AI może ukraść Polakom PESEL i pozbawić ich oszczędności!

Kategoria: Styl życia
Opublikowano: czwartek, 04, kwiecień 2024 09:29
Katarzyna Sekuła

38 proc. Polaków, którzy mają doświadczenie z wykorzystaniem sztucznej inteligencji (AI), obawia się, że w przyszłości mogą zostać zastąpieni przez nią w pracy. Jeszcze większy odsetek, bo aż 43 proc., jest przekonany, że ta technologia zawsze udziela odpowiedzi zgodnych z prawdą. Ten fakt coraz częściej wykorzystują cyberprzestępcy. Używają oni AI m.in. do wyłudzania danych osobowych czy loginów i haseł do różnych kont oraz aplikacji, w tym bankowych. Oszuści podszywają się też np. pod członków najbliższej rodziny przy pomocy fałszywego głosu, stworzonego w oparciu o sztuczną inteligencję. Metody różne, cel ten sam – wyłudzenie pieniędzy.

O ile dywagacje o tym, kto straci pracę przez sztuczną inteligencję, a kto dzięki niej zyska, przypominają na razie wróżenie z fusów, to zagrożenia związane z jej wykorzystaniem przez cyberprzestępców są bardzo realne. Z badania Deloitte Digital Consumer Trends 2023 na próbie ponad 2 tys. polskich internautów w wieku od 18 do 65 lat wynika, że 47 proc. z tego grona słyszało o generatywnej sztucznej inteligencji, a ponad połowa z tej grupy przynajmniej raz z niej korzystała.

Niepokojące jest to, że 43 proc. respondentów, którzy mają doświadczenie w używaniu AI, błędnie sądzi, że zawsze udziela ona odpowiedzi obiektywnych i zgodnych z prawdą. W zderzeniu z powszechnym jej wykorzystywaniem przez cyberprzestępców będzie to niechybnie prowadziło do tego, że coraz częściej będziemy padali ofiarą wyłudzeń. Prokuratura Krajowa nie prowadzi co prawda na razie statystyk spraw, w których posłużono się sztuczną inteligencję (AI) lub uczeniem maszynowym (ML), ale na podstawie analizy zaistniałych już przypadków przewiduje, że oszuści będą stosować coraz częściej tę technologię nie tylko do zdobycia dostępów do kont bankowych lub systemów biznesowych, lecz także profili w mediach społecznościowych, stalkowania czy pisania fałszywych e-maili i SMS-ów w celu wyłudzenia danych osobowych.

Phishing niemal idealny

– Kreatywność cyberprzestępców jest bardzo duża, zapewne jeszcze nie raz zostaniemy zaskoczeni ich pomysłami. Jednym z najprostszych zastosowań sztucznej inteligencji do wyłudzenia danych osobowych jest phishing, czyli wysyłanie e-maili podszywających się pod jakąś instytucję, w których jesteśmy proszeni o podanie danych osobowych, albo przekierowywani do fałszywych stron internetowych. Dotychczas można je było łatwo odróżnić, bo z reguły zawierały mnóstwo błędów gramatycznych czy ortograficznych. Wykorzystanie modeli językowych to eliminuje. Można AI nauczyć stosowania określonego stylu i zrobi to bezbłędnie – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

To jednak nie wszystko. W ubiegłym roku Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Komisji Nadzoru Finansowego (CSIRT KNF) ostrzegał m.in. przed wprowadzającymi w błąd reklamami platform inwestycyjnych, w których podszywano się pod znane instytucje lub osoby, w tym polityków. W kwietniu 2023 r. oszuści najczęściej wykorzystywali wizerunek Baltic Pipe (30 proc.), PGNiG (26 proc.), Tesli (11 proc.), spółek Skarbu Państwa (4 proc.) i banków (3 proc.).

– Takie reklamy zamieszczane w mediach społecznościowych również przekierowywały do fałszywych podstron z formularzami wymagającymi np. rejestracji. Pozyskane w ten sposób dane mogą prędzej czy później zostać wykorzystane do wyłudzeń – dodaje Bartłomiej Drozd.

Przykłady można mnożyć. W 2023 roku pojawiły się reklamy stworzone przy pomocy AI, które prowadziły do oficjalnego sklepu Google Play. Zachęcano w nich do pobrania niebezpiecznej aplikacji, której instalacja pozwoliłaby przestępcom przejąć kontrolę nad komputerem czy smartfonem. W ten sposób mogą oni uzyskać dostęp do znajdujących się na urządzeniu danych osobowych czy loginów i

haseł do kont bankowych. Z kolei Naukowa i Akademicka Sieć Komputerowa (NASK) ostrzegała przed oszustami podszywającymi się pod Allegro, którzy wysyłali e-maile sugerujące otrzymanie od serwisu premii lojalnościowej.

Nie udostępniaj własnego głosu w mediach społecznościowych

Cyberprzestępcy stosują również technikę deepfake, która przy użyciu sztucznej inteligencji umożliwia nie tylko stworzenie fałszywych filmów i obrazów, lecz także podszycie się pod członka najbliższej rodziny. Wystarczy, że oszuści będą mieć dostęp do nagrania głosowego z naszym udziałem, które pozyskają np. z mediów społecznościowych. Niestety przed tym zjawiskiem jest się bardzo trudno uchronić.

Z ankiety przeprowadzonej przez McAfee na ponad 7000 respondentów z siedmiu krajów wynika, że 53 proc. z nich dzieli się swoim głosem w Internecie przynajmniej raz w tygodniu. Z kolei 10 proc. ankietowanych osobiście doświadczyło próby oszustwa z wykorzystaniem fałszywego głosu w oparciu o sztuczną inteligencję, a kolejne 15 proc. zna osobę, która była celem takiego ataku. W Polsce na razie żadna instytucja nie prowadzi odrębnych statystyk dla przestępstw, w których wykorzystano AI. Jednak bez wątpienia jest to bardzo poważny problem, skoro ostrzega przed nim Instytut Wymiaru Sprawiedliwości, CSIRT KNF czy NASK.

Źródło: IP