



Sprawdź! Zabezpiecz! Aktualizuj!

– te trzy czynności, wykonywane podczas korzystania z elektronicznych form płatności, poprawiają bezpieczeństwo, zarówno w cyberprzestrzeni, jak i codziennej rzeczywistości.

Zgubiłeś telefon?

W razie zgubienia telefonu można zdalnie wyłączyć kartę w telefonie za pomocą systemu bankowości elektronicznej lub przez infolinię. Pamiętaj! Wyłączenie karty w telefonie nie jest tożsame z zablokowaniem karty płatniczej (plastikowej) – można jej wciąż używać.

Zgubiłeś kartę?

Zintegrowany System Zastrzegania Kart pozwala na szybkie zastrzeżenie karty płatniczej, nawet jeżeli nie pamiętasz numeru telefonu do infolinii banku, który wydał kartę. Można to zrobić pod numerem telefonu: 828 828 828 lub pod adresem: zastrzegam.pl



Zastrzeż kartę! – tel. 828 828 828 lub na zastrzegam.pl

Jeżeli podejrzewasz, że mogłeś paść ofiarą skimmingu, należy jak najszybciej zastrzec kartę, powiadomić bank oraz zgłosić zdarzenie na policję, ponieważ skimming jest przestępstwem. Kartę możemy zastrzec w każdym banku lub w Zintegrowanym Systemie Zastrzegania Kart – na stronie: zastrzegam.pl lub telefonicznie pod numerem 828-828-828.

Płatności BLIK

Inną formą szybkich płatności jest BLIK. To popularne, polskie rozwiązanie płatnicze.

Możesz zapłacić BLIK-iem, mając:

- smartfon o parametrach mogących obsłużyć aplikację bankową;
- aplikację bankową założoną w banku współpracującym z BLIK;
- dostęp do internetu poprzez sieć komórkową lub sieć Wi-Fi.

Za pomocą BLIK-a możesz: zapłacić w sklepie, zapłacić za zakupy w internecie, wpłacać i wypłacać pieniądze z bankomatu, przysyłać komuś pieniądze.

Chroń wszystkie dane, które są związane z możliwością dokonywania płatności elektronicznych, w tym: loginy, hasła, kody PIN do aplikacji banku, kody SMS, dane znajdujące się na Twojej karcie płatniczej czy jednorazowe kody BLIK. Pamiętaj, że te informacje mają charakter poufny. Zgodnie z obowiązującym w Polsce prawem nie mogą być udostępniane osobom trzecim.



Przeczytaj! Zapamiętaj!

Jak bezpiecznie korzystać z aplikacji mobilnych, płacić telefonem i używać kodu BLIK?

⚠ **Zabezpiecz telefon przed nieuprawnionym dostępem** – może to być kod PIN, biometria, czyli faceID bądź odcisk palca. Uważaj! Korzystanie ze specjalnego symbolu w celu odblokowania telefonu jest najsłabszym sposobem jego zabezpieczenia – łatwo go podejrzeć.

⚠ **Aplikację bankową zabezpiecz odpowiednio silnym hasłem, PIN-em** – innym niż wykorzystywanym do odblokowania telefonu lub w serwisach internetowych.

⚠ **Instaluj aplikacje tylko z pewnego źródła.** Wszystkie aplikacje instalowane na smartfonie również te, które nie są powiązane z obsługą konta bankowego (np. komunikator), powinny pochodzić z zaufanego źródła. Wybieraj programy, które są dostępne w oficjalnych sklepach z aplikacjami, czyli Sklepie Play dla Androida oraz App Store dla iPhone'a.

⚠ **Zadbaj, by telefon, na którym korzystasz z aplikacji bankowej, był zabezpieczony oprogramowaniem antywirusowym.** Dopytaj, czy instalowany program antywirusowy jest wyposażony w mechanizmy skanujące aplikacje, które pobierasz na telefon, oraz odwiedzane strony. W przypadku zidentyfikowanego zagrożenia, oprogramowanie powiadomi o tym, blokując lub chroniąc dostęp przed stroną rozpoznaną jako złośliwa.

⚠ **Regularnie aktualizuj system operacyjny i aplikacje zgodnie z powiadomieniami w telefonie.** Pamiętaj! Każda aktualizacja lepiej zabezpiecza system i pracujące w nim aplikacje.

⚠ **Nie pożyczaj telefonu innym osobom i nie pozostawiaj go bez kontroli.**

Pamiętaj! Nigdy nie loguj się do aplikacji bankowości elektronicznej z obcego smartfona.

⚠ **Unikaj korzystania z otwartych sieci Wi-Fi.** Otwarte sieci Wi-Fi w galeriach handlowych, na lotniskach czy w hotelach mogą być przechwycone przez hakerów. Uwaga! Nie używaj otwartych sieci Wi-Fi do przeprowadzania jakichkolwiek transakcji czy przesyłania ważnych danych.

⚠ **Korzystaj jedynie z własnych akcesoriów np. do ładowania telefonu.** Własne kable i własny powerbank to gwarancja, że Twoje dane pozostaną bezpieczne.

⚠ **Wszędzie, gdzie to możliwe, włącz uwierzytelnienie dwuskładnikowe.** Dodatkowa forma uwierzytelnienia zabezpieczy Cię jako faktycznego użytkownika danej aplikacji i pozwoli jeszcze lepiej zabezpieczyć Twój smartfon.

⚠ **Zawsze chroń dane dostępne przed oczami innych.** Logując się do aplikacji czy nawet do samego systemu operacyjnego telefonu, rób to dyskretnie, tak by nikt nie mógł podejrzeć wpisywanych haseł. Pamiętaj! Powiadomienia w smartfonie warto ustawić w taki sposób, by nie była wyświetlana treść wiadomości, a jedynie nadawca.

EDUKACJA NBP
NBP.PL/EDUKACJA



NARODOWY
BANK POLSKI

BEZPIECZEŃSTWO PŁATNOŚCI ELEKTRONICZNYCH



Każdy z nas był kiedyś na jarmarku lub targu. Poszukiwanie produktu, sprawdzanie jakości a w końcu wybór i decyzja poprzedzona rozmową ze sprzedającym, czasem zachętą do zakupu w postaci rabatu. W takich miejscach najczęściej płatności dokonuje się gotówką, choć coraz częściej można też zapłacić elektronicznie.

Polacy wciąż chętnie płacą gotówką. Gotówka nie ogranicza płacącego – nie zależy od dostępu do internetu, nie trzeba też pamiętać PIN-u do aplikacji lub karty.

Polacy cenią sobie wygodę i szybkość, więc często wybierają także elektroniczne sposoby płatności. Płatności elektroniczne dają możliwość przesyłania środków pieniężnych pomiędzy kontem bankowym kupującego i sprzedającego, a cała transakcja przebiega w czasie rzeczywistym.

Czym są płatności elektroniczne?

Płatności elektroniczne są transakcjami bezgotówkowymi, przeprowadzanymi za pośrednictwem internetu, przy pomocy takich urządzeń jak: karta płatnicza, smartfon, laptop czy smartwatch. Dzięki nim możemy bezpiecznie zapłacić za zakupy w sklepach internetowych. Do płatności elektronicznych zalicza się między innymi internetowy przelew bankowy, portfele elektroniczne np. Google Pay czy Apple Pay, a także płatność BLIK.

Karta płatnicza

Karta płatnicza jest instrumentem płatniczym, a płatność kartą określamy jako płatność zdalną. Karty są wydawane przez instytucje finansowe i służą do przeprowadzania transakcji bezgotówkowych w punktach usługowych lub handlowych. Kartą można też wpłacać lub wypłacać środki z bankomatów.

Jakie dane zawiera karta płatnicza?

Wymiary kart płatniczych zostały określone przez Międzynarodową Organizację Normalizacyjną i są standardowe dla każdej karty. Każda karta zawiera chip (mikroprocesor) oraz pasek magnetyczny – dzięki nim możliwe jest połączenie z internetem poprzez terminal płatniczy.



Na karcie znajdują się następujące informacje: nazwa oraz logo banku, imię i nazwisko posiadacza karty, numer karty, informacja o rodzaju karty debetowa/kredytowa, data ważności karty: miesiąc i rok, numer CVV2/CVC2, miejsce na podpis posiadacza karty.

Kod CVC (ang. Card Verification Code) stosowany w kartach organizacji płatniczej Mastercard, jest dokładnie tym samym, czym kod CVV (ang. Card Verification Value), stosowany w kartach Visa. Są to kody zabezpieczające, które umieszcza się na kartach płatniczych. Pojedynczy kod CVC/CVV składa się z trzech cyfr. Znajduje się on na rewersie, tuż obok miejsca na podpis właściciela karty. Lokalizacja nie jest przypadkowa: umieszczenie kodu w tym miejscu sprawia, że nie jest on widoczny w trakcie płatności kartą, więc ryzyko, że poznają go osoby postronne, jest zredukowane. Gdyby kod CVC/CVV znajdował się na drugiej stronie karty – możliwe byłoby odczytanie go np. z zapisów kamer.

Płatność kartą jest zaliczana do jednych z najbezpieczniejszych. W przypadku płatności kartą za zakupy internetowe należy podać dane karty, takie jak: kod CVV lub CVC, numer karty i datę jej ważności. Operatorzy zapewniają bezpieczeństwo transakcji poprzez wykorzystanie szyfrowanego połączenia podczas realizacji płatności. Ponadto większość banków wymaga obecnie dodatkowego zabezpieczenia płatności w postaci potwierdzenia transakcji kodem PIN w aplikacji bankowej lub np. kodu SMS wygenerowanego przez bank właściciela karty.



Gdy płacisz kartą za zakupy internetowe, sprawdź, czy strona sklepu internetowego ma szyfrowane połączenie, o czym świadczy wpis: <https://> w pasku przed adresem strony oraz dodatkowo ikona kłódki, która po kliknięciu pokazuje nazwę właściciela certyfikatu bezpieczeństwa.

Karta płatnicza nie musi mieć postaci plastikowego przedmiotu. Coraz częściej posługujemy się jej wirtualną formą, która jest skonfigurowana w aplikacji, zwanej wirtualnym portfelem na smartfonie bądź w smartwachu. Płatności mobilne, takie jak Google Pay oraz Apple Pay, są odpowiednikiem wirtualnego portfela połączonego z kartą kredytową lub debetową użytkownika. Płatność jest potwierdzana przy pomocy kodu SMS w przypadku Google Pay lub za pomocą odcisku linii papilarnych (TouchID) lub zdjęcia twarzy (FaceID) w przypadku Apple Pay.



Linie papilarne, zdjęcie twarzy lub zdjęcie tęczęwki to identyfikacja biometryczna. To dane wrażliwe, które trzeba chronić. Nie należy ich udostępniać np. aplikacjom lojalnościowym w zamian za korzyści!

Bezpieczne używanie karty płatniczej

⚠ Uwaga! Skimming

Fizyczne karty płatnicze mogą być narażone na kopiowanie danych z paska magnetycznego. Dane – takie jak numer karty czy data ważności – służą przestępcy do wykonania kopii karty, a następnie umożliwiają mu zrealizowanie płatności internetowej lub wypłaty środków z bankomatu. Takie przestępstwo nazywane jest skimmingiem. Kopiowanie danych z paska magnetycznego jest możliwe, gdy w bankomacie został zainstalowany tzw. skimmer (nakładka na wpust do wkładania karty do bankomatu). Dodatkowo przestępcy mogą zamontować małe kamery, które rejestrują wpisywany przez właściciela karty kod PIN. Ochroną przed tego typu atakiem jest chip wbudowany w karty płatnicze.

⚠ Uwaga! Przed włożeniem karty do bankomatu

Upewnij się, że wygląd klawiatury czy ekranu nie budzi podejrzeń. Jeżeli na urządzeniu widać element, który wydaje się nietypowy, zrezygnuj z transakcji. Podejrzenia może budzić m.in. obecność dodatkowych wkładek w szczelinie na kartę – wlot na kartę musi być pusty. Jeżeli bankomat nie budzi zastrzeżeń, pamiętaj, by zasłonić wpisywany kod PIN ręką – tak by nie zarejestrowała go żadna kamera.

Pamiętajmy, by płacąc kartą, nigdy nie tracić jej z pola widzenia. Ograniczamy w ten sposób możliwość skopiowania karty np. przez nieuczciwego sprzedawcę lub usługodawcę.

⚠ Pamiętaj! Ustaw limit transakcji bezgotówkowych

Ważnym zabezpieczeniem w płatnościach elektronicznych (szczególnie gdy przestępcy udało się zrobić duplikat naszej karty) jest posiadanie dziennego limitu transakcji bezgotówkowych – w ten sposób przestępca nie będzie mógł zrealizować transakcji powyżej ustalonej kwoty. Ustalenie limitów dla poszczególnych typów transakcji bezgotówkowych powinno być pierwszym krokiem zabezpieczającym płatności wykonanym przez użytkownika.



Podrabianie karty płatniczej jest zgodnie z przepisami ustawy Kodeks karny traktowane jako podrabianie „innego środka płatniczego”. Grozi za to odpowiedzialność karna – od 5 do 25 lat pozbawienia wolności.