

ABC BEZPIECZNYCH NOWOCZESNYCH TECHNOLOGII PŁATNICZYCH

PŁATNOŚCI ZBLIŻENIOWE

PŁATNOŚCI ZBLIŻENIOWE

1. Prawie wszystkie nowo wydawane karty debetowe i karty kredytowe posiadają, oprócz tradycyjnego paska magnetycznego, także mikroprocesor umożliwiający dokonywanie **tzw. płatności zbliżeniowych**.
2. Płatności zbliżeniowe polegają na dokonywaniu szybkich płatności poprzez zbliżenie karty do terminalu (co do zasady płatności do wysokości 100 zł nie wymagają weryfikowania ich za pomocą nr PIN, podanie kodu PIN wymagane jest przy transakcjach powyżej tej kwoty).
3. Płatności zbliżeniowych można dokonywać nie tylko kartą, ale urządzeniami elektronicznymi wyposażonymi w odpowiednie aplikacje np.: telefonem, zegarkiem.

PŁATNOŚCI ZBLIŻENIOWE

1. Karty zbliżeniowe posiadają wszystkie zalety klasycznych kart płatniczych poszerzone o możliwość dokonywania zbliżeniowych płatności.
2. Posiadacze kart płatniczych zbliżeniowych dotyczą te same zasady bezpieczeństwa, co posiadacze kart klasycznych.
3. **WAŻNE:** Mimo doniesień prasowych o teoretycznych możliwościach nieuprawnionego odczytu karty, sklonowania karty, ataku typu przekaźnikowego – znaczna część z tych zagrożeń ograniczona jest do minimum przez mechanizmy zabezpieczające wbudowane w technologię zbliżeniową. Należy jedynie pilnować, by nie zgubić karty lub aby nie została nam skradziona - podobnie jak w przypadku gotówki, czy innych kart płatniczych.

PŁATNOŚCI ZBLIŻENIOWE

1. W większości banków istnieje możliwość wprowadzenia dodatkowych limitów (*ilościowych i kwotowych*) na realizację płatności bezgotówkowych i wpłat gotówkowych (*np. co 10 płatność jest autoryzowana numerem PIN lub PIN konieczny każdorazowo po wydatkowaniu np. 300 zł*).
2. **Z Analizy poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy, przeprowadzonej przez Komisję Nadzoru Finansowego wynika, iż poziom ryzyka związanego z korzystaniem z tego typu kart jest jednak zbliżony do poziomu ryzyka związanego z korzystaniem z kart, które nie są wyposażone w tę funkcjonalność.**
3. Banki deklarują, iż transakcje oszukańcze dokonywane w trybie zbliżeniowym stanowią znikomy udział w ogóle tego typu transakcji (*liczony w promilach*).

ZASADY BEZPIECZNEGO POSŁUGIWANIA SIĘ KARTAMI PŁATNICZYMI

- 1. UWAGA:** W wielu bankach nowe karty płatnicze przekazywane klientom po utracie ważności poprzednich automatycznie wyposażone są w funkcjonalność płatności zbliżeniowych bez uprzedniego pytania posiadacza o wolę posiadania takiej funkcji.
2. Składając wniosek o kartę płatniczą należy koniecznie sprawdzić/zapytać, czy wydana karta ma funkcję płatności zbliżeniowej, a jeśli tak, to warto wykształcić nawyk systematycznego korzystania z niej, tak by w razie jej utraty - szybko to zauważyć i poczynić odpowiednie kroki celem jej zablokowania.
3. We wszystkich bankach istnieje **możliwość dezaktywowania funkcji zbliżeniowej.**

PŁATNOŚCI MOBILNE SMARTFONEM

BEZPIECZENSTWO PŁATNOŚCI MOBILNYCH SMARTFONEM - podstawowe zasady

- 1. Nie należy instalować na smartfonie aplikacji z nieznanych źródeł.**
- 2. 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 właściciela telefonu),**
- 3. Hasło do telefonu powinno być inne niż do aplikacji płatności mobilnych; hasła te powinny również być trudne do odgadnięcia.**
- 4. Nie należy zapisywać hasła do aplikacji płatności mobilnych na kartce (lub innym nośniku), zwłaszcza przechowywanej wraz z telefonem.**
- 5. Należy ograniczyć wartość transakcji, które można dokonać za pomocą aplikacji mobilnej.**

BEZPIECZENSTWO PŁATNOŚCI MOBILNYCH SMARTFONEM - podstawowe zasady

6. Należy wyłączyć w smartfonie opcję pozwalającą korzystać z otwartej sieci Wi-Fi w czasie, gdy wpisujemy loginy, hasła i PIN-y.
7. Dokonując płatności mobilnych za pomocą aplikacji zainstalowanej w smartfonie należy korzystać z internetu mobilnego w smartfonie, a nie z otwartych sieci Wi-Fi.
8. Telefon używany do dokonywania płatności mobilnych powinien być zawsze zabezpieczony przez **aktualne oprogramowanie antywirusowe**.
9. Oddając telefon do serwisu warto odinstalować aplikację płatności mobilnych.
10. Niezwłocznie po utracie telefonu, na którym zainstalowana była aplikacja płatności mobilnych, należy zgłosić ten fakt w swoim banku.

Dziękuję za uwagę!