**AI zagraża urządzeniom mobilnym!**

**AI nie tylko wyręcza nas w coraz większej liczbie obowiązków, ale również staje się coraz większym zagrożeniem dla cyberbezpieczeństwa. Eksperci Check Point Research zwracają uwagę, że najbardziej podatni na złośliwe działania cyberprzestępców jesteśmy korzystając z urządzeń mobilnych. Jak wynika z badań, aż 75% pracowników korzysta obecnie ze swoich prywatnych smartfonów w miejscu pracy, a niemal 83% firm decyduje się na wdrożenie u siebie polityki BYOD. Oznacza to, że słabo kontrolowane mobilne urządzenia osobiste mogą być głównym źródłem zagrożeń dla firm.**

Ja: *Czy możesz zostać wykorzystany do cyberataków?*

ChatGPT: *Jako model językowy sztucznej inteligencji nie mam własnej agendy ani intencji. Jednak, jak każda technologia, mogę potencjalnie zostać wykorzystany przez osoby o złych zamiarach.*

*Ostatecznie odpowiedzialność za wykorzystanie i potencjalne niewłaściwe użycie systemów AI spoczywa na użytkownikach. Ważne jest, aby osoby i organizacje korzystały z technologii AI w sposób etyczny i odpowiedzialny, przestrzegając prawnych i etycznych wytycznych oraz podejmując środki ostrożności, aby zapobiec wszelkim szkodom lub nadużyciom*.

**W tej rozmowie ChatGPT się nie myli…**

Narzędzia generatywnej sztucznej inteligencji (AI), takie jak Chat GPT i Google Bard, zyskują popularność na całym świecie. Pozwalają użytkownikom zwiększyć wydajność i produktywność w codziennych zadaniach i obowiązkach.

Jednak część z ich możliwości może być niewłaściwie wykorzystanych – np. do tworzenia [złośliwych programów](https://techcrunch.com/2023/01/10/app-store-and-play-store-are-flooded-with-dubious-chatgpt-apps/), z których wiele pojawiło się w oficjalnych sklepach z aplikacjami. Generatywna sztuczna inteligencja została wykorzystana również do tworzenia e-maili i kampanii phishingowych, czy generowania fałszywych filmów na YouTube.

Niestety firmy zajmujące się generatywną sztuczną inteligencją nie radzą sobie z tymi problemami. W [niedawnym raporcie](https://blog.checkpoint.com/security/lowering-the-bard-check-point-researchs-security-analysis-spurs-concerns-over-google-bards-limitations/?mkt_tok=NzUwLURRSC01MjgAAAGNCTLbiiH9gGnbw_0b5toQiI8PbHVDEb23VwQC9H8rmqOprseV6vMDFwSfiKzkTqG6ssJGHErYmQixOK8MdEaZfKfrwxaceaodJrDgmgK4_8mXK9Aq) zespół Check Point Research udowodnił, że Bard nie nakłada prawie żadnych ograniczeń na tworzenie wiadomości phishingowych i że przy małych zmianach można go wykorzystać do tworzenia keyloggerów i innego złośliwego oprogramowania, co stanowi zagrożenie dla bezpieczeństwa.

Z tych powodów niektóre firmy zdecydowały się zakazać korzystania z narzędzi sztucznej inteligencji na urządzeniach lub w sieciach korporacyjnych, natomiast część innych, które umożliwiały pracownikom dostęp do generatywnych narzędzi sztucznej inteligencji, padła ofiarą [wycieku wrażliwych danych.](https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/?guccounter=1&amp;amp;guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&amp;amp;guce_referrer_sig=AQAAAE0IHKl7t3ZVcNrvBXBRWxo5nCwKaK1ACkiQZ_gzTzYU8uh6n58BCUeDu1utMSdomjRKcnvVRqhnUuKpGrQ-GlWFz0LkJM7invUFlLVNcn0mbDJtSF8dIfib0JAWGmcM6XERVOnvhs6jX1ay_jB8RhzhW_GMLAtY8aGHpN5lp-q0)

Dlatego dopóki nie będą dostępne odpowiednie środki chroniące wrażliwe dane przed wyciekiem i kradzieżą informacji wewnętrznych, firmy powinny zachować szczególną ostrożność w swoich politykach bezpieczeństwa.

Eksperci Check Point Research zauważają, że urządzenia mobilne nie są wyjątkiem. W rzeczywistości użytkownicy mobilni częściej pobierają złośliwe aplikacje lub padają ofiarą prób phishingu. Mniejsze ekrany urządzeń mobilnych, duża liczba aplikacji i powiadomień mogą rozpraszać użytkowników, utrudniając im unikanie otwierania złośliwych łączy lub pobierania złośliwych plików. Dla wielu z nas sieci społecznościowe są najczęściej używanymi aplikacjami na naszych smartfonach, co oznacza, że użytkownicy mobilni są również bardziej narażeni na socjotechnikę i phishing.

Ponadto zacierają się granice między osobistym i zawodowym korzystaniem z urządzeń mobilnych, co czyni je głównym punktem wejścia do organizacji, więc [ochrona przed zagrożeniami AI](https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-cyber-security/) powinna być najwyższym priorytetem.

**Co należy zrobić, aby chronić swoją mobilną flotę przed zagrożeniami AI?**

l Najważniejszą rzeczą do uświadomienia sobie jest to, że użytkownikom urządzeń mobilnych nie można ufać. Ataki są coraz częstsze i bardziej wyrafinowane, a teraz są zbyt zaawansowane i skomplikowane, aby mógł je wykryć człowiek. Klasycznym przykładem są strony phishingowe, które ewoluowały tak bardzo, że wyglądają tak samo jak oryginalna strona. Aby poradzić sobie z tym poziomem zaawansowania, potrzebujesz zaawansowanej technologii do ochrony urządzenia i zapobiegania przedostawaniu się zagrożeń do Twojej organizacji.

l Urządzenia mobilne to punkt wejścia do Twojej organizacji. Sztuczna inteligencja ewoluuje tak szybko, że wykrywanie i naprawianie błędów to za mało. Twoje rozwiązanie bezpieczeństwa mobilnego musi zawierać funkcje zapobiegawcze, aby powstrzymać zagrożenie na poziomie urządzenia, zanim uzyskasz dostęp do zasobów korporacyjnych.

l Możliwości uczenia się generatywnej sztucznej inteligencji są przytłaczająco imponujące. Aby nadążyć, musisz używać sztucznej inteligencji do walki z sztuczną inteligencją. Upewnij się, że Twoje rozwiązanie zabezpieczające wykorzystuje sztuczną inteligencję i technologię uczenia maszynowego, aby zachować przewagę.