

Oszuści łączą AI i metodę „na wnuczka”

19 listopada 2024

Sztuczna inteligencja jest coraz mocniej wykorzystywana przez oszustów. Zamieszczają oni w social mediach zmanipulowane reklamy z udziałem znanych ludzi. Ofiarami stają się osoby inwestujące m.in. w kryptowaluty. Według ekspertów, AI ma potencjał, aby zarówno pomagać przestępcom, jak i ograniczyć ich działania. Sztuczna inteligencja pozwala np. na weryfikowanie tożsamości. A to szczególnie teraz nabiera na znaczeniu, bo tuż za rogiem mamy przecież tzw. metodę na wnuczka, w której babcia niedługo będzie widziała w komunikatorze faktyczną twarz swojego wnusia, mówiącego jego głosem. Nakładki AR są szybko rozwijającą się technologią, którą za chwilę masowo będą wykorzystywać przestępcy. Dlatego znawcy tematu przekonują, że trzeba poważnie postawić na edukację, nie tylko finansową.

Oszuści coraz częściej wykorzystują sztuczną inteligencję w swoich poczynaniach. Świadczą o tym przykłady z mediów społecznościowych, gdzie pojawiają się propozycje inwestycji, m.in. na rynku kryptowalut. Jak tłumaczy Aleksander Łapiński ze Stowarzyszenia Ekspertów Bezpieczeństwa Rzeczypospolitej Polskiej, schemat działania przestępców jest bardzo podobny, niezależnie od platformy. Oni sięgają po narzędzia oparte na AI, aby bez zgody znanych osób obrobić ich wizerunek czy głos. Takie technologie umożliwiają podmianę twarzy, klonowanie głosu i inne manipulacje przy stosunkowo niskich kosztach. Ze spreparowanych materiałów tworzą kampanie reklamowe. One kierują użytkowników na profesjonalnie wyglądające strony internetowe, które zachęcają do inwestycji poprzez specjalną aplikację lub formularz zwrotny. „Social media, oferując szerokie możliwości docierania do potencjalnych ofiar, de facto sprzyjają takim działaniom. Dla niedoświadczonego inwestora największym zagrożeniem jest możliwość natrafienia

na wysoce zmanipulowane treści, które są trudne do odróżnienia od prawdziwych ofert. A już za rogiem mamy przecież tzw. metodę na wnuczka, w której babcia będzie widziała w komunikatorze faktyczną twarz swojego wnusia, mówiącego jego własnym głosem. Nakładki AR to bowiem szybko rozwijająca się technologia” – komentuje prof. dr hab. Dariusz Jemielniak, kierownik Katedry Zarządzania w Społeczeństwie Sieciowym w Akademii Leona Koźmińskiego.

Do tego, jak przekonuje prof. Krzysztof Piech z Uczelni Łazarskiego, łatwy dostęp do AI jest potrzebny. Ale każda nowa, gwałtownie rozwijająca się innowacja przyciąga przestępców. Podobnie było w przypadku kryptowalut, a wcześniej – internetu. Z reguły początkowo wymiar sprawiedliwości i organy ścigania nie nadążają za nimi. Z czasem się to zmienia. Unia Europejska próbuje uregulować obszar AI. Ekspert zaznacza, że problem reklam dotyczy nie tylko Polaków, ale i innych narodowości. Generalnie tendencja jest taka, że im mniej wyedukowane jest społeczeństwo, tym łatwiej jest działać oszustom. A pod względem poziomu edukacji finansowej, Polska od wielu lat jest na jednym z ostatnich miejsc w Europie. „Pomagaliśmy odzyskać pieniądze osobom, które skorzystały z oferty takiej inwestycji. Przyznawały, że były zaskoczone wysokim poziomem profesjonalizmu oszustów, zarówno w sposobie komunikacji, języka, jak i znajomości mechanizmów finansowych” – dodaje Aleksander Łapiński.

Zdaniem znawców tematu, AI ma potencjał, aby pomagać zarówno oszustom, jak i przeciwdziałać im. Aleksander Łapiński zaznacza, że mechanizmy sztucznej inteligencji mogą ułatwić tworzenie bardziej wiarygodnych oszustw inwestycyjnych. Przykładowo przez automatyzację procesu generowania fałszywych reklam, stron internetowych czy wiadomości e-mail, które wyglądają niezwykle przekonująco. Do tego dochodzi tworzenie zaawansowanych deepfake’ów z wizerunkami znanych osób. Ekspert zwraca też uwagę na precyzyjną personalizację ataków. AI może analizować dane osobowe (np. po ich wycieku), aby stworzyć

bardziej spersonalizowane kampanie phishingowe. Ponadto sztuczna inteligencja jest w stanie stworzyć chatboty, które będą przekonująco udzielać fałszywych porad inwestycyjnych w czasie rzeczywistym. „Rozwój narzędzi opartych na AI, które potrafią analizować i wykrywać potencjalne oszustwa, jest kluczowy dla przyszłości bezpieczeństwa inwestycji kryptowalutowych. Ważne jest, aby równolegle rozwijać systemy ochrony i edukacji, które będą nadążać za ewolucją technologii. Niestety, ale media społecznościowe mają zerowy interes w tym, aby takie narzędzia rozwijać. Co więcej, wręcz blokują dostęp do swoich treści osobom ze świata nauki, które mogłyby analizować fenomen i pomagać mu przeciwdziałać” – podkreśla prof. dr hab. Dariusz Jemielniak.

Jak przekonuje Jakub Martenka z Ar10, sztuczna inteligencja już teraz jest wykorzystywana w pracy polegającej chociażby na weryfikacji tożsamości. Powstaje wiele programów, które są w stanie ocenić, czy nagranie zostało spreparowane, czy rozmowa odbywa się z prawdziwym człowiekiem. Te rozwiązania mają bardzo wysoką skuteczność, więc na pewno będzie to trend rozwijany. „Z reguły wymiar sprawiedliwości nie nadąża za danym rynkiem. Popatrzmy przykładowo na śledzenie adresów kryptowalutowych. Czy polska policja ma jakiekolwiek narzędzie pomagające namierzać tzw. brudne kryptowaluty? Nie, choć mogła je mieć. Zamiast tego korzysta z amerykańskich rozwiązań, niespecjalnie dostosowanych do naszych potrzeb. Podobnie będzie z AI” – zaznacza prof. Krzysztof Piech.

Do tego Jakub Martenka dodaje, że liczba tzw. deepfake'ów stale rośnie. Choć początkowo były to dość prymitywne narzędzia, których efekty odbiegały od rzeczywistych nagrań, obecnie stanowią poważne zagrożenie dla bezpieczeństwa osób publicznych, ze względu na rosnącą jakość generowanych materiałów. Coraz doskonalsze modele sprawiają, że odróżnienie prawdy od fałszu staje się naprawdę trudne. Choć widzimy osobę i słyszymy jej głos, to często mamy do czynienia z bezprawnym użyciem wizerunku oraz manipulacją. To oznacza, że dochodzimy

do momentu, w którym większość społeczeństwa po obejrzeniu spreparowanego materiału nie jest w stanie rozpoznać, że jest fałszywy.

Ponadto Jakub Martenka podkreśla, że często spontanicznie podejmujemy decyzje zakupowe. Te dotyczące inwestycji zawsze powinny być bardziej odpowiedzialne i dobrze przemyślane. Oszuści mogą kusić różnymi typami aktywów, bo wykorzystują nie tylko kryptowaluty. W opinii eksperta z Ar10, dziś mamy problem z tym, jak są traktowane kryptowaluty. Z powodu wielu tego typu oszustw pojawiło się sporo treści sugerujących straty. To sygnalizuje potencjalne zagrożenie, ale jednak nie pojawia się więcej komunikatów edukacyjnych. Wynika to też z tego, że takie treści przysłowiowo się nie klikają. „Problemem jest brak podstaw wiedzy i higieny finansowej Polaków. To są kwestie, o których trzeba uczyć nie tylko dzieci w szkołach. Należy też prowadzić szerokie kampanie informacyjne adresowane do różnych grup społecznych, wykorzystując kanały dotarcia specyficzne dla nich. To może być np. wpłatanie treści edukacyjnych do telenowel chętnie oglądanych przez seniorów. Pomysł został sprawdzony już kilkanaście lat temu w Wielkiej Brytanii” – analizuje prof. Krzysztof Piech.

Z kolei Aleksander Łapiński zaznacza, że skala problemu z oszustwami inwestycyjnymi jest ogromna, zarówno w Polsce, jak i na świecie. Przestępcy wykorzystują naiwność lub wręcz zaślepienie ofiary, obiecując szybki i łatwy zysk bez ryzyka. Jak dodaje ekspert, w naszym kraju CERT Polska oraz UKNF od dawna prowadzą kampanie mające na celu edukację użytkowników w tym zakresie. Według CERT Orange, oszustwa związane z fałszywymi inwestycjami są jednym z najczęstszych rodzajów stron internetowych, na które użytkownicy są kierowani w wyniku takich kampanii. „Przed decyzją o przesłaniu bądź wydaniu komukolwiek naszych pieniędzy, należy dobrze się zastanowić i skonsultować z innymi. Przykładowo jest na Facebooku grupa, na którą prawie codziennie przychodzą zapytania o sprawdzenie, czy dany podmiot lub projekt jest

oszustwem. Niestety, w ponad 90% przypadkach jest już za późno, żeby pomóc takim osobom. Zgłaszają się z reguły już po szkodzie, tj. po przekazaniu oszustom pieniędzy. Jeśli nie wiesz, na czym polegają i jak działają kryptowaluty, a jedynie słyszałeś o możliwościach zysków, to lepiej zrezygnuj. Jest dla Ciebie za wcześnie” – podsumowuje prof. Krzysztof Piech.

Źródło: MondayNews.pl