownika lub weryfikacji dostępu do rachunku w bankowości elektronicznej, np. login i hasło do panelu logowania. Danymi uwierzytelniającymi mogą być też dane osobowe lub inne dane wrażliwe, np. nazwisko panieńskie matki lub miejsce urodzenia etc.

Fotoprzelew – metoda realizacji przelewu polegająca na zeskanowaniu kodu QR z faktury w celu otrzymania w aplikacji mobilnej gotowego formularza przelewu z właściwą kwotą i danymi odbiorcy.

HCE (ang. host cardemulation) – technologia wykorzystywana na rynku płatności mobilnych, dzięki której bezpieczny element zawierający dane karty płatniczej jest zapisywany w chmurze. Dzięki temu rozwiązaniu użytkownik smartfona wyposażonego w technologię NFC może wykonać bezstykowo operację płatniczą bez uzyskiwania specjalnej karty SIM od operatora telefonii komórkowej (co często wiąże się z zawarciem umowy na świadczenie usług telekomunikacyjnych).

Informacje poufne – dane, które powinny być znane wyłącznie ich adresatowi (użytkownikowi bankowości), np. login i hasło do panelu logowania. Informacje poufne nigdy nie powinny być udostępniane osobom trzecim.

Karta zbliżeniowa – instrument płatniczy umożliwiający dokonywanie transakcji płatniczych poprzez przyłożenie do terminala płatniczego. W Polsce do kwoty 50 zł nie jest zazwyczaj wymagane potwierdzanie płatności za pomocą kodu PIN.

Komisja Nadzoru Finansowego (KNF) – państwowy organ nadzoru, sprawujący nadzór nad rynkiem finansowym, który obejmuje: nadzór bankowy, nadzór emerytalny, nadzór ubezpieczeniowy, nadzór nad rynkiem kapitałowym, nadzór nad instytucjami płatniczymi, biurami usług płatniczych, instytucjami pieniądza elektronicznego, oddziałami zagranicznych instytucji pieniądza elektronicznego, nadzór nad agencjami ratingowymi, nadzór uzupełniający nad konglomeratami finansowymi, a także nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową. Celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku.

NFC (ang. nearfield communication) – technologia umożliwiająca bezprzewodową łączność między urządzeniami i wymianę danych pomiędzy nimi. Często stosowana przy dokonywaniu bezstykowych płatności zbliżeniowych, niewymagających podawania numeru PIN.

Phishing – jedna z metod cyberataku, polegająca na pozyskaniu (przechwyceniu) danych osobowych lub danych do logowania do panelu bankowego,

które następnie mogą być wykorzystane w celu dokonania operacji płatniczej w serwisie transakcyjnym lub innej operacji z użyciem pozyskanych danych.

PIN – indywidualny numer identyfikacyjny służący do autoryzacji transakcji płatniczych. Użytkownik może w każdej chwili go zmienić i ustanowić nowy.

Płatność zbliżeniowa – realizacja transakcji poprzez przyłożenie do czytnika terminala płatniczego karty płatniczej lub urządzenia mobilnego, wyposażonego w bezpieczny element zawierający dane z karty płatniczej. Dokonując płatności zbliżeniowej do wartości nieprzekraczającej 50 zł, podanie kodu PIN nie jest wymagane każdorazowo, a jedynie co kilka losowych operacji.

Posiadacz rachunku – klient banku, który zawiera umowę z bankiem o prowadzenie rachunku. Umowa określa prawa i obowiązki obu stron.

Skimming – kopiowanie kart płatniczych, najczęściej poprzez instalowanie specjalnych nakładek na bankomatach, które sczytują dane z karty i przesyłają je do przestępcy.

System teleinformatyczny – zespół urządzeń i łączy transmisyjnych, obejmujący głównie sprzęt (np. serwery, macierze, stacje robocze), sieć teleinformatyczną (np. routery, przełączniki, zapory sieciowe), oprogramowanie systemowe oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów banku.

Urządzenia mobilne – sprzęt elektroniczny, przy pomocy którego dokonywane są płatności w bankowości elektronicznej, np. komputer przenośny, telefon komórkowy, tablet etc.

WiFi – sieć lokalna, która umożliwia połączenie się z Internetem. Korzystanie z publicznej sieci WiFi jest bardziej ryzykowne niż z prywatnej z uwagi na powszechność jej dostępu (często nie jest wymagana nawet rejestracja użytkownika i wygenerowanie hasła).

Zabezpieczenie kryptograficzne – metoda ochrony danych lub dostępu do danych, zawierająca specjalne techniki szyfrowania, np. algorytmy, funkcje haszujące, protokoły, podpisy cyfrowe etc.

KNF | CEDUR
Centrum Edukacji dla Uczestników Rynku

Publikacja stanowi cenne kompendium wiedzy z obszaru bankowości elektronicznej. Poparta praktycznymi przykładami jest doskonałym uzupełnieniem i rozwinięciem treści zawartych w podstawach programowych Ministerstwa Edukacji Narodowej z wiedzy o społeczeństwie i podstaw przedsiębiorczości. Biorąc pod uwagę przydatność i uniwersalność poruszanych w niej zagadnień, publikacja może mieć też zastosowanie na godzinach wychowawczych, zajęciach dodatkowych oraz pośrednio na zajęciach informatycznych i matematycznych. Z uwagi na obszerne teoretyczne ujęcie zagadnienia może też stanowić pomoc uczniom w przygotowaniu się do olimpiady z przedsiębiorczości lub wiedzy ekonomicznej.

Z pewnością jest to wartościowa pomoc dydaktyczna dla nauczycieli poruszających z uczniami tematy świadomego, odpowiedzialnego korzystania z Internetu, urządzeń mobilnych i bankowości elektronicznej.

Grażyna Kurowska, Ośrodek Rozwoju Edukacji

Jolanta Grędzińska-Kosiorek, Warmińsko-Mazurski Ośrodek Doskonalenia Nauczycieli w Olsztynie - Filia w Olecku

Publikacja otrzymała rekomendację ORE Ośrodek Rozwoju Edukacji

Komisja Nadzoru Finansowego
Pl. Powstańców Warszawy 1
Skr. poczt. nr 419, 00-950 Warszawa 1
Tel. (+48) 22 262 50 00
Fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl

ISBN 978-83-63380-11-3