ZWIĄZEK BANKÓW POLSKICH

REPREZENTUJĄC BANKI, SŁUŻYMY KLIENTOM

Bezpieczne wakacje dla naszych finansów

czerwiec 2011

21 czerwca 2011 r., Warszawa

Szanowni Państwo,

W związku ze zbliżającymi się wyjazdami wypoczynkowymi postanowiliśmy w Związku Banków Polskich przygotować dla Państwa kilka porad, dzięki którym będą to bezpieczne wakacje również od strony finansowej.

Okres wakacyjny to czas, w którym jesteśmy szczególnie narażeni na utratę lub kradzież dokumentów oraz kart płatniczych a tym samym możemy stać się ofiarami przestępstwa. W kurortach panuje duży tłok, jesteśmy bardziej rozluźnieni, nie zwracamy uwagi na portfele i dokumenty – to sytuacje które prowokują potencjalnych przestępców do działania. Zachowanie zdrowego rozsądku eliminuje jednak większość zagrożeń. Warto zwrócić na to uwagę, aby urlop był faktycznie czasem spokojnego wypoczynku.

Niestety przeprowadzone na zlecenie Związku Banków Polskich badania opinii pokazują, że wiele niebezpiecznych sytuacji prowokujemy sami. Aż 16% respondentów nosi ze sobą zapisane numery PIN do kart płatniczych i co więcej korzysta z tych notatek w trakcie dokonywania transakcji czy wypłat. Bardzo niepokojące jest również to, że aż 12% z nas korzysta z pomocy nieznanych osób przy wypłacie środków z bankomatów.

Większości tych zagrożeń możemy zapobiec przestrzegając kilku prostych zasad bezpieczeństwa korzystając z kart kredytowych i płatniczych oraz dokumentów. W tym krótkim raporcie postaramy się przypomnieć najważniejsze zasady i sposoby radzenia sobie w przypadku kradzieży lub utraty dokumentów i „plastikowych pieniędzy".

Mamy nadzieję, że te kilka chwil poświęconych na lekturę pozwoli na spokojne i pełne wypoczynku letnie dni.

Z wyrazami szacunku,

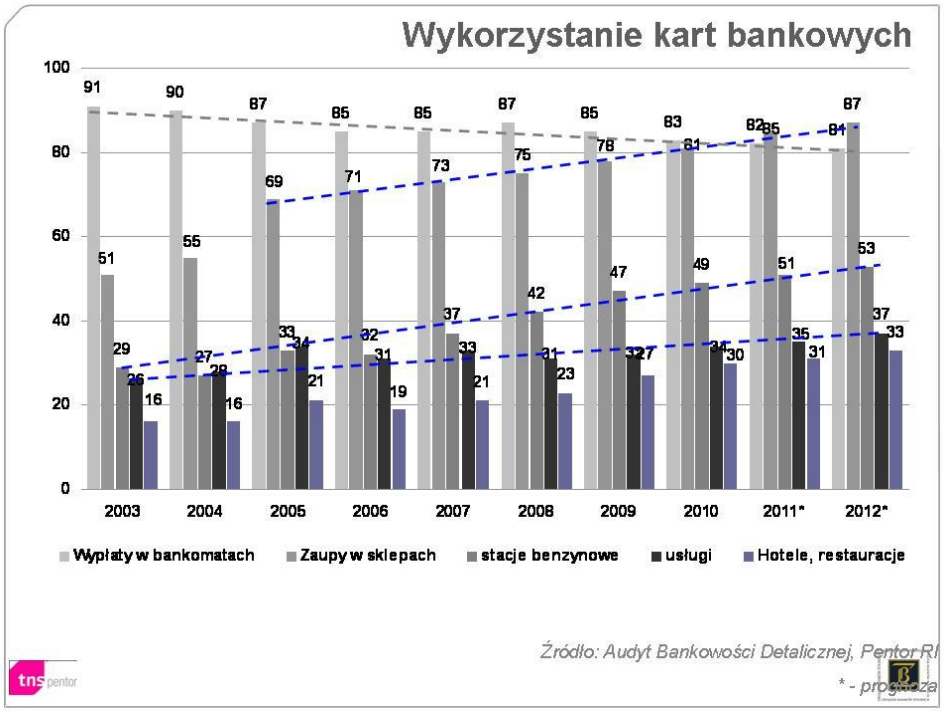
Krzysztof Pietraszkiewicz

Prezes ZBP

1. Karty płatnicze

Z roku na rok Polacy coraz chętniej i częściej korzystają z kart płatniczych. Rośnie liczba punktów, które obsługują transakcje, jest to coraz powszechniejszy sposób płacenia za zakupy i usługi.

Powyższy wykres dokładnie ilustruje wzrostową tendencję jeśli chodzi o liczbę osób posiadających karty płatnicze. W kolejnych latach można oczekiwać dalszych wzrostów. „Plastikowy pieniądz" jest bardzo wygodnym atrybutem urlopowicza. Nie wymaga posiadania gotówki w portfelu, czy też walut obcych w przypadku wyjazdów zagranicznych. Tym bardziej powinniśmy uważać na to gdzie i w jaki sposób dokonujemy transakcji.



Jak widać z powyższego wykresu rośnie liczba transakcji dokonywanych bezpośrednio w sklepach i punktach usługowych, a maleje wykorzystanie wypłat z bankomatów, by potem regulować rachunki gotówką. Przestępcy podążając za tym trendem starają się przechwycić już nie gotówkę, ale karty i numery PIN.

Mimo to karty płatnicze są bardzo bezpieczną formą dokonywania codziennych płatności. W przypadku przestępstwa odpowiedzialność użytkownika karty jest ustawowo ograniczona do 150 euro. Po zastrzeżeniu karty cała odpowiedzialność spoczywa na banku – wydawcy karty. Dodatkową ochronę stanowią ubezpieczenia karty kredytowej - ubezpieczenie na wypadek utraty karty oraz ubezpieczenie zaciągniętego kredytu. Bezpieczeństwo kart płatniczych potwierdzają statystyki. Transakcje oszukańcze wg danych przekazywanych przez agentów rozliczeniowych stanowiły 0,015 % ogólnej wartości transakcji kartami płatniczymi rozliczanych przez agentów. Z danych otrzymanych od agentów rozliczeniowych wynika, że dokonano 8,2 tys. operacji oszukańczych kartami płatniczymi na kwotę 6,7 mln zł. Według danych przekazywanych przez banki, w II półroczu 2010 r. liczba operacji oszukańczych dokonanych kartami płatniczymi wyniosła 14,6 tys. a wartość 9,0 mln zł[1].

Większość groźnych sytuacji prowokujemy sami, swoim często ryzykownych zachowaniem. Blisko co trzeci posiadacz karty wpisując kod PIN w terminalu lub bankomacie nie dba o odpowiednie jego ukrycie przed innymi osobami, a aż 16 proc. badanych posiada zapisany numer PIN na karcie płatniczej lub innych noszonych przy sobie przedmiotach, tyle samo badanych sprawdza przy transakcji czy wpisywany numer PIN jest właściwy. Wakacje są okresem kiedy zapominamy o codziennych nawykach narażając się tym samym na utratę zgromadzonych oszczędności.

Związek Banków Polskich przygotował katalog zasad które pozwolą konsumentom uchronić się przed nieprzyjemnościami a w razie kradzieży pozwolą odzyskać utracone oszczędności.

Przede wszystkim zachęcamy do zachowania ostrożności przy przekazywaniu informacji poufnych -a należy do nich numer naszej karty przez Internet, telefon i inne media, w każdym miejscu.

Najprostsza reguła bezpieczeństwa to kierować się zdrowym rozsądkiem.

Poniżej podajemy 25 rad przydatnych dla zachowania bezpieczeństwa podczas dokonywania transakcji płatniczych. Szersze materiały zwłaszcza dotyczące bezpieczeństwa w Internecie można znaleźć na stronie Forum Technologii Bankowych www.ftbforum.pl.

Poniższe rady są również przypomnieniem obowiązków ciążących na posiadaczach kart płatniczych wynikających z ustawy o elektronicznych instrumentach płatniczych, której tekst możecie znaleźć na niniejszej stronie.

[1] Ocena Funkcjonowania Polskiego Systemu Płatniczego w II Półroczu 2010 Roku, Narodowy Bank Polski Departament Systemu Płatniczego

25 rad jak się chronić – oszustwa kartowe

1. Podczas transakcji nie należy tracić karty z pola widzenia. Po transakcji należy ją odebrać bez zbędnej zwłoki.

2. Należy zachować rozwagę przy przekazywaniu numeru karty. Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Jeżeli to my inicjujemy połączenie, również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

3. Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie. Nigdy też nie odpowiadaj na maile które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywanych „phishingiem".

4. Nigdy nie należy podawać informacji o karcie na stronach, które nie są bezpieczne. Np. strony ze zdjęciami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach ?

5. Kartę należy podpisać natychmiast po jej otrzymaniu.

6. Niszcz przed ewentualnym wyrzuceniem wszystkie wnioski na karty kredytowe, które możesz otrzymać drogą pocztową.

7. Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą (na wypadek kradzieży portfela czy portmonetki).

8. Nigdy nie zostawiaj karty ani pokwitowań transakcji bez nadzoru.

9. Chroń swój numer karty i inne poufne kody umożliwiające dokonane transakcji (np. numer PIN, numer CVV 2, numer CVC2), by obcy nie mogli wejść w jego posiadanie np. robiąc zdjęcie karty przy użyciu telefonu komórkowego z aparatem fotograficznych, kamerą video lub w inny sposób.

10. Sporządź i przechowuj w bezpiecznym miejscu listę numerów kart oraz adresów i telefonów do każdego banku, którego karty posiadasz. Listę tę należy aktualizować za każdym razem, gdy otrzymujemy nowa kartę.

11. Należy ze sobą nosić tylko te karty, które się potrzebuje. Nie należy nosić ze sobą kart, z których się rzadko korzysta.

12. Traktuj transakcje kartowe z podobna starannością i rozwagą jak inne dokonane na rachunku. Sprawdzaj wykonane operacje niezwłocznie po otrzymaniu wyciągu rachunku dla kart debetowych i zestawienia transakcji dla pozostałych kart. Zachowanie pokwitowań dokonanych transakcji pozwala na szybką ich weryfikację.

13. W przypadku jakichkolwiek rozbieżności należy jak najszybciej złożyć pisemną reklamację w banku, który wydał kartę.

14. Zawsze niszcz nieprawidłowe pokwitowania, zbieraj pokwitowania transakcji, które nie doszły do skutku

15. Przed wyrzuceniem niszcz wszystkie dokumenty, które zawierają pełen numer karty.

16. Nigdy nie podpisuj pokwitowania in blanco. W przypadku transakcji w imprinterze (dotyczy to tylko kart tłoczonych) zawsze zakreślaj czyste części blankietu, tak by nie było możliwe oszukańcze dodanie dodatkowych opłat.

17. Kalka jest bardzo rzadko wykorzystywana, ale jeśli została użyta do transakcji kartą, zniszcz ją.

18. W restauracjach, gdy otrzymujesz wydruk z terminala z miejscem na wpisanie napiwku wpisz kwotę, lub przekreśl to miejsce poziomą kreską.

19. Nigdy nie zapisuj numeru karty w miejscu publicznie dostępnym (np. na pocztówce).

20. Dobrym pomysłem jest noszenie kart poza portfelem, najlepiej w oddzielnej zamykanej przegródce lub etui.

21. Nigdy nikomu nie udostępniaj kart.

22. Jeśli się przeprowadzasz, nie zapomnij jak najszybciej poinformować banku, który wydał karty, o zmianie adresu.

23. Nie zabieraj karty ze sobą, jeżeli jej użycie jest mało prawdopodobne, a możesz narazić się na jej utratę (np. zakupy na bazarach i w miejscach gdzie możesz być narażony na kradzież kieszonkową).

24. Jeżeli byłeś w sytuacji, która sprzyja kradzieży sprawdź czy masz karty (np. w przedziale pociągu, gdy rozpoczynasz podróż). Jeśli utraciłeś kartę płatnicza lub została ona skradziona pamiętaj aby niezwłocznie zarzec kartę.

25. Należy zachowywać szczególną ostrożność podczas korzystania z bankomatów. Oszuści mogą zamontować w bankomatach urządzeń do kopiowania kart lub kamery do podglądania kodów PIN.

Jak zastrzec kartę

Gdy doszło do utraty karty należy niezwłocznie skontaktować się z bankiem lub organizacją, która ją wydała. W tym celu należy skontaktować się z dostępnym przez 24 h centrum autoryzacji kart. Numer centrum otrzymują Państwo razem z przesyłką zawierającą kartę. Warto go wpisać do swojego telefonu komórkowego np. pod pozycją karty_nazwa banku.

Numery wszystkich banków są także dostępne na stronie internetowej Związku Banków Polskich w zakładce zastrzeż kartę.

Zgodnie z polskim prawem z chwilą zgłoszenia utraty karty odpowiedzialność za przeprowadzone nią transakcje ponosi jej wydawca. Zgodnie z ustawą o elektronicznych instrumentach płatniczych maksymalna odpowiedzialność właściciela karty (za transakcje przeprowadzone przed zgłoszeniem jej utraty) wnosi równowartość 150 €. Warunkiem jest jednak przestrzeganie umowy o wydanie karty oraz regulaminu karty, który stanowi integralną część umowy.

Jeśli będą Państwo postępować zgodnie z podanymi powyżej radami w znacznym stopniu zabezpieczycie się przed niedogodnościami i kłopotami jakie powodują oszustwa kartowe

2. Dokumenty

Nie tylko kradzież kart płatniczych, ale również kradzież dokumentów tożsamości może narazić ich posiadacza na duże straty materialne. Skradzione dokumenty mogą zostać wykorzystane do wyłudzania kredytów, dokonywania zakupów z odroczoną płatnością, kradzieży wypożyczanych przedmiotów, podpisywania umów najmu w celu kradzieży dobytku lub unikania opłat. Dlatego tak ważne jest zastrzeganie utraconych dokumentów w banku.

Problem dotyczy nas wszystkich, a liczby mówią same za siebie, w 2010 roku:

- udaremniono 7,5 tysiąca prób wyłudzenia kredytów przez osoby posługujące się cudzymi dokumentami tożsamości,
- łącznie próbowano wyłudzić ponad 458 milionów złotych.

Aby uniknąć problemów i spędzić spokojnie czas urlopu należy stosować się do kilku rad:

1. Nie eksponuj rzeczy wartościowych np. pieniędzy, dokumentów, telefonów.
2. Uważaj na obcych, nie obdarzaj ich nadmiernym zaufaniem.
3. Nie noś kart bankomatowej razem z zanotowanym numerem PIN.
4. Nie zostawiaj wartościowych rzeczy w samochodzie.
5. Torebkę , saszetkę zawsze noś zamkniętą.
6. Podczas podróży pilnuj swojego bagażu.
7. Będąc na plaży nie zostawiaj kosztowności bez opieki.
8. Klucze do mieszkania noś w innym miejscu niż dokumenty.

Co zrobić w przypadku utraty dokumentów?

1) Natychmiast zastrzec je w międzybankowym Systemie DOKUMENTY ZASTRZEŻONE (www.DokumentyZastrzezone.pl). W Systemie DZ uczestniczą wszystkie banki w Polsce oraz szereg innych firm i instytucji; pełna lista Uczestników, dla bezpieczeństwa całego Systemu, jest oczywiście objęta tajemnicą; zastrzeganie dokumentów jest możliwe wyłącznie w bankach (około 22.000 placówek w całym kraju).
2) Powiadomić policję (należy to zrobić w sytuacji, gdy utrata dokumentów nastąpiła w drodze kradzieży lub innego przestępstwa).
3) Zawiadomić najbliższy organ gminy lub placówkę konsularną i wyrobić nowy dokument.

System DOKUMENTY ZASTRZEŻONE, w którym gromadzone są informacje o skradzionych i zagubionych dokumentach tożsamości, chroni osoby, które utraciły swoje dokumenty. Ogranicza

możliwość ich późniejszego wykorzystania do celów przestępczych popełnianych w imieniu i na szkodę osoby, która je utraciła.

Wystarczy zastrzec utracony dokument w jednym banku, a dane te zostaną automatycznie przekazane do wszystkich banków i innych uczestników Systemu DZ. Co ważne, dokumenty zastrzegają nie tylko osoby korzystające z usług bankowych – mogą i powinni to robić wszyscy, także ci, którzy nigdy nie posiadali własnego rachunku bankowego (oni bowiem, jako osoby, o których banki nie miały wcześniej żadnej wiedzy, są najczęstszymi ofiarami oszustów).

Łącznie w Systemie DZ zgromadzono już ponad 970 tys. dokumentów. Ta liczba systematycznie wzrasta. Kwartalnie zgłaszanych jest nawet 30 tys. nowych dowodów osobistych, praw jazdy. Dzięki temu ich prawdziwi właściciele mogą uniknąć prób wyłudzeń dokonywanych przez przestępców na ich nazwisko. Po zastrzeżeniu dokumentu możliwe jest natychmiastowe zatrzymanie oszustów na gorącym uczynku, co zmniejsza ryzyko dla funkcjonowania całego obrotu gospodarczego. Poza bankami z dostępu do Systemu DZ korzystają także firmy telekomunikacyjne oraz inne podmioty, które w swojej działalności weryfikują tożsamość klientów na podstawie dokumentów.

Jakie dokumenty zastrzegać?

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,
- dowody rejestracyjne.

3. Dzieci

Warto przed wakacjami pomyśleć również o naszych dzieciach, dla ich bezpieczeństwa i naszego spokojnego snu w trakcie ich wyjazdów. Przez wiele lat tradycyjnym sposobem zaopatrywania dzieci przed wyjazdem było przekazanie im znacznych środków finansowych, tak aby wystarczyły na całą wycieczkę. Takie podejście ma kilka istotnych wad. Po pierwsze jeśli dziecko zgubi portfel lub ktoś go ukradnie traci wszystkie środki, po drugie skuszone wysokością posiadanych kwot może wydać je zbyt szybko. Oddzielną kwestią jest tez możliwość wglądu w to na co dzieci przeznaczają pieniądze.

Rodzicom można śmiało polecić założenie konta dla swoich pociech. Banki oferują szereg propozycji dla dzieci, które wskazane wyżej wady eliminuje. Rodzicie mogą kontrolować wysokość jednorazowych lub dziennych wydatków z domu poprzez system e-bankingu. Nie ma również problemu z różnymi walutami, koniecznością wymiany przed wyjazdami. W przypadku gdy zabraknie środków można je łatwo uzupełnić kolejnym przelewem. Dziecko nawet w przypadku utraty karty nie utraci środków jakie na niej posiada, nie naraża się na dodatkowe nerwy z tym związane, a może swobodnie korzystać z wakacji.

4. Stałe płatności w okresie wakacji

Nasz urlop trwa, ale niestety terminy płatności pozostają stałe. Raty kredytów, opłaty, abonament telefoniczny i telewizyjny mają nieubłagane i z góry określone daty kiedy musza być płacone. Wyjeżdżając na wakacje powinniśmy zadbać o to, aby wszystkie płatności o terminach zapadalności do końca naszego urlopu, były zapłacone. Dzięki temu na pewno unikniemy problemów i karnych odsetek po powrocie. Jeśli korzystamy ze zleceń stałych pamiętajmy o zabezpieczeniu odpowiedniego poziomu środków na koncie, aby mógł on zostać poprawnie wykonany.

Spora grupa urlopowiczów dokonuje płatności korzystając z bankowości internetowej poza granicami kraju. Jest to dobre rozwiązanie, o ile mamy pewność, że sieć jest bezpieczna i ma odpowiednie oprogramowanie antyspamowe i antywirusowe. Jeżeli nie mamy wiedzy na temat takich danych z hotelu, w którym planujemy się zatrzymać, bezpieczniej będzie dokonać przelewów jeszcze przed wyjazdem.

Aby bezproblemowo korzystać z bankowości elektronicznej należy zapoznać się z kilkoma radami:

1. Pamiętaj, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację. Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się ze swoim Bankiem i poinformuj o zdarzeniu.

2. Sprawdź na stronie Twojego Banku jakie zabezpieczenia stosowane są w serwisie internetowym. Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Banku.

3. Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany. Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

4. Dokonuj płatności internetowych tylko z wykorzystaniem „pewnych komputerów”. Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

5. Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on bezpiecznych kanałów dystrybucji tej usługi. Zwracaj szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez Twojego dostawcę. Jeśli masz jakieś wątpliwości w tym zakresie zawsze masz prawo zapytać się dostawcy o jakość bezpieczeństwa oferowanego przez niego.

6. Instaluj na swoim komputerze tylko legalne oprogramowanie. Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

7. Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji. Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.

8. Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe. Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.

9. Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia. Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

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

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

12. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego Banku.

13. Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing).

14. Używaj do tego celu adresu podanego Ci przez Bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek" (Firefox) lub „adresów Ulubionych" (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

15. Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania Twojego Banku. Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

16. Przed zalogowaniem sprawdź, czy połączenie z bankiem jest szyfrowane. Jeśli tak, adres witryny powinien rozpoczynać się od https://, a w dole ekranu przeglądarki www powinien pojawić się symbol zamkniętej kłódki, to oznacza, że informacje są przesyłane z wykorzystaniem 128-bitowych algorytmów szyfrujących. Brak kłódki lub otwarta kłódka oznacza brak szyfrowania, czyli, że Twoje dane są transmitowane przez Internet tekstem jawnym, co naraża Cię na ogromne niebezpieczeństwo.

17. Sprawdzaj prawidłowość certyfikatu. Zanim wpiszesz identyfikator bądź login i hasło, sprawdź certyfikat witryny (kliknięcie w kłódkę), czyli przede wszystkim jego datę ważności i dla kogo został wystawiony. Jeśli certyfikat utracił ważność lub nie można go zweryfikować zrezygnuj z połączenia.

18. Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu. Identyfikator jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić.

19. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie. Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na Tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.

20. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

21. Korzystaj z infolinii udostępnionej przez Twój bank. Zawsze masz prawo skorzystać z infolinii swojego banku jeśli masz wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem internetu.

22. Odwiedzaj regularnie Portal „Bezpieczny Bank" na stronie internetowej ZBP – www.zbp.pl Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie odwiedzaj ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

5. Podsumowanie

TNS Pentor na zlecenie Związku Banków Polskich przeprowadził badanie opinii dotyczące bezpieczeństwa korzystania z kart płatniczych. Niektóre wyniki są zaskakujące.

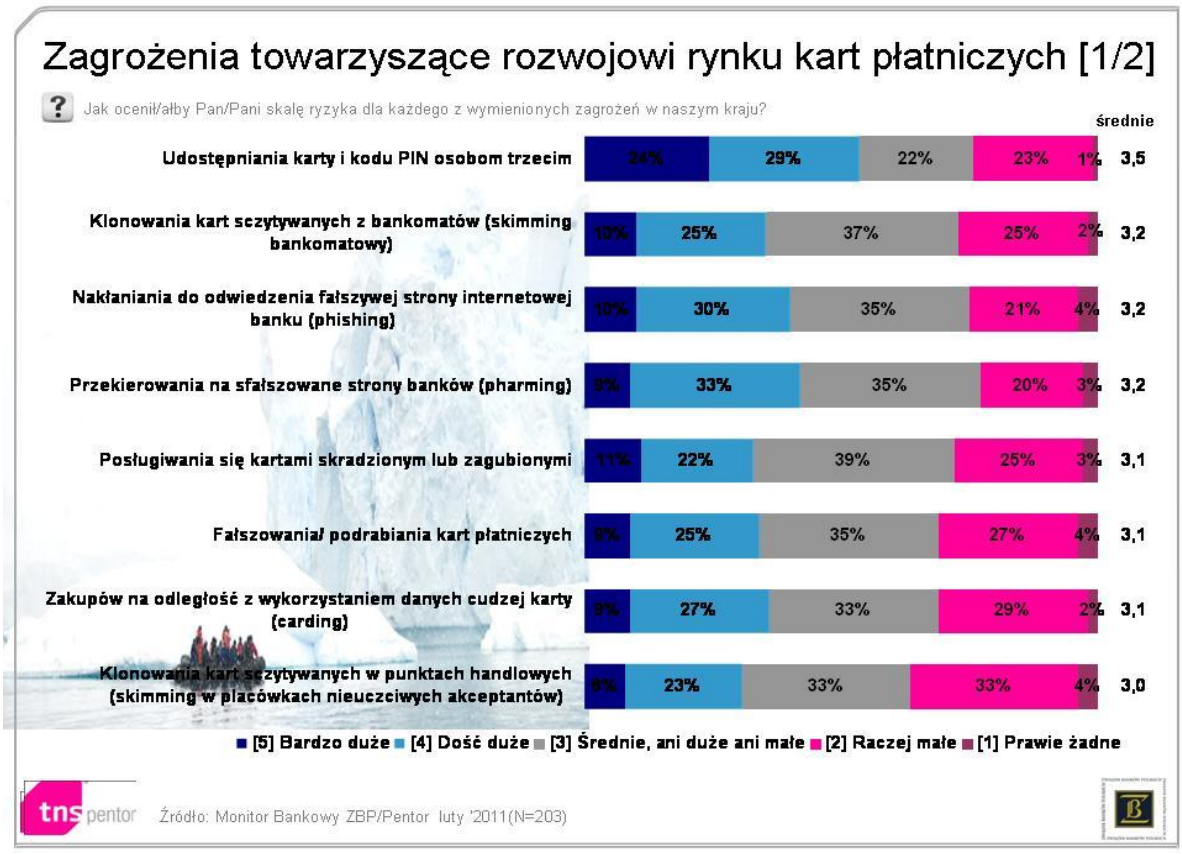
Ponad połowa respondentów obawia się udostępnienia karty i kodu PIN osobom trzecim. Mimo to, aż 16% posiada go ze sobą i korzysta z niego w trakcie wykonywania transakcji kartowych. Aż 12% z nas korzysta z pomocy osób trzecich dokonując wypłat z bankomatów. Dane te są bardzo niepokojące. Dla naszego bezpieczeństwa warto zachować więcej ostrożności i stosować porady przekazywane przez banki. Czasem warto zrezygnować z transakcji jeśli nie czujemy się bezpiecznie.

Ankietowani obawiają się też, że ich karty wpadną w niepowołane ręce w trakcie przesyłania z banku do klienta. Warto zwrócić uwagę, że banki aby minimalizować tego typu próby oszustw, od wielu lat wysyłają oddzielnie kody PIN i karty.

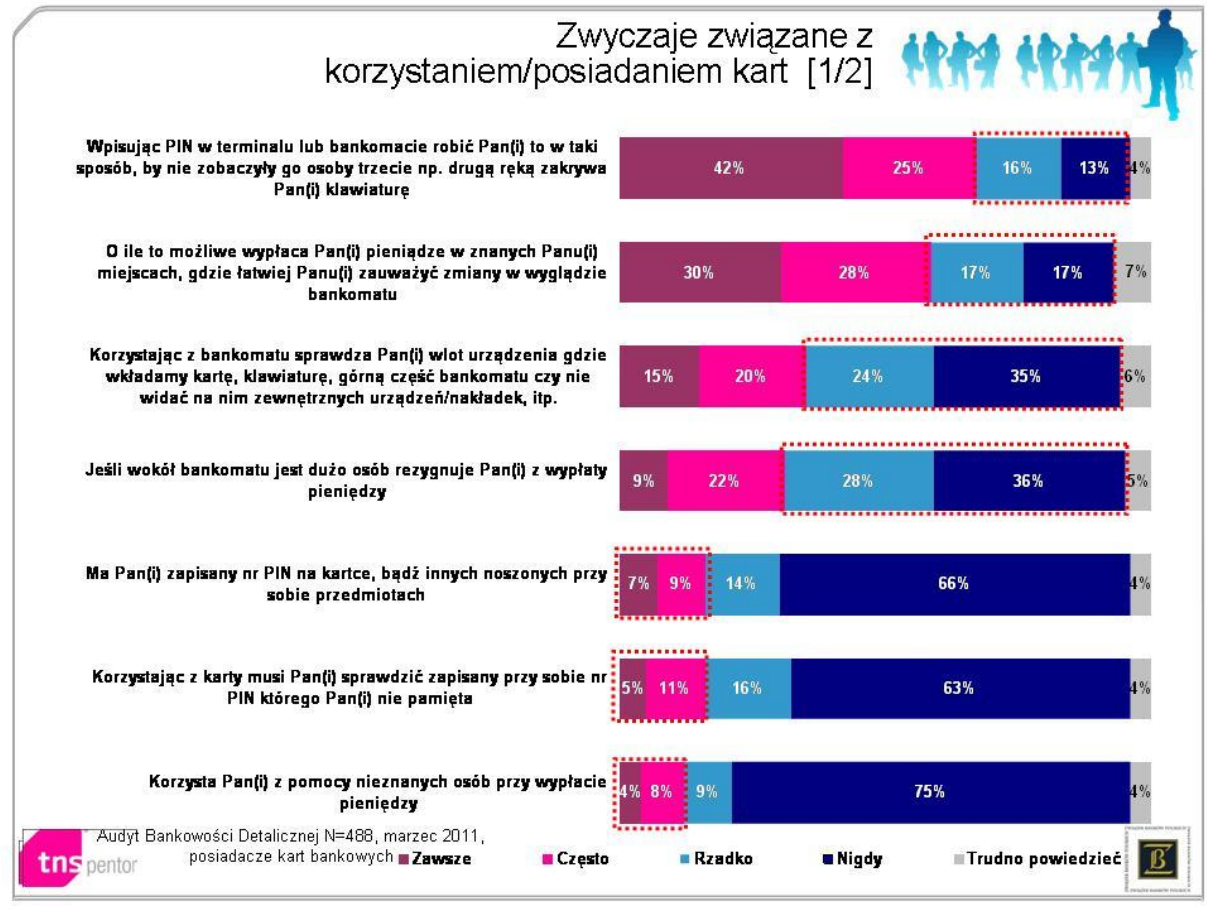
Wiele wskazanych poniżej zagrożeń występuje ze szczególną intensywnością w trakcie wakacji, w kurortach wypoczynkowych. Warto zwrócić uwagę na to czy bankomat nie nosi śladów montowania jakiś urządzeń, czy ma kamerę rejestrującą, zanim zdecydujemy się wypłacić środki. Większości zagrożeń można jednak uniknąć zachowując zdrowy rozsądek i nie łamiąc podstawowych zasad bezpieczeństwa.

Szczegółowe informacje na temat bezpieczeństwa dokumentów znaleźć można na stronie www.dokumentyzastrzezone.pl

Więcej informacji dotyczących bezpieczeństwa płatności w trakcie wakacji można znaleźć na stronie zbp.pl/bezpieczny_bank




Zagrożenia towarzyszące rozwojowi rynku kart płatniczych [2/2]
Jak ocenił/ałby Pan/Pani skalę ryzyka dla każdego z wymienionych zagrożeń w naszym kraju?
średnie
Posługiwania się kartami niedoręczonymi przez pocztę/kuriera prawowitym odbiorcom 6% 19% 22% 43% 9% 2,7
Kopiowania kart na dokumentach obciążeniowych 4% 13% 37% 37% 8% 2,7
Wydawania kart w oparciu o wnioski z fałszywymi danymi (wyłudzenia kat płatniczych) 5% 13% 26% 46% 10% 2,6
Napadu na klientów pobierających pieniądze z bankomatów 3% 15% 32% 42% 8% 2,6
Włamania hakerów do elektronicznych sieci banków 4% 15% 25% 44% 12% 2,5
Elektronicznej dezorientacji łącza między terminalem a serwerem w banku 2% 13% 29% 43% 13% 2,5
Wyłudzanie towarów/usług przez legalnych użytkowników kart 1% 11% 33% 46% 9% 2,5
Kradzieży/ włamania do bankomatów 2% 6% 20% 43% 29% 2,1
[5] Bardzo duże
[4] Dość duże
[3] Średnie, ani duże ani małe
[2] Raczej małe
[1] Prawie żadne
tns pentor
Źródło: Monitor Bankowy ZBP/Pentor luty '2011(N=203)


Zwyczaje związane z korzystaniem/posiadaniem kart [1/2]
Wpisując PIN w terminalu lub bankomacie robić Pan(i) to w taki sposób, by nie zobaczyły go osoby trzecie np. drugą ręką zakrywa Pan(i) klawiaturę 42% 25% 16% 13% 4%
O ile to możliwe wypłaca Pan(i) pieniądze w znanych Panu(i) miejscach, gdzie łatwiej Panu(i) zauważyć zmiany w wyglądzie bankomatu 30% 28% 17% 17% 7%
Korzystając z bankomatu sprawdza Pan(i) wlot urządzenia gdzie wkładamy kartę, klawiaturę, górną część bankomatu czy nie widać na nim zewnętrznych urządzeń/nakładek, itp. 15% 20% 24% 35% 6%
Jeśli wokół bankomatu jest dużo osób rezygnuje Pan(i) z wypłaty pieniędzy 9% 22% 28% 36% 5%
Ma Pan(i) zapisany nr PIN na kartce, bądź innych noszonych przy sobie przedmiotach 7% 9% 14% 66% 4%
Korzystając z karty musi Pan(i) sprawdzić zapisany przy sobie nr PIN którego Pan(i) nie pamięta 5% 11% 16% 63% 4%
Korzysta Pan(i) z pomocy nieznanych osób przy wypłacie pieniędzy 4% 8% 9% 75% 4%
tns pentor
Audyt Bankowości Detalicznej N=488, marzec 2011, posiadacze kart bankowych
Zawsze
Często
Rzadko
Nigdy
Trudno powiedzieć