RAPORT ZBP
Cyberbezpieczny portfel

Czerwiec, 2018 r.

Związek Banków Polskich

Bankowcy dla Edukacji
Program sektorowy

1

70 proc.

Polaków przyznaje, że nie zmieniało hasła do bankowości internetowej w ciągu ostatniego roku

Źródło: Komisja Europejska

2

o 72 proc.

wzrosła liczba użytkowników bankowości internetowej w latach 2010-2017

Źródło: Netbank

3

74 proc.

Polaków nie dostrzega potrzeby podnoszenia wiedzy w zakresie cyberbezpieczeństwa

Źródło: Kantar TNS na zlecenie ZBP

4

82 proc.

Polaków uważa, że rośnie ryzyko stania się ofiarą cyberataku

Źródło: Monitor Bankowy, kwiecień 2018

5

91 proc.

Polaków uważa korzystanie z bankowości internetowej i mobilnej za bezpieczne

Źródło: Kantar TNS na zlecenie ZBP

Szanowni Państwo,

w ostatnim dziesięcioleciu bankowość elektroniczna na dobre zagościła w domach i biurach Polaków. Nowoczesne technologie sprawiły, że klienci otrzymali zdalny dostęp do swojego banku przez komputer, tablet czy smartfon, a sama bankowość elektroniczna w szybkim czasie stała się ważną i nierozłączną już częścią bankowości. E-bankowość zwiększa wygodę klientów, poprawia dostępność usług i pozwala na redukcję kosztów. Musimy pamiętać jednak, że korzystanie ze zdalnego, elektronicznego dostępu do banku to nie tylko udogodnienie, ale również niezwykła odpowiedzialność. Z jednej strony odpowiedzialność banku, który musi stworzyć optymalną infrastrukturę zapewniającą najwyższy poziom bezpieczeństwa zgromadzonych w bankach środków, poufność informacji dotyczących klientów i dokonywanych przez nich transakcji, a jednocześnie umożliwi pewną i szybką weryfikację tożsamości klientów. Z drugiej strony klienci zobowiązani są do korzystania z oferowanych produktów w sposób odpowiedzialny i staranny, co wiążą się na przykład z koniecznością zapoznania się z regulaminami i podstawowymi zasadami bezpieczeństwa. Z pewnością w najbliższych latach infrastruktura polskiej bankowości będzie się stale dostosowywała do nowych wyzwań i zagrożeń, jednak również klienci powinni zachować otwartość na przyswajanie informacji, które pozwolą odpowiedzialnie budować bankowość elektroniczną. W tym zakresie widoczna jest potrzeba stałej edukacji, której naprzeciw wychodzą liczne działania i inicjatywy informacyjne sektora, w postaci zarówno kampanii społecznych promujących cyberbezpieczeństwo, jak i codziennych relacji z klientem.

Zawarte w poniższym materiale zestawienia wskazują, że Polacy czują się bezpiecznie zarówno w banku tradycyjnym, jak i w jego elektronicznej odsłonie, postrzegając banki wręcz jako synonim bezpieczeństwa. Ponad 90 proc. Polaków uważa, że korzystanie z bankowości elektronicznej i mobilnej jest bezpieczne. Jednak, aby pokładane w bankach zaufanie miało pokrycie w rzeczywistości, konieczne jest wiedza i świadomość po stronie klientów, tym bardziej, że dostęp do bankowości elektronicznej posiada już 35,5 mln Polaków, a korzystanie z niej deklaruje 60 proc. rodaków. Liczby te wskazują, że bankowość elektroniczna,

tak jak i gospodarka elektroniczna zaczynają mieć ogromne znaczenie dla całej polskiej gospodarki. Jestem przekonany , że rozwój gospodarki cyfrowej stanowi ogromną szanse na poprawę konkurencyjności polskich firm i efektywności działania administracji. Kluczowe jest tu wykorzystanie potencjału wielu bardzo dobrych informatyków, inżynierów, programistów, którzy przy odpowiednim zorganizowaniu mogą zmieniać naszą gospodarkę czyniąc pracę lżejszą, bezpieczniejszą i wydajniejszą. Aby tak się mogło stać zarówno bankowość elektroniczna, jak i e-commerce muszą być bezpieczne.

Związek Banków Polskich, również dostrzega potrzebę konsekwentnego zwiększania cyberbezpieczeństwa, dlatego właśnie z inicjatywy ZBP, powołane zostało Bankowe Centrum Cyberbezpieczeństwa, które monitoruje incydenty i zagrożenia w sieci oraz koordynuje i zarządza trudnymi sytuacjami. Realizując te zdania współpracujemy zarówno z odpowiednimi strukturami państwa, jak i innymi interesariuszami kluczowymi dla bezpieczeństwa e-bankowości. Związek działa również aktywnie na polu edukacji, upowszechniając wiedzę z zakresu cyberbezpieczeństwa poprzez cykliczne publikacje. Jedną z nich jest „Cyberbezpieczny portfel", który niniejszym przekazujemy w Państwa ręce. Zawiera on nie tylko analizę sytuacji, ale również zbiór prostych, podstawowych porad, które zwiększą bezpieczeństwo naszego portfela, a także pozwolą ochronić nasze dane osobowe przed ich wyłudzeniem i bezprawnym wykorzystaniem.

Liczymy, że lektura poniższego raportu nie tylko przybliży Państwu tematykę cyberbezpieczeństwa, ale również pomoże ustrzec przed zagrożeniami w sieci.

Krzysztof Pietraszkiewicz
Prezes Związku Banków Polskich

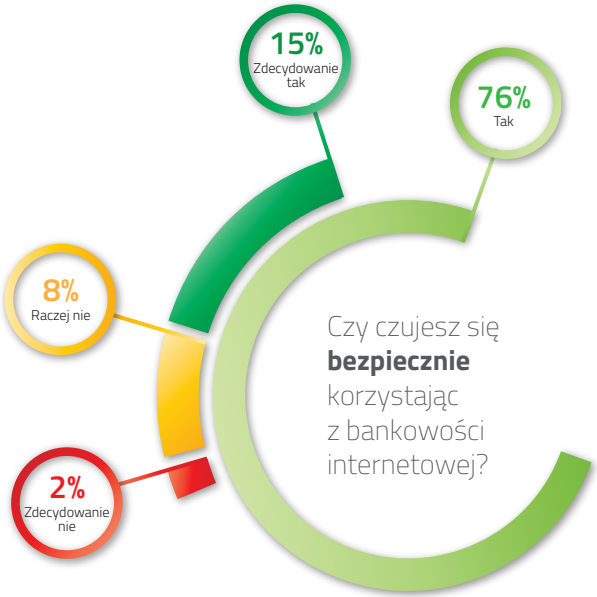
Spis treści

Zaufanie do nowoczesnych technologii bankowych

Polacy coraz chętniej korzystają z bankowości internetowej i mobilnej, bo uważają ją za bezpieczną, wygodną i szybką formę korzystania z produktów bankowych.

Niestety, poziom świadomości dotyczącej cyber-bezpieczeństwa nie przystaje do popularności korzystania z nowych technologii.

91 procent Polaków deklaruje, że korzystanie z bankowości internetowej i mobilnej jest bezpieczne. Tak odpowiedzieli respondenci w badaniu Związku Banków Polskich przeprowadzonym na potrzeby tego raportu. Liczba ta jest powodem do satysfakcji dla bankowców, który dbają o zapewnienie wysokiego poziomu bezpieczeństwa systemu bankowego. Cyber-bezpieczeństwo jest jednak obszarem, stwa-



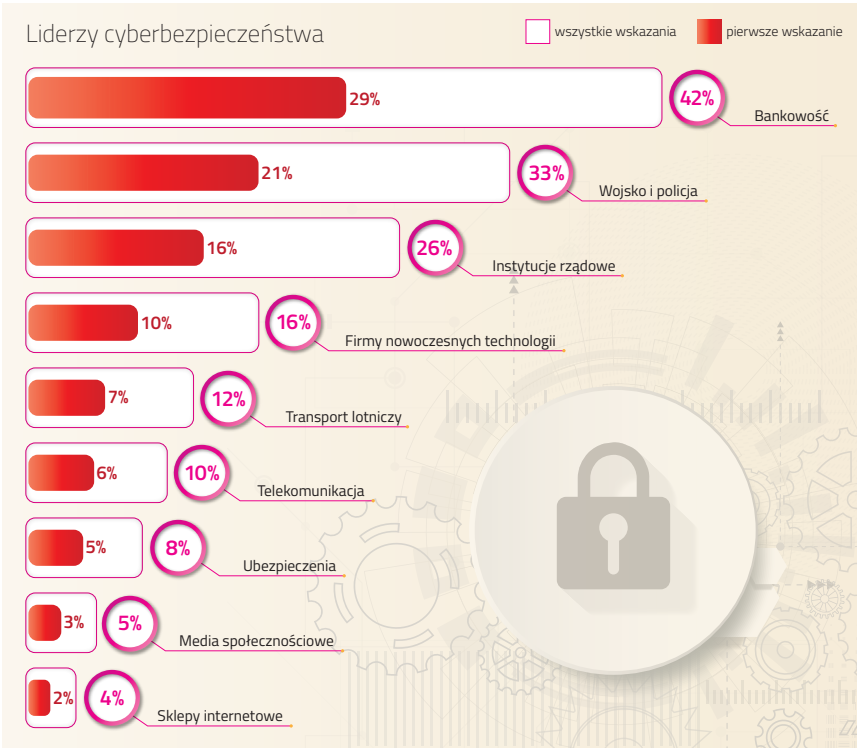
Źródło: Kantar TNS na zlecenie ZBP

91 PROCENT POLAKÓW deklaruje, że korzystanie z bankowości internetowej i mobilnej jest **BEZPIECZNE**.

Źródło: Kantar TNS na zlecenie ZBP

rzającym coraz więcej zagrożeń, których istnienie należy sobie uświadomić. Wychodząc naprzeciw temu celowi Związek Banków Polskich przygotował raport podsumowujący główne wnioski dotyczące podejścia Polaków do cyberbezpieczeństwa.

Polacy wskazują banki za jedne z najbezpieczniejszych podmiotów na polskim rynku. 42 proc. ankietowanych w badaniu ZBP postrzega banki jako liderów cyberbezpieczeństwa (tj. o 9 pp. więcej niż podmiot na drugim miejscu, czyli wojsko i policję).



Źródło: Kantar TNS na zlecenie ZBP

42 PROCENT POLAKÓW
uznaje banki za liderów cyberbezpieczeństwa

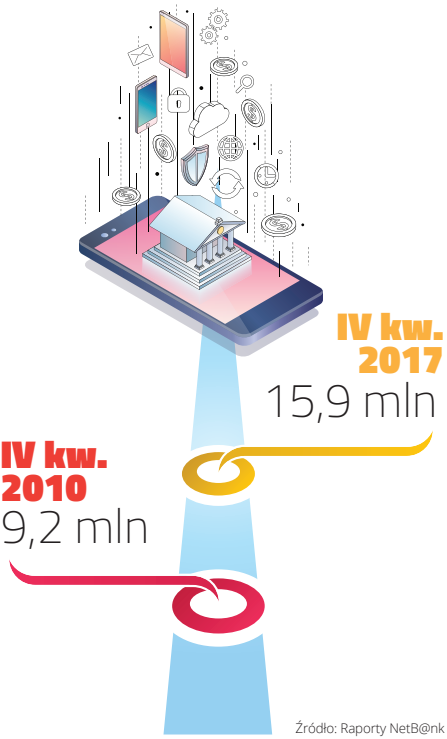
Źródło: Kantar TNS na zlecenie ZBP

Korzystanie z bankowości elektronicznej

Wysoki poziom konkurencji na polskim rynku bankowym spowodował, że krajowe instytucje finansowe pod względem rozwoju nowoczesnych technologii plasują się w ścisłej europejskiej czołówce. Polacy mają codzienny dostęp do rozwiązań dopiero wdrażanych na świecie – takie produkty jak kantory walutowe, płatności mobilne, czy karty wielowalutowe oferuje w tej chwili większość polskich banków. Chętnie z nich korzystają, co pokazują dane publikowane w raporcie NetB@nk – kwartalnym raporcie o bankowości elektronicznej, opracowywanym przez Związek Banków Polskich.

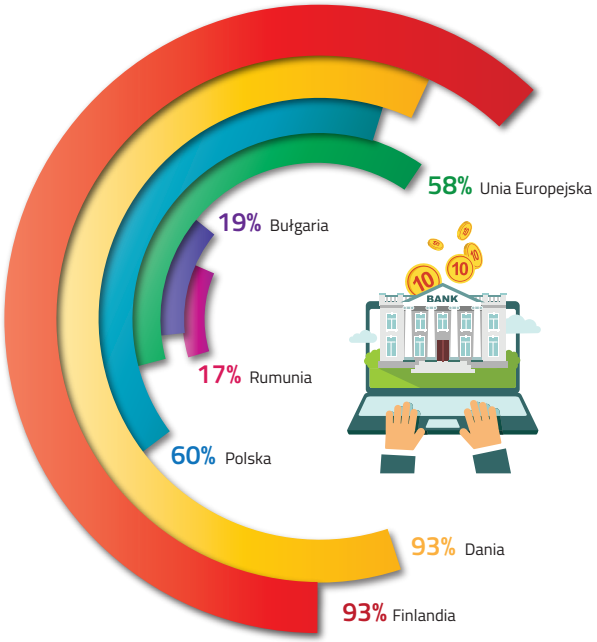
W ciągu ostatnich 7 lat wykorzystanie bankowości internetowej w Polsce wzrosło prawie dwukrotnie. W 2010 roku liczba aktywnych użytkowników bankowości internetowej wynosiła niewiele ponad 9 milionów. W 2017 r. z bankowości internetowej korzystało prawie 16 milionów Polaków. Dziś dostęp do takich na-

Liczba Polaków korzystająca z bankowości internetowej (w milionach)



Źródło: Raporty NetB@nk

Odsetek populacji korzystający z bankowości internetowej

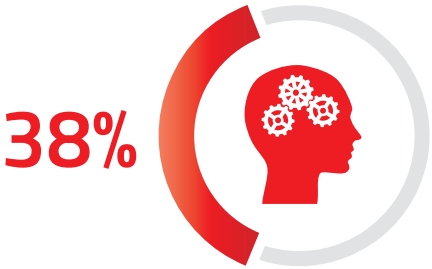


Źródło: Komisja Europejska

rzędzi jest bardzo prosty – liczba klientów mających podpisane z bankami umowy dające im możliwość korzystania z tego rodzaju usług posiada 35, 5 miliona Polaków (dla porównania w IV kw. 2010 roku było to 16,2 miliona klientów).

Porównując do pozostałych państw Unii Europejskiej, w zakresie korzystania z bankowości elektronicznej Polacy plasują się w środku stawki. Według badania przeprowadzonego przez Komisję Europejską, w Polsce 60 proc. respondentów odpowiedziało, że korzysta z bankowości internetowej, czyli o 2 pp. więcej niż średnia dla państw UE. Nowoczesne formy bankowości najbardziej popularne są w krajach skandynawskich, najmniej w Rumunii i Bułgarii, w tych krajach korzysta z niej zaledwie kilkanaście procent ludności. Wykorzystanie usług elektronicznych regularnie się powiększa – grupa użytkowników bankowości internetowej rośnie we wszystkich krajach Unii Europejskiej i jest obecnie o 3 pp. większa w Polsce w porównaniu z badaniem z 2014 r.

Z wprowadzaniem nowych technologii nieodłącznie związany jest jednak wymóg utrzymania bezpieczeństwa oraz obowiązek stałego inwestowania w technologie podnoszące poziom zabezpieczeń. Koszty ponoszone przez banki związane z zapewnieniem techno-

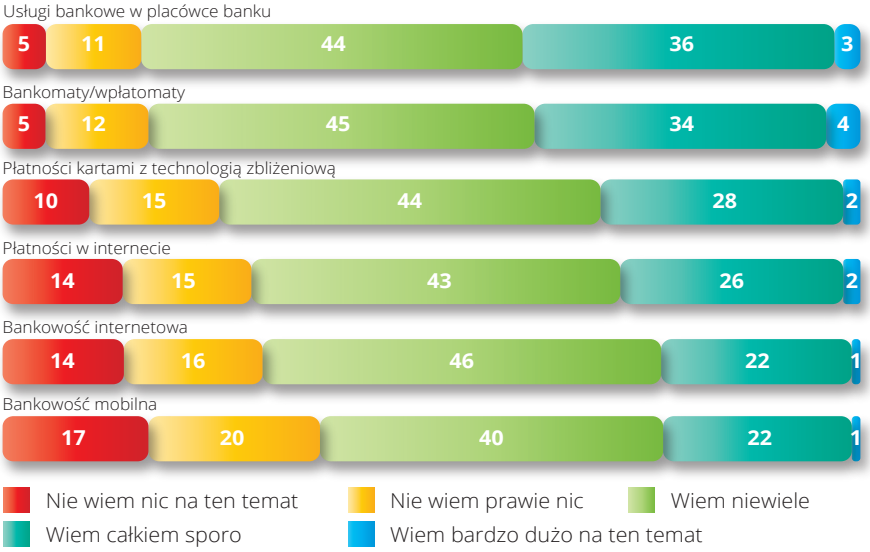


38 PROCENT POLAKÓW
uznaje swoją wiedzę dotyczącą cyberbezpieczeństwa za niewystarczającą

Źródło: Warszawski Instytut Bankowości

logicznego bezpieczeństwa wdrażanych rozwiązań są gwarancją funkcjonowania całego systemu finansowego. Niestety, z szybkim przyswajaniem nowych technologii przez Polaków nie wiąże się wzrost poziomu świadomości w zakresie bezpieczeństwa w sieci. O czym świadczą badania opinii zrealizowane w 2018 roku przez Kantar TNS dotyczące deklarowanej wiedzy Polaków w zakresie różnych aspektów cyberbezpieczeństwa w sieci. Sektor bankowy w tym Związek Banków Polskich od lat prowadzi liczne działania, których celem jest poprawa świadomości klientów w obszarze cyberbezpieczeństwa. Zarówno kampanie medialne, publikacje prasowe, debaty, badania opinii jak i codzienny kontakt z klientami banków nakierowany jest na poprawę świadomości w tym zakresie. Od 2016 roku przy ZBP funkcjonuje również Komitet - Bankowe Centrum Cyberbezpieczeństwa"

Percepcja cyberbezpieczeństwa w zakresie bankowości elektronicznej – deklarowana wiedza Polaków



Źródło: Kantar TNS na zlecenie ZBP

Według badania przeprowadzonego przez Warszawski Instytut Bankowości Poziom edukacji finansowej 2018 cyberbezpieczeństwo jest jednym z tematów, co do których Polacy czują największy niedobór wiedzy. Rezultaty badania pokazują, że niedostatecznie poinformowanymi w tym zakresie czuje się 38 proc. Cyberbezpieczeństwo jest bardzo wyspecjalizowanym obszarem wiedzy, co może sprawiać, że Polacy nisko oceniają swój poziom kompetencji w tej dziedzinie.

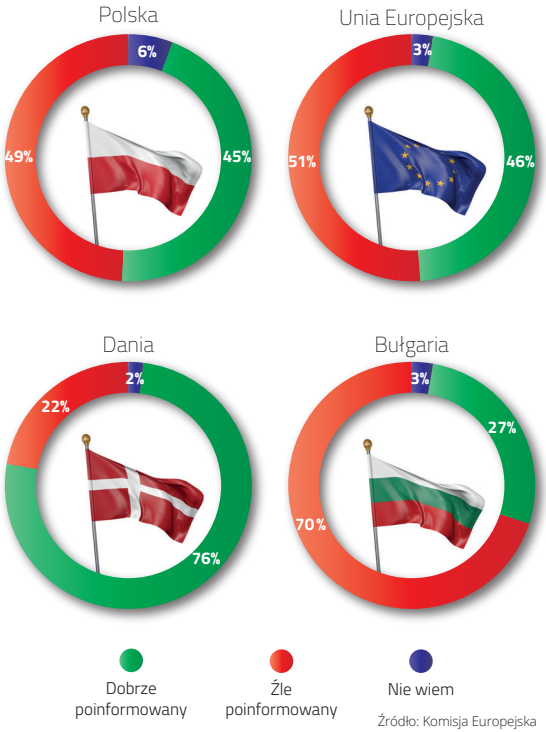
Brak znajomości ryzyk związanych z bezpieczeństwem w sieci może wynikać z podobnych odczuć w zakresie wiedzy o usługach bankowych. 77 proc. badanych uznało swój poziom kompetencji w zakresie użytkowania b. mobilnej za niski, a 76 proc. odnosi się w ten sposób także do bankowości internetowej (dane ZBP).

Dane Komisji Europejskiej są jeszcze bardziej niepokojące – aż 49 proc. Polaków czuje się źle poinformowana o cyberbezpieczeństwie.

Najmniejszą wiedzę spośród mieszkańców Unii Europejskiej w zakresie cyberbezpieczeństwa deklarują Bułgarzy – w taki sposób odpowiedziało 70 proc. respondentów. Najlepiej poinformowani czują się Duńczycy – tylko 22 procent z nich czuje czuje w tym zakresie duże niedostatki.. W Polsce poziom opanowania tego obszaru wiedzy jest zbliżony do średniej w Unii Europejskiej.

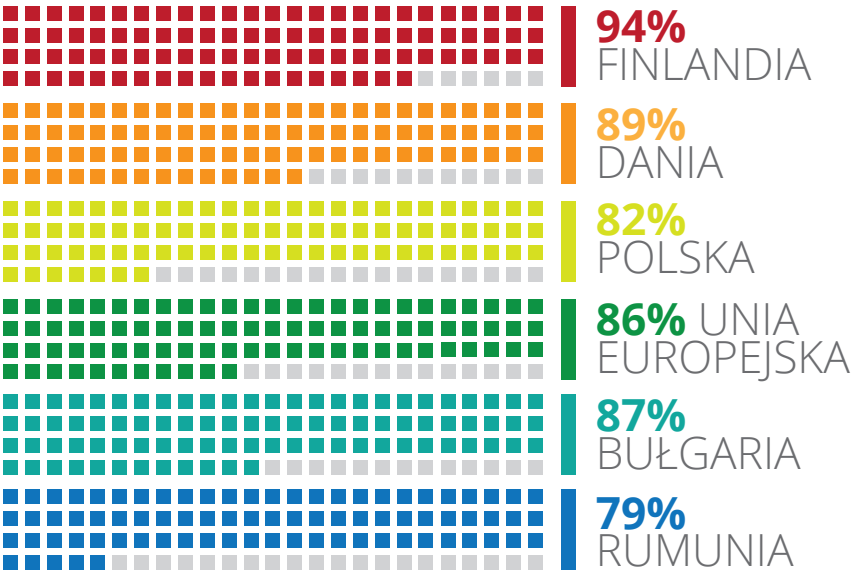
Większość Europejczyków jest jednak świadoma rosnącego ryzyka funkcjonowania w cyberprzestrzeni. 86 proc. mieszkańców Unii Europejskiej uważa, że ryzyko stania się ofiarą cyberataku rośnie. Podobną opinię mają Polacy – 82 procent z nich jest takiego samego zdania w tej kwestii.

Deklarowany poziom wiedzy dot. cyberbezpieczeństwa w wybraniach krajach europejskich



Źródło: Komisja Europejska

Odsetek populacji, który uważa, że rośnie ryzyko stania się ofiarą cyberataku



Źródło: Komisja Europejska

Zagrożenie cyberbezpieczeństwa nie musi być bowiem związane tylko i wyłącznie z wyspecjalizowanym cyberatakiem. Awarie systemów elektronicznych różnego pochodzenia mogą zagrozić naszemu bezpieczeństwu – związane z przerwą w dostawie energii elektrycznej, czy zwykłą awarią serwerów również.

Za wysoce prawdopodobne bankowcy uznają również ryzyko kradzieży danych kart płatniczych i danych dostępowych do bankowości elektronicznej. Z kolei za mało prawdopodobne uznaje się ataki na poziomie całego kraju i wycieki danych bezpośrednio z banków.

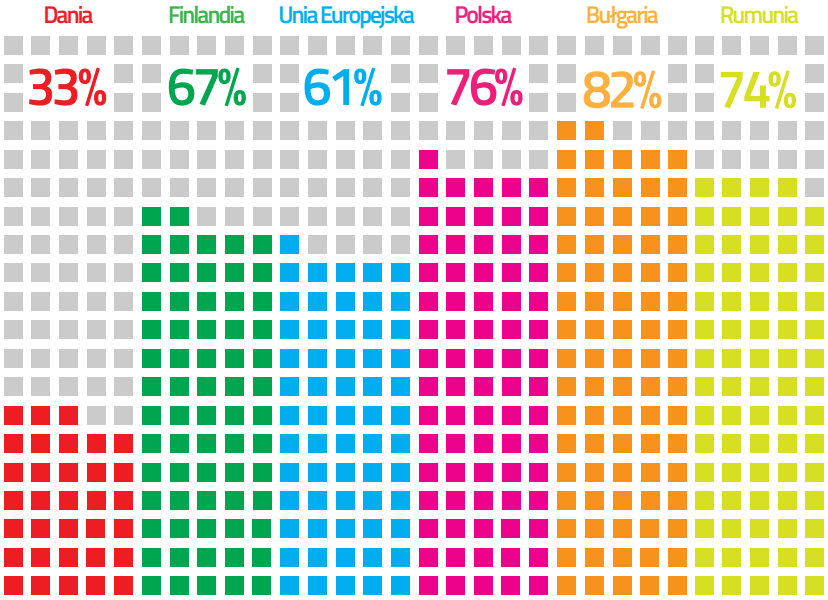
Za zaskakujące, w stosunku do świadomości Polaków w zakresie cyberbezpieczeństwa, można uznać odpowiedzi Polaków na pytanie dotyczące potrzeb edukacji w tym obszarze. Aż 74 proc. respondentów uważa, że nie potrzebuje podnosić swojej wiedzy na temat bezpiecznego korzystania z bankowości internetowej i mobilnej (badanie Kantar TNS na zlecenie ZBP).

Polacy nie uważają, że powinni podnosić swoją wiedzę związaną z korzystaniem z usług bankowych

Jak często zdarzają się cyberataki?

Europejczycy uważają, że ryzyko stania się ofiarą cyberataku jest coraz większe, mimo że potencjalnie niebezpieczne sytuacje nie zdarzają nam się często. Na tle innych krajów Unii Europejskiej Polska w ocenie klientów wypada dość dobrze – 23 proc. respondentów z Polski odpowiedziało, że doświadczało prób wyłudzeń prywatnych informacji (w tym dostępu do komputera i bankowości internetowej) poprzez wiadomości e-mailowe i telefony. Najwięcej prób wyłudzeń poufnych informacji jest odnotowywanych przez mieszkańców Danii (66 proc.), co nie musi jednak świadczyć o tym, że w tym kraju przeprowadzana jest największa liczba ataków. Duńczycy czują się najlepiej wyedukowani w zakresie cyberbezpieczeństwa w Europie, przez co częściej mogą oni identyfikować próby oszustwa. W Finlandii, kraju w którym 93 proc. ludności korzysta z bankowości elektronicznej, jedna trzecia twierdzi, że była w sytuacji potencjalnie zagrażającej bezpieczeństwu w sieci. W Polsce odsetek ten wynosi 38 proc.

Odsetek osób, które doświadczyły takiej sytuacji jak otrzymanie wiadomości e-mail lub telefonu, podczas którego ktoś próbował uzyskać prywatne dane (np. hasła i loginy do bankowości, dane dotyczące płatności online).

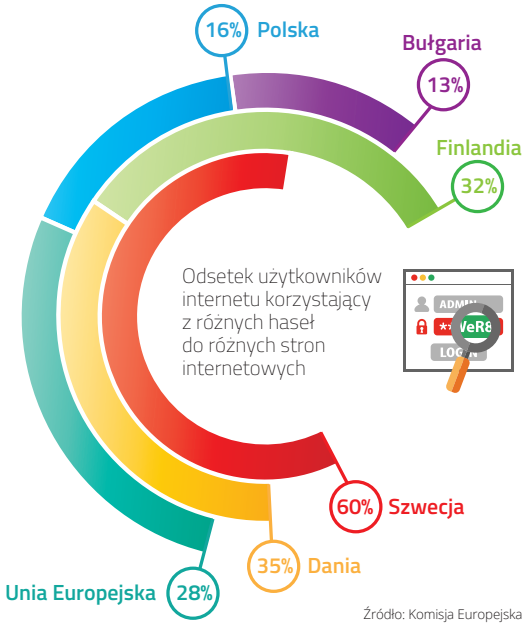


Źródło: Komisja Europejska

Jak się zabezpieczamy przed cyberatakami?

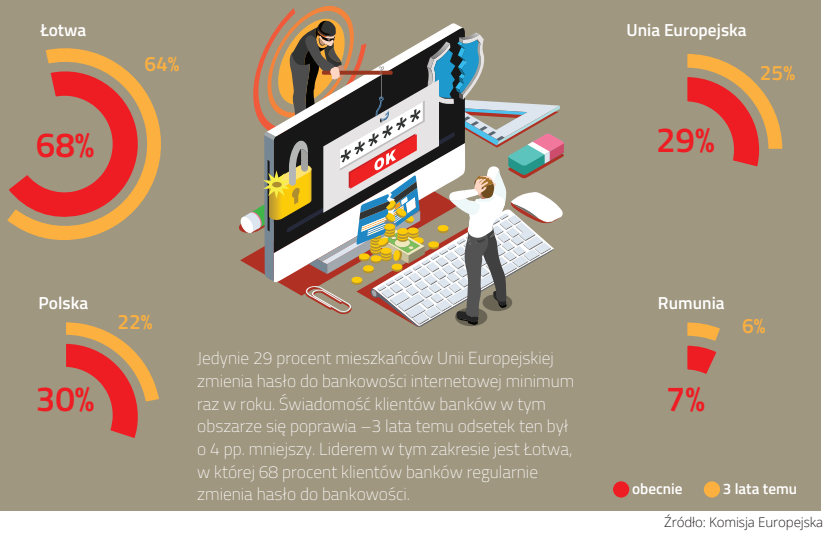
Niestety wraz ze wzrostem świadomości o rosnącym ryzyku stania się ofiarą cyberataku nie rośnie poziom indywidualnej ochrony przez niebezpieczeństwami w cyberprzestrzeni.

Obowiązkiem instytucji przechowujących wrażliwe dane jest odpowiednie ich zabezpieczenie przed kradzieżą, jednak istnieją sposoby ograniczenia ryzyka wyłudzenia prywatnych informacji, które może wykonać konsument. Wszak nawet



Źródło: Komisja Europejska

Odsetek osób, które w ciągu ostatnich 12 miesięcy zmieniły hasło do bankowości internetowej



Jedynie 29 procent mieszkańców Unii Europejskiej zmienia hasło do bankowości internetowej minimum raz w roku. Świadomość klientów banków w tym obszarze się poprawia – 3 lata temu odsetek ten był o 4 pp. mniejszy. Liderem w tym zakresie jest Łotwa, w której 68 procent klientów banków regularnie zmienia hasło do bankowości.

Źródło: Komisja Europejska

13 PROC. POLAKÓW podejmowała w ostatnim roku konkretne działania, by czuć się bezpieczniej w trakcie korzystania z bankowości elektronicznej

Źródło: Komisja Europejska

najbardziej zaawansowane systemy bezpieczeństwa nie będą efektywne, jeśli podstawowe zasady nie będą przestrzegane przez użytkowników internetu i nowoczesnych usług bankowych. Do takich czynności należą między innymi częsta zmiana haseł do kont, nie używanie prostych skojarzeń w ich tworzeniu, czy nie zapisywanie ich na papierze. Według badania przeprowadzonego przez KE nawyki użytkowników internetu zmieniają się na lepsze, jednak w wielu krajach Unii Europejskiej pozostaje w tym zakresie jeszcze wiele do zrobienia. Jedną z podstawowych i prostych czynności, jaką jest zmiana hasła do konta bankowego minimum raz w roku wykonuje w Polsce tylko ok. 30 procent osób korzystających z bankowości elektronicznej. Jeszcze mniej Polaków różnicuje trudność hasła dostępu w zależności od strony na którą się loguje – jedynie 16 procent, w porównaniu do 28 procent w Unii Europejskiej.

Ochrona banków przed cyberzagrożeniami

Z danych zebranych w badaniu przeprowadzonym wśród bankowców przez Kantar TNS wynika, że pracownicy banków dobrze oceniają poziom zabezpieczeń przed cyberatakami stosowany przez ich instytucje. 84 proc. bankowców uważa, że banki chronią klientów przed kradzieżą danych z kart debetowych i kredytowych, a 92 proc. – przed oszustwami dokonywanymi podczas płatności elektronicznych. Najlepiej oceniana jest ochrona banków przed wyciekiem danych klientów z samego banku – ten rodzaj ochrony wysoko ocenia 96 proc. bankowców.

Odpowiedzi bankowców dotyczące poziomu zabezpieczeń stosowanych przez banki wskazują, że w ich opinii głównym ogniwem podatnym na cyberataki jest klient banku. Teza ta jest o tyle uzasadniona, że banki posiadają wyspecjalizowane departamenty IT które na bieżąco analizują ryzyko cyberataku i identyfikują zagrożenia. W przypadku indywidualnych jednostek często dokonanie oszustwa umożliwia zwykła nieuwaga użytkownika.

Czy banki chronią klientów przed zdarzeniami takimi jak...?
(Badanie wśród bankowców, suma odpowiedzi „Zdecydowanie tak", „Raczej tak")

Źródło: Monitor bankowy, kwiecień 2018

Za najbardziej prawdopodobne zdarzenia z zakresu cyberprzestępczości bankowcy uważają kradzież danych kart debetowych i kredytowych oraz przechwycenie danych do konta bankowego. Jednocześnie uważają oni, że ochrona banków przed tego rodzaju zagrożeniami jest najmniejsza (z uwagi na to, że duża część odpowiedzialności spoczywa w tych przypadkach na kliencie). Najwyższą ochronę w ich opinii banki zapewniają w sytuacji włamań na internetowy rachunek bankowy i wycieku danych, nieco mniejszą w przypadku krajowych i transgranicznych cyberataków.

Bez względu na dostępne dane nt. społecznej wiedzy i z racji dużej dynamiki w dziedzinie cyberbezpieczeństwa (zarówno pod kątem potencjalnych zagrożeń, jak i metod ich zwalczania), niezbędne pozostaje prowadzenie szerokich działań edukacyjnych.

83 PROC. POLAKÓW oczekuje, że po wystąpieniu cyberataku instytucja niezwłocznie poinformuje ich o jego zajściu i jego skutkach i natychmiast wprowadzi procedury rozwiązujące problem

Źródło: Kantar TNS na zlecenie ZBP

Jednym z przykładów efektywnej współpracy jest połączenie sił sektora bankowego, IT i samorządów terytorialnych w ramach projektu „Bezpieczeństwo w Cyberprzestrzeni", realizowanego od 2017 r. Jest on elementem jednego z największych programów edukacji finansowej w Europie – „Bankowcy dla Edukacji".

Celem porozumienia „Bezpieczeństwo w Cyberprzestrzeni" zawartego między bankami (ZwiązekBankówPolskich, Pekao, BZ WBK, ING BŚ, mBank), fundacjami (Cyberium, Polska Bezgotówkowa), sklepami internetowymi (Allegro) i firmami IT (IBM Polska, Microsoft) jest m.in. prowadzenie lekcji z zakresu cyberbezpieczeństwaw polskich szkołach. W samym 2017 roku w ramach porozumienia przeprowadzono blisko 800 lekcji i wykładów, w których uczestniczyło ponad 16 000 uczniów i blisko 3 500 studentów w całej Polsce.

Największe finansowe cyberataki 2017 r.

WannyCry, maj 2017r.

Atak WannaCry, którego nazwa pochodzi od rozszerzenia pliku infekującego komputery .WNCRY. Jest to rodzaj oprogramowania szantażującego *ransom ware*, czyli takiego który blokuje dostęp do danych użytkownika zanim ten nie wpłaci oszustom wymaganego okupu. Według danych Europolu (policyjnej agencji Unii Europejskiej) atak WannaCry był największym tego rodzaju w ostatnich kilku latach. Ofiarą cyberwirusa były między innymi hiszpańskie banki i firmy telekomunikacyjne, angielskie związki szpitali oraz rosyjskie Ministerstwo Spraw Wewnętrznych. W sumie mówi się, że zainfekowanych zostało ponad 300 tys. komputerów w 99 krajach[1], a przestępcy żądali zapłaty w 28 językach (w tym polskim). O dokonanie ataku posądzana jest Korea Północna.

1 Maciej Czarnecki, Oto Marcus Hutchins, 22-letni Brytyjczyk, który zatrzymał światowy cyberatak, wyborcza.pl, 16 maja 2017

Według bankowców **78 PROC. KLIENTÓW** zgłasza incydenty w obszarze cyberbezpieczeństwa co najmniej raz w roku

Źródło: Monitor bankowy, kwiecień 2018

Notpetya, czerwiec 2017

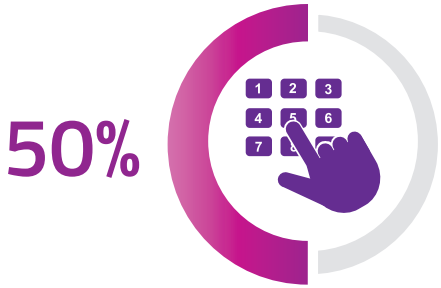
Odmiana wirusa Petya – ransom ware odkrytego w 2016 roku. Wirus blokował dostęp do systemu operacyjnego i żądał okupu w kryptowalucie, co miało umożliwiać przywrócenie dostępu do systemu. W czerwcu 2017 r. zidentyfikowany został cyberatak na Ukrainie, w którym wirus był nowym wariantem Petya (nazwany przez KasperskyLab Notpetya). Cyberataki Notpetya dotknęły przede wszystkim ukraińskie i rosyjskie instytucje (80 firm, w tym m.in. ukraiński bank centralny), jednak ataki zostały zidentyfikowane także we Francji, Niemczech, Włoszech, Polsce, Stanach Zjednoczonych i Wielkiej Brytanii.

Atak na organy sprawujące kontrolę nad rynkiem finansowym, luty 2017 r.

Atak był jednym z pierwszych dużych cyberataków na instytucje publiczne w Polsce i zaliczany jest do kategorii zwanej techniką wodopoju. Celem ataku nie była bowiem sama instytucja, ale osoby, które odwiedzają konkretne obszary jej strony internetowej. Dzięki temu atakujący nie musi docierać do tej grupy ofiar, która go interesuje, tylko czeka, aż ofiary same trafią na zainfekowaną stronę. Wirus dokonuje selekcji osób poprzez adres IP, następnie przekierowuje ofiarę na stronę, która atakuje przeglądarkę internauty. W tym przypadku atak odbywał się poprzez wtyczki do przeglądarki, skąd płynie ważny wniosek o wyłączaniu wtyczek w przeglądarce. Atak wykryty został przez pracowników banków, dzięki czemu nie zostały one zainfekowane wirusem, a dane klientów banków pozostały bezpieczne.

Atak na włoski bank, lipiec 2017 r.

Bank oświadczył, że hakerzy włamując się do systemów banku uzyskali dostęp do danych 400 tys. klientów. Do serii ataków miało dojść we wrześniu i październiku 2016 r. oraz



50 PROC. POLAKÓW nie zmienia regularnie pinu-u i hasła do bankowości internetowej

Źródło: Kantar TNS na zlecenie ZBP

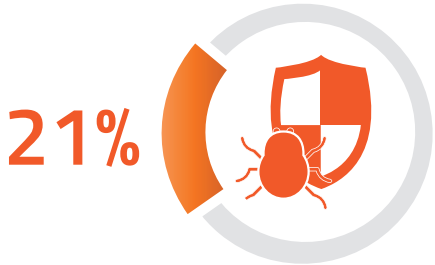
czerwcu i lipcu 2017r. Hakerzy prawdopodobnie uzyskali dostęp do numerów IBAN i danych osobowych, nie mieli oni jednak uzyskać haseł dostępu do kont i transakcji. Do ataku mogło dojść poprzez zagranicznego partnera banku.

Atak na rosyjski bank, luty 2017 r.

W lutym 2018 r. rosyjski bank centralny podał informację o kradzieży 18,9 mln zł z jednego z rosyjskich banków. Atak miał miejsce w 2017r., hakerzy mieli włamać się do systemu banku poprzez system płatności SWIFT (Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej), międzynarodowe stowarzyszenie utrzymujące sieć telekomunikacyjną służącą do wymiany informacji o transakcjach finansowych między bankami i innymi instytucjami sektora.

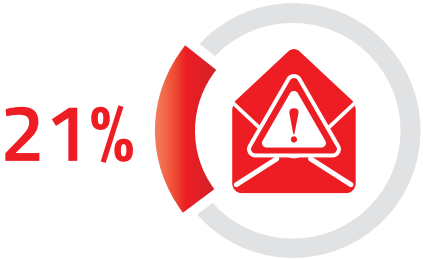
Ataki na biura informacji gospodarczej, lipiec 2017 r.

W lipcu celem ataku hakerskiego stało się jedno z większych amerykańskich biur informacji gospodarczej. Przestępcy ukradli dane osobowe 145 milionów osób. Kilka miesięcy



21 PROC. POLAKÓW nie posiada zainstalowanego i aktualnego programu antywirusowego

Źródło: Kantar TNS na zlecenie ZBP



21 PROC. POLAKÓW otwiera załączniki lub klika w linki w mailach od nieznanych nadawców

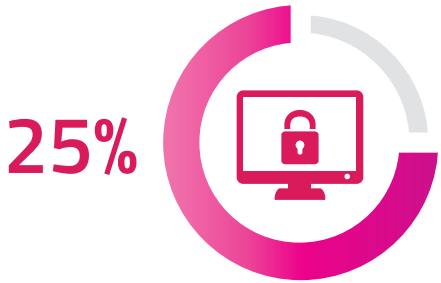
Źródło: Kantar TNS na zlecenie ZBP

później celem ataku stało się drugie biuro gospodarcze w Stanach. Nie wiadomo kto stał za obydwoma atakami.

Spoofing

Pod mianem spoofingu kryje się zjawisko podszywania się pod znane firmy i instytucje (domain spoofing – podszywanie się pod domeny znanych instytucji, e-mail spoofing – wysyłanie wiadomości z adresów instytucji). Ta metoda oszustwa, nawet jeśli mniej efektowna, niż globalne cyberataki, to z uwagi na skalę należy wg ekspertów do najniebezpieczniejszych narzędzi przejmowania danych. Ofiarą takich ataków najczęściej stają się bowiem zwykli obywatele. Oszuści najczęściej podszywają się pod gigantów technologii, takich jak Amazon, Apple, czy PayPayl, jednak w ostatnich miesiącach cyberprzestępcy podszywali się również pod linie lotnicze, serwis Netflix, pracowników instytucji publicznych, w tym ministerstw, ale także polskich banków.

Jak wygląda taki sfałszowany e-mail? Treścią i obrazem przypomina prawdziwa wiadomość, jedyną różnicą jest adres, pod jaki użytkownik zostaje przenoszony po kliknięciu w zawarty w wiadomości link. Spoofing od phishingu różni się tym, że poza wyłudzeniem danych wrażliwych wirus instaluje w systemie operacyjnym użytkownika złośliwe oprogramowanie, które może na przykład masowo wysyłać nieprawdziwe wiadomości używając do tego tożsamości użytkownika, co czyni oszustwo skuteczniejszym.



25 PROCENT POLAKÓW nie zwraca uwagi na symbol kłódki i https:// na początku adresu strony internetowej

Źródło: Kantar TNS na zlecenie ZBP

O czym pamiętać?

- **Ustaw silne hasło**
  - Silne hasła to takie, które składają się z wielkich i małych liter, cyfr i znaków specjalnych.
  - Trudne do wykrycia są hasła nie związane z charakterystycznymi danymi, które można przypisać do danej osoby, np. miejscem urodzenia, imieniem bliskiej osoby itd.

- **Regularnie zmieniaj hasło**
  - Zrób z tego nawyk (zmieniaj je np. pierwszego dnia każdego miesiąca razem z opłacaniem rachunków)
  - Jeśli masz problemy z zapamiętaniem hasła, nie musisz zmieniać całego hasła - wystarczy, że w jakiś sposób je zmodyfikujesz

- **Stosuj różne hasła do różnych serwisów**
  - Nie używaj tego samego hasła do wielu serwisów (np. do bankowości internetowej, poczty e-maila czy serwisów społecznościowych). Jeśli któreś z kont zostanie przejęte przez hackera, pozwoli to uchronić twoje pozostałe dane.
  - Profiluj trudność hasła do tego, jak ważne dla Ciebie informacje ono chroni

- Nie udostępniaj swojego komputera innym osobom, jeśli nie musisz - nie masz kontroli nad tym, czy te osoby nie narażą go na niebezpieczeństwo
- Wyłącz automatyczne zapamiętywanie haseł w swojej przeglądarce internetowej.
- Nie zapisuj nigdzie swoich haseł i numerów pin.
- Zainstaluj na swoim komputerze program antywirusowy i regularnie go aktualizuj.

Systemy antywirusowe zazwyczaj same przypominają o koniecznych do wprowadzenia aktualizacjach, wystarczy włączyć opcje przypominania o nich.

- Nie podłączaj się do publicznych sieci Wi-Fi, jeśli nie musisz. Gdy z nich korzystasz, nie loguj się do portali społecznościowych czy bankowości elektronicznej
- Nie płać kartą na stronach internetowych, które wydają Ci się podejrzane
- Sprawdzaj domeny (końcówki adresu internetowego) stron bankowych. Złodzieje często tworzą „duplikaty" takich stron
- Sprawdzaj z jakiego adresu e-mailowego przyszła dana wiadomość. Nie wchodź na strony bankowe poprzez załączniki wysyłane w e-mailach (hakerzy często podszywają się w ten sposób pod banki).
- Nie podawaj żadnych swoich danych w e-mailowej korespondencji z bankiem (numery autoryzacyjne do transakcji, hasło i login do konta etc.). Bank nigdy nie będzie prosił Cię o podawanie takich informacji przez e-mail.

Co zrobić gdy padniemy ofiarą cyberataku?

Jeśli podejrzewasz, że padłeś ofiara cyberataku:

- Zgłoś swoje podejrzenie na policję oraz do instytucji, z którą związany jest cyberatak (swojego banku etc.)
- Zgłoś incydent w CERT (Computer Emergency Response Team) (+48 22 380 82 74 lub poprzez stronę https://www.cert.pl/zglos-incydent/)
- Możesz skontaktować się z tzw. pogotowiem komputerowym. Wiele z nich czynne jest całą dobę i oferuje dojazd informatyka do domu

Bankowe Centrum Cyberbezpieczeństwa

Bankowe Centrum Cyberbezpieczeństwa (BCC) to instytucja, której celem jest zapewnienie sektorowi bankowemu rozwiązań pozwalających na utrzymanie poziomu bezpieczeństwa adekwatnego do ryzyka związanego z oferowanymi w cyberprzestrzeni produktami i usługami bankowymi.

BCC realizuje swoje cele poprzez:

1) Budowanie wiedzy i świadomości pracowników i klientów sektora;
2) Ustalenie wspólnych i skutecznych zasad postępowania w obszarze ograniczania ryzyka;
3) Realizacja zadań zdefiniowanych przez Członków w celu osiągnięcia efektu synergii i optymalizacji kosztów przez nich ponoszonych;
4) Współpracę z pozostałymi uczestnikami krajowego systemu cyberbezpieczeństwa.

Źródła

1) Aneks do raportu z wyników badań reputacji sektora bankowego, Kantar TNS na zlecenie Związku Banków Polskich, 2018 r.

2) Monitor Bankowy, kwiecień 2018 r.

3) European attitudes towards cybersecurity Report, Komisja Europejska 2017 r.

PAMIĘTAJ

NIGDY

Nie zapisuj hasła do bankowości internetowej.

#CYBERBEZPIECZNI

NIGDY

Nie podawaj nikomu danych logowania do bankowości internetowej.

#CYBERBEZPIECZNI

NIGDY

Nie wchodź na stronę internetową swojego banku za pośrednictwem linków znajdujących się w przychodzących mailach.

#CYBERBEZPIECZNI

NIGDY

Nie używaj wyszukiwarek internetowych do znalezienia strony logowania banku.

#CYBERBEZPIECZNI

ZAWSZE

Miej włączone oprogramowanie antywirusowe.

#CYBERBEZPIECZNI

ZAWSZE

Płać kartą w internecie tylko u zaufanych sprzedawców.

#CYBERBEZPIECZNI

ZAWSZE

Korzystaj z zaufanych sieci bezprzewodowych i komputerów.

#CYBERBEZPIECZNI

ZAWSZE

Ignoruj maile, w których jesteś proszony o podanie danych do logowania lub autoryzacji. Banki nigdy o to nie proszą.

#CYBERBEZPIECZNI

ZAWSZE

Gdy zgubisz kartę zadzwoń i zastrzeż ją (+48) 828 828 828.

#CYBERBEZPIECZNI

ZWIĄZEK BANKÓW POLSKICH

Bankowcy dla Edukacji
Program sektorowy

WIĘCEJ INFORMACJI:

ZWIĄZEK BANKÓW POLSKICH

dr Przemysław Barbrich
tel. (0-22) 48 68 121
przemyslaw.barbrich@zbp.pl

Paweł Minkina
tel: (0-22) 48 68 153
pawel.minkina@zbp.pl

Michał Polak
tel. (0-22) 48 68 119
michal.polak@zbp.pl