OSZUSTWA FINANSOWE I WYŁUDZENIA W INTERNECIE Z WYKORZYSTANIEM SZTUCZNEJ INTELIGENCJI

BĄDŹ CZUJNY I ZADBAJ O SWOJE BEZPIECZEŃSTWO

Oszustwa finansowe i wyłudzenia online nie są niczym nowym, jednak wraz z pojawieniem się sztucznej inteligencji (AI) stały się one bardziej wyrafinowane i trudniejsze do wykrycia. Przestępcy wykorzystują obecnie fałszywe wiadomości i strony internetowe, nieprawdziwe profile celebrytów, a nawet generowane przez AI głosy lub filmy, które naśladują Twój bank, znajomych lub rodzinę.

Oszuści mogą kontaktować się z Tobą za pośrednictwem mediów społecznościowych, aplikacji do komunikacji, e-maili i nieoczekiwanych telefonów, które brzmią realistycznie.

Zwracamy zatem szczególną uwagę na ryzyko utraty pieniędzy, kradzieży tożsamości i możliwości doznania wysokiego stopnia stresu. Bądź ostrożny i stosuj się do poniższych wskazówek, żeby zapewnić swoje i innych bezpieczeństwo:

Zachowaj czujność wobec istniejących oszustw finansowych i wyłudzeń w Internecie wykorzystujących sztuczną inteligencję, np. podszywanie się pod inne osoby, *phishing*, oszustwa inwestycyjne i ubezpieczeniowe, a nawet oszustwa oparte na zbudowaniu relacji i zaufania. Aby dowiedzieć się więcej o różnych rodzajach oszustw i przekrętów zobacz s. 5-7.

i na temat oszustw charakterystycznych dla kryptoaktywów- **zobacz specjalną broszurę informacyjną** ( ).

Rozpoznawaj sygnały ostrzegawcze:
naucz się rozpoznawać podejrzane zachowania, wiadomości lub oferty (zobacz s. 2).

Zadbaj o swoje bezpieczeństwo:
zabezpiecz swoje dane osobowe (zobacz s. 3) oraz

Dowiedz się, co zrobić, jeśli padniesz ofiarą oszustwa lub wyłudzenia
(zobacz s. 4).

Znaki ostrzegawcze

Obietnica, która wydaje się zbyt piękna, aby mogła być prawdziwa.

Nieoczekiwany telefon z nieznanego numeru.

Pilna prośba o pieniądze lub dane osobowe - w tym od osoby, która udaje członka rodziny, znajomego, a nawet osobę publiczną.

Prośba o przejęcie kontroli nad urządzeniem, pobranie aplikacji, zeskanowanie kodu QR lub kliknięcie łącza.

Prośba o podanie danych osobowych lub bankowych (np. haseł, numerów kart kredytowych, danych logowania do bankowości internetowej lub kodów zabezpieczających).

Prośba o dokonanie płatności za pomocą metod, których nie można śledzić (np. kryptoaktywa, karty podarunkowe, przelewy bankowe lub przedpłacone karty debetowe).

Podejrzany lub nieprawidłowy adres e-mail lub link (np. błędy ortograficzne w adresie URL lub nietypowe adresy internetowe).

Załącznik z nieznanego źródła - zwłaszcza plik .exe, .scr, .zip lub plik Office z włączoną obsługą makr (.docm, .xlsm).

Błędy gramatyczne lub formatowanie w dokumencie o oficjalnym wyglądzie. Sztuczna inteligencja jednak może pozwolić oszustom na skuteczne maskowanie tych wad.

Strona internetowa, która wygląda profesjonalnie, ale nie zawiera zweryfikowanych danych kontaktowych lub informacji rejestracyjnych firmy.

Nienaturalna intonacja, brak pauz i nadmierna płynność lub robotyczność. Należy zwrócić uwagę na „klonowanie głosu". Należy mieć jednak na względzie to, że mowa generowana przez sztuczną inteligencję może również brzmieć bardzo naturalnie i realistycznie.

Filmy, w których głos może brzmieć robotycznie lub nadmiernie płynnie, a ruchy warg i mimika mogą być niezgodne z mową. Z kolei tło, oświetlenie i cienie mogą być niespójne. Takie przypadki często stanowią filmy generowane przez sztuczną inteligencję („*deepfake*").

Kroki służące zabezpieczeniu swojego interesu

1 **Nigdy nie udostępniaj danych osobowych ani informacji bankowych:**

Wiarygodne firmy nigdy nie proszą o podanie kodów PIN, haseł, danych logowania do bankowości internetowej ani kodów zabezpieczających za pośrednictwem poczty elektronicznej, SMS-ów, mediów społecznościowych lub telefonu.

2 **Zanim podejmiesz działanie, zastanów się:**

Nie spiesz się z wysyłaniem pieniędzy, udostępnianiem informacji lub klikaniem w linki – oszuści celowo wywołują poczucie pilności (np. poprzez imitację problemów informatycznych w Twoim banku, pilne telefony dotyczące Twoich przyjaciół i członków rodziny, groźby itp.). W razie jakichkolwiek wątpliwości, nawet najmniejszych, nie podejmuj żadnych działań- zakończ rozmowę i dokładnie sprawdź źródło lub tożsamość rozmówcy.

3 **Sprawdź dokładnie źródło/tożsamość osoby, która się z Tobą komunikuje:**

- Zawsze sprawdzaj, skąd pochodzą wiadomości, połączenia, e-maile i linki- nawet jeśli wyglądają wiarygodnie, wydają się pochodzić od przyjaciela lub rodziny, a nawet osoby publicznej. Tytułem przykładu, zadzwoń lub napisz do nich za pomocą znanego Tobie numeru, bądź spróbuj się z nimi skontaktować za pośrednictwem jakiegokolwiek innego zaufanego kanału. Zwróć uwagę na błędy ortograficzne, podejrzanie wyglądające adresy URL lub brakujące wskaźniki bezpieczeństwa (np. sprawdź, czy link do strony internetowej zawiera literę „s" w „HTTPS", aby upewnić się, że strona jest bezpieczna, oraz sprawdź, czy w nazwie firmy nie ma dodanych lub brakujących liter).

- Nie otwieraj linków z niechcianych wiadomości, instaluj tylko oficjalne aplikacje z zaufanych sklepów z aplikacjami i nie skanuj nieznanych kodów QR.

- Uzgodnij z rodziną "bezpieczną", tajną frazę, której możesz użyć do potwierdzenia tożsamości, jeśli ktoś o znajomym głosie zadzwoni do Ciebie z pilną prośbą o pieniądze i będzie twierdzić, że jest członkiem Twojej rodziny (np. rodzicem, siostrą/bratem, dzieckiem).

- Porozumiej się bezpośrednio z firmą lub z osobą fizyczną, która się z Tobą kontaktowała, korzystając ze sprawdzonych danych kontaktowych. Nigdy nie polegaj na informacjach podanych przez osobę podejrzewaną przez Ciebie o oszustwo (przykładowo samodzielnie wyszukaj nazwę firmy, skorzystaj ze sprawdzonych rejestrów firm, bądź to wcześniej potwierdzonych metod kontaktowych). Oszuści mogą podawać się za upoważnione osoby lub naśladować stronę internetową rzeczywistej firmy. Sprawdź, czy krajowy organ nadzoru nad rynkiem finansowym wydał jakieś ostrzeżenia lub czy zostały one uwzględnione na liście IOSCO I-SCAN (https://www.iosco.org/i-scan/). W przypadku dostawców kryptoaktywów sprawdź, czy są oni autoryzowani w Unii Europejskiej (np. sprawdź rejestr ESMA ( ).

4 **Zwracaj uwagę na potencjalne sztuczki AI:**

Nawet przy zastosowaniu najlepszych wskazówek dotyczących bezpieczeństwa, wraz z rozwojem technologii AI oszustwa stają się coraz bardziej przekonujące. Jeśli coś wydaje Ci się nietypowe lub zauważysz którykolwiek z powyższych sygnałów ostrzegawczych, spróbuj ponownie ocenić sytuację.

5 **Nigdy nie instaluj oprogramowania zdalnego dostępu ani nie udostępniaj ekranu:**

Banki i instytucje finansowe nigdy Cię o to nie poproszą.

6 **Zabezpiecz urządzenia i konta:**

Używaj silnych i unikalnych haseł, zachowaj je w tajemnicy i unikaj ponownego wykorzystywania tych samych danych uwierzytelniających na różnych platformach. Włącz uwierzytelnianie wieloskładnikowe tam, gdzie jest to możliwe. Zobacz kilka wskazówek dotyczących haseł tutaj ( ). Aktualizuj oprogramowanie i ochronę antywirusową oraz miej je zawsze włączone.

7 **Zachowaj ostrożność w przypadku nieoczekiwanych i ograniczonych czasowo możliwości inwestycyjnych:**

Jeśli coś brzmi zbyt pięknie, aby mogło być prawdziwe- prawdopodobnie tak nie jest.

8 **Zastanów się, zanim udostępnisz informację w mediach społecznościowych:**

Grupy czatowe, fora, posty w mediach społecznościowych i zdjęcia mogą być cennym źródłem wiedzy dla oszustów. Ujawnianie zbyt wielu informacji o sobie lub własnych inwestycjach może spowodować, że staniesz się łatwym celem.

Co zrobić, gdy staniesz się ofiarą oszustwa lub wyłudzenia

Natychmiast wstrzymaj transakcje,

Aby zablokować dalsze przelewy na podejrzane konta i uniknąć dodatkowych strat. Zaprzestań wszelkich kontaktów z oszustami – zignoruj ich połączenia i e-maile oraz zablokuj nadawcę.

Skontaktuj się ze swoim bankiem lub firmą inwestycyjną:

Poinformuj natychmiast swój bank lub firmę inwestycyjną za pośrednictwem oficjalnych kanałów kontaktowych, aby zbadać możliwości wstrzymania lub odwrócenia transakcji.

Zmień hasła na wszystkich swoich urządzeniach i aplikacjach/stronach internetowych.

Oszuści kupują wyciekające hasła online i próbuje je wykorzystywać na wielu kontach. Zmiana tylko jednego hasła nie wystarczy. Pamiętaj, aby zmienić je wszystkie, aby oszuści nie mogli ich ponownie użyć.

Zgłoś i ostrzeż najbliższych:

Zgłoś incydent policji lub krajowemu organowi nadzoru nad rynkiem finansowym i jednocześnie poinformuj swoich najbliższych (np. znajomych i rodzinę), aby zwiększyć ich świadomość i uczulić. Te działania mogą pomóc Ci chronić siebie samego i innych.

Uważaj na oszustwa typu *„recovery room”*:

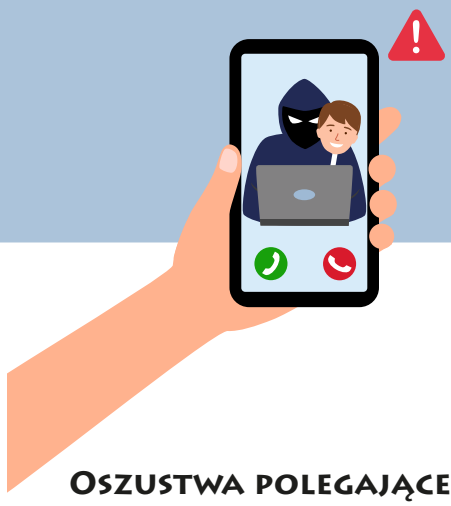
Oszust może skontaktować się z Tobą, mając świadomość, że jesteś ofiarą poprzedniego oszustwa. Może on twierdzić, że jest organem administracji publicznej (np. policją, urzędem skarbowym). Często jednak jest to kolejna próba oszustwa. Biorąc powyższe pod uwagę, pamiętaj o jednym: bycie oszukanym jeden raz, nie stoi na przeszkodzie, aby zostać oszukanym ponownie.

Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych, Europejski Urząd Nadzoru Giełd i Papierów Wartościowych, 2025

Luksemburg: Urząd Publikacji Unii Europejskiej, 2025

PDF ISBN 978-92-9407-258-0 doi:10.2853/4296717 DZ-01-25-146-PL-N

RODZAJE OSZUSTW FINANSOWYCH I WYŁUDZEŃ W INTERNECIE Z WYKORZYSTANIEM SZTUCZNEJ INTELIGENCJI (AI)



Oszustwa polegające na podszywaniu się i korzystaniu z *deep fake*

Otrzymujesz nieoczekiwany telefon od osoby podającej się za przedstawiciela Twojego banku, organu administracji publicznej (np. policji, urzędu skarbowego lub organu nadzoru nad rynkiem finansowym itp.), dystrybutora ubezpieczeń, firmy informatycznej, a nawet członka rodziny. Osoba dzwoniąca może nakłaniać Cię do przekazania środków celem zapewnienia Tobie lub innym bezpieczeństwa. Jednocześnie będzie ona powoływać się na podejrzaną aktywność na Twoim koncie lub w Twojej polisie ubezpieczeniowej. Może również poprosić Cię o podanie danych bankowych (np. numeru karty płatniczej, danych logowania do bankowości internetowej lub haseł), kliknięcie linku lub zainstalowanie oprogramowania, udając, że może szybko rozwiązać problem. Co więcej, osoba dzwoniąca może użyć sfałszowanego numeru, który często odpowiada numerowi telefonu Twojego banku, aby wyglądać na wiarygodną („*spoofing*").

Oszuści mogą wykorzystywać sztuczną inteligencję do tworzenia fałszywych filmów, obrazów lub dźwięków, które naśladują czyjś głos (np. Twojego bankiera lub członka rodziny), twarz (np. celebryty) lub ruchy. **Jest to powszechne zjawisko znane jako „*deep fake*".**

Co może się zdarzyć:

Podając dane osobowe i tworząc poczucie pilności, oszust nakłania Cię do działań, których nie zamierzałeś podjąć, takich jak wysyłanie pieniędzy na wskazane przez nich konto, kliknięcie złośliwego linku lub zainstalowanie złośliwego oprogramowania. Może to dać oszustowi bezpośredni dostęp do Twoich danych bankowych, bądź to innych. Dzięki tym informacjom może zmienić hasło, uzyskać dostęp do konta bankowego i ukraść środki, które zgromadziłeś. Pamiętaj: tylko dlatego, że osoba dzwoniąca zna Twoje dane osobowe, nie oznacza automatycznie, że jest ona godna zaufania.

Phishing i inżynieria społeczna (socjotechnika)

Otrzymujesz wiadomość e-mail lub SMS, która wygląda jakby pochodziła z Twojego banku lub firmy inwestycyjnej, z ostrzeżeniem o „podejrzanej działalności" na Twoim koncie. Logo, układ i język wyglądają profesjonalnie, a wiadomość może pojawić się w tym samym wątku, co inne rozmowy z Twoim bankiem. Komunikat zachęca do kliknięcia w link celem zweryfikowania konta lub zresetowania hasła. Link prowadzi do fałszywej strony internetowej, która wygląda identycznie jak Twoja bankowość internetowa. Nie zdając sobie sprawy z oglądu sytuacji, wprowadzasz swoje dane na stronę internetową zaprojektowaną w celu kradzieży Twoich danych osobowych.

Tytułem wyjaśnienia, oszuści wykorzystują sztuczną inteligencję do tworzenia przekonujących wiadomości *phishingowych*, analizując dane z mediów społecznościowych, celem zidentyfikowania swoich ofiar i dostosowania treści do ich celu.

Co może się zdarzyć:

Oszust uzyskuje dostęp do Twojego konta bankowego i kradnie Twoje pieniądze lub tworzy fałszywy profil z Twoimi danymi osobowymi celem popełnienia oszustwa.

Oszustwa inwestycyjne lub ubezpieczeniowe

W mediach społecznościowych lub na losowej stronie internetowej widzisz reklamę promującą „ograniczoną czasowo możliwość inwestowania o niskim ryzyku" lub „ograniczoną czasowo zniżkę" na ofertę od znanego zakładu ubezpieczeń, lub firmy inwestycyjnej. Reklama zawiera zdjęcie celebryty i rekomendacje, które niejednokrotnie w rzeczywistości okazują się być fałszywe. Po wyrażeniu zainteresowania poprzez kliknięcie linku lub wypełnienie formularza, oszust kontaktuje się z Tobą i przekieruje Cię na platformę lub kanał komunikacyjny, gdzie otrzymujesz profesjonalnie wyglądające porady i dokumenty. Zachęca Cię do zainwestowania niewielkiej kwoty, a kolejno coraz to większych, bądź to do wpłacenia składki na to, co wydaje się być bezpieczne.

Z powyższego wynika, że oszuści wykorzystują narzędzia sztucznej inteligencji, aby te fałszywe propozycje lub e-maile były bardzo przekonujące i trudne do wykrycia. Ponadto, wykorzystują boty mediów społecznościowych zasilane sztuczną inteligencją do tworzenia fałszywych kont, które wchodzą z Tobą w interakcje, rozpowszechniają dezinformację i symulują prawdziwe zachowania, aby zdobyć zaufanie i wpłynąć na Twoje decyzje.

Co może się zdarzyć:

Po próbie wypłaty pieniędzy lub zgłoszenia roszczenia osoba kontaktowa przestaje odpowiadać. Odkrywasz, że firma nie istnieje lub że ryzyko ubezpieczeniowe nie jest objęte ochroną. Wtedy zdajesz sobie sprawę, że wysłałeś pieniądze bezpośrednio do oszusta w ramach fałszywego schematu. Niestety nie możesz odzyskać swoich pieniędzy, a Twoje dane osobowe i finansowe mogą zostać wykorzystane do popełnienia dalszych oszustw (np. podpisania umów w Twoim imieniu, co może doprowadzić do utraty jeszcze większej ilości pieniędzy).

Oszustwa i wyłudzenia polegające na budowie zaufania i relacji

Skontaktowała się z Tobą osoba, której nie znasz w rzeczywistości, za pośrednictwem mediów społecznościowych, aplikacji randkowych lub telefonicznie/SMS-em. Osoba ta prowadzi częste, osobiste i romantyczne rozmowy, budując Twoje zaufanie z pomocą fałszywego profilu. Z biegiem czasu rozmowa schodzi na temat pieniędzy lub możliwości finansowych, takich jak krypto-inwestycje z obietnicami wysokich zwrotów i niskiego ryzyka. Osoba ta prosi Cię o przesłanie pieniędzy na podane przez nią konto lub pomaga Ci założyć gdzieś konto i dokonać niewielkiej, początkowej wpłaty. Celem tych działań jest wywołanie w Tobie wrażenia bezpieczeństwa i legalności schematu, zanim zachęci Cię do zainwestowania większej kwoty.

Oszuści wykorzystują sztuczną inteligencję do generowania fałszywych profili, identyfikowania swoich ofiar w mediach społecznościowych, czy aplikacjach randkowych przy użyciu udostępnionych danych lub używają chatbotów do generowania wiadomości.

Co może się zdarzyć:

Oszust wyciąga jak najwięcej pieniędzy, a następnie odcina wszelką komunikację i znika. Nieuczciwa strona internetowa lub aplikacja inwestycyjna zostaje wyłączona, co uniemożliwia dostęp do rzekomych inwestycji. Oprócz strat finansowych udostępnione przez Ciebie dane osobowe mogą być wykorzystane ponownie do atakowania Twoich znajomych i rodziny lub do kradzieży tożsamości, która może skutkować konsekwencjami o charakterze finansowym i prawnym (np. oszust może dokonywać zakupów, brać pożyczki w Twoim imieniu lub możesz zostać pociągnięty do odpowiedzialności za długi lub przestępstwa popełnione pod własnym imieniem i nazwiskiem, chyba że nie udowodnisz, że jest inaczej).

Oszustwa związane z zakupami

Natrafiasz na atrakcyjną ofertę zakupu na platformie internetowej. Firma oferująca produkt lub usługę prosi o płatność poza oficjalną platformą, twierdząc, że korzysta z „bezpiecznego systemu płatności" i wysyła Ci link celem finalizacji zakupu. Link przekierowuje Cię na fałszywą stronę uwierzytelniającą banku, która imituje oficjalną stronę bankowości internetowej i wykorzystuje jego logo i wygląd. Nie będąc niczego świadomym, wprowadzasz swoje prywatne dane, aby dokonać płatności.

Z powyższego przykładu wynika, że oszuści aktywnie wykorzystują sztuczną inteligencję do tworzenia wysoce przekonujących fałszywych stron internetowych banków, potwierdzeń zamówień i faktur. Sztuczna inteligencja pomaga im naśladować ton, markę i styl prawdziwych firm. W niektórych przypadkach używają chatbotów AI, aby odpowiadać na pytania, sprawiając wrażenie, że transakcja wydaje się bardziej wiarygodna.

Co może się zdarzyć:

Płatność za pośrednictwem linku ze strony trzeciej omija zabezpieczenia platformy internetowej. Oszust uzyskuje dostęp do danych logowania na Twoje konto bankowe i kradnie zgromadzone tam środki.