

OD FAŁSZYWEJ REKLAMY DO UTRATY OSZCZĘDNOŚCI

Jak rozpoznać oszustwo inwestycyjne?



Publikacja jest rozpowszechniana na zasadach licencji Creative Commons. Uznanie autorstwa - Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe.

Ilustracje zawarte w publikacji zostały wygenerowane przy użyciu narzędzi sztucznej inteligencji (AI).

SPIIS TREŚCI

01

Wprowadzenie

02

Poznaj historię Tomasza

03

Jak manipulują cyberprzestępcy

04

Oszustwa inwestycyjne z perspektywy CSIRT KNF

05

Lista zachowań ochronnych

06

Gdzie szukać pomocy?

07

Słowniczek



WPROWADZENIE

Europejski Miesiąc Cyberbezpieczeństwa (European Cybersecurity Month, ECSM) to ogólnoeuropejska kampania edukacyjna, która co roku odbywa się w październiku. Jej celem jest zwiększanie świadomości na temat cyfrowych zagrożeń i promowanie dobrych praktyk z obszaru cyberbezpieczeństwa wśród obywateli w całej Europie.

Inicjatywa została zapoczątkowana w 2012 roku przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa oraz Komisję Europejską.

W ramach tegorocznej edycji Europejskiego Miesiąca Cyberbezpieczeństwa CSIRT KNF przygotował poradnik poświęcony oszustwom inwestycyjnym. To odpowiedź na stale rosnącą skalę zagrożeń, w których cyberprzestępcy podszywają się pod legalnie działające instytucje, znane marki i osoby.

Głównym bohaterem publikacji jest Tomasz, 58-letni nauczyciel historii. Choć sama postać jest fikcyjna, jego historia opisuje metody manipulacji stosowane przez cyberprzestępców. Zrozumienie tych mechanizmów jest pierwszym krokiem do ochrony naszych pieniędzy.

Cyberbezpieczeństwo to nie tylko zaawansowane technologie, ale także nasze codzienne nawyki, emocje i decyzje. W starciu z precyzyjnie wyreżyserowaną manipulacją każdy z nas, bez względu na wiek czy wykształcenie, może stać się jej ofiarą. Naszą największą przewagą w walce z cyberprzestępcami pozostają świadomość zagrożeń i konsekwentne stosowanie zasad cyberhigieny.



POZNAJ HISTORIĘ TOMASZA

Tomasz ma pięćdziesiąt osiem lat. Od ponad trzydziestu lat pracuje w szkole podstawowej jako nauczyciel historii. Lubi swoją pracę, chociaż przyznaje, że z roku na rok jest coraz bardziej wymagająca. Tomasz chętnie korzysta z internetu, często płaci kartą i załatwia wiele spraw przez telefon. Dobrze odnajduje się w cyfrowym świecie, ale czasami ma poczucie, że nie nadąża za tempem zmian technologicznych.

Tomasz stara się rozsądnie gospodarować pieniędzmi i regularnie odkłada część pensji. Nigdy nie interesował się giełdą. Uważał, że to zajęcie dla ludzi, którzy znają się na ekonomii. Inwestowanie kojarzyło mu się ze skomplikowanymi analizami i zbyt dużym ryzykiem. Mimo że przez lata udało mu się odłożyć około 100 tysięcy złotych, Tomasz coraz częściej zastanawiał się, czy te pieniądze wystarczą na spokojną emeryturę.

Podczas przeglądania mediów społecznościowych Tomasz zobaczył sponsorowany materiał wideo. Występował w nim znany polityk, który opowiadał o nowym programie inwestycyjnym związanym z budową strategicznej infrastruktury energetycznej na Bałtyku.



Materiał nie przypominał typowej reklamy. Wyglądał raczej jak fragment programu informacyjnego. Na ekranie pojawiały się logotypy spółek Skarbu Państwa i znanych banków. Głos wydawał się nieco nienaturalny, ale Tomasz uznał, że tak po prostu brzmi dźwięk z telefonu. Nie przyszło mu do głowy, że ten film mógł zostać wygenerowany przez sztuczną inteligencję (*deepfake*).

Tomasz kliknął link widoczny w opisie filmu. Formularz kontaktowy otworzył się na platformie społecznościowej. Na stronie widniał napis: „Bezpłatna konsultacja, bez zobowiązań”. Wystarczyło wpisać tylko imię i numer telefonu.

Tomasz nie podjął decyzji od razu. Zastanawiał się, czy w przeszłości nie popełnił błędu, ignorując podobne okazje. Pomyślał, że nie zaszkodzi dowiedzieć się czegoś więcej. W końcu konsultacja była bezpłatna. Zostawił swój numer telefonu i wrócił do oglądania meczu.



GŁOS, KTÓREMU MOŻNA ZAUFAĆ

Telefon zadzwonił następnego dnia, tuż po godzinie szesnastej. Mężczyzna przedstawił się jako doradca inwestycyjny. Używał pojęć, które brzmiały profesjonalnie: dywersyfikacja portfela, algorytmy inwestycyjne, strategiczny program rozwoju infrastruktury energetycznej.

Doradca od początku podkreślał, że platforma inwestycyjna dysponuje ograniczoną liczbą miejsc, a zainteresowanie ofertą jest bardzo duże. Rozmowa trwała blisko dwadzieścia minut. Mężczyzna pytał Tomasza o pracę, rodzinę i plany na emeryturę. Dopiero pod koniec rozmowy przeszedł do tematu inwestycji. Kiedy Tomasz przyznał, że nigdy wcześniej nie interesował się giełdą, rozmówca odpowiedział:



Proszę się nie martwić. To nawet lepiej. Nie ma Pan złych nawyków. Nasz system wykonuje większość pracy za inwestora. Nie musi Pan wpłacać większych kwot, dopóki nie zobaczy Pan, jak to wszystko funkcjonuje. Oczywiście w każdej chwili ma Pan dostęp do swoich środków.

Wszystko brzmiało rozsądnie. Pod koniec rozmowy doradca poprosił Tomasza o zainstalowanie programu do zdalnego dostępu. Wyjaśnił, że dzięki temu będzie mógł przeprowadzić Tomasza przez proces rejestracji i pierwszej wpłaty. Doradca zapewniał, że z tego rodzaju programów korzystają banki i firmy informatyczne na całym świecie. Tomasz przyznał, że samodzielna instalacja programu mogłaby sprawić mu trudność, dlatego chętnie skorzystał z pomocy rozmówcy.

Po zalogowaniu Tomasz zobaczył nowoczesną platformę inwestycyjną. Dynamiczne wykresy, logotypy znanych banków i informacje o zabezpieczeniach sprawiały wrażenie profesjonalnego serwisu maklerskiego.

Tomasz wpłacił 800 złotych. Ku jego zaskoczeniu po trzech dniach saldo wynosiło już 1320 złotych. Zysk był widoczny na ekranie.



CORAZ WIĘKSZE ZAANGAŻOWANIE

W kolejnych tygodniach Tomasz wykonał jeszcze dwa przelewy. Najpierw wpłacił 5 tysięcy złotych, a kilka dni później kolejne 13 tysięcy. Na platformie widział coraz wyższy zysk.

Doradca regularnie dzwonił, gratulował trafnych decyzji i informował o kolejnych możliwościach inwestycyjnych. Z czasem Tomasz zaczął odczuwać wrażenie, że rozmawia z kimś, kto naprawdę troszczy się o jego pieniądze. Po kilku dniach doradca zaproponował zwiększenie inwestycji.



Panie Tomaszu, gratuluję kolejnego sukcesu! Przy takich wynikach szkoda nie wykorzystać pełnego potencjału. Pański portfel zaczyna pracować bardzo efektywnie. Nie powinienem tego mówić, informacja jest poufna, ale już wkrótce pojawi się świetna okazja inwestycyjna.

Tomasz wpłacił kolejne środki. Łącznie zainwestował ponad 70 tysięcy złotych. Na platformie wartość jego portfela wynosiła już ponad 132 tysiące złotych.

Z każdym logowaniem z satysfakcją patrzył na rosnące liczby. Zastanawiał się, co zrobić z zarobionymi pieniędzmi. Coraz częściej myślał o tym, by część zysku przeznaczyć na wymarzoną zagraniczną wycieczkę albo remont łazienki.



MOMENT PRAWDY

Pewnego dnia Tomasz postanowił wypłacić część środków. Kliknął przycisk „wypłać”. Zamiast potwierdzenia przelewu pojawił się komunikat informujący o konieczności wcześniejszego opłacenia prowizji i podatku od zysków kapitałowych. Zgodnie z komunikatem wpłacone kwoty miały zostać zwrócone po zakończeniu procedury.



Tomasz zapłacił. Po chwili otrzymał komunikat o dodatkowej opłacie. Tym razem z żądaniem uiszczenia 250 zł za ekspresową realizację wypłaty. Zapłacił ponownie, ale pieniądze nie pojawiły się na jego koncie bankowym. Wtedy Tomasz po raz pierwszy poczuł niepokój. Najpierw próbował dodzwonić się do doradcy. Bez skutku. Później napisał wiadomość e-mail, ale również nie otrzymał odpowiedzi.

Dopiero kiedy usiadł przy komputerze i wpisał w wyszukiwarkę nazwę platformy inwestycyjnej oraz słowo „opinie”, zaczął rozumieć, co się wydarzyło. Pierwsze wyniki prowadziły do forów internetowych i grup w mediach społecznościowych. Dziesiątki oszukanych osób opisywały niemal identyczny scenariusz. Ten sam panel inwestycyjny, rozmowy telefoniczne i rosnące liczby na ekranie. A potem kolejne opłaty, które nigdy nie prowadziły do wypłaty pieniędzy.

Tomasz był załamany. Długo nie potrafił znaleźć odpowiedzi, jak mógł nie zauważyć sygnałów ostrzegawczych. Przestępcy wykorzystali jednak nie tylko jego nadzieję na bezpieczną przyszłość, lecz także wizerunek osób publicznych, profesjonalnie wyglądającą platformę i zaufanie budowane podczas kolejnych rozmów. Każdy z tych elementów sprawiał, że oferta wydawała się coraz bardziej wiarygodna, a Tomasz stopniowo tracił czujność.



CO TERAZ?

Ofiary oszustw inwestycyjnych bardzo często odczuwają głęboki wstyd, poczucie winy i paraliżujący lęk przed oceną ze strony otoczenia. To naturalna reakcja, ale niezwykle ważne jest, aby uświadomić sobie, że odpowiedzialność za przestępstwo ponoszą oszuści.



Nie zostawaj z tym problemem sam. Pierwszym krokiem do odzyskania kontroli nad sytuacją jest przerwanie milczenia i rozmowa z zaufaną osobą. Wsparcie emocjonalne pomaga spojrzeć na sytuację z dystansem i podjąć racjonalne działania.

Niezwłoczne zgłoszenie sprawy do banku, na policję oraz do odpowiednich zespołów reagowania (CSIRT KNF i CERT Polska) ma kluczowe znaczenie. Każde zgłoszenie dostarcza cennych informacji, które pozwalają blokować fałszywe strony, usuwać konta oszustów i skutecznie chronić kolejne osoby przed utratą oszczędności.



DWA TYGODNIE PÓŹNIEJ...

Tomasz odebrał telefon z nieznanego numeru. Kobieta przedstawiła się jako pracownica kancelarii, która pomaga odzyskiwać pieniądze utracone w oszustwach internetowych. Znała nazwę platformy, a nawet kwotę, którą stracił Tomasz.



Pomogliśmy wielu poszkodowanym odzyskać środki. W Pana przypadku sprawa jest prosta. Musimy tylko najpierw pokryć koszty postępowania, ponieważ Pana pieniądze są na zagranicznym koncie.

Tym razem Tomasz nie wykonał przelewu. Rozłączył się i zadzwonił do swojego banku, korzystając z numeru podanego na oficjalnej stronie internetowej. Konsultant wyjaśnił mu, że to kolejna odsłona tego samego oszustwa (*recovery scam*). Przestępcy, którzy mają dane ofiary, często wracają do niej, podszywając się pod osoby oferujące pomoc. Tego samego dnia Tomasz zgłosił sprawę na policję.



CZEGO UCZY NAS HISTORIA TOMASZA?



OSZUSTWO INWESTYCYJNE TO STARANNIE WYREŻYSEROWANY PROCES

Historia Tomasza pokazuje, że utrata oszczędności rzadko jest wynikiem jednej decyzji. Najczęściej jest to ciąg pozornie niegroźnych kroków: obejrzenie atrakcyjnej reklamy w mediach społecznościowych, wypełnienie formularza kontaktowego, zaufanie rzekomemu doradcy, a następnie dokonanie pierwszej, niewielkiej wpłaty.



TO, CO WYGLĄDA WIARYGODNIE, NIE MUSI BYĆ PRAWDZIWE

Przekonująca reklama, specjalistyczne słownictwo, regularny kontakt telefoniczny czy rosnące saldo na ekranie smartfona dawały Tomaszowi poczucie bezpieczeństwa. Żaden z elementów przestępczego scenariusza nie stanowił jednak dowodu, że oferta jest legalna, a pieniądze są naprawdę inwestowane. Cyberprzestępcy w pełni kontrolują przekaz i obraz sytuacji, który prezentują swojej ofierze.



UTRATA PIENIĘDZY NIE ZAWSZE KOŃCZY KONTAKT Z PRZESTĘPCAMI

Nawet gdy oszustwo wychodzi na jaw, ofiara wciąż pozostaje potencjalnym celem dla cyberprzestępców. Bardzo często dochodzi do kolejnych prób wyłudzenia. Tym razem ze strony podmiotów, które rzekomo oferują „gwarantowane odzyskanie utraconych środków”. Przestępcy wykorzystują wiedzę o wcześniejszym wyłudzeniu, obiecując szybką pomoc w zamian za wstępną opłatę.

JAK MANIPULUJĄ CYBERPRZESTĘPCY

PODSZYWANIE SIĘ POD AUTORYTETY

Cyberprzestępcy bezprawnie wykorzystują wizerunki znanych osób oraz logotypy banków, spółek Skarbu Państwa i instytucji publicznych. W ten sposób próbują wykorzystać nasze zaufanie do marek i autorytetów, aby uwiarygodnić fałszywą ofertę inwestycyjną.



PERSONALIZACJA

Cyberprzestępcy nie proszą od razu o pieniądze. Zaczynają od życzliwej rozmowy, aby poznać życiowe plany i obawy finansowe rozmówcy. W ten sposób zbierają informacje i budują zaufanie.

PRESJA CZASU

Cyberprzestępcy sugerują, że okazja jest dostępna tylko chwilowo, powołując się na ograniczoną liczbę miejsc lub kończącą się promocję. W ten sposób stwarzają presję, która utrudnia nam weryfikację faktów.



FIKCYJNE ZYSKI

Cyberprzestępcy na fałszywych platformach inwestycyjnych prezentują zmanipulowane wykresy i fikcyjne wzrosty salda. W ten sposób usypiają naszą czujność i zachęcają do wpłacania coraz wyższych kwot.

ESKALACJA ZAANGAŻOWANIA

Cyberprzestępcy początkowo zachęcają do wpłacania niewielkich kwot, by z czasem nakłaniać do coraz większych wpłat. W ten sposób wykorzystują nasze rosnące zaangażowanie, przez co z każdą wpłatą coraz trudniej zrezygnować i wycofać się z inwestycji.



OSZUSTWA INWESTYCYJNE Z PERSPEKTYWY CSIRT KNF

Jak poważnym problemem są obecnie oszustwa inwestycyjne?

Skala zagrożeń jest bardzo duża. Fałszywe inwestycje od kilku lat są jednym z głównych zagrożeń dla pieniędzy użytkowników internetu. W 2025 roku CSIRT KNF zgłosił do zablokowania ponad 41 tys. domen, z czego 96 proc. stanowiły domeny związane z fałszywymi inwestycjami. Warto też spojrzeć na ten problem w dłuższej perspektywie. W latach 2021–2025 zgłosiliśmy do zablokowania ponad 126 tys. domen związanych z fałszywymi inwestycjami. Od stycznia do sierpnia 2026 roku zgłosiliśmy ponad 5 tys. profili w mediach społecznościowych publikujących takie reklamy. Te liczby pokazują, z jak złożoną infrastrukturą wykorzystywaną do oszustw mamy do czynienia. Należy podkreślić, że są to wyniki naszych działań operacyjnych, które nie odzwierciedlają pełnej skali zjawiska ani liczby poszkodowanych.

Co wiemy o metodach działania cyberprzestępców?

Przestępcy stale dopracowują sposoby uwiarygodniania fałszywych ofert. Bardzo często wykorzystują logotypy znanych, cieszących się zaufaniem firm, podszywają się pod instytucje i posługują się wizerunkami znanych osób. Sztuczna inteligencja pozwala przestępcom przygotowywać reklamy fałszywych inwestycji znacznie szybciej i na większą skalę. Dla odbiorcy oznacza to, że nawet przekonująco wyglądające materiały graficzne lub wideo nie mogą stanowić wystarczającej podstawy do zaufania ofercie. Równocześnie oszuści stale próbują omijać zabezpieczenia platform reklamowych i utrudniać pracę analitykom.



Karol Paciorek, kierownik CSIRT KNF

Jaką rolę pełni CSIRT KNF w walce z oszustwami inwestycyjnymi?

Naszym zadaniem jest jak najwcześniejsze identyfikowanie zagrożeń i ograniczanie możliwości dotarcia przestępców do kolejnych osób. Monitorujemy kampanie, analizujemy ich przebieg oraz zgłaszamy niebezpieczne domeny, reklamy i profile do zablokowania. Współpracujemy z innymi zespołami reagowania oraz operatorami platform. Szybkie przekazanie informacji ma znaczenie, bo każda aktywna reklama może przyciągać kolejnych odbiorców. Równolegle publikujemy ostrzeżenia, raporty i materiały edukacyjne.

W jaki sposób możemy zadbać o swoje bezpieczeństwo?

Cyberbezpieczeństwo to także nasze codienne nawyki. W przypadku fałszywych inwestycji cyberhigiena oznacza przede wszystkim sprawdzanie informacji przed przekazaniem danych lub pieniędzy, ostrożność wobec obietnic wyjątkowego zysku i umiejętność zatrzymania się, kiedy ktoś wywiera presję. Edukacja powinna pomagać rozpoznawać te mechanizmy. Właśnie dlatego aktywnie uczestniczymy również w Europejskim Miesiącu Cyberbezpieczeństwa, żeby pokazać konkretne przykłady zagrożeń i sposoby ich rozpoznawania.

LISTA ZACHOWAŃ OCHRONNYCH

ZANIM KLIKNIESZ W ATRAKCYJNĄ REKLAMĘ

- Każdą obietnicę wysokiego zysku przy niskim lub zerowym ryzyku traktuj jako sygnał ostrzegawczy, a nie okazję.
- Nie ufaj bezkrytycznie wizerunkowi znanych osób w reklamach. Sprawdź, czy dana osoba lub instytucja rzeczywiście potwierdziła udział w ofercie (np. na jej oficjalnym profilu).
- Nie oceniaj wiarygodności reklamy wyłącznie na podstawie wyglądu lub brzmienia nagrania. Materiały wygenerowane lub zmodyfikowane przy użyciu sztucznej inteligencji mogą być trudne do rozpoznania.

ZANIM ZOSTAWISZ DANE KONTAKTOWE

- Nie wypełniaj formularzy kontaktowych w reklamach obiecujących inwestycje, zwłaszcza jeśli deklarują „brak zobowiązań”.
- Sprawdź firmę w CEIDG lub KRS, zanim podejmiesz jakikolwiek kontakt.
- Zweryfikuj podmiot na Liście ostrzeżeń publicznych KNF (dostępnej na stronie www.knf.gov.pl/dla_konsumenta/ostrezenia_publiczne).
- Wyszukaj w internecie nazwę firmy lub platformy razem ze słowem „opinie” lub „oszustwo”.

LISTA ZACHOWAŃ OCHRONNYCH

PODCZAS ROZMOWY Z „DORADCĄ”

- Nie zaciągaj kredytu ani nie pożyczaj pieniędzy na inwestycję pod wpływem nacisku osoby oferującej produkt.
- Nie podejmuj decyzji finansowych pod presją.
- Skonsultuj każdą ofertę inwestycyjną z niezależnym specjalistą niezwiązanym z osobą, która się z Tobą skontaktowała.
- Porozmawiaj o ofercie z bliską osobą, zanim podejmiesz decyzję inwestycyjną.

JEŚLI JUŻ ZAINWESTOWAŁEŚ

- Zachowaj szczególną ostrożność, jeśli przed wypłatą środków platforma żąda kolejnych przelewów, np. na poczet podatku, prowizji, ubezpieczenia lub odblokowania transakcji.
- Nie wpłacaj dodatkowych pieniędzy bez niezależnego potwierdzenia zasadności żądania.
- Skontaktuj się z bankiem, korzystając z danych kontaktowych pozyskanych z oficjalnego źródła.



GDZIE SZUKAĆ POMOCY?

Jeśli podejrzewasz, że padłeś ofiarą oszustwa, liczy się czas. Im szybciej zareagujesz, tym większa szansa na zatrzymanie przelewów i ograniczenie strat.

- Przerwij kontakt.
- Niezwłocznie skontaktuj się z bankiem, dzwoniąc pod numer podany na jego oficjalnej stronie internetowej.
- Zabezpiecz dowody (zrzuty ekranu, wiadomości, numery kont i dane kontaktowe).
- Zgłoś sprawę na policję.
- Uważaj na kontakt od rzekomych „kancelarii” oferujących odzyskanie utraconych środków za opłatą z góry.



Bądź na bieżąco z cyberbezpieczeństwem!

Obserwuj oficjalne profile społecznościowe CSIRT KNF na platformach X, LinkedIn oraz Facebook.

SŁOWNICZEK

Socjotechnika

Wykorzystywanie mechanizmów psychologicznych i technik manipulacji w celu nakłonienia do określonego działania, np. ujawnienia danych, przekazania pieniędzy lub umożliwienia dostępu do urządzenia czy systemu.

Deepfake

Materiał audio, wideo, obraz wygenerowany lub zmodyfikowany przy użyciu sztucznej inteligencji w celu realistycznego przedstawienia wypowiedzi lub zdarzeń, które nie miały miejsca. Deepfake jest wykorzystywany do uwiarygodniania fałszywych reklam i ofert.

Recovery scam

Oszustwo polegające na obietnicy odzyskania utraconych pieniędzy. Przestępcy podszywają się np. pod kancelarie prawne lub przedstawicieli instytucji finansowych i żądają opłaty z góry, po której nie świadczą obiecanej usługi.

Domena phishingowa

Domena internetowa wykorzystywana do podszywania się pod zaufany podmiot lub do nakłaniania użytkowników do przekazania danych, pieniędzy albo wykonania innych działań na korzyść przestępców. Może przypominać adres prawdziwej strony internetowej.

Fałszywa platforma inwestycyjna

Serwis internetowy lub aplikacja, które sprawiają wrażenie legalnej platformy inwestycyjnej, ale w rzeczywistości służą do wyłudzenia pieniędzy. Zwykle prezentują fikcyjne salda, wykresy i zyski, aby skłonić użytkownika do kolejnych wpłat.