Fałszywe inwestycje – czym są?

To metoda oszustwa, która polega na **podszywaniu się pod maklerów i brokerów giełdowych**. Proponują nowe możliwości zainwestowania Twoich środków, które np. wcześniej nie były dostępne na rynku dla każdego. Doskonale przedstawiona oferta staje się przekonująca, przez co ciężko rozpoznać kłamstwo. Przestępcy starają się dopasować swoje ataki socjotechniczne do specyfiki rynku krajowego oraz obecnej sytuacji geopolitycznej. Co więcej, bardzo często wykorzystują wizerunki znanych osób czy firm. Dzięki temu oferta i możliwość szybkiego oraz wysokiego zarobku wydają się jeszcze bardziej wiarygodne.

Przykładem takich działań oszustów mogą być próby podszywania się pod spółki skarbu państwa, np. Orlen lub KGHM. Przestępcy mogą podszywać się też pod hurtownie lub składy oferujące np. cukier czy węgiel.

Jak przebiega takie oszustwo?

- Oszust kontaktuje się z Tobą telefonicznie, e-mailowo lub przez media społecznościowe. Oferuje szansę zainwestowania w produkt, który przynosi bardzo wysokie zyski w krótkim czasie. Co ważne, fałszywe oferty są też publikowane na specjalnie przygotowanych serwisach lub w serwisach społecznościowych, np. na Facebooku.
- Oferta wydaje Ci się bardzo atrakcyjna, a oszust gwarantuje brak ryzyka inwestycyjnego, co jeszcze bardziej usypia Twoją czujność.
- Oszust chce uwiarygodnić swoją historię, więc nielegalnie wykorzystuje wizerunki znanych i powszechnie szanowanych osób. Udowadnia, że nawet oni zainwestowali swoje środki w ten produkt.
- Najważniejszy etap dla oszusta to instalacja oprogramowania zdalnego pulpitu na Twoim urządzeniu (np. popularny Any Desk).
- Oszust przez telefon instruuje Cię jak „zainwestować", a jednocześnie wyprowadza środki z Twojego konta. Wmawia Ci, że to „inwestycja", a w rzeczywistości przelewa pieniądze na inny rachunek, aby Cię okraść.
- Pamiętaj, że oszust może też nakłaniać Cię do przelania środków na wskazy przez niego rachunek. Wówczas po przelaniu pieniędzy otrzymujesz konto na fikcyjnym serwisie, gdzie widoczne są potencjalne zyski, „wypracowane" właśnie dzięki Twoim

środkom. To wszystko jest oszustem, które ma na celu nakłonić Cię do wykonania większej ilości przelewów na konto przestępcy.

- Kiedy próbujesz wypłacić pieniądze z inwestycji, kontakt z oszustem się urywa lub wręcz przeciwnie – oszust nakłania Cię do dopłaty pieniędzy.

Ważne: innym etapem tego oszustwa jest to, że możesz przyjąć przelew na swój rachunek. Pamiętaj, **w żadnym wypadku nie przelewaj tak przyjętych pieniędzy dalej!** Weźmiesz wówczas udział w oszustwie – pomożesz przestępcom „przeprać" pieniądze pochodzące z kradzieży od innej osoby. W ten sposób oszuści tworzą złudzenie zysku, który natychmiast trzeba „zainwestować dalej".

Jak się chronić?

- Omijaj podejrzane inwestycje. Zawsze przemyśl wszystkie za i przeciw.
- Weryfikuj informacje o danej firmie w internecie, najlepiej w kilku źródłach.
- Podmioty oferujące inwestycje muszą mieć zezwolenie na prowadzenie takiej działalności. Firmy, które w Polsce są objęte nadzorem KNF znajdziesz w wyszukiwarce podmiotów nadzorowanych: www.knf.gov.pl/podmioty/wyszukiwarka_podmiotow.
- Sprawdzaj listę ostrzeżeń publicznych KNF. Tam znajdziesz komunikaty o podejrzanych firmach, które działają bez zezwolenia KNF: www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne.
- Czytaj opinie innych osób o danej firmie. Oszukani klienci często sami publikują ostrzeżenia przed nieuczciwymi podmiotami.
- Nigdy nie podawaj identyfikatora i hasła do bankowości internetowej czy danych swojej karty płatniczej (numer karty, CVV, data ważności) – te informacje są poufne, powinny być znane tylko Tobie.
- Nie instaluj dodatkowego oprogramowania (np. Any Desk) na urządzeniach, z których logujesz się do aplikacji bankowej.
- Jeśli otrzymasz przelew z obcego rachunku, który wygląda jak „zwykły" od innej osoby, nie przekazuj go dalej. Jeśli to zrobisz, weźmiesz udział w przestępstwie.
- Jeśli masz podejrzenie, że to oszustwo, zadzwoń na policję.

Jeśli dojdzie do oszustwa…

Nie czekaj, reaguj! Jak najszybciej zablokuj dostęp do bankowości elektronicznej oraz skontaktuj się z Bankiem!