# Cyfrowa rewolucja finansowa

## Zagrożenia związane z płatnościami bezgotówkowymi i on-line

W dobie dynamicznego rozwoju technologii cyfrowych i rosnącej popularności transakcji bezgotówkowych, płatności on-line stają się nieodłącznym elementem codziennego życia. Coraz więcej osób rezygnuje z gotówki na rzecz kart płatniczych, aplikacji mobilnych oraz bankowości internetowej, które oferują szybkie, wygodne i dostępne z dowolnego miejsca na świecie rozwiązania finansowe. Dzięki nim możemy dokonywać zakupów, płacić rachunki, zarządzać oszczędnościami, a nawet inwestować za pomocą kilku kliknięć na ekranie smartfona. Ta cyfrowa rewolucja zmienia nasze podejście do finansów, sprawiając, że codzienne operacje stają się bardziej efektywne i komfortowe.

Jednakże, wraz z tymi udogodnieniami pojawiają się również liczne zagrożenia, które mogą narazić użytkowników na poważne straty finansowe. Cyberprzestępcy wykorzystują coraz bardziej zaawansowane techniki ataków, które mogą obejmować kradzież danych, oszustwa phishingowe, złośliwe oprogramowanie, a także manipulacje związane z nieautoryzowanymi transakcjami. Dodatkowo, rosnąca liczba urządzeń podłączonych do internetu, jak również rozwój płatności mobilnych, stwarzają nowe wyzwania związane z bezpieczeństwem danych oraz ochroną prywatności.

Celem publikacji jest dostarczenie czytelnikom kompleksowej wiedzy na temat zagrożeń i sposobów ochrony, aby mogli oni cieszyć się korzyściami płynącymi z płatności cyfrowych, nie narażając się na niepotrzebne ryzyko.

# Spis treści:


1. Techniki manipulacji i socjotechnika w oszustwach skierowanych do seniorów
2. Kroki do podjęcia w przypadku podejrzenia oszustwa
3. Kroki do rozpoznawania oszustw
4. Oszustwa przy zakupach online: Praktyczne porady i działania
5. Jak płacić przez Internet? Przegląd najpopularniejszych metod
6. Transakcje przez karty płatnicze
7. Transakcje przez aplikacje mobilne
8. Transakcje przez przelewy bankowe


# Techniki manipulacji i socjotechnika w oszustwach skierowanych do seniorów

Oszukiwanie seniorów jest poważnym problemem, który przybiera na sile wraz z postępem technologicznym i rosnącą liczbą osób starszych korzystających z nowoczesnych narzędzi komunikacji, takich jak internet, telefony komórkowe czy media społecznościowe. Oszuści doskonale zdają sobie sprawę, że seniorzy często są bardziej ufni, mniej zaznajomieni z nowoczesnymi technologiami oraz mniej świadomi zagrożeń płynących z sieci, co czyni ich szczególnie podatnymi na różnego rodzaju oszustwa.

Metody, które wykorzystują oszuści, są niezwykle zróżnicowane i stale ewoluują, aby dostosować się do zmieniających się realiów technologicznych i społecznych. Wykorzystując socjotechnikę, oszuści celowo manipulują emocjami i zaufaniem seniorów, próbując wywołać u nich strach, niepokój lub poczucie pilności. Często podszywają się pod bliskich, pracowników instytucji zaufania publicznego, takich jak banki, urzędy czy organizacje charytatywne, a także tworzą fałszywe sytuacje, które mają na celu wywołanie natychmiastowej reakcji.

Typowe oszustwa skierowane do seniorów obejmują m.in. fałszywe powiadomienia o wygranych, alarmujące wiadomości o problemach z kontem bankowym, prośby o pomoc finansową od rzekomych członków rodziny, a także bardziej skomplikowane schematy, takie jak phishing, w których oszuści próbują uzyskać dostęp do prywatnych danych lub zainstalować złośliwe oprogramowanie na komputerze ofiary.

# Techniki manipulacji i socjotechnika w oszustwach skierowanych do seniorów

Oto kilka konkretnych przykładów oszustw, z którymi mogą się spotkać seniorzy:

## 1 E-maile:

- Fałszywe powiadomienia o nagrodach: E-maile informujące o wygranej w losowaniu lub konkursie, w którym nie brało się udziału. Proszą o podanie danych osobowych lub opłatę za "weryfikację" nagrody.
  - **Przykład:** ***"Gratulacje! Wygrałeś 1 000 000 PLN w naszym losowaniu. Aby odebrać nagrodę, prosimy o przesłanie opłaty w wysokości 200 PLN na podany rachunek bankowy."***

- Fałszywe alerty bankowe: E-maile podszywające się pod bank, informujące o podejrzanych transakcjach lub problemach z kontem, z prośbą o kliknięcie w link i zalogowanie się na stronie, która jest imitacją prawdziwej strony banku.
  - **Przykład:** ***"Twoje konto zostało zablokowane z powodu nietypowej aktywności. Kliknij ten link, aby zweryfikować swoje dane i odblokować konto."***

- *Fałszywe powiadomienia o aktualizacji oprogramowania: E-maile informujące o konieczności natychmiastowej aktualizacji oprogramowania na komputerze lub telefonie. Link prowadzi do złośliwego oprogramowania, które infekuje urządzenie.*
  - ***Przykład: "Nowa aktualizacja zabezpieczeń Twojego systemu operacyjnego jest dostępna. Kliknij tutaj, aby zainstalować aktualizację i ochronić swoje urządzenie."***

## 2 Wiadomości SMS:

- Fałszywe powiadomienia o problemach z przesyłkami: SMS-y informujące o problemach z dostawą paczki i prośbą o kliknięcie w link, który może prowadzić do fałszywej strony lub zainfekować telefon.
  - **Przykład:** "***Twoja przesyłka nie mogła zostać dostarczona. Kliknij tutaj, aby zaktualizować swoje dane dostawy.***"

- Fałszywe powiadomienia o wygranej: Wiadomości informujące o rzekomej wygranej w konkursie lub promocji, z prośbą o kontakt lub przekazanie danych osobowych.
  - **Przykład**: ***"Wygrałeś 5000 PLN! Aby odebrać nagrodę, skontaktuj się z nami pod tym numerem."***

## 3 Połączenia telefoniczne

- Fałszywe telefony od rzekomych pracowników banku: Telefon z informacją o nietypowej aktywności na koncie, z prośbą o podanie danych osobowych lub numerów kart kredytowych.
  - **Przykład:** ***"Dzień dobry, na Twoim koncie zauważyliśmy podejrzaną transakcję. Aby zabezpieczyć konto, proszę podać numer karty kredytowej i PIN."***

- Fałszywe prośby o pomoc: Oszuści mogą podszywać się pod bliskich, twierdząc, że są w nagłej potrzebie finansowej i proszą o przekazanie pieniędzy.
  - **Przykład:** ***"Cześć, to Twoja wnuczka. Miałam wypadek i potrzebuję pilnie 2000 PLN. Proszę, prześlij pieniądze na ten numer konta."***

## 4 Media społecznościowe: Facebook

- Fałszywe profile i oszustwa na Messengerze: Oszuści mogą tworzyć fałszywe profile, aby nawiązać kontakt z seniorami, a następnie próbować wyłudzić pieniądze lub dane osobowe.
  - **Przykład:** ***"Cześć, jestem nowym przyjacielem Twojego wnuka. Potrzebuję pilnie pieniędzy na leczenie. Czy możesz pomóc?"***

- Phishing w wiadomościach: Wiadomości z fałszywymi linkami, które kierują do strony imitującej logowanie na Facebooku, gdzie seniorzy mogą wprowadzić swoje dane logowania.
  - **Przykład:** ***"Twoje konto Facebook wymaga natychmiastowej weryfikacji. Kliknij tutaj, aby potwierdzić swoje dane."***

# Kroki do podjęcia w przypadku podejrzenia oszustwa

Jeśli podejrzewasz, że padłeś ofiarą oszustwa lub zauważyłeś próbę oszustwa, ważne jest, aby podjąć odpowiednie kroki, aby zminimalizować straty i zgłosić sprawę odpowiednim organom.

Oto co należy zrobić:

## 1 Zgłoszenie do Policji

- W przypadku przestępstwa: Jeśli uważasz, że doszło do przestępstwa (np. wyłudzenia pieniędzy, kradzieży tożsamości), zgłoś to na najbliższym komisariacie policji lub telefonicznie pod numerem 112.
- Cyberprzestępczość: Możesz zgłosić cyberprzestępstwa (np. phishing, oszustwa internetowe) bezpośrednio na stronie internetowej Policji lub w specjalnych jednostkach zajmujących się cyberprzestępczością.

## 2 Zgłoszenie do banku

- Podejrzane transakcje: Jeśli zauważysz podejrzane transakcje na swoim koncie bankowym, natychmiast skontaktuj się z bankiem i zablokuj konto.
- Oszustwa związane z bankiem: Zgłoś sprawę do banku, który następnie może wszcząć dochodzenie wewnętrzne.

## 3 Zgłoszenie do instytucji finansowych

- Oszustwa związane z płatnościami: Jeśli oszustwo dotyczy np. płatności kartą kredytową lub platformy płatniczej (np. PayPal), zgłoś to bezpośrednio do dostawcy usługi.

# Kroki do podjęcia w przypadku podejrzenia oszustwa

## 4 Zgłoszenie do CERT Polska

- Cyberprzestępczość: CERT Polska (Computer Emergency Response Team) zajmuje się bezpieczeństwem w sieci i reaguje na incydenty związane z cyberprzestępczością. Możesz zgłosić incydenty za pośrednictwem formularza na ich stronie internetowej.

## 5 Zgłoszenie do Urzędu Ochrony Konkurencji i Konsumentów (UOKiK)

- Nieuczciwe praktyki rynkowe: Jeśli oszustwo jest związane z zakupami, umowami lub innymi sprawami konsumenckimi, możesz zgłosić sprawę do UOKiK. Możesz to zrobić online na stronie **UOKiK**.

**Wnioski:**
Bądź zawsze czujny i nie ufaj nieznanym źródłom. Regularnie sprawdzaj swoje finanse, komunikuj się z zaufanymi osobami i instytucjami, a w przypadku podejrzeń, nie wahaj się zgłosić sprawy odpowiednim organom. Edukacja i świadomość to najlepsze sposoby na uniknięcie oszustwa.

# Kroki do podjęcia w przypadku podejrzenia oszustwa

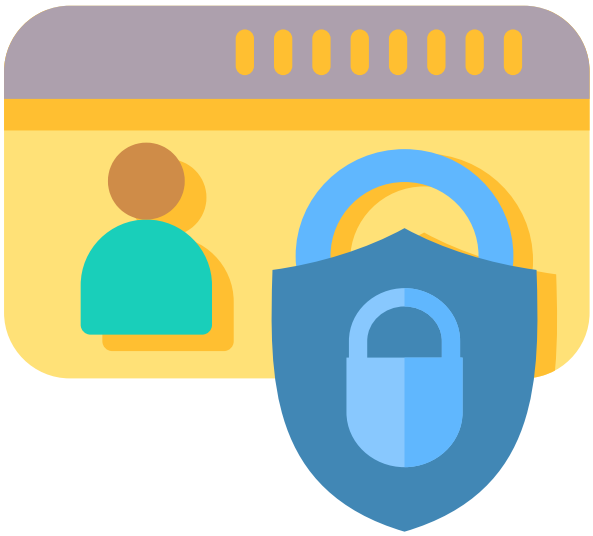
## Postępowanie, gdy sądzisz, że coś jest nie tak:

1. **Zachowaj spokój:** Nie podejmuj pochopnych decyzji. Zastanów się, czy sytuacja jest wiarygodna.
2. **Nie podawaj danych osobowych:** Nigdy nie udostępniaj swoich danych osobowych, numerów kart kredytowych ani haseł, dopóki nie upewnisz się, że masz do czynienia z legalną instytucją lub osobą.
3. **Zweryfikuj informacje:** Zanim odpowiesz na wiadomość lub oddzwonisz na podejrzany numer, sprawdź jego autentyczność, np. kontaktując się bezpośrednio z instytucją, którą rzekomo reprezentuje osoba dzwoniąca.
4. **Skontaktuj się z bliskimi:** Jeśli masz wątpliwości, porozmawiaj z kimś z rodziny lub przyjacielem, aby wspólnie ocenić sytuację.
5. **Zablokuj podejrzane kontakty:** W przypadku podejrzanych SMS-ów, e-maili lub telefonów, zablokuj nadawcę i nie odpowiadaj na wiadomości.
6. **Zapisuj dowody:** Przechowuj wszelkie dowody, takie jak SMS-y, e-maile, czy notatki z rozmów telefonicznych, które mogą być przydatne w zgłoszeniu oszustwa.

# Kroki do rozpoznawania oszustw

**Aby być na bieżąco z nowymi metodami oszustw, warto:**

- **śledzić wiadomości w mediach**, regularnie czytać wiadomości, ponieważ wiele portali informacyjnych i programów telewizyjnych ostrzega o nowych zagrożeniach.
- **odwiedzać strony rządowe i instytucje,** takie jak UOKiK, CERT Polska czy Policja, gdzie często publikowane są ostrzeżenia o nowych metodach oszustw.
- **dołączać do grup społecznościowych i forów** na Facebooku lub innych platformach, gdzie użytkownicy dzielą się informacjami o oszustwach i zagrożeniach.
- **korzystać z aplikacji bankowych**, które często mają wbudowane funkcje ostrzegania o nowych rodzajach oszustw, oraz śledzić powiadomienia i newslettery od swojego banku.
- **uczestniczyć w edukacji i szkoleniach**, organizowanych przez instytucje finansowe, szkoły lub organizacje pozarządowe, które uczą o bezpieczeństwie w internecie.
- **utrzymywać kontakt z zaufanymi dostawcami usług** regularnie komunikując się z bankiem i innymi dostawcami, aby dowiadywać się o nowych zagrożeniach.



# Oszustwa przy zakupach online: Praktyczne porady i działania

Oszustwa przy zakupach online mogą przybierać różne formy. Oto kilka przykładów oszustw związanych z zakupami:

## 1 Brak przesyłki po zapłacie

- **Opis**: Dokonujesz zapłaty za przedmiot, ale sprzedawca nigdy nie wysyła towaru. Po dokonaniu płatności sprzedawca przestaje odpowiadać na wiadomości lub podaje fałszywe informacje o wysyłce.
- **Przykład:** Kupujesz laptopa na Allegro od sprzedawcy z niską ceną. Po opłaceniu zamówienia nie otrzymujesz żadnej przesyłki, a kontakt ze sprzedawcą się urywa.
- **Jak zapobiegać:** Zanim dokonasz zakupu, sprawdź opinie o sprzedawcy i upewnij się, że ma dobrą reputację.
- **Jak reagować:** Skontaktuj się ze sprzedawcą poprzez platformę. Jeśli nastąpi brak reakcji, zgłoś problem na platformie zakupowej i poinformuj operatora płatności. Rozważ zgłoszenie sprawy na policję.

## 2 Otrzymanie produktu niezgodnego z opisem

- **Opis:** Otrzymujesz towar, który znacznie różni się od opisu w ofercie – może być uszkodzony, niekompletny lub zupełnie inny niż zamówiony produkt.
- **Przykład:** Zamawiasz nowy telefon komórkowy, ale otrzymujesz używany, zniszczony model, który nie działa.
- **Jak zapobiegać:** Przeczytaj dokładnie opisy produktów i sprawdź zdjęcia. Jeśli coś wydaje się podejrzane, zrezygnuj z zakupu.
- **Jak reagować:** Zgłoś niezgodność produktu na platformie zakupowej i skontaktuj się z obsługą klienta w celu zwrotu lub wymiany towaru.

## 3 Fałszywe potwierdzenie wysyłki

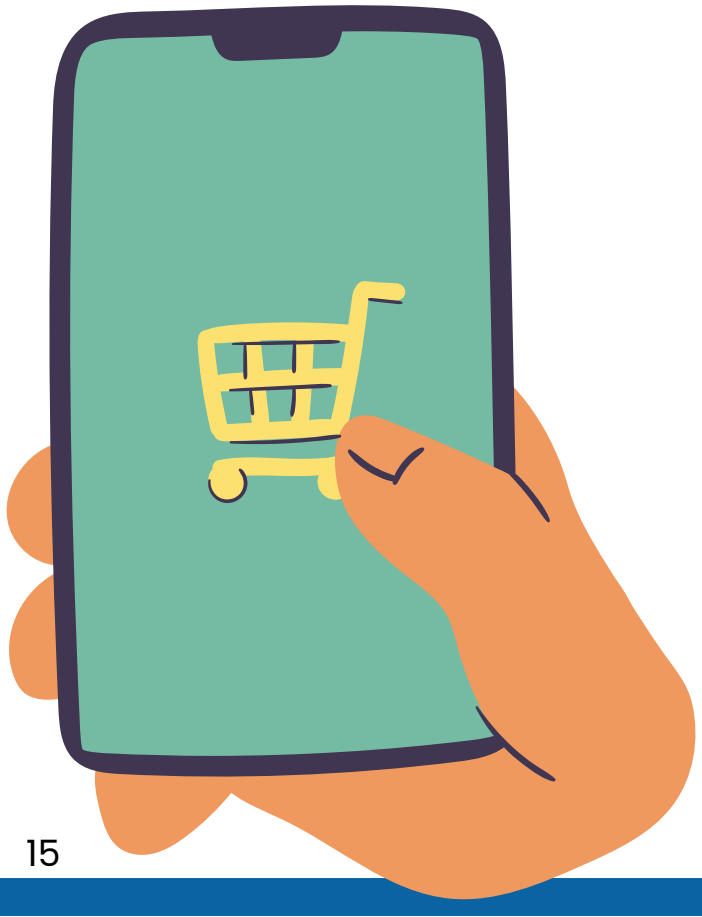
- **Opis:** Otrzymujesz fałszywe potwierdzenie nadania paczki lub numer śledzenia, który nie działa lub wskazuje na inną przesyłkę.
- **Przykład:** Sprzedawca podaje fikcyjny numer paczki, co utrudnia Ci wykazanie, że towar nie został wysłany.
- **Jak zapobiegać:** Upewnij się, że numer śledzenia jest prawidłowy, sprawdzając go na stronie przewoźnika.
- **Jak reagować:** Skontaktuj się ze sprzedawcą i dostawcą, aby wyjaśnić sytuację. Jeśli problem nie zostanie rozwiązany, zgłoś to na platformie zakupowej i operatorowi płatności.

## 4 Oszustwo przez fałszywe strony transakcyjne

- **Opis:** Oszuści tworzą fałszywe strony internetowe, które przypominają strony platform handlowych (jak Allegro). Wprowadzasz swoje dane logowania lub płatności, które są następnie przechwytywane przez oszustów.
- **Przykład:** Otrzymujesz e-mail z fałszywej strony, proszący o zalogowanie się w celu potwierdzenia zamówienia. Klikając na link, trafiasz na fałszywą stronę, która kradnie Twoje dane.
- **Jak zapobiegać:** Nigdy nie klikaj w linki zawarte w e-mailach lub wiadomościach tekstowych, które proszą o podanie danych logowania lub płatności, zanim dokładnie nie zweryfikujesz źródła wiadomości. Upewnij się, że wiadomość pochodzi od autoryzowanego sprzedawcy lub strony, na której dokonałeś zakupu.
- **Jak reagować:** Jeśli podejrzewasz, że padłeś ofiarą oszustwa internetowego, możesz zgłosić taki incydent na stronie internetowej **incydent.cert.pl**.

## 5 Płatność poza platformą

- **Opis:** Sprzedawca proponuje dokonanie płatności poza platformą (np. przez przelew bankowy), obiecując niższą cenę. Po dokonaniu płatności sprzedawca znika, a kupujący nie ma możliwości odzyskania pieniędzy przez system ochrony kupujących.
- **Przykład:** Kupujesz przedmiot przez platformę sprzedażową jak Allegro, ale sprzedawca proponuje zapłatę przez bezpośredni przelew bankowy. Po zapłaceniu nie dostajesz towaru, a sprzedawca przestaje odpowiadać.
- **Jak zapobiegać:** Dokonuj płatności wyłącznie przez oficjalne kanały płatności platformy zakupowej. Unikaj płatności na zewnętrzne konta bankowe.
- **Jak reagować:** Zgłoś sytuację na platformie zakupowej i operatorowi płatności. Jeśli oszustwo jest potwierdzone, skontaktuj się z policją.



## 6 Oszustwa z ofertami wyjątkowych okazji

- **Opis:** Oszust tworzy atrakcyjną ofertę z dużą zniżką na popularny produkt. Oferta może być czasowo ograniczona, aby wywołać presję na szybką decyzję. Po zapłacie towar nigdy nie zostaje wysłany.
- **Przykład:** Znajdujesz ofertę na nowy telewizor za połowę ceny, kupujesz go, ale nigdy nie otrzymujesz przesyłki, a sprzedawca okazuje się fałszywy.
- **Jak zapobiegać:** Bądź ostrożny wobec zbyt atrakcyjnych ofert i sprawdzaj wiarygodność sprzedawców. Upewnij się, że oferta jest zgodna z cenami rynkowymi.
- **Jak reagować:** Zgłoś oszustwo na platformie zakupowej, skontaktuj się z operatorem płatności i rozważ zgłoszenie sprawy na policję.

Każdy z tych przykładów ilustruje różne metody oszustw i wskazuje, jak można zapobiegać takim sytuacjom oraz jak na nie reagować, aby minimalizować straty i odzyskać swoje pieniądze.

# Jak płacić przez Internet? Przegląd najpopularniejszych metod

W dzisiejszych czasach płatności internetowe stały się nieodłącznym elementem codziennego życia, a preferencje konsumentów zdecydowanie skłaniają się ku metodom bezgotówkowym. Jak pokazują dane Narodowego Banku Polskiego (NBP), liczba i wartość transakcji realizowanych w Internecie stale rośnie. W II kwartale 2022 roku Polacy wykonali 53,7 milionów transakcji kartami płatniczymi na łączną kwotę 8,3 miliarda złotych, co oznacza wzrost o 9% w porównaniu do kwartału poprzedniego.

Wnioski pochodzą ze strony www.fingerprints.digital

W zależności od naszych potrzeb, w Internecie możemy skorzystać z różnych metod płatności, które różnią się między sobą szybkością, wygodą oraz poziomem bezpieczeństwa.

**Oto najczęściej wybierane opcje:**

## 1 Tradycyjny przelew bankowy:

- To podstawowa metoda, która wymaga ręcznego wpisania danych do przelewu. Mimo że czas zaksięgowania wpłaty jest dłuższy, wielu klientów ceni sobie tę formę płatności za poczucie kontroli nad procesem oraz bezpieczeństwo.

## 2 Przelew online:

- Ta metoda płatności jest wygodniejsza i szybsza niż tradycyjny przelew. Po dokonaniu zakupów system przekierowuje nas do wybranego banku, gdzie możemy szybko zalogować się na swoje konto i potwierdzić automatycznie uzupełniony przelew. Główne zalety to krótki czas księgowania i prostota obsługi.

# Jak płacić przez Internet? Przegląd najpopularniejszych metod

## 3 BLIK:

- BLIK to nowoczesna metoda płatności oparta na jednorazowym, sześciocyfrowym kodzie generowanym przez system bankowy. Użytkownik nie musi podawać swoich danych osobowych, wystarczy wprowadzić kod na stronie płatności i zatwierdzić transakcję. BLIK jest wygodny i charakteryzuje się wysokim poziomem bezpieczeństwa.

## 4 Karta kredytowa lub debetowa:

- Płatność kartą sprawdza się zarówno w sklepach internetowych, jak i przy wykupowaniu abonamentów. Aby dokonać transakcji, należy podać 16-cyfrowy numer karty, imię i nazwisko, datę ważności karty oraz kod CVV/CVC. Dzięki funkcji chargeback płatności kartą są bezpieczne, a bank w razie problemów z kradzieżą środków pomaga w ich odzyskaniu.

## 5 Karta wirtualna:

- Przeznaczona wyłącznie do płatności internetowych, szczególnie przydatna przy transakcjach międzynarodowych. Nie można jej używać w terminalach ani bankomatach, co zwiększa poziom bezpieczeństwa. Karta wirtualna pozwala na bezpieczne zakupy online bez ryzyka związanych z fizyczną kartą.

## 6 Karta prepaid (przedpłacona):

- Jest to karta, którą można zasilić określoną kwotą, a następnie używać do płatności w Internecie. Składa się z 16 znaków wpisywanych podczas realizacji transakcji. Karta prepaid jest doskonałym rozwiązaniem dla osób, które chcą bezpiecznie płacić za zakupy online bez konieczności posiadania rachunku bankowego czy karty kredytowej.

Każda z tych metod ma swoje unikalne zalety i jest odpowiednia dla różnych potrzeb użytkowników. Wybór odpowiedniej opcji zależy od indywidualnych preferencji, poziomu komfortu z technologią oraz potrzeb związanych z bezpieczeństwem finansowym.

# Transakcje przez karty płatnicze

Podczas korzystania z różnych typów kart płatniczych – kredytowych, debetowych i przedpłaconych – należy być świadomym kilku potencjalnych zagrożeń. Każdy rodzaj karty niesie ze sobą inne ryzyka, które warto zrozumieć, aby uniknąć problemów finansowych i zabezpieczyć się przed oszustwami.

## Karty kredytowe

1. **Ryzyko nadmiernego zadłużenia:**
   - Umożliwiają dokonywanie zakupów na kredyt, co może prowadzić do gromadzenia się długu, zwłaszcza jeśli użytkownik nie spłaca całości zadłużenia na czas.
   - Jak unikać:
     - Ustal budżet i pilnuj, aby nie wydawać więcej, niż możesz spłacić.
     - Spłacaj całość zadłużenia przed upływem okresu bezodsetkowego, aby uniknąć naliczania odsetek.
2. **Opłaty i odsetki:**
   - Niespłacenie zadłużenia w całości może skutkować wysokimi odsetkami oraz dodatkowymi opłatami za opóźnienia w spłacie.
   - Jak unikać:
     - Regularnie monitoruj terminy płatności.
     - Korzystaj z karty kredytowej tylko wtedy, gdy masz pewność, że możesz spłacić zadłużenie w terminie.
3. **Oszustwa i kradzieże:**
   - Karty kredytowe są narażone na kradzież danych, co może skutkować nieautoryzowanymi transakcjami.
   - Jak unikać:
     - Regularnie sprawdzaj historię transakcji.
     - Zgłaszaj natychmiast wszelkie podejrzane transakcje.
     - Unikaj używania karty w podejrzanych miejscach lub witrynach internetowych.

## Karty debetowe

1. **Kradzież danych:**
   - Opis: Ponieważ karty debetowe są bezpośrednio połączone z kontem bankowym, kradzież danych może prowadzić do natychmiastowego opróżnienia konta.
   - Jak unikać:
     - Używaj kart debetowych w zaufanych miejscach.
     - Korzystaj z usług takich jak alerty SMS lub e-mail, aby szybko wykryć nieautoryzowane transakcje.
     - Rozważ stosowanie dodatkowych zabezpieczeń, takich jak dwuskładnikowe uwierzytelnianie.
2. **Ograniczona ochrona w przypadku oszustwa:**
   - Opis: W przypadku kradzieży lub oszustwa, odzyskanie środków może być trudniejsze i bardziej czasochłonne niż w przypadku karty kredytowej.
   - Jak unikać:
     - Nie udostępniaj nikomu danych karty debetowej.
     - Regularnie sprawdzaj stan konta i zgłaszaj wszelkie nieprawidłowości.
3. **Brak środków na koncie:**
   - Opis: Używanie karty debetowej wymaga posiadania środków na koncie. W przypadku braku środków, transakcje mogą zostać odrzucone, co może prowadzić do nieprzyjemnych sytuacji.
   - Jak unikać:
     - Regularnie monitoruj stan swojego konta.
     - Ustaw alerty informujące o niskim saldzie.

## Karty przedpłacone

1. **Ograniczona ochrona prawna:**
   - Opis: Karty przedpłacone mogą nie oferować takiej samej ochrony konsumenckiej jak karty kredytowe lub debetowe, zwłaszcza w przypadku oszustw lub sporów.
   - Jak unikać:
     - Upewnij się, że korzystasz z kart wydawanych przez renomowane instytucje finansowe.
     - Zachowaj paragony i inne dowody zakupu.
2. **Ograniczone środki:**
   - Opis: Karty przedpłacone są ograniczone do kwoty, którą wcześniej zdeponowałeś, co może być problematyczne w nagłych sytuacjach wymagających większych wydatków.
   - Jak unikać:
     - Planuj wydatki z wyprzedzeniem i doładowuj kartę odpowiednimi kwotami.
     - Trzymaj zapasowe środki na innym koncie lub karcie na wypadek nagłych sytuacji.
3. **Niektóre ograniczenia dotyczące użytkowania:**
   - Opis: Niektóre karty przedpłacone mogą nie być akceptowane w każdym miejscu, szczególnie za granicą lub na stronach internetowych wymagających kart kredytowych.
   - Jak unikać:
     - Sprawdź, czy karta przedpłacona jest akceptowana tam, gdzie zamierzasz z niej skorzystać.
     - Zawsze miej alternatywną formę płatności.

# Transakcje przez karty płatnicze

Zeskanuj kod QR, aby poznać szczegóły **metod jak uniknąć oszustwa związanego z kartą kredytową w Internecie.**

Zeskanuj kod QR, aby poznać szczegóły **która karta jest bezpieczniejsza w Internecie** - karta debetowa czy karta kredytowa.

Zeskanuj kod QR, aby poznać szczegóły **czym jest i jak działa karta przedpłacona.**

# Transakcje przez aplikacje mobilne

Transakcje bezgotówkowe realizowane przez aplikacje mobilne stają się coraz bardziej popularne, ale niosą ze sobą pewne zagrożenia, na które warto zwrócić uwagę. Poniżej przedstawiam najważniejsze niebezpieczeństwa związane z korzystaniem z aplikacji mobilnych do dokonywania transakcji oraz sposoby, jak można się przed nimi chronić.

## 1 Kradzież i utrata urządzenia

- Jeśli telefon lub tablet, na którym zainstalowana jest aplikacja mobilna, zostanie skradziony lub zgubiony, złodziej może uzyskać dostęp do aplikacji i dokonywać nieautoryzowanych transakcji.
- Jak unikać:
  - Ustaw silne hasło, PIN lub korzystaj z biometrii (odcisk palca, rozpoznawanie twarzy) do zabezpieczenia urządzenia.
  - Zainstaluj aplikację do zdalnego blokowania i lokalizowania urządzenia na wypadek kradzieży lub zgubienia.
  - Skonfiguruj ustawienia aplikacji mobilnej tak, aby wymagała ponownego logowania po każdym uruchomieniu.

## 2 Złośliwe oprogramowanie

- Złośliwe aplikacje lub oprogramowanie zainstalowane na urządzeniu mogą przechwytywać dane logowania lub przejąć kontrolę nad transakcjami realizowanymi przez aplikację mobilną.
- Jak unikać:
  - Pobieraj aplikacje wyłącznie z oficjalnych sklepów (Google Play, App Store) i unikaj instalowania aplikacji z nieznanych źródeł.
  - Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe na swoim urządzeniu mobilnym.
  - Nie klikaj w podejrzane linki w wiadomościach SMS, e-mailach lub na stronach internetowych.

## 3 Phishing i socjotechniki

- Cyberprzestępcy mogą próbować oszukać użytkowników, aby podali swoje dane logowania do aplikacji mobilnych przez fałszywe strony internetowe lub aplikacje podszywające się pod legalne instytucje finansowe.
- Jak unikać:
  - Nigdy nie podawaj danych logowania ani poufnych informacji na stronach lub w aplikacjach, które nie są w pełni zaufane.
  - Zawsze sprawdzaj adres URL strony lub autentyczność aplikacji, zanim wprowadzisz dane logowania.
  - Banki i inne instytucje finansowe nigdy nie proszą o podanie danych logowania przez e-mail lub SMS – jeśli otrzymasz taką prośbę, zgłoś to jako próbę phishingu.

## 4 Niezabezpieczone połączenie internetowe

- Korzystanie z aplikacji mobilnych do dokonywania transakcji przez publiczne, niezabezpieczone sieci Wi-Fi może narazić dane na przechwycenie przez cyberprzestępców.
- Jak unikać:
  - Unikaj korzystania z aplikacji mobilnych do dokonywania transakcji w publicznych sieciach Wi-Fi. Zamiast tego korzystaj z połączenia danych mobilnych lub sieci VPN.
  - Sprawdź, czy połączenie jest szyfrowane (np. przez https), zanim dokonasz jakiejkolwiek transakcji.

## 5 Słabe hasła i brak dodatkowych zabezpieczeń

- Używanie słabych haseł lub brak dodatkowych zabezpieczeń może ułatwić dostęp do aplikacji mobilnej osobom niepowołanym.
- Jak unikać:
  - Używaj silnych, unikalnych haseł do aplikacji mobilnych.
  - Włącz funkcję dwuskładnikowego uwierzytelniania (2FA), aby zwiększyć bezpieczeństwo transakcji.
  - Regularnie zmieniaj hasła i nie używaj tego samego hasła do różnych aplikacji.

## 6 Niedostateczne zabezpieczenia aplikacji

- Niektóre aplikacje mobilne mogą mieć luki w zabezpieczeniach, które mogą zostać wykorzystane przez hakerów do przejęcia kontroli nad kontem użytkownika.
- Jak unikać:
  - Regularnie aktualizuj aplikacje mobilne do najnowszych wersji, aby korzystać z najnowszych zabezpieczeń.
  - Wybieraj aplikacje od renomowanych dostawców, którzy dbają o regularne aktualizacje i bezpieczeństwo.

## 7 Podszywanie się

- Atakujący mogą tworzyć fałszywe aplikacje lub strony internetowe, które wyglądają jak legalne aplikacje bankowe lub płatnicze, w celu wyłudzenia danych logowania.
- Jak unikać:
  - Zainstaluj aplikację mobilną bezpośrednio ze strony banku lub z oficjalnego sklepu z aplikacjami.
  - Sprawdź opinie i liczbę pobrań aplikacji przed jej zainstalowaniem.

Świadomość tych zagrożeń i stosowanie odpowiednich środków ostrożności pomoże zabezpieczyć Twoje transakcje bezgotówkowe realizowane przez aplikacje mobilne.

# Transakcje przez przelewy bankowe

Przelewy krajowe są powszechnie stosowane do transferów środków między kontami bankowymi, jednak mimo swojej popularności, wiążą się z różnymi zagrożeniami.

Zagrożenia związane z trzema typami przelewów: standardowymi, natychmiastowymi i wewnętrznymi, oraz sposoby, jak można się przed nimi chronić.

## 1 Przelewy Standardowe

- **Błędy w danych odbiorcy:**
  - W przypadku błędnego wprowadzenia danych odbiorcy (numer konta, kwota, tytuł przelewu), pieniądze mogą trafić na niewłaściwe konto. Odzyskanie środków może być trudne i czasochłonne.
  - Jak unikać:
    - Zawsze dokładnie sprawdzaj dane przed zatwierdzeniem przelewu.
    - Skorzystaj z funkcji zapisu danych odbiorcy w bankowości internetowej, aby uniknąć pomyłek przy kolejnych przelewach.
- **Opóźnienia w księgowaniu:**
  - Przelewy standardowe mogą być przetwarzane nawet przez jeden dzień roboczy, co może powodować opóźnienia, szczególnie gdy pilnie potrzebujesz, aby środki dotarły do odbiorcy.
  - Jak unikać:
    - Planuj przelewy z wyprzedzeniem, aby uniknąć problemów z opóźnieniami.
    - W sytuacjach wymagających szybkiej płatności rozważ skorzystanie z przelewu natychmiastowego.

- **Oszustwa i phishing:**
  - Przestępcy mogą wysyłać fałszywe faktury lub wiadomości, podszywając się pod znane firmy lub osoby, aby skłonić cię do wykonania przelewu na ich konto.
  - Jak unikać:
    - Zawsze sprawdzaj autentyczność wiadomości oraz dane odbiorcy przed dokonaniem przelewu.

Kontaktuj się bezpośrednio z firmą lub osobą, od której otrzymałeś prośbę o przelew, aby potwierdzić jej prawdziwość

## 2 Przelewy natychmiastowe

- **Nieodwracalność transakcji:**
  - Przelewy natychmiastowe są realizowane w czasie rzeczywistym, co oznacza, że po ich zatwierdzeniu nie można ich anulować. Jeśli przelew zostanie wysłany na błędne konto, odzyskanie środków może być bardzo trudne.
  - Jak unikać:
    - Sprawdź dokładnie wszystkie dane przed zatwierdzeniem przelewu, zwłaszcza numer konta odbiorcy.
    - Używaj przelewów natychmiastowych tylko wtedy, gdy masz pewność co do poprawności danych odbiorcy.

# Transakcje przez przelewy bankowe

- **Wyższe opłaty:**
  - Przelewy natychmiastowe często wiążą się z wyższymi opłatami niż standardowe przelewy, co może prowadzić do nieprzewidzianych kosztów, zwłaszcza przy częstym ich stosowaniu.
  - Jak unikać:
    - Przed dokonaniem przelewu natychmiastowego sprawdź, jakie opłaty wiążą się z tą usługą.
    - Używaj przelewów natychmiastowych tylko wtedy, gdy jest to konieczne.
- **Awaria systemu:**
  - W rzadkich przypadkach może dojść do awarii systemu realizującego przelewy natychmiastowe (np. Express Elixir lub BlueCash), co może opóźnić przetwarzanie transakcji.
  - Jak unikać:
    - Przed wykonaniem przelewu natychmiastowego sprawdź status serwisów bankowych.
    - W przypadku problemów skontaktuj się z bankiem, aby uzyskać informacje na temat statusu transakcji.

## 3 Przelewy wewnętrzne

- **Brak dodatkowych zabezpieczeń:**
  - Przelewy wewnętrzne, choć wygodne i szybkie, mogą być realizowane bez dodatkowych zabezpieczeń, takich jak dwuskładnikowe uwierzytelnianie (2FA), co zwiększa ryzyko nieautoryzowanych transakcji, jeśli ktoś uzyska dostęp do twojego konta.
  - Jak unikać:
    - Włącz dwuskładnikowe uwierzytelnianie na swoim koncie bankowym, jeśli jest dostępne.
    - Regularnie zmieniaj hasła i nie udostępniaj danych logowania nikomu.
- **Oszustwa wewnątrz banku:**
  - Jeśli ktoś uzyska dostęp do twojego konta bankowego, może łatwo dokonać przelewów wewnętrznych na inne rachunki w tym samym banku, co może być trudniejsze do wykrycia, ponieważ transakcje te często nie wymagają potwierdzeń SMS.
  - Jak unikać:
    - Monitoruj regularnie historię transakcji na koncie i ustaw powiadomienia o każdej zmianie salda.
    - Zgłaszaj wszelkie podejrzane transakcje do banku natychmiast po ich wykryciu.

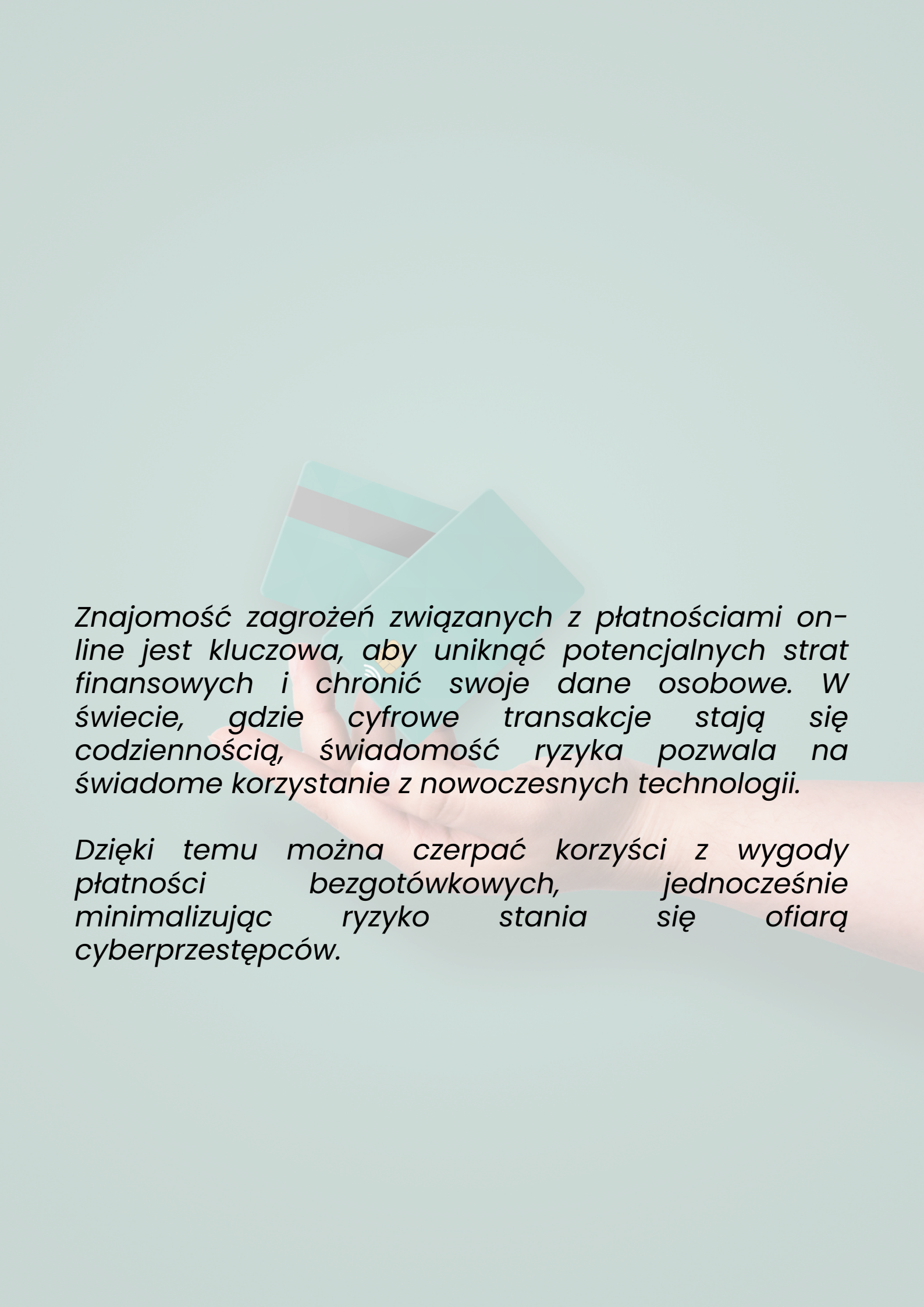
## Transakcje przez przelewy bankowe

- **Brak powiadomień o transakcjach:**
  - W przypadku przelewów wewnętrznych banki nie zawsze wysyłają powiadomienia SMS lub e-mail, co może utrudniać wykrycie nieautoryzowanych transakcji.
  - Jak unikać:
    - Ustaw alerty dotyczące wszystkich transakcji na swoim koncie, jeśli bank oferuje taką opcję.
    - Regularnie sprawdzaj stan konta i historię transakcji w bankowości internetowej lub mobilnej.

Zrozumienie tych zagrożeń i podejmowanie odpowiednich środków ostrożności pomoże zabezpieczyć twoje środki i uniknąć problemów związanych z przelewami krajowymi.

# Literatura


- www.fingerprints.digital/strefa-eksperta/zagrozenia-zwiazane-z-platnosciami-karta-w-sieci/
- www.keepersecurity.com/blog/pl/2023/09/27/how-to-avoid-credit-card-fraud-online/
- www.legionowo.pl/a/jak-zadbac-o-bezpieczenstwo-platnosci-bezgotowkowych
- www.keepersecurity.com/blog/pl/2023/10/27/debit-card-vs-credit-card-which-is-more-secure-online/
- www.pluxee.pl/blog/karta-przedplacona-czym-jest-jak-dziala-i-gdzie-ja-kupic/



*Znajomość zagrożeń związanych z płatnościami online jest kluczowa, aby uniknąć potencjalnych strat finansowych i chronić swoje dane osobowe. W świecie, gdzie cyfrowe transakcje stają się codziennością, świadomość ryzyka pozwala na świadome korzystanie z nowoczesnych technologii.*

*Dzięki temu można czerpać korzyści z wygody płatności bezgotówkowych, jednocześnie minimalizując ryzyko stania się ofiarą cyberprzestępców.*