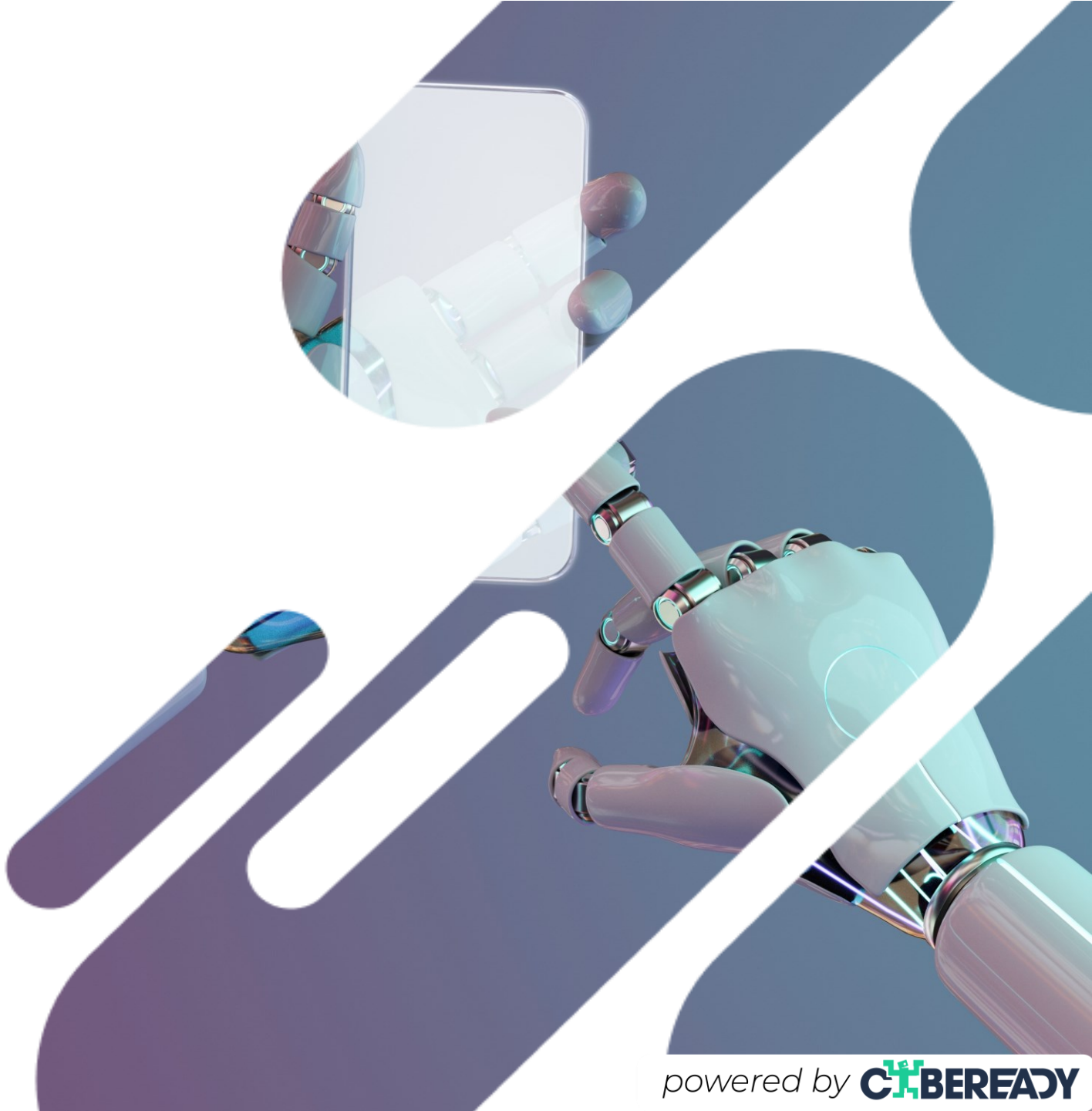
CYBEREADY

Narzędzia AI zmieniają zasady gry dla hakerów.

Czy jesteś przygotowany?



Wcześniej...

Wysoce zwodnicze ataki wymagały dużo czasu i wysiłku i mogły być tworzone jedynie przez wykwalifikowanych hakerów.

W rezultacie **większość prób phishingu była na poziomie początkującym** (np. z błędami ortograficznymi, dziwnymi układami, kaleczoną gramatyką itp.), dlatego wykrycie oszustwa było dość łatwe.

Obecnie...

Narzędzia sztucznej inteligencji umożliwiają hakerom szybkie i łatwe tworzenie bardzo profesjonalnie wyglądających e-maili i treści.

Z tego powodu **na nasze skrzynki pocztowe zaczęły docierać bardziej wyrafinowane ataki.** Te wysoce zwodnicze ataki są trudniejsze do zidentyfikowania jako zagrożenia, co zwiększa ryzyko, że damy się na nie nabrać.

Jak teraz wykryć phishing?

- W wiadomościach e-mail upewnij się, że **adres nadawcy** wygląda dokładnie tak, jak się tego spodziewasz. Hakerzy nie są w stanie podrobić tego szczegółu.

- Najedź kursorem na **linki** przed kliknięciem, aby upewnić się, że wyglądają na prawdziwe. Hakerzy mogą imitować wzory znanych firm, ale nie są w stanie używać ich oryginalnych domen.

Co nie jest już wiarygodnym znakiem autentyczności?

- Profesjonalny wygląd
- Dobrze napisany tekst
- Nagranie głosu kogoś, kogo znasz
- Wysokiej jakości filmy wideo

CYBERREADY

Pamiętaj: Nasze bezpieczeństwo jest w naszych rękach.

Wyrób sobie nawyk sprawdzania każdego e-maila przed kliknięciem jakichkolwiek linków i nigdy nie sprawdzaj wiadomości w stanie rozproszenia.