Dlaczego cyberbezpieczeństwo w płatnościach jest ważne

VISA

Dlaczego cyberbezpieczeństwo w płatnościach jest ważne

Płatności cyfrowe dokonywane za pomocą kart płatniczych, portfeli mobilnych, czy bankowości internetowej są wygodne, szybkie i bezpieczne, a Polacy chętnie z nich korzystają. Jednocześnie, oszuści ciągle szukają nowych narzędzi i metod, by przechytrzyć konsumentów, np. poprzez kradzież tożsamości czy przejęcia kont. Cyberprzestępcy atakują także poprzez phishing, złośliwe oprogramowania, wykorzystując socjotechnikę oraz bazują na wyciekach danych. Aby chronić przed nimi swoje płatności cyfrowe i zminimalizować ryzyko, warto zwiększać swoją świadomość o zagrożeniach, wdrożyć kilka mądrych nawyków i znać kolejne kroki, które możemy podjąć w przypadku podejrzenia oszustwa.

Najczęstsze rodzaje zagrożeń

W dzisiejszym krajobrazie płatności zagrożenia stale ewoluują, a hakerzy wykorzystują różne kanały dotarcia do konsumentów. Wśród tych najczęściej występujących są:

1. **Phishing i socjotechnika –** fałszywe e-maile, SMS-y lub telefony, które nakłaniają użytkowników do ujawnienia danych płatniczych.
2. **Skimming kart i ataki na terminale** – fizyczne urządzenia przechwytują dane kart w bankomatach lub terminalach płatniczych.
3. **Złośliwe oprogramowanie i kradzież danych** – oprogramowanie tego typu przechwytuje dane do logowania i informacje finansowe.
4. **Przejęcie konta (*ang. Account Take Over.- ATO*)** – hakerzy uzyskują kontrolę nad kontami w bankowości internetowej lub aplikacjach płatniczych.
5. **Wycieki danych** – dochodzi do ujawnienia danych kart płatniczych lub kont posiadanych u sprzedawców lub dostawców usług.
6. **Ryzyko związane z wykorzystaniem publicznego Wi-Fi** – ataki polegające na przejęciu przez cyberprzestępców danych przesyłanych między dwoma podmiotami lub osobami podczas używania niezabezpieczonych sieci.
7. **Oszustwo SIM swap** – atakujący przejmują numer telefonu, aby przechwycić kody weryfikacyjne.

Środki bezpieczeństwa, które możesz wdrożyć

Dzisiejsze metody oszustów są zróżnicowane. Dlatego, aby skutecznie chronić się przed ich działaniem w świecie płatności:

Zabezpiecz urządzenia osobiste

- Używaj silnych, unikalnych haseł dla urządzeń i kont; włącz uwierzytelnianie wieloskładnikowe (MFA) wszędzie tam, gdzie to możliwe.
- Aktualizuj systemy operacyjne, przeglądarki i aplikacje, instalując poprawki związane z bezpieczeństwem.
- Zainstaluj renomowane oprogramowanie antywirusowe lub przeciwko złośliwemu oprogramowaniu.

Chroń płatności

- Korzystaj z wirtualnych numerów kart lub tokenizowanych metod płatności, aby ograniczyć ujawnianie rzeczywistych danych karty.
- Unikaj publicznych sieci Wi-Fi do transakcji finansowych; jeśli musisz, używaj VPN.
- Podczas zakupów online sprawdź, czy w pasku adresu przeglądarki widnieje szyfrowanie HTTPS.

Monitoruj konta

- Skonfiguruj alerty transakcyjne w banku lub u wystawcy karty, aby otrzymywać powiadomienia w czasie rzeczywistym.
- Regularnie sprawdzaj wyciągi bankowe, by ewentualnie zidentyfikować nieautoryzowane transakcje.
- Zgłaszaj podejrzane działania od razu – szybkie zgłoszenie może zmniejszyć jego potencjalne skutki.

Broń się przed phisingiem

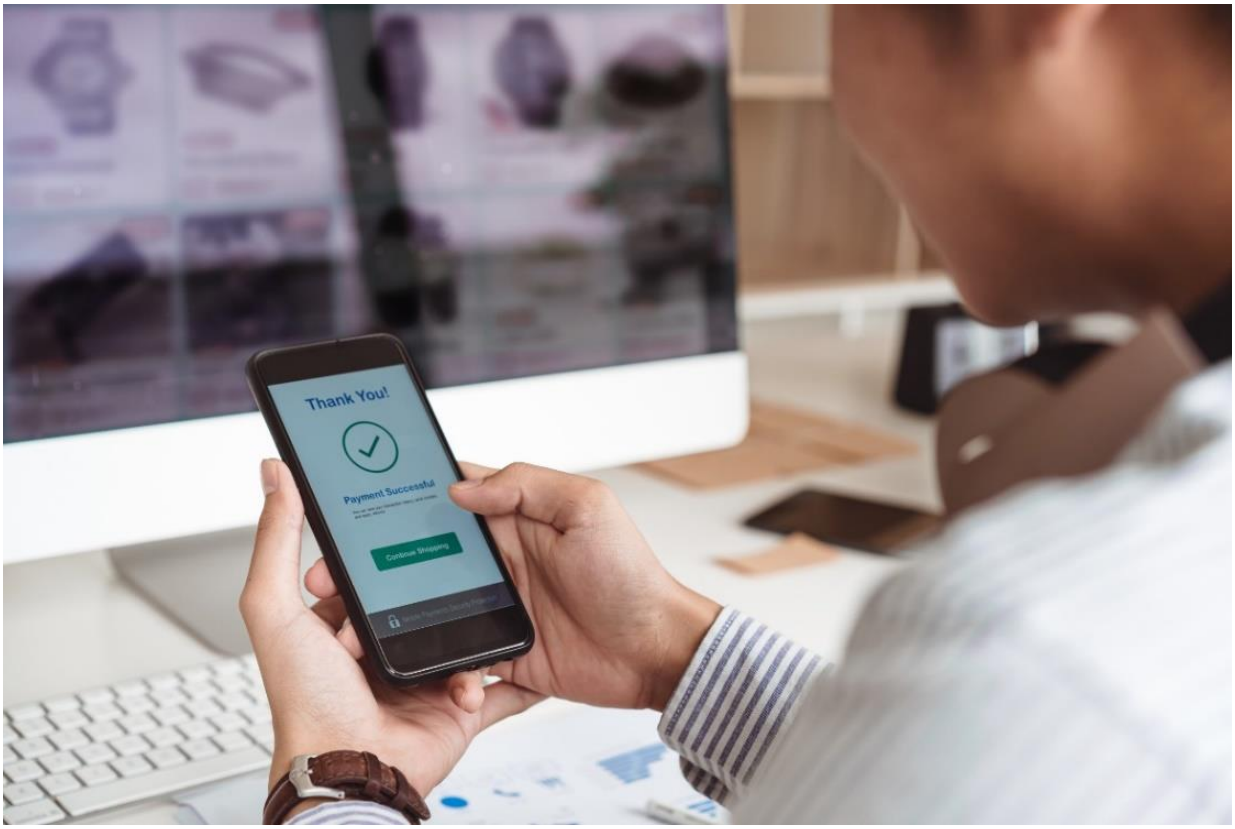
- Sprawdzaj adresy e-mail nadawców i adresy URL przed kliknięciem w link.
- Nie podawaj danych płatniczych przez e-mail lub SMS, chyba, że to zweryfikowany odbiorca lub inicjacja kontaktu wyszła od Ciebie.
- Używaj filtrów spamu i funkcji bezpieczeństwa oferowanych przez usługi mailowe.
- Jeśli coś brzmi zbyt dobrze, by było prawdziwe – prawdopodobnie tak jest.

Zadbaj o bezpieczeństwo fizyczne

- Zasłaniaj PIN podczas wpisywania go w bankomatach lub terminalach płatniczych.
- Korzystaj z bankomatów znajdujących się w oddziałach banków, a nie z wolnostojących urządzeń.
- Chroń portfele i karty; rozważ użycie etui blokujących RFID.
- Unikaj odczytywania na głos numeru karty w miejscach, gdzie inni mogą to usłyszeć.

Wdrożenie powyższych działań może przynieść Ci szereg korzyści, w tym:

1. Zapobiec nieautoryzowanemu dostępowi do urządzenia lub aplikacji.
2. Ochronić poufne dane w Internecie i podczas ich przesyłania.
3. Pomóc we wczesnym wykryciu oszustwa.
4. Udaremnić kradzież danych uwierzytelniających.
5. Zapobiec kopiowaniu danych z karty płatniczej (skimmingowi).



Co zrobić, gdy mogło dojść lub doszło do oszustwa

Oszustwa lub przejęcia kont należy niezwłocznie zgłaszać zarówno do instytucji finansowej, jak i odpowiednich organów krajowych. Poniżej znajdziesz informacje o najważniejszych podmiotach, kanałach i kontekstach, w jakich warto się do nich zwrócić:

1. **Bank lub dostawca płatności**

   Punkt kontaktu: infolinia bankowa lub oddział.

   Cel: zatrzymanie dokonywania transakcji, zabezpieczenie konta .

2. **Policja**

   Punkt kontaktu: 112 (numer alarmowy), 997 (bezpośredni).

   Cel: oficjalne zgłoszenie oszustwa, rozpoczęcie dochodzenia .

3. **Urząd Ochrony Konkurencji i Konsumentów (UOKiK)**

   Punkt kontaktu: https://uokik.gov.pl

   Cel: Wsparcie w zakresie praw konsumentów.

4. **Biuro Informacji Kredytowej (BIK)**

   Punkt kontaktu: https://www.bik.pl

   Cel: Zabezpieczenie aktywności kredytowej.

5. **Ministerstwo Cyfryzacji**
   Punkt kontaktu: https://cyber.gov.pl/
   Cel: informacje dotyczące cyberbezpieczeństwa przeznaczone dla obywateli, przedsiębiorców i podmiotów Krajowego Systemu Cyberbezpieczeństwa.

Oto zalecana procedura zgłaszania oszustw i kroki, które warto podjąć:

Skontaktuj się ze swoim bankiem lub dostawcą usług płatniczych

Natychmiast powiadom swój bank lub dostawcę usług płatniczych (za pośrednictwem oficjalnej infolinii lub bezpiecznego portalu internetowego). Polskie banki zazwyczaj posiadają infolinie ds. oszustw dostępne przez całą dobę – sprawdź informacje na odwrocie karty lub stronie internetowej banku. Wówczas poproś o:

- Zablokowanie lub zamrożenie zagrożonego konta/karty.
- Cofnięcie nieautoryzowanych transakcji, jeśli to możliwe.
- Wydanie nowych danych uwierzytelniających lub kart.

Zgłoś sprawę na policję

Udaj się na lokalny posterunek policji lub zadzwoń pod numer alarmowy 112 (jeśli zagrożenie jest pilne).

W przypadku oszustw, które nie wymagają natychmiastowej interwencji, możesz również zadzwonić pod numer 997 (bezpośrednia linia policji).

W takiej sytuacji, przedstaw dokumentację: zapisy transakcji, zrzuty ekranu, korespondencję.

Policja nada Twojej sprawie numer protokołu, który może być potrzebny do zgłoszenia roszczenia ubezpieczeniowego lub bankowego.

Zadbaj o zebranie dowodów i zmianę haseł

W ciągu kilku godzin od wykrycia oszustwa należy podjąć odpowiednie działania. W Polsce odpowiedzialność za nieautoryzowane transakcje może zostać zmniejszona, jeśli zostaną one niezwłocznie zgłoszone.

Pamiętaj wtedy, aby zachować wszystkie dowody (e-maile, wiadomości SMS, rejestry połączeń).

Zmień wszystkie powiązane hasła i włącz uwierzytelnianie wieloskładnikowe dla kont o znaczeniu krytycznym.

Powiadom Urząd Ochrony Konkurencji i Konsumentów (UOKiK)

Urząd Ochrony Konkurencji i Konsumentów może pomóc w sprawach dotyczących praw konsumentów związanych z oszustwami finansowymi.

- Strona internetowa Urzędu: https://uokik.gov.pl
- Urząd może udzielić Ci wskazówek dotyczących odzyskania środków lub dochodzenia roszczeń wobec usługodawców.

A

Chroń swoją tożsamość i aktywność kredytową

Zgłoś alert kredytowy lub zablokuj dostęp do danych w głównym Biurze Informacji Kredytowej (BIK).

- Strona internetowa Biura: https://www.bik.pl
- Zapobiega to zaciąganiu nowych kredytów lub otwieraniu rachunków kredytowych w Twoim imieniu bez wcześniejszej weryfikacji.

Zgłoś sprawę przez platformę Cyber.gov.pl

Cyber.gov.pl to:

- nowoczesna platforma przygotowana przez Ministerstwo Cyfryzacji i NASK z myślą o ochronie cyfrowej obywateli, firm oraz instytucji publicznych;
- wiarygodne źródło wsparcia dla obywateli w podnoszeniu poziomu cyberbezpieczeństwa;
- integracja w jednym miejscu kluczowych usług do zgłaszania incydentów, udostępniania informacji o zagrożeniach oraz dostęp do narzędzi takich jak S46, moje.cert.pl czy bezpiecznedane.gov.pl.

Najczęściej zadawane pytania (FAQ)

1. Co to jest uwierzytelnianie wieloskładnikowe (MFA)?

Wyobraź sobie swoje konto online jako dom. Hasło to klucz do jego drzwi wejściowych. Przez długi czas to wystarczało. Ale co, jeśli ktoś ukradnie lub skopiuje Twój klucz? Właśnie tutaj wchodzi MFA, czyli uwierzytelnianie wieloskładnikowe. To jak dodanie drugiego zamka, np. zasuwy lub łańcucha zabezpieczającego, do drzwi wejściowych.

MFA to środek bezpieczeństwa, który wymaga podania dwóch lub więcej elementów – tzw. „czynników" – aby potwierdzić, że jesteś tym, za kogo się podajesz podczas logowania do konta. Takie warstwowe podejście znacznie utrudnia nieautoryzowanym osobom uzyskanie dostępu, nawet jeśli uda im się ukraść Twoje hasło.

MFA działa poprzez połączenie co najmniej dwóch z poniższych typów identyfikacji:

- Coś, co wiesz: zazwyczaj jest to hasło lub PIN.
- Coś, co masz: fizyczny przedmiot w Twoim posiadaniu, np. smartfon, klucz sprzętowy lub karta bankowa.
- Coś, czym jesteś: chodzi tu o biometrię, czyli unikalne cechy fizyczne, takie jak odcisk palca, rozpoznawanie twarzy czy głos.

2. Jak stworzyć silne hasło?

Silne hasło to kombinacja kilku elementów, które sprawiają, że jest trudne do odgadnięcia zarówno przez ludzi, jak i komputery.

- **Długość to Twój sprzymierzeniec:** im dłuższe hasło, tym większe bezpieczeństwo. Celuj w minimum 12 znaków, a najlepiej 14 lub więcej (jeśli to możliwe). Każdy dodatkowy znak zwiększa trudność złamania hasła wykładniczo.
- **Różnorodność znaków**: używaj kombinacji wielkich i małych liter, cyfr oraz symboli (np. !, @, #, $). Im większa różnorodność, tym trudniej je złamać.
- **Unikalność:** nigdy nie używaj tego samego hasła na różnych stronach. Jeśli jedno zostanie przejęte, hakerzy spróbują użyć go w innych popularnych serwisach (np. e-mail, bank). To częsty atak zwany „credential stuffing".
  Wskazówka: Używaj menedżera haseł do generowania i przechowywania silnych, unikalnych haseł.

Czego unikać:

- **Danych osobowych:** nie używaj imion, dat urodzenia, imion dzieci, zwierząt ani informacji łatwych do znalezienia w mediach społecznościowych.
- **Popularnych słów i wzorców:** unikaj pojedynczych słów z dodaną cyfrą (np. „hasło123") oraz prostych sekwencji klawiaturowych („qwerty", „123456").
- **Sekwencji liter lub cyfr:** hasła typu „abcdefg" czy „987654" są jednymi z pierwszych, których hakerzy spróbują użyć.

Siła haseł

Zapamiętanie złożonych, losowych ciągów znaków może być trudne. Bardziej praktyczną i równie bezpieczną metodą jest utworzenie „hasłowej frazy".

Fraza hasłowa to sekwencja kilku niepowiązanych ze sobą słów połączonych w ciąg np. „PrawidłowyKońBateriaZszywka". Takie rozwiązanie jest przykładem silnego, łatwego do zapamiętania hasła, a jednocześnie jest długie i niezwykle trudne do odgadnięcia przez komputery.

Aby hasło było jeszcze silniejsze, można zwiększyć jego złożoność, pisząc niektóre litery wielkimi literami, dodając cyfry lub zastępując litery symbolami (np. „Praw!dłowyK0ńB@teri@Zszywka). Jeśli strona internetowa na to pozwala, można nawet używać spacji między słowami.

3. Czym są płatności tokenizowane?

Płatności tokenizowane zastępują rzeczywisty numer karty unikalnym, jednorazowym „tokenem" podczas transakcji. Oznacza to, że sprzedawcy nigdy nie widzą ani nie przechowują rzeczywistych danych karty.

Przykład: podczas korzystania z portfeli cyfrowych informacje dotyczące płatności są przekształcane w bezpieczny token. Nawet jeśli haker przechwyci ten token, nie będzie on przydatny do przyszłych transakcji.

Dlaczego ma to znaczenie? Tokenizacja znacznie zmniejsza ryzyko oszustwa w przypadku włamania do sklepu internetowego lub przechwycenia danych płatniczych.

4. Na co należy zwrócić uwagę w witrynie HTTPS?

HTTPS oznacza, że połączenie z witryną jest szyfrowane, co chroni poufne dane, takie jak numery kart i hasła.

Jak to sprawdzić? Poszukaj ikony kłódki w pasku adresu przeglądarki i upewnij się, że adres URL zaczyna się od https:// (a nie http://).

Dlaczego ma to znaczenie? Bez szyfrowania cyberprzestępcy mogą potencjalnie „podsłuchiwać” Twoją aktywność online i wykraść Twoje dane.

5. Czym jest VPN i dlaczego warto z niego korzystać?

Wirtualna sieć prywatna (VPN) szyfruje połączenie internetowe i ukrywa adres IP, utrudniając hakerom lub podmiotom śledzącym dostęp do informacji o Twojej aktywności online.

Przykład: Jeśli musisz dokonywać płatności podczas podróży lub korzystając z publicznej sieci Wi-Fi, użycie zaufanej sieci VPN zapewni bezpieczeństwo Twoich danych.

Dlaczego ma to znaczenie? Zaufane sieci VPN chronią poufne transakcje przed przechwyceniem w niezabezpieczonych sieciach.

6. Czy publiczne sieci Wi-Fi są bezpieczne do dokonywania płatności?

Publiczne sieci Wi-Fi (np. w kawiarniach, na lotniskach lub w hotelach) są często niezabezpieczone, co oznacza, że każdy w pobliżu może potencjalnie przechwycić Twoje dane.

Bezpieczna praktyka: unikaj dokonywania płatności lub logowania się na poufne konta w publicznych sieciach Wi-Fi, chyba że korzystasz z sieci VPN.

Dlaczego ma to znaczenie: Hakerzy mogą wykorzystać ataki typu „man-in-the-middle” do kradzieży danych płatniczych podczas ich przesyłania.

7. Czym jest skimming kart i jak można go uniknąć?

Skimming kart ma miejsce, gdy urządzenie podłączone do bankomatu lub terminala płatniczego potajemnie kopiuje dane z paska magnetycznego karty.

Jak się chronić:

- Przed skorzystaniem z bankomatu sprawdź, czy w szczelinie na kartę nie ma żadnych luźnych lub nietypowych elementów.
- Zasłaniaj dłonią miejsce wprowadzania kodu PIN.
- Korzystaj z bankomatów w dobrze oświetlonych, bezpiecznych miejscach (najlepiej wewnątrz banku).

Dlaczego ma to znaczenie: Tzw. „skimmerzy”, czyli oszuści, którzy wykorzystują tę metodę mogą skopiować Twoją kartę i ukraść środki bezpośrednio z Twojego konta.