1 STYCZNIA 2017

BEZPIECZEŃSTWO W BANKOWOŚCI ELEKTRONICZNEJ

MATERIAŁY DYDAKTYCZNE DLA KLIENTA

BANKOWOŚĆ ELEKTRONICZNA
BANK SPÓŁDZIELCZY WE WŁOSZCZOWIE
Opracowano w oparciu o materiały Związku Banków Polskich

Spis treści

WSTĘP

Rozwój bankowości elektronicznej, w tym dynamicznie rozwijającej się bankowości internetowej, opartej na elektronicznym przetwarzaniu danych, pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności wymierzonej przeciwko bezpieczeństwu danych, zagrażających bezpieczeństwu finansowemu na rynku usług bankowych, w szczególności bezpieczeństwu środków zgromadzonych na rachunku bankowym, do których dostęp możliwy jest na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak komputer, telefon itp.

Nie ulega wątpliwości, że skala zagrożeń przestępczością w bankowości elektronicznej będzie wciąż rosła wraz z nieuniknionym, dalszym rozpowszechnianiem się usług bankowości elektronicznej, m.in. ze względu na coraz łatwiejszy do nich dostęp oraz atrakcyjność tych usług polegającą na wygodnym, niewymagającym osobistego udania się do banku, dostępie do środków zgromadzonych na rachunku bankowym, praktycznie nieograniczonym co do miejsca i czasu.

Nie można pominąć faktu, że na rozmiar przestępczości w elektronicznym obrocie bankowym ma również wpływ zachowanie indywidualnych uczestników rynku finansowego, którzy nie zawsze w dostatecznym stopniu są świadomi istniejących zagrożeń. Często nie posiadają też wiedzy o tym, jak mogą się przed nimi bronić.

Ważne było więc stworzenie opracowania, którego celem będzie wzrost świadomości uczestników rynku finansowego w sferze zagrożeń związanych z korzystaniem z bankowości elektronicznej oraz upowszechnienie wiedzy na temat zasad postępowania, których przestrzeganie w znacznym stopniu pozwoli ustrzec się przed nimi, a także przybliżenie problematyki dotyczącej istoty i specyfiki przestępstw związanych z bankowością elektroniczną.

CO ZAGRAŻA NASZEMU BEZPIECZEŃSTWU W BANKOWOŚCI ELEKTRONICZNEJ I JAK SIĘ PRZED TYM BRONIĆ?

Wyłudzenia danych pozwalających na przeprowadzenie transakcji

Przykład

Po ciężkim dniu spędzonym w pracy zmęczony Pan Robert w końcu wsiadł do samochodu i ruszył w kierunku domu. Nagle usłyszał dzwonek telefonicznego zestawu głośnomówiącego.

– Dzień dobry Panie Robercie. Dzwonię z pańskiego banku w związku z realizowanym przez nas projektem, którego celem jest znaczące podniesienie poziomu bezpieczeństwa naszych klientów oraz deponowanych przez nich środków pieniężnych. W celu potwierdzenia pańskiej tożsamości, uprzejmie proszę podać swój login do bankowości internetowej.

– Bardzo proszę: robkow123.

– Dziękuję. Proszę jeszcze podać pierwsze sześć znaków pańskiego hasła.

– „L", „u", „b", „i", „e", „K".

– Niestety, coś się nie zgadza. Proszę w takim razie podać sześć ostatnich znaków.

– Przepraszam, musiałem coś pomylić. Ostatnie sześć znaków to: „i", „e", „K", „o", „t", „y".

– Dziękuję, już wszystko się zgadza. Jednym z elementów naszego projektu jest przeniesienie funkcji potwierdzeń SMS na nowoczesne, super bezpieczne serwery. W związku z tym, w celu przełączenia pańskiego konta na nowy serwer, za chwilę prześlemy panu SMS testowy. Proszę sprawdzić, czy tytuł przelewu testowego w SMSie to „SMS testowy – bezpieczne transakcje".

– Tak, zgadza się.

– Czy kwota operacji to 10 000 PLN?

– Tak.

– Doskonale, wygląda na to, że wszystko działa poprawnie. Już tylko jeden krok dzieli pana od pełnego zabezpieczenia pańskiego konta. W celu ostatecznej weryfikacji, proszę jeszcze tylko o podanie ośmiocyfrowego kodu zawartego w SMSie.

– Proszę bardzo: 01021418.

– Dziękuję, operacja przebiegła poprawnie. Teraz może pan spać spokojnie. Jeszcze raz dziękuję za współpracę i życzę miłego wieczoru.

Nastrój Pana Roberta bardzo się poprawił. W końcu to miło, że jego bank sam z siebie dba o wzmacnianie poziomu bezpieczeństwa jego pieniędzy. Po powrocie do domu postanowił jeszcze sprawdzić, czy w związku z „przełączeniem jego konta na nowy serwer" uległ zmianie wygląd serwisu jego bankowości internetowej. Po zalogowaniu okazało się jednak, że jedyne, co uległo zmianie, to stan jego konta – zostało ono bowiem uszczuplone o 10 000 złotych.

Zapamiętaj!

Żaden bank nigdy, pod żadnym pozorem nie prosi o podawanie żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z kart-zdrapek ani przesyłanych SMSem itp.), czy to telefonicznie, czy poprzez pocztę elektroniczną, czy w jakikolwiek inny sposób – poza serwisem internetowym bankowości elektronicznej i udostępnianymi przez banki aplikacjami (np. instalowanymi na telefonach komórkowych).

Jest to podstawowa zasada bezpieczeństwa korzystania z bankowości internetowej, o której zawsze należy pamiętać. O ile bowiem opisana powyżej historia Pana Roberta może wydawać się stosunkowo naiwna, o tyle przestępcy potrafią wymyślać bardzo zróżnicowane i wyrafinowane metody wyłudzania tego rodzaju danych. Niekiedy są to np. wiadomości e-mail (również rzekomo przesyłane przez bank), w których potencjalne ofiary proszone są o wprowadzenie kilkudziesięciu kodów jednorazowych z kart-zdrapek. Innym sposobem często wykorzystywanym przez przestępców jest przesyłanie w wiadomościach e-mail linków rzekomo prowadzących do serwisów bankowości internetowej, a w praktyce będących stronami internetowymi na serwerach przestępców, które zwykle do złudzenia przypominają te serwisy.

Użytkownik wprowadzając na takiej stronie swoje dane logowania oraz dane autoryzacyjne płatności w praktyce przekazuje je przestępcom. Taki rodzaj przestępczej działalności często nazywany jest phishingiem. Warto tu również

zwrócić uwagę, że w celu zwiększenia skuteczności tego rodzaju działań przestępcy często stosują różnorodne metody manipulacji (co jest niekiedy nazywane socjotechniką lub inżynierią społeczną), takie jak informowanie ofiar o „jedynej, niepowtarzalnej okazji", która za chwilę ucieknie ofierze „sprzed nosa", czy też opisywanie swoich przestępczych działań jako nakierowanych właśnie na rzekome zwiększenie bezpieczeństwa ofiary.

Zapamiętaj!

W celu zabezpieczenia się przed wyłudzeniem danych pozwalających na przeprowadzenie transakcji bankowości internetowej, należy bezwzględnie przestrzegać następujących zasad:

1) nigdy, pod żadnym pozorem nie należy podawać żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z kart-zdrapek ani przesyłanych SMSem itp.) w żadnym innym miejscu niż strona internetowa banku prowadzącego dany rachunek lub w udostępnianej przez niego aplikacji (np. instalowanej na telefonie),

2) wejście do serwisu bankowości internetowej powinno zawsze odbywać się poprzez wprowadzenie jego adresu w pasku przeglądarki – nie należy korzystać w tym zakresie z wyszukiwarek internetowych ani – w szczególności – z linków przesyłanych w otrzymanych wiadomościach e-mail,

3) przed zalogowaniem do serwisu bankowości internetowej zawsze należy sprawdzić, czy połączenie jest szyfrowane, tj. czy przed adresem strony znajduje się przedrostek „https://" (a nie „http://"), a obok niego widnieje symbol kłódki; dodatkowo należy kliknąć we wspomniany symbol kłódki i sprawdzić, czy nie pojawia się informacja o błędnym certyfikacie klucza publicznego.

Kradzieże z wykorzystaniem złośliwego oprogramowania

Przykład

„Uwaga! Ostateczne wezwanie do wpłaty.

Termin uregulowania należności minął w dniu 30 Lipiec 2015. Nie uregulowanie należności w wysokości 5 000 PLN do w ciągu 3 dni od otrzymania tej wiadomości spowoduje wpisanie Twojej firmy do bazy dłużników oraz oczekuj odpowiedzialności karnej. Szczegóły znajdź w załączonym pliku.

Po więcej informacji zadzwoń – 00960 555 12 45.

Z poważaniem,

Zespół Zarządzanie Długami Suriw".

W pewien poniedziałkowy poranek e-mail o takiej treści wybudził Pana Wojciecha skuteczniej niż jego ulubione espresso. Dbając o wizerunek swojej firmy, szybko pobrał załącznik do powyższej wiadomości i spróbował go otworzyć, nie zważając ani na łamaną polszczyznę, którą napisana była wiadomość, ani nawet na ostrzeżenia zgłaszane przez zainstalowany na jego komputerze program antywirusowy. Ponieważ jednak na ekranie nic więcej nie pojawiło się, spróbował zadzwonić pod wskazany w wiadomości numer telefonu, którego nikt nie odbierał. Po przeprowadzeniu szybkiego rachunku sumienia uznał, że nikomu z żadnymi płatnościami nigdy nie zalegał, w związku z czym uznał całą sprawę za żart i zajął się zupełnie innymi sprawami – akurat miał w planach właśnie wykonanie kilku przelewów.

Jakież było jego zdziwienie, gdy po kilku dniach wszedł na swój rachunek bankowości internetowej z komputera żony i zobaczył, że saldo na jego koncie wynosi równe zero złotych, a w historii operacji widnieją przelewy na wysokie kwoty do osób, o których nigdy nie słyszał. Szybko udał się do placówki swojego banku, gdzie został poinformowany, że przelewy, które przekazywał (w swoim mniemaniu) do swoich kontrahentów w rzeczywistości trafiły zupełnie gdzie indziej i faktycznie na jego rachunku nie ma już środków. Zadzwonił do znajomego informatyka, który poinformował go, że jest to typowy sposób działania szkodliwego oprogramowania wykradającego pieniądze z kont klientów banków (teraz Panu Wojciechowi przypomniało się mgliście, że jego bank przesyłał mu wiadomości informujące o tego rodzaju zagrożeniach, on jednak – w ferworze codziennej walki o byt – skutecznie je ignorował). Natychmiastowa diagnoza komputera Pana Wojciecha przeprowadzona przez owego znajomego potwierdziła jego najgorsze przypuszczenia... Jego komputer padł ofiarą wirusa, a on sam został skutecznie okradziony przez przestępców. Na domiar złego, z otrzymanego na koniec feralnego miesiąca rachunku telefonicznego wynikało, że Pan Wojciech wykonał krótkie połączenie z numerem premium na Malediwach, w wyniku czego musi uiścić dodatkową opłatę w wysokości kilkudziesięciu złotych. Wtedy przypomniał sobie, że numer telefonu, na który zadzwonił w związku z owym oszukańczym e-mailem faktycznie wyglądał nietypowo, on jednak nie zwrócił na to uwagi, chcąc jak najszybciej wyjaśnić sprawę rzekomo nieuregulowanej płatności.

Takie sytuacje, jak opisana powyżej, zdarzają się niestety coraz częściej. Przestępcy już dawno zorientowali się bowiem, że środowiska teleinformatyczne instytucji finansowych są z reguły bardzo dobrze zabezpieczone, w związku z czym zaczęli szukać innych rozwiązań, w których przy możliwie niskich nakładach pracy możliwe jest uzyskanie możliwie wysokiego prawdopodobieństwa przeprowadzenia skutecznego ataku. Takim rozwiązaniem okazały się być właśnie komputery (i inne urządzenia dostępowe, jak np. tablety czy telefony komórkowe) użytkowników bankowości internetowej, które często są zabezpieczone jedynie w ograniczonym zakresie lub nawet wcale.

Zapamiętaj!

Dlatego niezmiernie ważne jest, aby każdy użytkownik bankowości internetowej pamiętał o podstawowych zasadach bezpieczeństwa w tym zakresie:

1) do korzystania z bankowości internetowej należy zawsze używać znanych sobie, zaufanych urządzeń, nie zaś np. komputerów w kafejkach internetowych, na których ktoś wcześniej mógł zainstalować szkodliwe oprogramowanie; nie należy również w tym celu łączyć się z obcymi punktami dostępowymi do sieci bezprzewodowych, jak np. publicznie dostępne hot-spoty,

2) urządzenia używane do korzystania z bankowości internetowej powinny zawsze być zabezpieczone poprzez aktualne oprogramowanie antywirusowe i zaporę sieciową (ang. firewall),

3) na urządzeniach tych należy również zawsze instalować najnowsze aktualizacje bezpieczeństwa, zarówno samego systemu operacyjnego, jak i innego oprogramowania

(przeglądarek internetowych i ich wtyczek, oprogramowania biurowego itp.),

4) nie należy ignorować alertów bezpieczeństwa zgłaszanych przez oprogramowanie antywirusowe,

5) nie należy także korzystać z pirackiego oprogramowania – poza łamaniem przepisów prawa, często instalacja takiego oprogramowania wiąże się z ukrytym wprowadzeniem do urządzenia szkodliwego oprogramowania.

Stosowanie się do powyższych zasad znacząco obniża prawdopodobieństwo stania się ofiarą skutecznego ataku przeprowadzonego przy użyciu szkodliwego oprogramowania.

Kopiowanie kart płatniczych

Przykład

Pani Maria i Pan Wojciech wraz z dziećmi zdecydowali się w długi weekend majowy pojechać do Torunia, aby pokazać swoim potomkom to piękne miasto. Pogoda sprzyjała spacerom i korzystaniu z usług kawiarni na rynku toruńskim, których tam akurat nie brakuje. Pani Maria i Pan Wojciech przyzwyczajeni są do płacenia gotówką, więc i tym razem zdecydowali się podjąć drobną kwotę z bankomatu. Wybrali taki, który akurat był blisko rynku i poszli delektować się kawą i lodami w rodzinnej atmosferze.

Po paru miesiącach, zapomniawszy już o podróży do Torunia, Pani Maria przed zrobieniem zakupów w sklepie poszła ponownie do bankomatu w centrum handlowym. Tym razem okazało się, że mimo iż upłynęło ledwie parę dni od wypłaty pensji, żadnych pieniędzy na rachunku nie ma. Zatrwożona wróciła do domu, żeby sprawdzić operacje na koncie. Zobaczyła zaksięgowane parę wypłat z bankomatu w jednym z krajów w Ameryce Południowej, w której nigdy w życiu nie była, a na pewno nie w okresie ostatnich paru miesięcy.

Pani Maria i Pan Wojciech stali się ofiarami tzw. skimmingu. Przestępcy na bankomatach umieszczają urządzenia, dzięki którym zczytują dane z naszych kart.

Co do zasady nie zawsze korzystając z bankomatu możemy zorientować się, że ktoś go „ulepszył” na swoje potrzeby. Aby skutecznie zczytać zawartość karty, przestępcy instalują nakładkę na otwór, w który wsuwamy kartę. Tym sposobem skanują całą zawartość paska magnetycznego, którą następnie mogą nagrać na dowolny kawałek plastiku z paskiem magnetycznym lub przesłać elektronicznie do swoich kolegów w dowolnej części świata, aby oni to zrobili. W niektórych bankomatach karta po włożeniu do bankomatu wsuwa się, jednocześnie wibrując. mechanizm ten zabezpiecza nas przed skimmingiem utrudniając w takim przypadku zczytanie danych z paska przez urządzenie zamontowane na bankomacie. Dodatkowo banki często montują „zęby” bądź

inne plastikowe wypustki wokół otworu na kartę, aby uniemożliwić zamontowanie tam tzw. skimmera.

Jednak sama zawartość paska to za mało. Potrzebny jest przecież jeszcze PIN. Tutaj pomagają przestępcom dwie technologie. Montują nad klawiaturą listwy z miniaturową kamerą albo używają fałszywej klawiatury, którą przyklejają na tę prawdziwą. Dzięki temu możemy wpisać PIN i wypłacić pieniądze, a przestępcy wiedzą, jakie klawisze zostały naciśnięte.

Skimming najczęściej dotyka bankomaty w dobrych lokalizacjach turystycznych, nie zlokalizowane w oddziałach bankowych, do których jest swobodny dostęp, i z którego korzysta dużo ludzi. Nikogo wtedy nie dziwią ślady zużycia na bankomacie, które mogłyby wskazywać na jakąś podejrzaną działalność, ani fakt, że ciągle w okolicach bankomatu znajdują się ludzie.

Obecnie znaczna część klientów banków posiada karty z wbudowanym chipem mającym na celu ochronę przed pozyskiwaniem przez przestępców danych dotyczących karty.

Wiadomość, że karta posiada chip jest zapisana na pasku magnetycznym karty. Bankomat czyta tę informację i inicjuje tzw. moduł EMV, który porozumiewa się z chipem na karcie.

Wówczas na ekranie bankomatu wyświetla się komunikat o możliwym wydłużonym czasie oczekiwania na przeprowadzenie danej operacji, jak np. wypłata środków, w związku ze wspomnianym odczytem danych z karty.

Po zeskimowaniu karty z chipem przestępcy nie mogą jej użyć w bankomacie, który obsługuje moduł EMV, a takich jest w Polsce większość, jeśli nie wszystkie. Taki bankomat odczyta informacje o tym, że karta ma chip, poszuka go na zeskimowanej karcie i oczywiście nie znajdzie i nie przeprowadzi transakcji. Są jednak kraje, w których technologia EMV nie działa tak dobrze albo w ogóle (np. Ameryka Południowa czy USA). Tam komunikat o chipie z paska magnetycznego karty nie będzie zinterpretowany przez bankomat, a przestępcy mając zawartość paska magnetycznego karty i numer PIN bez przeszkód dokonają wypłaty.

Oczywiście banki chronią siebie i swoich klientów przed tym rodzajem przestępstw i bardzo często takie wypłaty blokują przed ich dokonaniem. Nie zawsze jednak pojedyncze transakcje uda się wychwycić, dlatego niezbędna jest czujność.

Uwaga!

Nie zalecamy korzystania z bankomatów, które nie są umiejscowione w oddziałach banków. Jeśli musimy skorzystać z bankomatu poza oddziałem, należy sprawdzić czy żadne jego części nie wyglądają „dziwnie", „jakby doklejone", „nadmiernie wystające" i niezintegrowane z całym bankomatem. Jeśli klawiatura sprężynuje przy wprowadzaniu PINu albo nawet odkleja się, należy transakcję przerwać. W razie jakichkolwiek wątpliwości lepiej skorzystać z innego bankomatu, a swoje podejrzenia zgłosić na infolinii banku.

Kradzieże związane z kartami zbliżeniowymi

Przykład

Rok akademicki nareszcie zakończył się! Robertowi wydawało się, że czekał na ten moment od wieków. Teraz poczuł, że życie jednak może być piękne. Zaliczona sesja, odłożone pieniądze zdobyte dzięki różnym zleceniom, które z zapałem realizował przez ostatnich kilka miesięcy – nareszcie można rozpocząć wymarzone wakacje. Z tą myślą – oraz z grupą najbliższych znajomych – Robert wsiadł do pociągu i już po kilku godzinach znalazł się nad polskim morzem. Plaża, wizyta w restauracji i nagle już widać wschodzące słońce. Takie wakacje mogłyby trwać cały rok!

„Hola hola, gdzie moja karta" – pomyślał Robert budząc się następnego dnia w okolicach południa i zaglądając do portfela. Niestety, nawet dogłębna inwentaryzacja wszystkiego, co tylko dało się zinwentaryzować, nie przyniosła dobrych dla Roberta rezultatów. Karty nie było nigdzie! Chcąc nie chcąc, Robert z wyjątkowo kwaśną miną musiał wykonać telefon w celu zastrzeżenia karty (na szczęście pamiętał uniwersalny numer telefonu, pod którym 24 godziny na dobę i 7 dni w tygodniu można zastrzec swoją kartę płatniczą: +48 828 828 828). Następnie swoje kroki skierował do placówki swojego banku, gdzie dokonał ze swojego rachunku wypłaty środków, które powinny pozwolić mu godnie przeżyć najbliższych kilka dni, a przy okazji dowiedział się, że z jego konta w tym czasie zniknęło niemal 600 PLN – było to kilkanaście transakcji zbliżeniowych poniżej 50 PLN, w przypadku których nie jest wymagane podanie kodu PIN. W pierwszej chwili ta kwota niemal zwaliła Roberta z nóg, na szczęście pani w okienku od razu poinformowała go, że w takiej sytuacji jego odpowiedzialność za utracone środki wynosi 50 EUR , musi tylko zgłosić stosowną reklamację i poczekać na jej

pozytywne rozpatrzenie. Humor Roberta uległ dzięki temu minimalnej poprawie, a smaczne śniadanie w nadmorskiej karczmie niemal zupełnie rozwiało jego czarne myśli. Po powrocie do domu postanowił natomiast zgłębić temat bezpieczeństwa kart zbliżeniowych – w tym celu zapoznał się z opublikowanym przez Urząd Komisji Nadzoru Finansowego raportem.

Karty zbliżeniowe to nowoczesna i wygodna forma płatności. Wbrew spotykanym niekiedy opiniom nie są one również mniej bezpieczne niż karty pozbawione funkcji zbliżeniowej. Należy bowiem zwrócić uwagę, że wprawdzie faktycznie utrata karty zbliżeniowej umożliwi przestępcy dokonanie za jej pomocą kilku transakcji, jednak odpowiedzialność klienta w tym zakresie jest ograniczona do maksymalnie 50 EUR.

Dodatkowo warto zauważyć, że jednym z najistotniejszych problemów w zakresie kart płatniczych pozostają działania przestępcze nakierowane na kradzież danych z kart (zwłaszcza kredytowych) – niezależnie od tego, czy są one zbliżeniowe, czy nie – i dokonywanie nimi tzw. transakcji typu „card-not-present" (bez fizycznej obecności karty, np. przez internet). W tym kontekście należy zwrócić uwagę, że dzięki użyciu technologii zbliżeniowej posiadacz karty w przypadku wielu transakcji nie musi tracić z nią fizycznego kontaktu, dzięki czemu ograniczane jest ryzyko sklonowania karty poprzez skimming lub nieuprawnionego odczytania z niej danych umożliwiających dokonanie transakcji typu „card-not-present".

Zapamiętaj!

W przypadku utraty karty niezwłocznie zgłoś ten fakt w placówce banku lub pod ogólnopolskim numerem telefonu +48 828 828 828.

Kradzieże przy użyciu danych karty płatniczej

Przykład

Krzysztof kończy w tym roku gimnazjum. Żeby ułatwić wszystkim życie, zakłada sobie konto w banku i dostaje kartę płatniczą, dzięki której będzie mógł korzystać z pieniędzy, których rodzice już nie będą musieli mu dawać do ręki. Jako że rodzice ufają Krzysztofowi, postanowili na wakacje wyrobić mu kartę kredytową podpiętą pod ich rachunek kredytowy w banku, żeby w razie nieprzewidzianej sytuacji miał się czym ratować.

Karta ta ucieszyła Krzysztofa niezmiernie, więc jej zdjęcie miało być pierwszym w albumie z pierwszych prawie dorosłych wakacji relacjonowanych na Instagramie.

Krzysztof jednak utracił zaufanie rodziców, kiedy w tym samym dniu, w którym zrobił zdjęcie karty i opublikował je na Instagramie, rodzice stracili wszystkie pieniądze z konta kredytowego.

Nie jest to wina Instagrama czy Facebooka czy innego medium społecznościowego.

Obecnie informacje publikowane w Internecie pozostają tam na zawsze. Z pomocą tego środka komunikacji możemy znaleźć prawie wszystkie informacje, jakich potrzebujemy – poczytać książki w bibliotekach na całym świecie czy zobaczyć z bliska obrazy wielkich mistrzów. W Internecie działają też przestępcy, dla których zdjęcie karty kredytowej wystarczy do „wyczyszczenia” nam konta. Nie jest to przesadnie trudne, gdyż wystarczy spisać dane z karty i posłużyć się nimi w sklepie internetowym za granicą. Ci, którzy płacą kartami w polskich i europejskich sklepach doskonale wiedzą, że do przeprowadzenia transakcji trzeba podać „kod zabezpieczający” znajdujący się na odwrocie karty. Więc w jaki sposób okradziono Krzysztofa, który sfotografował tylko front karty? Niestety są kraje, w których kod CVC2/CVV2 (bo o nim mówimy), trzycyfrowy kod wydrukowany z tyłu karty obok miejsca na podpis, nie jest wymagany i do skutecznego przeprowadzenia transakcji wystarczy numer karty, data ważności i dane personalne na niej wytłoczone.

Przykład

Słynna jest już historia pewnej Pani, która po przejściu huraganu nad USA opublikowała na Facebooku zdjęcie karty, którą dostała od Amerykańskiego Czerwonego Krzyża, na której znajdowały się pieniądze dla niej, jako poszkodowanej w tej katastrofie. W ciągu paru minut od zamieszczenia zdjęcia pieniądze zostały wypłacone z konta, podobnie jak w przypadku naszego Krzysztofa.

Wszystkie dane dotyczące naszej karty musimy bezwzględnie chronić. Nie polega to tylko na powstrzymaniu się od robienia jej zdjęć i publikowaniu ich w Internecie, ale też na tym, aby uważnie obserwować co robią z nią osoby, u których płacimy. Przy transakcjach w terminalu nie ma potrzeby, aby pracownik sklepu tę kartę odwracał, chyba że porównuje nasz podpis. Odpowiednio zlokalizowane kamery ochrony, skierowane na kasy (np. na stacjach benzynowych) mogą wtedy nagrać wszystkie dane potrzebne do wyczyszczenia naszego rachunku, jeśli pracownik kartę niepotrzebnie odwraca. Jeśli nie zamierzamy korzystać z karty w Internecie – najlepiej wyzerować limit na te transakcje, co można zrobić w oddziale swojego banku, albo w ogóle zablokować ten kanał, na co niektóre banki pozwalają. Wszystkie pozostałe transakcje będą wymagały fizycznej obecności karty, ale w ten sposób nie będzie możliwe np. zagwarantowanie rezerwacji w hotelu, co może być uciążliwe dla osób podróżujących.

Zagrożenia dotyczące płatności mobilnych

Przykład

Anna nigdy nie miała pamięci do liczb. Dlatego pierwszą rzeczą, którą zrobiła po instalacji aplikacji pozwalającej na dokonywanie płatności mobilnych na swoim telefonie było zapisanie kodu PIN do tej aplikacji na kartce i umieszczenie jej w etui aparatu. Dzięki temu – jak pomyślała – nie była już zagrożona nienawistnymi spojrzeniami sprzedawcy i osób stojących za nią w kolejce w momencie, w którym nerwowo próbowałaby przypomnieć sobie PIN i zapłacić za zakupy. I faktycznie – kilka razy dzięki tej swoistej „zapobiegliwości" udało jej się uniknąć blamażu. Jednak pewnego dnia padła ofiarą złodzieja, który wykorzystując chwilę nieuwagi Anny ukradł jej telefon wprost z kawiarnianego

stolika. Początkowo nie była tą sytuacją zbyt zmartwiona (w końcu „to tylko telefon"), jakież jednak było jej zdziwienie, kiedy następnego dnia po zalogowaniu do swojego konta zobaczyła, że w ciągu ostatnich 24 godzin jej środki finansowe zostały uszczuplone o ponad 1000 złotych. Dopiero wtedy przypomniała sobie o zainstalowanej na telefonie aplikacji do płatności mobilnych (i o zapisanym w telefonie kodzie PIN) i błyskawicznie dezaktywowała funkcję dokonywania takich płatności.

Płatności mobilne to stosunkowo nowa forma dokonywania transakcji płatniczych. Dla wielu użytkowników wiąże się ona ze znaczącą wygodą – nie muszą bowiem nosić przy sobie portfela ani kart płatniczych, zaś operacji (zarówno w punktach sprzedaży, w bankomatach, jak i w Internecie) mogą dokonywać wyłącznie przy użyciu aparatu telefonicznego. Jednakże – tak jak w przypadku każdej innej technologii płatniczej – bezpieczne korzystanie z tej formy płatności wymaga zapamiętania pewnych podstawowych zasad, które pozwolą na zabezpieczenie się przed grożącymi nam niebezpieczeństwami.

Zapamiętaj!

1) Telefon z zainstalowaną aplikacją do płatności mobilnych powinien mieć włączoną blokadę ekranu, której dezaktywacja powinna wymagać wprowadzenia hasła (lub w inny sposób była możliwa do dokonania jedynie dla prawowitego właściciela telefonu),

2) nie należy zapisywać hasła do aplikacji płatności mobilnych na kartce (lub innym nośniku), zwłaszcza przechowywanej wraz z telefonem,

3) hasło do telefonu powinno być inne niż do aplikacji płatności mobilnych; hasła te powinny również być trudne do odgadnięcia,

4) telefon używany do dokonywania płatności mobilnych powinien zawsze być zabezpieczony przez aktualne oprogramowanie antywirusowe,

5) na telefonie służącym do dokonywania płatności mobilnych należy zawsze instalować najnowsze aktualizacje bezpieczeństwa systemu operacyjnego,

6) oddając telefon do serwisu warto odinstalować aplikację płatności mobilnych,

7) niezwłocznie po utracie telefonu, na którym zainstalowana była aplikacja płatności mobilnych, należy zgłosić ten fakt w swoim banku.

A jak zapamiętać taki trudny do odgadnięcia kod PIN? To – wbrew pozorom – bardzo proste. Warto sobie przypomnieć, że na ekranowej klawiaturze numerycznej telefonu do cyfr od 2 do 9 przypisanych jest po kilka liter (np. cyfrze 2 odpowiadają litery „ABC", cyfrze 3 – „DEF" itd.). Mając na uwadze ten fakt, można ułożyć sobie jakiś łatwy do zapamiętania tekst (np. „lubię bezpieczne płatności mobilne"), wziąć pierwsze litery z tego tekstu (dla naszego przykładu będą to litery „L", „B", „P" i „M"), wprowadzić ich „cyfrowy odpowiednik" jako hasło (w tym przypadku 5276) i... gotowe!

Kradzieże tożsamości

Przykład

Pani Ania chce uzyskać kartę kredytową z drobnym limitem, bo czasami poduszka finansowa się przydaje. Znalazła ofertę jednego z banków i aby nie tracić czasu kontaktuje się z nim telefonicznie. Konsultant wypytuje ją o wszystkie szczegóły: dane osobowe, miejsce pracy, zarobki, kto może te zarobki potwierdzić. Nic nie budzi wątpliwości Pani Ani, bo są to standardowe pytania, jakie bank zadaje, a przy małej kwocie nie wymaga zaświadczenia o zarobkach tylko potwierdzi je telefonicznie z pracodawcą. Pani Ania, aby nie tracić czasu, całą rozmowę z konsultantem przeprowadza w tramwaju linii 17, jadąc do pracy na 9 rano. Już po dwóch dniach Pani Ania cieszy się przyznanym limitem kredytowym.

Po pół roku Pani Ania decyduje się zwiększyć nieco limit na swojej karcie. Lecz tym razem bank jej mówi, że nie spłaca innych kredytów w innych bankach. Ale Pani Ania innych kredytów nigdy nie zaciągała.

Niestety, wśród osób podróżujących z Panią Anią w tramwaju linii 17 koło godziny 9 rano, znalazła się jedna nieuczciwa osoba, która całą rozmowę z konsultantem nagrała przy użyciu swojego telefonu komórkowego. Następnie wszystkie dane Pani Ani wykorzystała w paru bankach, zmieniając oczywiście tylko adres korespondencyjny, aby ofiara nie wiedziała co się dzieje. W księgowości w firmie Pani Ani też telefony z banków nie wzbudziły podejrzenia, bo przecież uprzedziła, że stara się o kartę i będą dzwonić.

Przy mniejszych kwotach, w zależności od zarobków klienta i jego zdolności kredytowej, banki nie muszą potwierdzać zarobków poprzez pisemne zaświadczenie o zarobkach.

Tym sposobem, jeśli nie chronimy swoich danych osobowych, mogą one zostać wykorzystane do zaciągania kredytów. Nie tylko jednak musimy uważać na podawanie naszych danych osobowych w zatłoczonych środkach komunikacji miejskiej. Niejednokrotnie niektóre osoby podają wszystkie swoje dane osobowe przy poszukiwaniu pracy. W odpowiedzi na nasze CV, fałszywy pracodawca kontaktuje się w celu ustalenia terminu rozmowy kwalifikacyjnej i z prośbą o wypełnienie bardzo szczegółowego kwestionariusza osobowego na stronie internetowej lub o przesłanie odpowiednich danych w pliku na adres e-mail. Na potrzeby procesu rekrutacji szczegółowe dane o nas nie są potrzebne. Należy wystrzegać się tego typu ofert, mimo że mogą być bardzo kuszące. Tak pozyskane dane niekoniecznie muszą służyć do wyłudzeń kredytów.

Uwaga!

Jeśli podamy numer naszego rachunku bankowego, wszystkie dane osobowe i numer telefonu komórkowego – przestępcy mogą wykorzystać te informacje do zakładania rachunków bankowych, które następnie są używane np. do przesyłania pieniędzy pochodzących z przestępstw. Wtedy stajemy się tzw. słupami, np. w procederze prania pieniędzy.

Oczywiście pozostaje kwestia „aktywacji" tego fałszywego rachunku, do czego potrzebny jest mały przelew z oryginalnego konta osoby, której dane wykorzystano. Można tego dokonać wykorzystując inne metody opisane w tej publikacji, bądź poprzez zainfekowanie naszego telefonu w sposób zdalny wirusem, dzięki czemu przestępcy uzyskają dostęp do SMSów, którymi autoryzujemy przelewy i logujemy się do swojego rachunku. A przelew na 1 złoty może przejść przez nas niezauważony.

Dane osobowe są wielkim dobrem, które musimy chronić, nawet wbrew naszemu wrodzonemu zaufaniu do innych ludzi, w szczególności do potencjalnych pracodawców. Wzmożona czujność jest wymagana w sytuacjach, gdy ktokolwiek chce, abyśmy podawali więcej informacji niż wydaje się nam to konieczne.

„Oszustwa nigeryjskie”

Przykład

„Jestem najbliższym współpracownikiem Jego Wysokości Księcia Mahammada III – zaczynał się e-mail, który Pan Marek otrzymał pewnego dnia rano – Ze względu na bardzo mało rozwinięty system bankowy w naszym kraju, potrzebujmy pomocy, aby środki prawowitego Króla przemieścić do Europy i ukryć przed juntą wojskową. Oczywiście pomoc zostanie wynagrodzona, 5% kwoty przelewu”.

Pan Marek zapalił się do pomysłu, bo niby nie wiadomo ile tych pieniędzy trzeba przekazać, ale król mało ich nie ma, więc można liczyć na duży zysk. Po szybkiej wymianie korespondencji okazało się, że aby wszystko przebiegło prawidłowo, Pan Marek musi wnieść małą opłatę manipulacyjną, którą sobie zrekompensuje dość szybko paroma tysiącami dolarów, jakie przypadną mu z prowizji. Widząc już te pieniądze swoimi oczami (i właściwie już je wydawszy), Pan Marek wykonał przelew. Dalszego kontaktu już w tej sprawie nie było.

Niestety, takie wiadomości dość często wysyłane są drogą elektroniczną. Zazwyczaj ich treść napisana jest w języku angielskim i niewiele osób zwraca na nie uwagę. Niemniej są tacy, którzy widzą w tym procederze szanse na zarobienie pieniędzy w łatwy i szybki sposób. Taki system postępowania oszustów doczekał się osobnej penalizacji w nigeryjskim kodeksie karnym (art. 419) ze względu na swoją powszechność. Pieniądze przekazane oszustom są nie do odzyskania. Co do zasady trzeba powiedzieć, że Pan Marek i tak miał szczęście. Odpowiadając na podobne e-maile i wikłając się w tego typu przedsięwzięcia można również narazić się na dużo większe problemy niż tylko utrata oszczędności.

Zapamiętaj!

Przyjęcie pieniędzy niewiadomego pochodzenia na swój rachunek bankowy i przekazanie ich dalej może być udziałem w większym oszustwie – praniu pieniędzy czy nawet finansowaniu terroryzmu. Bardzo często środki pieniężne przekazywane zgodnie z opisanym procederem mogą pochodzić z tzw. phisingu.

Kradzieże w sklepach internetowych

Przykład

Pani Julia i Pan Adam znaleźli dawno poszukiwany okap kuchenny w jednym ze sklepów internetowych i to aż o 200 złotych tańszy niż w innych. Okazja, której nie można przepuścić. Towar został zamówiony i opłacony przelewem, ponieważ sklep nie wysyła towaru za pobraniem i jeszcze nie wdrożył płatności kartą ze względu na zbyt krótki okres swej działalności.

Zamówiony i opłacony towar oczywiście nigdy do kupujących nie dotarł.

Ofiarą takiego oszustwa może zostać każdy i to nie tylko poprzez dokonywanie zakupów w sklepach internetowych, ale również na portalach aukcyjnych. Sprawcy wykorzystują w tym przypadku przelewy na rachunki, płatności przy użyciu PayPal bądź podobnych rozwiązań. Czasami – czego nie jesteśmy świadomi – tak przelane pieniądze trafiają prosto na rachunek karty pre-paid, z której są natychmiast podejmowane. Za najbezpieczniejszą formę płatności w sklepach internetowych uznaje się płacenie kartą. W ten sposób, w razie gdybyśmy mieli dalsze problemy, możemy w swoim banku uruchomić procedurę tzw. charge-back.

Dzięki niej, organizacje specjalizujące się w zakresie rozwiązań płatniczych, jak VISA i Mastercard, zabezpieczają swoich klientów przed oszustwami. Po udowodnieniu bankowi incydentu oszustwa i wszczęciu wspomnianej wyżej procedury, to bank podejmuje działania mające na celu odzyskanie utraconych przez poszkodowanego pieniędzy z banku, w którym rachunek posiadają przestępcy.

Dlatego też w większości przypadków tylko sprawdzone sklepy oferują płatności kartami. Inną, bezpieczną formą dokonywania płatności za towar zakupiony w Internecie może być płatność za pobraniem, lecz wtedy musimy przy kurierze otworzyć przesyłkę i wszystko dokładnie sprawdzić.

Proszę pamiętać, że dane podawane w systemach autoryzacyjnych instytucji płatniczych są bezpieczne, lecz pod żadnym pozorem nie wolno tych danych podawać w e-mailu bądź w inny sposób umożliwiający ich pozyskanie przez inne osoby.

Niestety, po raz kolejny należy powtórzyć, że zbyt duże okazje nie zdarzają się często a niska cena towaru pełnowartościowego powinna zwrócić naszą uwagę w negatywnym tego słowa znaczeniu. Płatności przelewami, czy przedpłaty należy realizować w sklepach o uznanej renomie lub takich, w których już kupowaliśmy z powodzeniem. Pozytywne komentarze w portalach aukcyjnych też nie zawsze są dla nas sprzymierzeńcem, ponieważ można je fałszować czy kupować, tak jak „lajki" na Facebooku. Zdrowy rozsądek jest kluczem do naszego bezpieczeństwa.

Co zrobić, gdy pieniądze znikną z rachunku bankowego w wyniku przestępstwa?

Mimo najwyższej staranności, ostrożności i stosowania wszystkich zasad opisanych w tej publikacji może zdarzyć się, że staniemy się ofiarami przestępstw, o których była mowa. Najważniejsze jest zachowanie czujności i weryfikowanie wyciągów z kont kart kredytowych, bądź uważne przeglądanie historii naszych rachunków. W chwili, w której zauważymy transakcje nie przeprowadzone przez nas, mimo zdenerwowania należy zachować spokój. Przed niezwłocznym poinformowaniem banku, należy ponownie sprawdzić wszystkie przeprowadzone transakcje i upewnić się, czy nie były one zrealizowane przez osoby nieuprawnione.

Zapamiętaj!

Najszybszą drogą poinformowania banku o podejrzeniu popełnienia przestępstwa jest złożenie reklamacji przez telefon, gdzie musimy wskazać transakcje nie przeprowadzone przez nas i oświadczyć, że nikomu nie udostępnialiśmy karty i jej numeru, jak również loginów i haseł do bankowości elektronicznej. W trakcie przyjmowania reklamacji, pracownik banku zastrzeże naszą kartę bądź zablokuje dostęp do bankowości elektronicznej, a bank rozpocznie procedurę wyjaśniania naszego zgłoszenia.

W zależności od przyjętej w danym banku praktyki, możemy być zobowiązani do złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa. Można tego dokonać dwojako: udać się na najbliższą nam komendę policji i złożyć ustnie takie zawiadomienie, z którego sporządzony zostanie protokół. Wtedy zostaniemy jednocześnie przesłuchani w charakterze pokrzywdzonego. Dlatego też należy mieć ze sobą wyciąg z karty bądź wydruk z historii rachunku, aby udokumentować naszą stratę. Zawiadomienie można również złożyć w formie pisemnej, przesyłając je do prokuratury rejonowej

właściwej ze względu na nasze miejsce zamieszkania (właściwość tę można ustalić w Internecie). Prokuratura prześle nasze zawiadomienie do właściwej komendy policji, do której i tak będziemy musieli zgłosić się w celu złożenia zeznań w charakterze pokrzywdzonego.

Niezależnie od tych działań, w miarę możliwości dobrze jest poinformować właścicieli sklepów lub innych placówek, w których użyto naszej karty albo które otrzymały nasze pieniądze. Dane adresowe większości firm można znaleźć w Internecie. Niektórym poszkodowanym podjęcie opisanych działań może sprawić trudności w przypadku próby skontaktowania się z zagraniczną firmą ze względu na barierę językową.

Zazwyczaj duże firmy posiadają procedury postępowania w przypadku nieuprawnionego użycia karty i mogą pomóc w działaniach naszemu bankowi, który z pewnością zgłosi się do nich.

W przypadku, gdy przestępstwo zostało popełnione z wykorzystaniem naszej karty kredytowej lub płatniczej bądź ich numerów, należy udać się do placówki bankowej w celu złożenia tzw. polecenia charge-back (choć są również banki, które umożliwiają złożenie takiego polecenia przez telefon). Jest to procedura reklamacyjna przeprowadzana przez organizację specjalizującą się w rozwiązaniach płatniczych, jak Visa czy MasterCard, polegająca na tym, że w przypadku oszustwa pieniądze są nam zwracane przez bank, który we współpracy ze wspomnianą organizacją podejmuje działania w celu ich odzyskania. Należy pamiętać, że w niektórych bankach charge-back to osobna procedura niż reklamacja składana w razie oszustwa, a co więcej, nie jest ona popularna wśród klientów, co oznacza, że konsultanci nie zawsze muszą o niej wiedzieć. Należy pamiętać, iż w przypadku organizacji takich, jak Visa czy MasterCard, przysługuje nam prawo zgłoszenia oszustwa i domagania się uruchomienia procedury charge-back.

Ale najważniejszą zasadą postępowania w takiej sytuacji jest zachowanie spokoju. Wszyscy, z którymi będziemy mieli styczność chcą nam pomóc i rozumieją nasze trudne położenie.

PODSUMOWANIE

Należy zawsze pamiętać, że wraz z użytkowaniem nowych technologii przez klientów, niektóre systemy zabezpieczeń są rozwijane, a inne są wprowadzane zupełnie od nowa. Wynika to z konieczności dynamicznego reagowania na zagrożenia, które czasami są w praktyce nie do przewidzenia w momencie wprowadzania technologii na rynek. Dopiero użytkowanie nowych produktów przez klienta pokazuje, gdzie potencjalnie mogą wystąpić słabości w zabezpieczeniach.

Niemniej żadne zabezpieczenia techniczne nie pomogą nam, jeśli sami nie będziemy stosować się do podstawowych zasad bezpieczeństwa, których podsumowanie można znaleźć w dalszej części niniejszej publikacji.

Poufność

Wszystkie nasze dane zawarte w dowodzie osobistym pozwalają nas jednoznacznie zidentyfikować. Ujawnienie ich komukolwiek, za wyjątkiem osób uprawnionych, bardzo poważnie może zagrozić naszemu bezpieczeństwu. Skoro na podstawie tych danych możemy założyć rachunek bankowy czy otrzymać kredyt, to często dokładnie to samo będą mogli zrobić przestępcy podszywający się pod nas. Nie powinno się podawać danych osobowych w miejscach, gdzie mogą one być podsłuchane lub zapisane przez inną osobę. Dane te nie mogą być wysyłane do osób, których nie znamy – nieważne jak intratną ofertę pracy czy przyszłego biznesu dla nas rzekomo mają. Tak samo złym pomysłem jest umieszczanie ich w internecie, który niektórym kojarzyć się może jako medium zapewniające anonimowość. Niestety, tak nie jest. Nie mamy kontroli nad tym, kto ma tam dostęp do naszych danych i co dalej z nimi zrobi. Należy również pamiętać, że informacja raz umieszczona w internecie, nawet po jej usunięciu, dalej tam pozostaje. W powszechnym użyciu są narzędzia, które pozwalają na sprawdzenie historycznej zawartości poszczególnych stron internetowych.

To samo dotyczy wszystkich danych, z których korzystamy w celu logowania się do bankowości internetowej, czy też numerów naszych kart płatniczych bądź kredytowych. Wiele osób ma na szczęście pełną świadomość tego, że w sytuacji utraty karty płatniczej (w wyniku jej kradzieży, czy zagubienia) należy ją jak najszybciej zastrzec. Z drugiej jednak strony wiele osób nie ma

świadomości tego, że równie niebezpieczną sytuacją jest zrobienie zdjęć karcie i opublikowanie ich w Internecie czy w jakikolwiek inny sposób podanie jej numeru osobom nieuprawnionym. Wiele transakcji może być bowiem przeprowadzonych bez fizycznej obecności karty, jedynie przy użyciu jej numeru (niekiedy nawet bez konieczności podania kodu bezpieczeństwa – tzw. CVC2/ CVV2 – umieszczonego na odwrocie karty).

Spokój

Wiele schematów, o których pisaliśmy wcześniej bazuje na wykorzystaniu naszego zdenerwowania lub podekscytowania. Przestępcy będą próbowali nami manipulować wmawiając nam, że przedstawiana oferta zakupu jakiegoś towaru jest jedyna, niepowtarzalna i kończy się już za chwilę (wystarczy tylko wprowadzić na obcej stronie internetowej swoje dane do logowania do bankowości internetowej), że grożą nam ogromne kary finansowe i inne konsekwencje za nasze rzekome zaniechania (i dlatego musimy jak najszybciej pobrać załącznik do podejrzanego maila), czy też że zostaliśmy wytypowani jako najlepszy kandydat spełniający warunki najwspanialszej pod słońcem oferty pracy (i wystarczy jedynie, że podamy „przyszłemu pracodawcy" nasze szczegółowe dane osobowe i dokonamy przelewu na złotówkę). W takich sytuacjach często niewystarczająco zastanawiamy się, czy to, co robimy, nie przyniesie nam więcej szkody niż potencjalnego pożytku – zwłaszcza, że możemy już więcej takiej oferty nie dostać. I właśnie ten schemat myślowy wykorzystują przestępcy. Za każdym razem, gdy jesteśmy zdenerwowani bądź podekscytowani, nasze myśli nie idą tym torem, którym poszłyby normalnie. Chcemy działać szybko, aby jak najefektywniej rozwiązać problem czy doprowadzić daną sytuację do szczęśliwego finału. Wtedy właśnie możemy pominąć te sygnały ostrzegawcze, które w normalnej sytuacji byśmy zauważyli.

Dobrym rozwiązaniem jest zawsze na chwilę zatrzymać się. Zastopować wszechogarniającą potrzebę szybkiego działania, chęć „żeby szybko załatwić sprawę i mieć z głowy kolejny problem" i gonitwę myśli, która temu towarzyszy. Jeśli pozwolimy sobie na chwilę zatrzymania i spokoju, możemy zastanowić się i sprawdzić polegając na naszej wewnętrznej, zazwyczaj bardzo dobrej intuicji, czy aby wszystko jest w porządku.

Zdrowy rozsądek

Zaryzykujmy stwierdzenie, iż każdy w podejmowanych działaniach kieruje się zdrowym rozsądkiem. Jednakże w sytuacjach wzmożonego stresu postępujemy nierozważnie i zapominamy o podstawowych zasadach bezpieczeństwa.

Zazwyczaj nasze działania powinny być poparte wiedzą i temu ma służyć niniejsza publikacja.

Co więcej – zawsze, gdy mamy wątpliwości powinniśmy pytać, choćby dlatego, że zwykle większym wstydem jest dać się oszukać niż przyznać do niewiedzy, która jest przecież przez nas niezawiniona. Pracownicy banków są również od tego, aby dzielić się swoją wiedzą, ostrzegać klientów i ich informować. Tak, jak w Państwa interesie leży nie być oszukanym, tak samo w interesie banku jest aby Państwo nie zostali oszukani, bowiem niejednokrotnie oznacza to znaczne straty również po stronie banku.

Walka z oszustami i innymi przestępcami jest wspólnym zmaganiem instytucji finansowych i klientów.

Proszę również pamiętać, że wszystkie sytuacje, które wydadzą się nam dziwne, takie jak e-maile z banku, telefony z prośbą o potwierdzenie danych przez bank, w którym nie mamy rachunku, możemy zgłosić do oddziału swojego banku, co pomoże w wykryciu ewentualnego oszustwa.

Wiedza

Dużo już powiedzieliśmy o wiedzy. Warto jednak podkreślić, jak istotne jest to, żebyśmy wiedzieli z jakich technologii korzystamy, jak one działają, jakie są ich plusy i potencjalne zagrożenia. Oczywiście, w chwili wprowadzania nowych technologii są one gruntownie testowane, ale żadna z nich nie daje stuprocentowej gwarancji bezpieczeństwa. Jednak wszystkie instytucje wprowadzając nowe produkty czy technologie dbają o to, aby ich klienci byli dobrze poinformowani. Korzystajmy z tej okazji, czytajmy i starajmy się zapamiętać najistotniejsze zagrożenia, aby móc się ich ustrzec. W tym miejscu warto wspomnieć, że artykuły prasowe również mogą okazać się cenne, niemniej zazwyczaj nie są one pisane przez profesjonalistów i mogą zawierać przekłamania, niejednokrotnie istotne. Jeśli rzeczywiście jakaś istotna luka w

zabezpieczeniach produktów bankowych zostanie wykryta, klienci zostaną o tym poinformowani przez bank, który ma również obowiązek taką lukę usunąć. Bezpieczeństwo klientów leży w dobrze pojętym interesie banku.

Wiedza o mechanizmach funkcjonowania bankowości elektronicznej oraz o potencjalnych zagrożeniach wynikających z jej korzystania pozwoli konsumentom ustrzec się przed działaniem przestępców.