

ZŁOTE SZKOŁY



NARODOWY
BANK POLSKI

V edycja programu NBP
**CYBERBEZPIECZNE
FINANSE**

SPIS TREŚCI

1. PŁATNOŚCI MOBILNE
2. BANKOWOŚĆ INTERNETOWA
3. PŁATNOŚCI ONLINE
4. PIENIĄDZ ELEKTRONICZNY
5. CYBERZAGROŻENIA
6. FAŁSZYWE WIADOMOŚCI
7. OCHRONA DANYCH
8. PUSTYNIE BANKOMATOWE
9. KONSEKWENCJE PUSTYŃ
BANKOMATOWYCH

PŁATNOŚCI MOBILNE

To płatności bezgotówkowe dokonywane za pomocą urządzenia mobilnego. Dokonywane są za pomocą aplikacji bankowej lub aplikacji spełniającej funkcję portfela elektronicznego, z którą użytkownik może powiązać kartę płatniczą

ZBLIŻENIOWE

Wykorzystujące technologie NFC i stosowane w terminalach płatniczych POS, niektórych bankomatach, parkomatach, maszynach vendingowych, czy innych zautomatyzowanych punktach sprzedaży.

ZDALNE

Wykorzystujące połączenie internetowe i stosowane przy zakupach w sklepach internetowych, w płatnościach pomiędzy użytkownikami, a także do płatności za inne produkty i usługi, tj opłaty parkingowe, bilety.

BEZPIECZNE KORZYSTANIE Z BANKOWOŚCI INTERNETOWEJ

PODSTAWOWE ZASADY:

1. Silne hasła.
2. Dwustopniowa autentykacja.
3. Bezpieczne połączenie (HTTPS).
4. Ostrożność przy korzystaniu z publicznych sieci Wi-Fi.
5. Regularne aktualizowanie oprogramowania i aplikacji.

PŁATNOŚCI ONLINE

To proces dokonywania transakcji finansowych przez Internet.

Oto kluczowe informacje:

1. Metody płatności:

- karty kredytowe/debetowe - najczęściej używane do zakupów online;
- portfele elektroniczne - usługi umożliwiające szybkie płatności;
- przelewy bankowe - bezpośrednie przelewy między kontami bankowymi.

2. Bezpieczeństwo:

- używaj secure connections (https) podczas dokonywania płatności;
- zawsze sprawdzaj recenzje sprzedawców;
- stosuj silne hasła i dwuskładnikowe uwierzytelnienia.

PIENIĄDZ ELEKTRONICZNY

Pieniądz elektroniczny to wartość pieniężna przechowywana elektronicznie, w tym magnetycznie, wydawaną, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowana przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego.

FinTech (Finicial Technology), czyli technologie finansowe. To sektor łączący innowacje technologiczne z usługami finansowymi, aby ułatwić i poprawić sposób, w jaki zarządzamy pieniędzmi. Może obejmować mobilne aplikacje do płatności, platformy do inwestycji, usługi pożyczkowe online i wiele innych.

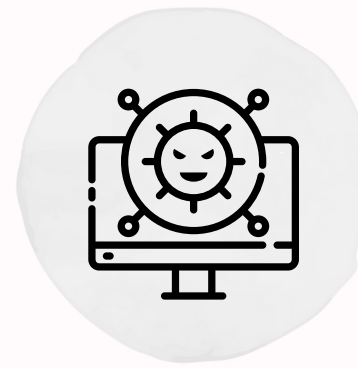
CZYM SĄ CYBERZAGROŻENIA?

To wszelkie niebezpieczeństwa związane z nieautoryzowanym dostępem do systemów komputerowych lub sieci, które mogą prowadzić do utraty, kradzieży lub uszkodzenia danych.



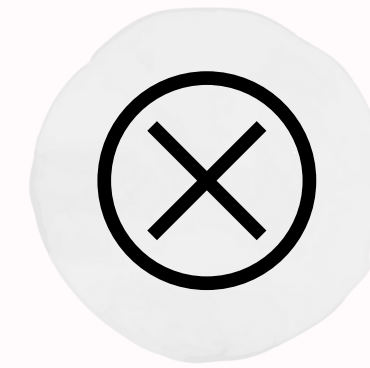
PHISHING

Oszuści mogą wysyłać fałszywe e-maile lub wiadomości, aby wyłudzić dane logowania do Twojego konta.



MALWARE

Złośliwe oprogramowanie, które może zainfekować Twój komputer i wykraść dane kart płatniczych.



RANSOMWARE

Złośliwe oprogramowanie, które blokuje dostęp do danych osobistych lub systemów firmy, żądając okupu za ich odblokowanie.



HAKERSTWO

Odnosi się do nielegalnych działań hakerów mających na celu uzyskanie dostępu do systemów finansowych lub danych osobowych w celu kradzieży pieniędzy lub informacji.



KRZADZIEŻ DANYCH

Nielegalne pozyskiwanie poufnych informacji, które mogą być używane do oszustw lub wyłudzeń. Hakerzy mogą kraść numery kart kredytowych, dane osobowe, loginy do banków czy informacje o transakcjach.

Temat: Pilne: Potwierdzenie płatności w Twoim koncie bankowym.

Szanowny Kliencie,

Zauważyliśmy podejrzaną aktywność na Twoim koncie bankowym. Została złożona płatność w wysokości 1000 PLN z Twojego konta, która może być nieautoryzowana.

Aby chronić Twoje środki i zwrócić pełną kontrolę nad kontem, prosimy o natychmiastowe potwierdzenie twojej tożsamości. Kliknij poniższy link, aby zalogować się do swojego konta i zakończyć weryfikację.

[Potwierdź swoje dane](#)

Pamiętaj, że jeśli nie zweryfikujesz swojej tożsamości w ciągu 24 godzin, Twoje konto zostanie zablokowane, a dostęp do środków zostanie zawieszony.

Dziękujemy za współpracę i przepraszamy za wszelkie niedogodności.

Z poważaniem,
Zespół Bezpieczeństwa Banku
Bank XYZ

DLACZEGO TO OSZUSTWO?

1. Podstawowy błąd językowy.
2. Link w wiadomości.
3. Pilność i presja czasu.
4. Brak personalizacji.

Wskazówka:

Zawsze weryfikuj takie wiadomości, kontaktując się bezpośrednio z bankiem lub instytucją finansową, używając numeru telefonu lub adresu e-mail, które znajdziesz na oficjalnej stronie. Nigdy nie klikaj w podejrzanе linki ani nie podawaj danych osobowych w odpowiedzi na takie wiadomości.

SMS:

Uwaga! Twoja subskrypcja „*Premium Video*” została odnowiona na kwotę 299,99 PLN. Jeśli nie autoryzowałeś tej transakcji, kliknij tutaj, aby anulować płatność i uzyskać pełny zwrot: [link]. Jeśli nie dokonasz płatności w ciągu 24 godzin, Twoje konto zostanie zablokowane. Pozdrawiamy, Zespół Obsługi Klienta.

DLACZEGO TO OSZUSTWO?

1. Niezamówiona subskrypcja.
2. Link do nieznanej strony.
3. Presja czasu.
4. Brak personalizacji.

Wskazówka:

Zamiast klikać w link, najpierw sprawdź historię swoich subskrypcji bezpośrednio w aplikacji lub na stronie danej usługi, a jeśli masz jakiegokolwiek wątpliwości, skontaktuj się z firmą za pomocą oficjalnych kanałów komunikacji.

Szanowny Kliencie,

Dziękujemy za zainteresowanie naszymi produktami!

Mamy dla Ciebie wyjątkową ofertę: 50% rabatu na wszystkie produkty w naszym sklepie internetowym.

Aby skorzystać z tej ekskluzywnej promocji, wystarczy, że klikniesz poniższy link, aby sfinalizować swoje zamówienie i podać dane swojej karty kredytowej, abyśmy mogli zakończyć transakcję:

Zrealizuj rabat teraz!

Oferta jest ważna tylko przez 24 godziny, dlatego nie zwlekaj i wykorzystaj tę wyjątkową okazję, zanim zniknie!

Pamiętaj, że rabat będzie automatycznie naliczony przy składaniu zamówienia, ale tylko jeśli podasz dane swojej karty kredytowej w formularzu.

Z pozdrowieniami,
Zespół Obsługi Klienta
Sklep XYZ

DLACZEGO TO OSZUSTWO?

1. Prośba o dane karty kredytowej.
2. Nieznany link.
3. Nagła promocja i presja czasu.
4. Brak personalizacji.

OCHRONA SWOICH DANYCH

Pamiętaj, aby zawsze chronić swoje dane:

1. Weryfikując ustawienia prywatności w profilach mediów społecznościowych.
2. Rozpoznając sposoby wpływu i manipulacji w przestrzeni internetowej.
3. Kontrolując strach i pośpiech.

Zawsze sytuacje naruszające bezpieczeństwo w sieci należy zgłaszać do Cert Polska:

1 na numer 8080

2 incydent.cert.pl

PUSTYNIE BANKOMATOWE

Badania prowadzone przez ekspertów NBP wykazały, że aż 12% polskich gmin boryka się z problemem braku bankomatu. Zwracając uwagę na liczbę osób zamieszkujących ten obszar, jest to duży problem. Jak się okazuje, jeszcze większym problemem na tych obszarach jest utrudniony dostęp do Internetu, co wiąże się z kłopotem płatności bezgotówkowych.

Z podobnym problemem zmagają się niektóre regiony Francji, Hiszpanii czy Wielkiej Brytanii co było powodem do monitorowania zasobów gotówki. Europejski Bank Centralny podkreśla, że banknoty to część naszej tożsamości, naszej gospodarki i naszej kultury., a EBC odpowiedzialny jest za zaufanie ludzi.

Wszystkie znaki pieniężne emitowane przez NBP to prawne środki płatnicze na obszarze Rzeczypospolitej Polskiej. W związku z tym wszystkie znaki pieniężne wprowadzane do obiegu odpowiednim zarządzeniem emisyjnym Prezesa NBP powinny być akceptowane jako forma rozliczenia za sprzedany towar lub świadczoną usługę.

KONSEKWENCJE PUSTYŃ BANKOMATOWYCH

Jakie są konsekwencje pustyń bankomatowych?

- Trudniejszy dostęp do gotówki;
- Problemy dla osób starszych;
- Ograniczenie rozwoju lokalnego biznesu;
- Wzrost przestępczości;
- Zwiększenie czasu transakcji;
- Ograniczenie możliwości płatności.



DZIĘKUJĘ ZA UWAGĘ!

