

Przestrzegamy przed fałszywymi telefonami od przestępców, którzy podszywają się pod pracowników zaufanych instytucji, w tym banków, by wyłudzić wrażliwe dane potencjalnych ofiar.

To tzw. vishing!

“Legenda”, czyli fałszywa informacja oszustów, może dotyczyć rzekomego sprawdzenia transakcji w bankowości internetowej czy weryfikacji wniosku kredytowego. Przestępcy pod pretekstem weryfikacji podejrzanej transakcji, namawiają często potencjalne ofiary do instalacji aplikacji, np. Any Desk czy TeamViewer. Dzięki niej mogą przejąć kontrolę nad urządzeniem, z którego korzystasz.

Oszuści często wykorzystują techniki tzw. **spoofingu**, czyli podmiany numeru telefonu w taki sposób, by na Waszym urządzeniu wyświetlił się numer infolinii Banku lub zaufanego pracownika Banku!

Zachowaj ostrożność podczas takiej rozmowy!

UWAŻAJ
NA FAŁSZYWE TELEFONY



Jak się chronić przed takimi oszustwami?

- Pamiętaj, że pracownicy Banku podczas rozmowy telefonicznej nigdy nie poproszą o instalację dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do bankowości internetowej i mobilnej, a także podanie haseł dostępu, kodów PIN/SMS lub innych danych, które pozwalają na dokonanie transakcji.
- Pracownicy naszego Banku nigdy nie zadzwonią do Ciebie z numeru Infolinii SGB 800 888 888. Z tego numeru korzystamy tylko, aby odbierać połączenia.
- Nigdy nie podawaj przez telefon nadmiarowych informacji oraz szczegółów swoich transakcji, w tym również informacji, w jakim banku posiadasz konto!
- Jeśli masz jakiegokolwiek wątpliwości, zakończ połączenie i skontaktuj się osobiście z placówką Banku lub Infolinią SGB. Tylko samodzielnie kontaktując się z Bankiem na numer widoczny na jego stronie www, podawaj informacje, niezbędne do weryfikacji tożsamości Klienta. Pamiętaj- przy podejrzanym kontakcie, samodzielnie wybieraj numer telefonu Banku, nie oddzwaniaj!

UWAŻAJ
NA FAŁSZYWE TELEFONY



Więcej: www.esbank.pl ➔ Bank ➔ **BEZPIECZEŃSTWO**

Przestrzegamy przed oszustwami, które polegają najczęściej na wyłudzeniu kodu płatności. Wynikają one z braku uwagi oraz ostrożności użytkowników, bo sam BLIK jest bezpieczny.

Jak może wyglądać oszustwo z użyciem kodu BLIK?

- Oszuści włamują się na konta w social mediach, następnie kontaktują się ze znajomymi lub z członkami rodziny osoby, której wykradły dostęp. Proszą wówczas ofiary o pilną pożyczkę i namawia do przesłania wygenerowanego kodu BLIK.
- Przestępcy podszywają się pod instytucje finansowe jak banki i wysyłają fałszywe wiadomości SMS, np. z prośbą o potwierdzenie transakcji lub informacją o próbie zaciągnięcia zobowiązania na rachunek ofiary. Nieświadomy użytkownik podaje przestępcy kod BLIK, czym umożliwia mu nieautoryzowaną transakcję.
- Podczas zakupów online przestępca podszywa się pod potencjalnego klienta bądź sprzedawcę na platformie sprzedażowej. Prosi o płatność za pośrednictwem BLIKA, a ofiara nie weryfikuje dokładnie transakcji, tylko od razu podaje lub wpisuje kod i tym sposobem traci pieniądze, nie dostając towaru.

UWAŻAJ
NA FAŁSZYWE PROŚBY
O KOD BLIK



Jak się chronić przed takimi oszustwami?

- Nie podawaj szczegółowych danych przez telefon, szczególnie w przypadku rzekomych próśb ze strony banku. Sprawdzaj autentyczność rozmówcy – po prostu zadzwoń bezpośrednio do banku.
- W przypadku próśby o kod BLIK od znajomego na komunikatorze, zawsze warto potwierdzić jego tożsamość – przez bezpośredni kontakt.
- Przed potwierdzeniem przelewu BLIK, dwukrotnie sprawdzaj kwotę i odbiorcę.
- Unikaj klikania w linki od nieznanymi numerów czy osób na platformach społecznościowych, bo mogą one prowadzić do fałszywych stron, które wyłudzą dane. Warto też regularnie sprawdzać adres strony internetowej banku przed zalogowaniem się do bankowości.
- Dodatkowym zabezpieczeniem przed przejęciem kont społecznościowych jest dwuskładnikowe uwierzytelnienie (2FA) przy logowaniu, które utrudnia dostęp nieuprawnionym osobom. Dzięki temu możesz zwiększyć swoją ochronę przed oszustwami BLIK na komunikatorach.

UWAŻAJ
NA FAŁSZYWE PROŚBY
O KOD BLIK



Przestrzegamy przed aktywnością oszustów, którzy za pośrednictwem popularnych serwisów sprzedażowych wyłudniają dane i pieniądze od osób sprzedających różne produkty online.

Na czym polega takie oszustwo?

Sprzedajesz coś przez OLX, Vinted, Allegro lub Marketplace? Wystawiasz ogłoszenie o sprzedaży, a kupujący kontaktuje się z Tobą za pomocą komunikatora (np. WhatsApp) i chce kupić przedmiot? Później możesz dostać od oszusta link na WhatsAppie do rzekomego odbioru pieniędzy. Fałszywa instrukcja wraz z linkiem może przyjść na Twój adres e-mail.

Uważaj! To oszustwo. Link prowadzi do fałszywej strony, na której masz ujawnić swoje dane do logowania lub dane karty płatniczej. Taka strona zwykle łudząco przypomina stronę logowania do banku. Jeśli ujawnisz na niej swój login, hasło oraz kod SMS – te dane trafią bezpośrednio do oszusta.

UWAŻAJ
NA FAŁSZYWE WIADOMOŚCI,
GDY SPRZEDAJESZ COŚ ONLINE



Pamiętaj!

- Zawsze czytaj dokładnie SMS-y od Banku. Zwracaj uwagę na to, co autoryzujesz. Jeśli w treści SMS-a masz informację, że aktywujesz aplikację bankową – a tego nie zlecasz – to właściwie pewne, że na Twoim koncie bankowym jest zalogowany oszust.
- Nie otwieraj linków, które rzekomo mają pozwolić na odbiór pieniędzy za wystawiony przez Ciebie przedmiot.
- Nawet, gdy klikniesz w taki link, nie podawaj nigdy swoich danych logowania do bankowości internetowej oraz informacji z kart płatniczych. Nie podawaj też kodów z wiadomości SMS od banku!
- Zwracaj uwagę na błędy językowe – mogą wskazywać, że masz do czynienia z oszustwem.
- Rozliczaj i komunikuj się bezpośrednio przez dany portal.
- Uważaj na próby nawiązania kontaktu poza portalem czy aplikacją, np. WhatsApp, e-mail.
- Jeśli Twoja intuicja podpowiada Ci, że przedstawiona okazja jest podejrzana – wycofaj się z niej.

UWAŻAJ

**NA FAŁSZYWE WIADOMOŚCI,
GDY SPRZEDAJESZ COŚ ONLINE**



WAŻNE!

Jeśli jakiś kontakt budzi Twoje wątpliwości lub podejrzewasz, że Cię oszukano, przerwij transakcję i skontaktuj się z naszą **Infolinią SGB 24/7**:

- **800 88 88 88** (bezpłatne krajowe, połączenie)
- **61 647 28 46** (z zagranicy; opłata zgodna z taryfą operatora).

O oszustwie poinformuj organy ścigania.

Bądź na bieżąco z naszymi komunikatami bezpieczeństwa oraz zasadami bezpiecznego bankowania, które znajdziesz na naszej stronie www.esbank.pl w zakładce "**Bezpieczeństwo**".

