Bezpieczeństwo Twoich płatności w Provident Polska SA to nasz priorytet.

Chcemy, żeby każdy Klient czuł się pewnie, korzystając z karty kredytowej, dlatego pomagamy wprowadzić dobre nawyki ograniczające nieautoryzowane transakcje.

Poniżej znajdziesz wyjaśnienie, czym jest **Silne Uwierzytelnienie Klienta (SCA)** stosowane podczas Twoich transakcji oraz jakie są **główne zasady korzystania z naszych usług płatniczych.**

Czym jest Silne Uwierzytelnienie?

SCA to proces dwuetapowego potwierdzenia Twojej tożsamości – jego pozytywny wynik umożliwia zrealizowanie transakcji kartą kredytową. W praktyce oznacza to, że musisz potwierdzić bycie właścicielem karty kredytowej lub wprowadzić kod PIN w aplikacji ProviGo.

Obowiązek stosowania procedury SCA nakładają europejska dyrektywa o usługach płatniczych (PSD2) oraz polska ustawa o usługach płatniczych. Jej celem jest zwiększenie bezpieczeństwa korzystania z usług płatniczych drogą elektroniczną i ograniczenie ryzyka oszustw w cyfrowych płatnościach.

Kiedy stosujemy Silne Uwierzytelnienie?

Procedurę SCA stosujemy zwłaszcza przy zleceniu przez Ciebie transakcji w POS (terminal w sklepie stacjonarnym), transakcji gotówkowej w bankomacie oraz transakcji przeprowadzanej w internecie (e-commerce). Dodatkowo wymagamy pozytywnego przejścia dwuetapowej weryfikacji przy nadaniu kodu PIN/e-PIN.

13 dobrych nawyków płatniczych

1. **Chroń kody PIN/e-PIN i hasła**
Nigdy nie udostępniaj kodu PIN/e-PIN ani haseł innym osobom. Nie zapisuj ich na karcie ani w łatwo dostępnych miejscach – w ten sposób skutecznie zabezpieczysz się przed ich przypadkowym ujawnieniem.

2. **Zachowaj ostrożność w związku z numerem karty i kodem CVV/CVC**
Nigdy nie podawaj numeru karty kredytowej ani kodu CVV/CVC osobom trzecim. Nie wpisuj ich na nieznanych lub niesprawdzonych stronach. Zawsze upewniaj się, że są to strony bezpieczne i zaufane.

czytaj dalej >

13 dobrych nawyków płatniczych

3 **Przechowuj kartę bezpiecznie**
Noś kartę w zamkniętym, bezpiecznym miejscu, na przykład w etui lub osobnej przegródce portfela. Dzięki temu zmniejszasz ryzyko jej zgubienia lub kradzieży.

4 **Zadbaj o bezpieczeństwo płatności online**
Kupuj w internecie tylko na zaufanych stronach z zabezpieczeniem HTTPS (z kłódką przy adresie). Jeśli to możliwe, włączaj dodatkowe uwierzytelnienie (np. 3D Secure) zwiększające ochronę transakcji.

5 **Korzystaj z oficjalnych aplikacji mobilnych**
Pobieraj aplikacje wyłącznie z autoryzowanych sklepów, takich jak App Store lub Google Play. Nie instaluj aplikacji ProviGo z innych źródeł. Unikniesz w ten sposób ryzyka zainstalowania złośliwego oprogramowania, które może przechwycić Twoje dane.

6 **Regularnie sprawdzaj historię transakcji**
Regularnie przeglądaj historię transakcji w aplikacji lub na miesięcznym zestawieniu. Dzięki temu szybciej zauważysz podejrzane operacje, co pozwoli na szybką reakcję – zgłaszaj nam wszystkie nieprawidłowości.

7 **Uważaj na fałszywe telefony i wiadomości**
Uważaj na telefony, SMS-y lub e-maile z prośbą o podanie danych karty. Nie podawaj tych informacji, zwłaszcza gdy osoba dzwoniąca podaje się za przedstawiciela Provident Polska SA. Zakończ rozmowę i skontaktuj się z Centrum Obsługi Klienta.

8 **Nie przekazuj nieznajomym danych osobowych**
Nie podawaj danych karty ani innych informacji osobom dzwoniącym z nieznanych numerów, nawet jeśli podają się za przedstawicieli Provident Polska SA. Zawsze weryfikuj podejrzane kontakty.

9 **Trzymaj się oficjalnych zasad kontaktu z Provident Polska SA**
Pamiętaj, że nasi pracownicy nigdy nie proszą Cię o podanie pełnych danych karty, PIN-u czy haseł przez telefon, SMS lub e-mail. Taka prośba to próba oszustwa. Natychmiast nas o niej poinformuj.

10 **Korzystaj bezpiecznie z bankomatów**
Wybieraj bankomaty w dobrze oświetlonych miejscach. Zanim włożysz kartę, sprawdź, czy urządzenie nie ma podejrzanych elementów, na przykład skimmerów (mogą kopiować dane karty).

11 **Korzystaj bezpiecznie z terminali płatniczych**
Podczas płatności trzymaj kartę na widoku. Jeśli terminal działa nietypowo lub obsługa zabiera kartę poza Twoje pole widzenia (np. w restauracji), zachowaj ostrożność.

12 **Blokuj kartę zdalnie**
W przypadku zgubienia lub podejrzenia kradzieży karty natychmiast ją zablokuj. Możesz to zrobić, kontaktując się z Centrum Obsługi Klienta. Blokada uniemożliwi nieuprawnione transakcje.

13 **Pamiętaj o możliwości zastrzeżenia numeru PESEL**
Jeśli podejrzewasz lub wiesz, że osoba trzecia mogła ukraść Twoją tożsamość albo uzyskać Twoje dane osobowe, natychmiast zastrzeż swój numer PESEL w Rejestrze zastrzeżeń numerów PESEL (więcej: https://www.mobywatel.gov.pl/twoje-dane/rzp-pesel) do czasu wyjaśnienia sprawy.