RAPORT

#CYBERBEZPIECZNY PORTFEL – ZASADY BEZPIECZEŃSTWA

grudzień 2016 r.

Związek Banków Polskich

25 LAT 1991-2016

Raport powstał w ramach działań edukacyjno-informacyjnych prowadzonych przez Warszawski Instytut Bankowości

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

Spis treści

Wstęp

Szanowni Państwo

Zbliża się okres świąteczny. Dla większości Polaków wiąże się on nie tylko z miłą, rodzinną atmosferą ale również z okolicznościowymi zakupami. Przedświąteczna gorączka zakupów to także czas, w którym z racji roztargnienia jesteśmy narażeni na utratę lub kradzież nie tylko gotówki, ale także równie ważnych dla nas dokumentów. Pamiętajmy, że gdy utracimy dowód tożsamości, paszport, prawo jazdy, kartę płatniczą czy np. dowód rejestracyjny możemy stać się ofiarami przestępstwa

Mówiąc o bezpieczeństwie naszych finansów, nie należy zapominać o transakcjach dokonywanych kartami płatniczymi, również podczas zakupów online. W związku z rozwojem technologii w sektorze finansowym, związanym z uruchamianiem nowych usług, ale także z uwagi na popularność urządzeń mobilnych i rosnące znaczenie *cloud computingu*, zasady bezpieczeństwa w sieci nie powinny być lekceważone. Im szybciej je poznamy i zastosujemy, tym bezpieczniejsze będą nasze pieniądze i tożsamość.

Nowoczesne technologie sprawiły, że klient otrzymał zdalny dostęp do swojego banku poprzez komputer, telefon i inne urządzenia mobilne. Ważne, by w parze z korzystaniem z innowacji, szła również świadomość o cyber zagrożeniach. Tym bardziej jest to istotne w okresie przedświątecznym, kiedy wzrasta aktywność cyber przestępców, a nasza uwaga może być skupiona na innych, ważnych dla nas, sprawach.

Poniżej przedstawiamy Państwu zbiór prostych porad, które zwiększą bezpieczeństwo naszego portfela, a także pozwolą ochronić nasze dane osobowe przed ich wyłudzeniem i bezprawnym wykorzystaniem.

Związek Banków Polskich

Bezpieczeństwo kart płatniczych

Karta płatnicza jest wygodnym, przyjaznym i bezpiecznym instrumentem płatniczym o szerokim zastosowaniu, jednak korzystając z niej należy pamiętać o zasadach rozsądnego postępowania. Przede wszystkim używajmy karty w miejscach, do tego przystosowanych i właściwie oznaczonych np. znakami graficznymi wydawców kart. Pamiętajmy, że karta powinna zawsze znajdować się w polu naszego widzenia. Niedopuszczalne są sytuacje, w której np. osoba z obsługi sklepu bierze od nas kartę i znika z nią na zapleczu w celu dokonania transakcji. Równie niebezpieczne może być użyczenie karty innej, nawet najbardziej zaufanej osobie. Pamiętajmy, że w razie ewentualnych szkód lub strat, wydawca karty (bank) ma pełne prawo do odrzucenia naszych roszczeń, w przypadku gdy nie posługiwał się nią właściciel.

Coraz więcej Polaków spędzą urlop świąteczny zagranicą. Gdy wypłacamy gotówkę z lokalnych bankomatów, jeśli to możliwe, poszukajmy systemów podobnych do tych znanych z Polski. Jeśli wygląd bankomatu budzi nasz niepokój zrezygnujmy z wypłaty pieniędzy w takim urządzeniu i poszukajmy innego lub poprośmy o pomoc np. w hotelu lub punkcie informacji turystycznej.

W przypadku gdy bankomat nie wydał nam karty lub pieniędzy, jak również gdy otrzymana przez nas kwota różni się od kwoty którą mieliśmy wypłacić- skontaktujmy się z wydawcą karty (numer telefonu do wydawcy znajduje się w internecie oraz na odwrocie karty płatniczej – warto ten numer zapisać)

Również w przypadku utraty karty (kradzieży, zgubienia) konieczny jest niezwłoczny kontakt z wydawcą w celu dokonania zastrzeżenia karty. Kontakt ten ułatwi nam jednolity numer do zastrzegania kart **828 828 828** poprzez który połączymy się z naszym bankiem celem zastrzeżenia karty. Infolinia ta jest dostępna z każdego miejsca na świecie, przez 24 godziny na dobę i 7 dni w tygodniu.

Warto pamiętać

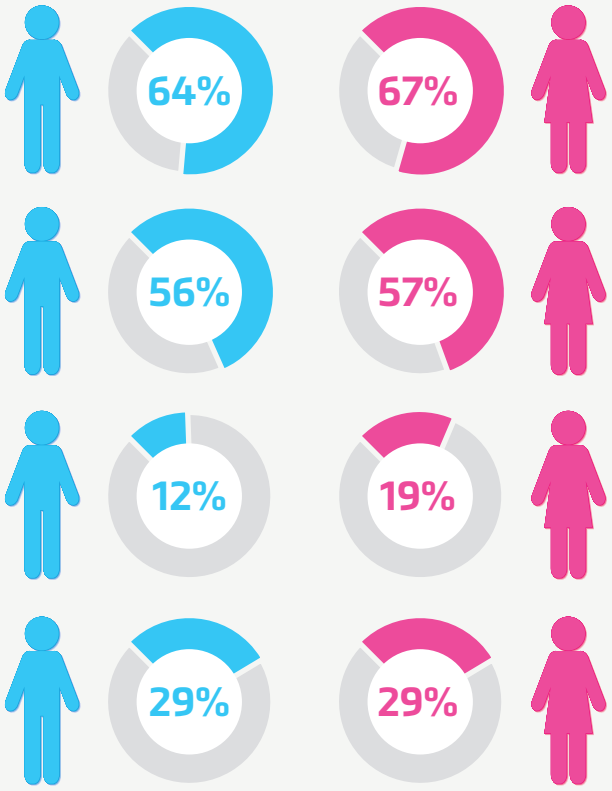
- Nigdy nie zapisujmy numeru PIN na kartkach przechowywanych razem z kartą płatniczą, ani na samej karcie.
- Zawsze zasłaniajmy ręka klawiaturę na której wprowadzamy numer PIN.
- Podstawową zasadą w przypadku problemów z kartą jest jak najszybszy kontakt z jej wydawcą.

6 największych zagrożeń związanych z korzystaniem z kart płatniczych

(na podstawie TNS Polska 2014 r.)

1. **Udostępnianie karty i kodu PIN osobom trzecim**
2. **Nakłanianie do odwiedzenia fałszywej strony internetowej banku (phishing)**
3. **Przekierowanie na sfałszowane strony banków (pharming)**
4. **Posługiwanie się kartami skradzionymi lub zagubionymi**
5. **Zakupy na odległość z wykorzystaniem danych cudzej karty (carding)**
6. **Klonowanie kart zczytywanych z bankomatów (skimming bankomatowy)**

Pamiętaj, aby unikać typowych błędów i złych nawyków!



Utrata dokumentów

System DOKUMENTY ZASTRZEŻONE to ogólnopolski system zastrzegania skradzionych i zagubionych dokumentów tożsamości chroniący przed wyłudzeniami z ich użyciem.

Do najważniejszych dokumentów wykorzystywanych do poświadczania tożsamości zalicza się: dowód osobisty, paszport, prawo jazdy, książeczka marynarska, książeczka wojskowa, karta pobytu. Zastrzegać należy także: karty płatnicze i dowody rejestracyjne.

Jeżeli dojdzie do sytuacji, w której zostaną utracone ważne dokumenty, w tym dowód osobisty, prawo jazdy i paszport, w pierwszej kolejności należy:

- **Zastrzec je w banku** – najłatwiej w swoim. Jeżeli ktoś nie ma rachunku, może to zrobić w banku przyjmującym zastrzeżenia od wszystkich (lista: **www.DokumentyZastrzezone.pl**). Można także skorzystać z **www.bik.pl** (jeżeli założyliśmy tam wcześniej konto na utracony dokument).
- **Zgłosić się do najbliższej jednostki Policji** – tylko jeżeli dokumenty zostały skradzione.
- **Zawiadomić gminę lub placówkę konsularną** – w celu wyrobienia nowego dokumentu.

Dokumenty mogą również zastrzegać osoby, które nie są klientami żadnego banku.

Łączna kwota udaremnionych prób wyłudzeń kredytów wyniosła

64 829 324 zł

(III kw. 2016 r.) Źródło: Związek Banków Polskich

Dlaczego należy zastrzec utracone dokumenty?

Dziennie notuje się nawet kilkadziesiąt prób posłużenia się cudzym lub podrobionym dokumentem! Wykorzystywane są m.in. do:

- wyłudzenia pożyczki,
- wynajęcia mieszkania lub pokoju hotelowego w celu kradzieży wyposażenia czy unikania opłat,
- kradzieży wypożyczonego samochodu lub innych przedmiotów,
- zakładania fikcyjnych firm oraz wyłudzania kredytów i zwrotu podatków.

Jak działa System DOKUMENTY ZASTRZEŻONE?

System DZ to jedyna ogólnokrajowa, powszechnie dostępna baza danych o zastrzeżonych dokumentach tożsamości w Polsce. System działa w trybie on-line. Dane o zastrzeżeniach trafiają do banków, ale są dostępne także dla innych podmiotów. Są to m.in.: operatorzy telefonii komórkowych, Poczta Polska, pośrednicy finansowi, agencje rozliczeniowe, firmy leasingowe, notariusze, firmy ochroniarskie, hotele, wypożyczalnie i agencje pośrednictwa sprzedaży pośrednictwa sprzedaży i wynajmu nieruchomości.

Wielkość Centralnej Bazy Danych Systemu DZ (dokumenty tożsamości)		**1 655 665** 30 września 2016 r
Liczba zastrzeżonych dokumentów tożsamości	**39 119** III kwartał 2016 r.	**132 145** ostatnich 12 miesięcy
Liczba udaremnionych prób wyłudzeń dokumentów	**1 552** III kwartał 2016 r.	**6 409** ostatnich 12 miesięcy
Średnia kwota udaremnionych prób wyłudzeń kredytów	**28 422 zł** III kwartał 2016 r.	**30 939 zł** ostatnich 12 miesięcy
Kwota największej udaremnionej próby wyłudzenia kredytu	**6 398 000 zł** III kwartał 2016 r.	**6 398 000 zł** ostatnich 12 miesięcy

27. Raport o dokumentach infoDOK (III kwartał 2016 r.)

Związek Banków Polskich

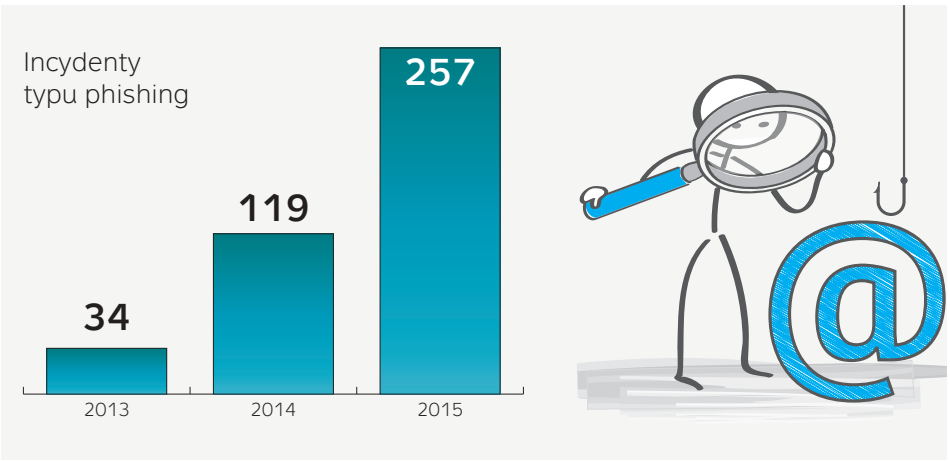
Bezpieczeństwo płatności elektronicznych i transakcji bankowych

Korzystając z płatności lub bankowości elektronicznej poprzez komputer i urządzenia mobilne zadbaj o instalację programu antywirusowego oraz jego częstą aktualizację. Okresowo dokonuj także skanowania systemu w celu wykrycia niepożądanych wirusów i innych zagrożeń. Nie korzystaj z bankowości internetowej w nieznanych sieciach bezprzewodowych lub na ogólnie dostępnych komputerach.

Jeśli chcesz sprawdzić stan swojego rachunku, a jesteś w podróży, bezpieczniejszym rozwiązaniem będzie połączenie z infolinią Twojego banku.

W 2015 r. ABW zarejestrowało około 116 procentowy wzrost zagrożeń typu phishing (oszustwa w cyberprzestrzeni).

Źródło: CERT.GOV.pl, 2016 r.

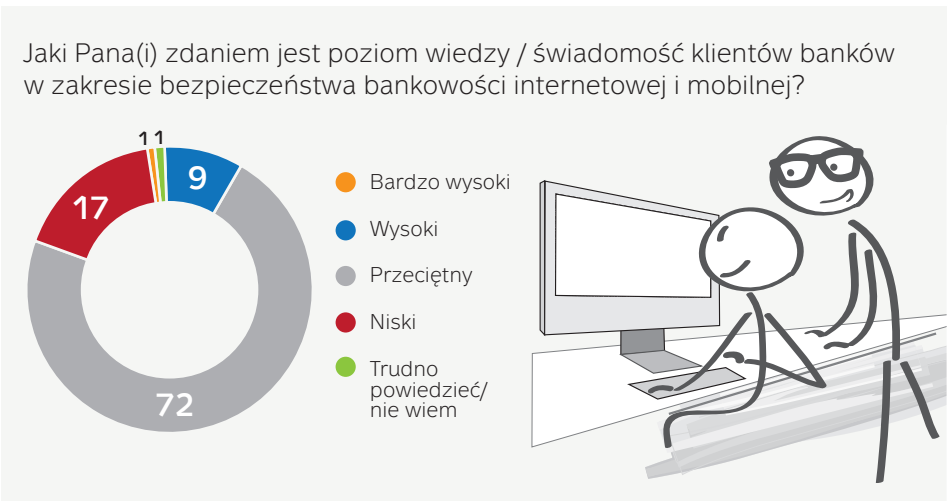


Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje. Z pozoru niewinne strony zawierające programy typu: „freeware" również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.

Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing). Nie używaj również wyszukiwarek w celu odnalezienia strony logowania. Bezpieczniejszym rozwiązaniem jest wpisywanie adresu ręcznie. Ponadto, upewnij się,

Wiedza klientów banków nt. bezpieczeństwa bankowości internetowej i mobilnej

(TNS 2016 r.)



czy nie jesteś na stronie internetowej podszywającej się pod stronę Twojego banku/sklepu. Cyber przestępcy tworzą strony o podobnej nazwie i wyglądzie w celu zmylenia i wyłudzenia pieniędzy.

Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.

10 proc. uczestników badania jako wysoką ocenia wiedzę klientów banków nt. bezpieczeństwa bankowości internetowej i mobilnej. Około trzy czwarte (72 proc.) ocenia poziom wiedzy klientów w tym zakresie jako przeciętny, a 17 proc. jest zdania, że poziom ten jest niski.

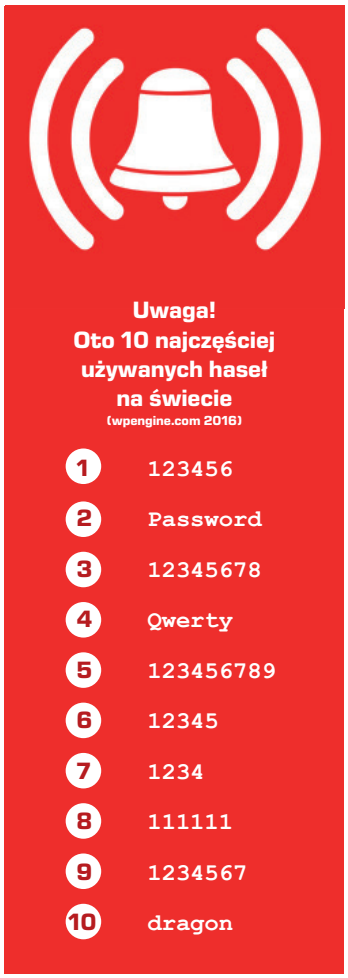
28 proc. badanych jest zdania, że klienci banków poświęcają tylko **10 minut miesięcznie** na zapoznanie się z zasadami lub aktualizowanie wiedzy nt. bezpieczeństwa bankowości internetowej lub mobilnej.

27 proc. badanych jest zdania, że klienci banków poświęcają tylko **10 minut w roku.**

Zdaniem **8 proc.** respondentów klienci w ogóle nie są zainteresowani zasadami bezpieczeństwa.

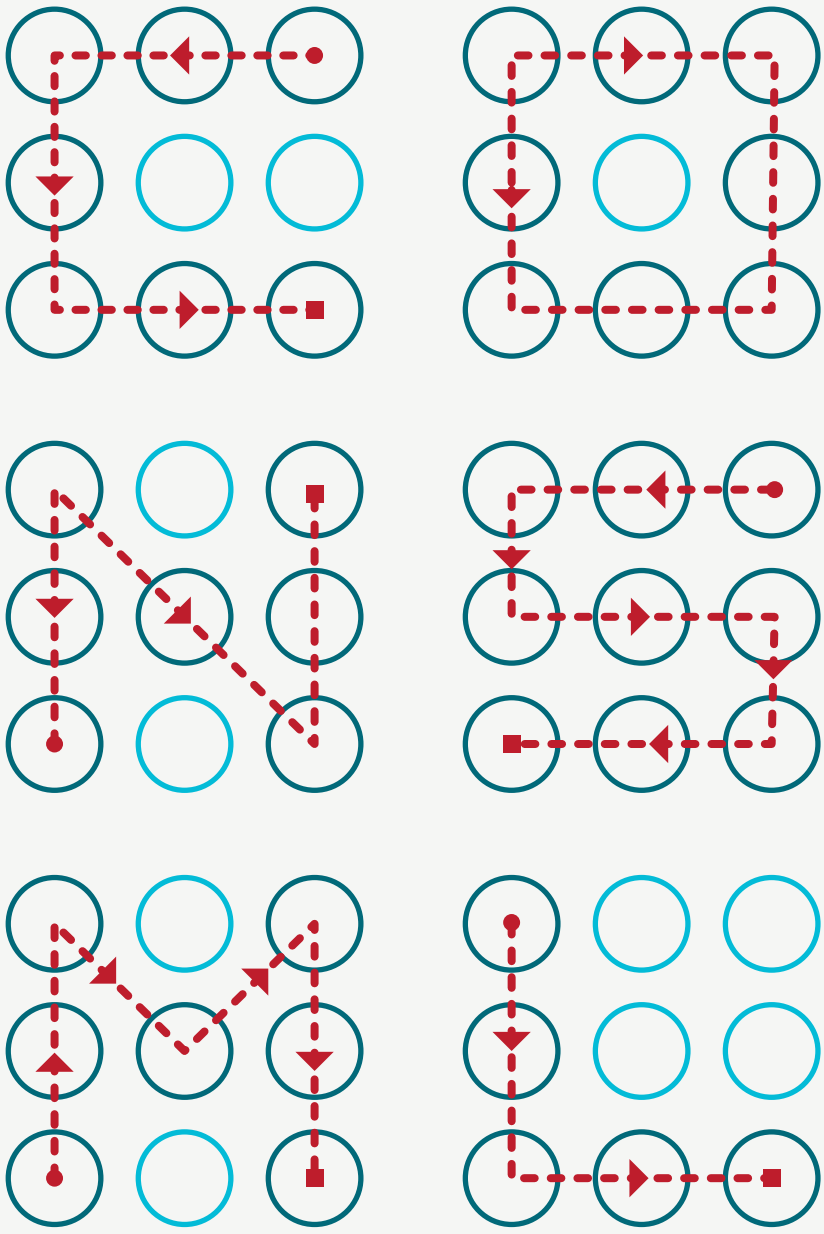
Zainteresowanie bezpieczeństwem bankowości internetowej i mobilnej

(TNS 2016 r.)



Pamiętaj, aby właściwie zabezpieczyć telefon!

Unikaj wykorzystywania popularnych haseł i typowych form zabezpieczenia telefonu.



Więcej na temat bezpiecznego korzystania z produktów usług bankowych znajdziecie Państwo na portalu internetowym **www.zbp.pl/dla-konsumentow**

Związek Banków Polskich

25 LAT
1991-2016

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