Przestępstwa inwestycyjne w dwóch odsłonach
– Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP,
Centralnego Biura Zwalczania Cyberprzestępczości oraz Komendy Głównej Policji
z dnia 26 marca 2024 r.

Informujemy, że pomimo nieustannej edukacji i działań ostrzegawczych podejmowanych przez sektor finansowy nadal obserwujemy ataki oszustów tzw. DORADCÓW INWESTYCYJNYCH na klientów.

Ostrzegamy, oszuści nie ustępują i kontaktują się z osobami, które przy pierwszym kontakcie nie były zainteresowane inwestycją. Oszuści ponawiają kontakt i używając socjotechniki informują o rzekomo zainwestowanych pieniądzach w imieniu klienta.

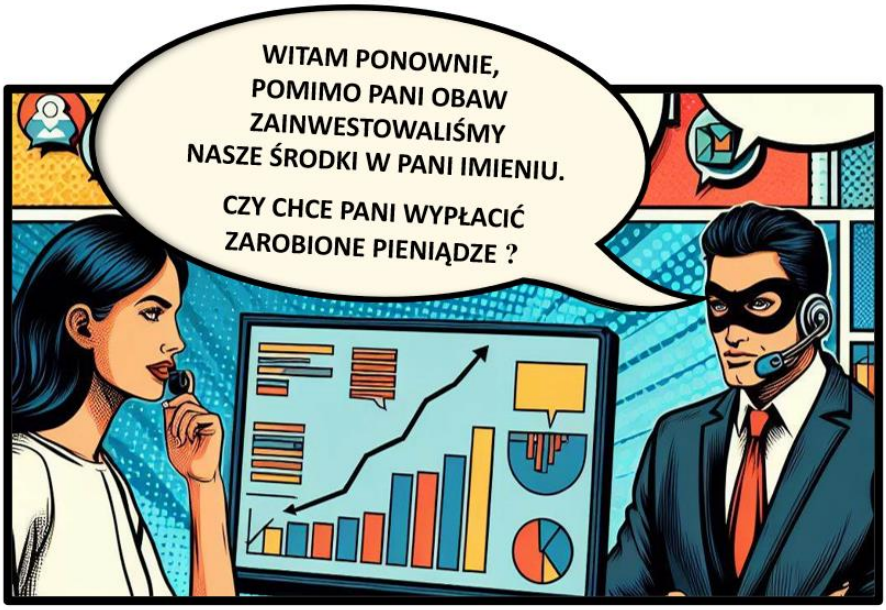
Poniżej prezentujemy przykładową rozmowę.

Klika tygodni temu....

Grafika wygenerowana przy użyciu AI

Oszuści „DORADCY INWESTYCYJNI" coraz częściej po pierwszym, nieskutecznym kontakcie z potencjalną ofiarą ponawiają rozmowę.

Dzisiaj….



Grafika wygenerowana przy użyciu AI

Przestępcy przekonują klientów, że mimo ich obaw lub sprzeciwu zainwestowali drobną kwotę w ich imieniu. Oszuści mogę prezentować fałszywe wyniki rzekomej inwestycji oraz namawiają klienta do wypłaty „zarobionych" środków.

Zmanipulowany klient wykonuje polecenia oszusta np. dokonuje wpłaty za tzw. „opłatę manipulacyjną" lub instaluje np. oprogramowanie do zdalnej obsługi na swoim urządzeniu. W następstwie oszust przejmuje pełną kontrolę nad nim. To oznacza, że jeśli używasz tego urządzenia do bankowości internetowej przestępcy znają Twoje poufne informacje oraz mogą zarządzać Twoimi finansami.

Po co oszuści to robią ?
By ukraść Twoje pieniądze i przejąć Twoją tożsamość!

Co robić aby nie dać się oszukać ?

- nie ulegaj presji czasu czy wizji łatwego zarobku, który może wynikać z przekazywanych informacji, zachowaj zdrowy rozsądek i przeanalizuj sytuację;

- pamiętaj, że NIGDY inwestycje nie są dokonywane bez Twojej zgody i wkładu finansowego – nie daj się nabrać, że ktoś wpłacił SWOJE pieniądze byś TY mógł zarobić!
- nigdy nie instaluj tzw. zdalnego pulpitu np. AnyDesk, TeamViewer, QuickSupport czy Zoom, na prośbę „DORADCY INWESTYCYJNEGO" lub „PRACOWNIKA BANKU". Takie oprogramowanie może umożliwiać dostęp do Twojego urządzenia i przejęcie pełnej kontroli nad nim.

W przypadku podejrzenia usiłowania popełnienia przestępstwa lub w sytuacji, gdy przestępstwo to zostało popełnione niezwłocznie poinformuj o tym fakcie swój bank oraz złóż stosowne zawiadomienie na Policję lub do Prokuratury.

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego
Centralne Biuro Zwalczania Cyberprzestępczości
Komenda Główna Policji

_____

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków lub ich klientów.