AI Skills, Powered by Values

values

www.valuesai.eu

MODUŁ 05

Prywatność danych oraz bezpieczne użytkowanie narzędzi AI

Udostępniaj mniej. Chroń więcej.
Korzystaj z sztucznej inteligencji
w sposób odpowiedzialny.

Co-funded by the European Union

Współfinansowane przez Unię Europejską. Wyrażone poglądy i opinie są wyłącznie poglądami i opiniami autora lub autorów i niekoniecznie odzwierciedlają stanowisko Unii Europejskiej ani Fundacji Rozwoju Systemu Edukacji. Ani Unia Europejska, ani instytucja przyznająca grant nie ponoszą za nie odpowiedzialności.

Zawartość

y Values

Co-funded by the European Union

Współfinansowane przez Unię Europejską. Wyrażone poglądy i opinie są wyłącznie poglądami i opiniami autora lub autorów i niekoniecznie odzwierciedlają stanowisko Unii Europejskiej ani Fundacji Rozwoju Systemu Edukacji. Ani Unia Europejska, ani instytucja przyznająca grant nie ponoszą za nie odpowiedzialności.

01

Dlaczego bezpieczeństwo danych jest istotne w kontekście sztucznej inteligencji

(15 minut)

Dane oraz sztuczna inteligencja

Udostępnianie danych sztucznej inteligencji w miejscu pracy wiąże się z ryzykiem, ponieważ może prowadzić do ujawnienia informacji, naruszeń przepisów oraz szkód wizerunkowych lub operacyjnych, jeśli dane wejściowe zostaną zapisane, ponownie wykorzystane lub wyciekają do modeli innych firm.

AI Skills,
Powered
by Values
values

Kluczowe zagrożenia

- **Ujawnienie danych wrażliwych**: monity lub pliki przesyłane do platform AI mogą być przechowywane lub pojawić się w wynikach modelu, co może prowadzić do ujawnienia własności intelektualnej, danych osobowych klientów lub zapisów finansowych.
- **Shadow AI i niekontrolowane wykorzystanie**: pracownicy korzystający z nieautoryzowanych narzędzi AI tworzą martwe strefy, w których dane wymykają się spod kontroli korporacyjnej, a dostawcy mogą przechowywać lub ponownie wykorzystywać dane wejściowe.
- **Naruszenia przepisów prawnych i zgodności**: korzystanie z zewnętrznych usług AI bez odpowiednich umów lub porozumień dotyczących przetwarzania danych może prowadzić do naruszenia przepisów o ochronie prywatności i skutkować sankcjami.
- **Brak przejrzystości i możliwości audytu**: wielu dostawców sztucznej inteligencji nie ujawnia, w jaki sposób przechowywane są dane wejściowe, gdzie są przetwarzane ani czy są wykorzystywane do trenowania modeli, co utrudnia ocenę ryzyka.
- **Rozszerzona powierzchnia ataku**: integracja sztucznej inteligencji zwiększa podatność techniczną (interfejsy API, wtyczki, punkty końcowe), którą mogą wykorzystać atakujący do uzyskania dostępu do danych.

Trzy negatywne konsekwencje: prywatność, niesprawiedliwość i iluzoryczne zaufanie

01

Ryzyko naruszenia prywatności (eksponowanie):

Nadmierne udostępnianie informacji może prowadzić do ujawnienia danych osobowych, poufnych lub pochodzących od osób trzecich, czasami nawet w sposób pośredni.

02

Ryzyko integralności (szkoda)

Jeżeli dane są stronnicze, niekompletne lub zawierają niesprawiedliwe etykiety, wyniki sztucznej inteligencji mogą potęgować stereotypy lub dyskryminować określone grupy.

03

Ryzyko niezawodności (błędne zaufanie):

Sztuczna inteligencja potrafi generować płynne odpowiedzi, które brzmią poprawnie, nawet gdy dane wejściowe są słabe, pozbawione kontekstu lub mylące.

CO WOLNO

- **Zapytaj**: Czego brakuje? Kogo brakuje? Czy ten wynik może zaszkodzić komuś?
- **Kontrola użytkowania**: Consent Gate + Fair Data Check + SAFE Workflow Ladder

CZEGO NIE WOLNO

- **Traktuj wyniki sztucznej inteligencji jako obiektywną prawdę.**
- **Wykorzystuj wyniki sztucznej inteligencji do oceny ludzi lub podejmowania decyzji bez uwzględnienia kontekstu.**

Soczewka wartości.

Bezpieczne dane to mądre wybory oparte na wartościach.

Za każdym razem, gdy korzystasz ze sztucznej inteligencji opartej na danych, zadaj sobie cztery pytania dotyczące wartości:

1. **Decyzyjność**: Czy podejmuję świadomy wybór, czy klikam automatycznie?
2. **Prywatność**: Czy udostępniam więcej informacji (o sobie lub innych), niż jest to konieczne?
3. **Uczciwość**: Czy wykorzystanie moich danych może zaszkodzić komuś lub wyrządzić szkody?
4. **Przejrzystość**: Czy mogę przedstawić, jakie dane zostały wykorzystane i z jakiego powodu?

Szczególne kategorie danych osobowych.

Przy udostępnianiu tych danych systemom sztucznej inteligencji należy zachować szczególną ostrożność.

1. Dane osobowe
2. Dane poufne
3. Informacje zdrowotne
4. Dane finansowe
5. Dane do logowania
6. Dane Klienta
7. Wewnętrzne dokumenty administracyjne
8. Nieopublikowane wyniki badań
9. Dane objęte tajemnicą handlową

02

Jak bezpiecznie dzielić się danymi?

(15 minut)

Zanim rozpoczniesz korzystanie ze sztucznej inteligencji: Twoje dane wejściowe stają się danymi.

Wiele osób koncentruje się na tym, na jakie pytania odpowiada sztuczna inteligencja.

Bezpieczne dane zaczynają się na wcześniejszym etapie:
zależą od tego co wpisujesz, wklejasz lub przesyłasz.

W praktyce narzędzia sztucznej inteligencji mogą współpracować z:

- tekstem (monity, wiadomości, skopiowana treść)
- plikami (dokumenty, arkusze kalkulacyjne, pliki PDF)
- obrazami (fotografie, zrzuty ekranu)
- kontekstem (szczegóły umożliwiające wyciąganie wniosków)

Zanim rozpoczniesz korzystanie ze sztucznej inteligencji: Twoje dane wejściowe stają się danymi.

Jeśli udostępnisz zbyt wiele, możesz narazić się na ryzyko, które jest trudne do odwrócenia: zagrożenie dla prywatności, wyrządzenie szkody innym oraz publikowanie nieuczciwych lub wprowadzających w błąd treści.

Bezpieczne korzystanie ze sztucznej inteligencji rozpoczyna się od podstawowego nawyku: udostępniaj jedynie niezbędne informacje lub w ogóle ich nie udostępniaj.

Co wolno

- **Pamiętaj**: Wszystko, co wpisujesz, wklejasz lub przesyłasz, stanowi dane, którymi się dzielisz.

Czego nie wolno

- **NIE ZAKŁADAJ:** „To jedynie tekst” lub „To tylko szybka wiadomość”.

„Wygląda na nieszkodliwe”, ale takie nie jest (mit a rzeczywistość)

Mit

„Będzie bezpieczniej, jeśli usunę nazwę.”

Fakt

Ludzi można zidentyfikować pośrednio za pomocą kombinacji takich jak:

- wiek + miasto + szkoła/staż
- unikatowe szczegóły wydarzenia
- zrzuty ekranu z wyraźnymi, drobnymi wskazówkami
- wzorce lokalizacji i czasu

Mit

„To tylko zrzut ekrany, jest bezpieczny.”

Fakt

Zrzuty ekranu często zawierają imiona, twarze, dane kontaktowe lub kontekst, który może umknąć Twojej uwadze.

Zadanie: Zidentyfikuj sygnały ostrzegawcze

Zadanie (60–90 sekund):

Oznacz każdą pozycję jako Nigdy / Unikaj / Zwykle w Porządku:

- Kod do resetowania hasła
- CV z kompletnym adresem i numerem telefonu
- Zrzut ekranu czatu z widocznymi nazwami użytkowników
- Pytanie ogólne: „Jak stworzyć CV?”
- Lista szkół zawierająca nazwy oraz adresy e-mail.
- Podsumowanie ankiety zawierające jedynie sumy (bez nazwisk)

Nigdy nie wiesz.

- Nie zawsze jest oczywiste, gdzie odbywa się przetwarzanie danych.
- Dane mogą być archiwizowane w historii rozmów.
- Mogą być wykorzystywane do doskonalenia usług, w zależności od ustawień oraz warunków korzystania z usługi.
- Użytkownik może nieumyślnie ujawnić poufne informacje.

03

Prywatność, prawa oraz zgoda

(15 minut)

Zdecyduj, zanim podzielisz się danymi o innych osobach.

Używaj tej metody zawsze, gdy Twoje dane wejściowe zawierają informacje pochodzące od innych osób (wiadomości, zdjęcia, listy, opowieści, dokumenty).

Zadaj trzy pytania:

- **Prawo/pozwolenie**: Czy posiadam pozwolenie (lub wyraźne prawo) na wykorzystanie tych danych przez sztuczną inteligencję?
- **Ryzyko**: Czy może to kogoś zidentyfikować, zawstydzić lub skrzywdzić w chwili obecnej lub w przyszłości?
- **Bezpieczniejsza alternatywa**: Czy mogę zrealizować cel, korzystając z mniejszej ilości danych (lub nie wykorzystując żadnych danych osobowych)?

Reguła

Jeśli na jakiekolwiek pytanie odpowiesz „Nie” lub „Nie mam pewności”, nie przesyłaj danych. Wybierz bezpieczniejszy sposób pracy (np. zadaj ogólne pytanie bez ujawniania danych osobowych). „Nie mam pewności” to sygnał ostrzegawczy.

Zgoda oraz dane innych osób: na czym polega odpowiedzialne wykorzystanie danych.

Prywatność i prawa to nie tylko zagadnienia techniczne – dotyczą one szacunku oraz zapobiegania szkodom.

CO WOLNO

Dozwolone (bezpieczniejsze opcje):

- Poproś o zgodę i uszanuj odpowiedź „nie”.
- Zastąp nazwy rolami: Osoba A / przyjaciel / nauczyciel / kolega.
- Usuń szczegóły unikalne (konkretne lokalizacje, daty, identyfikatory).
- Zadaj ogólne pytanie: „W jaki sposób mogę wesprzeć przyjaciela w trudnej sytuacji?” (bez osobistej historii)

CZEGO NIE WOLNO

Niedozwolone (znaczne ryzyko):

- Wklejanie prywatnych wiadomości innej osoby do AI „w celu uzyskania porady”.
- Prześlij listy grupowe zawierające nazwy i adresy e-mail w celu ich „uporządkowania”.
- Dziel się osobistymi historiami o innych, nie zadając pytań.

Szybkie ćwiczenie: czy reguła zgody jest spełniona?

Instrukcje

W każdym scenariuszu podejmij decyzję: spełniona (wystarczająco bezpiecznie), niespełniona (wybrać bezpieczniejszą opcję). Następnie podaj jeden krótki powód.

- „Podsumuj list z opinią mojego nauczyciela, zawierający imię i nazwisko nauczyciela oraz nazwę szkoły.”
- „Proszę o pomoc w napisaniu przeprosin. Opiszę sytuację, nie wklejając całego czatu.”
- „Przeanalizuj listę wolontariuszy, która zawiera imiona, nazwiska oraz numery telefonów, aby zidentyfikować osoby „niegodne zaufania”.

Czy mam prawo do korzystania z tych danych?

Bezpieczne korzystanie ze sztucznej inteligencji to nie tylko kwestia prywatności, ale także praw: czy masz prawo do używania, udostępniania lub przetwarzania danych, zwłaszcza gdy należą one do innej osoby lub organizacji.

Zazwyczaj nie masz prawa do dzielenia się z sztuczną inteligencją:

- Prywatnymi wiadomościami innych użytkowników (nawet jeśli uczestniczysz w czacie)
- Listami osób (listy klasowe, listy wolontariuszy, listy klientów)
- Dokumentami, które nie są Twoją własnością (umowy, notatki działu HR, wewnętrzne e-maile)
- Osobistymi historiami, które zostały Ci powierzone w zaufaniu (zdrowie, relacje, problemy rodzinne)

Zazwyczaj przysługuje Ci prawo do korzystania z:

- Twojego osobisty tekstu, który nie zawiera żadnych poufnych informacji.
- Pytań ogólnych bez informacji osobowych
- Anonimizowanych przykładów, które samodzielnie stworzyłeś (fikcyjne lub zanonimizowane)

Zgoda: jak definiuje się „prawdziwą zgodę” (a czym nie jest?)

Zgoda to nie tylko „ktoś kiedyś powiedział tak”. W kontekście sztucznej inteligencji, zgoda:

- **Jest wydawana przez osobę doinformowaną**: osoba jest świadoma, co zostanie udostępnione oraz z jakiego powodu.
- **Jest konkretna**: zgoda na określony cel, a nie „cokolwiek zechcesz”
- **Jest dobrowolna**: bez przymusu, bez obaw o konsekwencje
- **Jest odwoływalna**: osoba ma możliwość zmiany zdania.
- **Ważne**: zgoda jest uzależniona od odbiorców oraz narzędzia. Ktoś może zgodzić się przekazać ci pewne informacje, ale nie wyrazić zgody na ich udostępnienie narzędziu opartemu na sztucznej inteligencji lub na ich przechowywanie w systemie.

Identyfikacja pośrednia: Kiedy „usunięcie nazw” okazuje się niewystarczające?

Ludzi można zidentyfikować nawet bez imion, jeśli szczegóły umożliwiają innym odgadnięcie, kim są.

Typowe identyfikatory pośrednie:

- Dokładny wiek, precyzyjna lokalizacja, szkoła/pracodawca, konkretne daty oraz wydarzenia związane z daną rolą („jedyna osoba, która…”)
- Kombinacje (wiek + miasto + pasja + okoliczność)
- Zrzuty ekranu z wyraźnymi wskazówkami (zdjęcia profilowe, nazwy grup)

Bezpieczniejsze opcje (wybierz jedną):

- **Streszczenie**: przedstaw sytuację bez ujawniania szczególnych detali.
- **Uogólnienie**: zakresy zastosowania (grupa wiekowa), rozległe obszary (region)
- **Oparcie na rolach**: Osoba A / Osoba B zamiast rzeczywistych tożsamości
- **Nie wysyłaj**: jeśli nie jesteś w stanie usunąć kontekstu identyfikującego

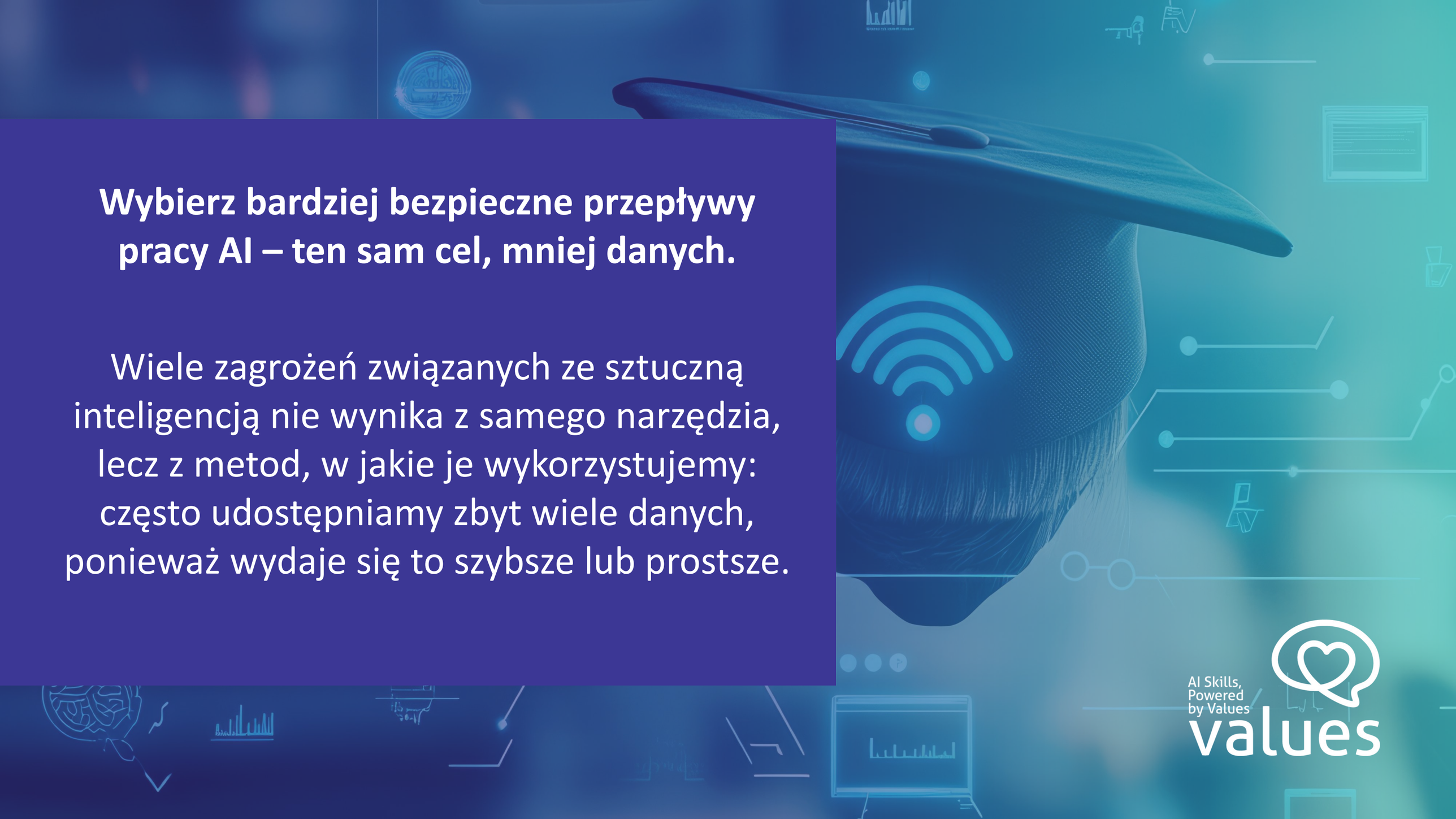
04

Wybór bardziej bezpiecznych przepływów pracy AI

(25 minut)

Wybierz bardziej bezpieczne przepływy pracy AI – ten sam cel, mniej danych.

Wiele zagrożeń związanych ze sztuczną inteligencją nie wynika z samego narzędzia, lecz z metod, w jakie je wykorzystujemy: często udostępniamy zbyt wiele danych, ponieważ wydaje się to szybsze lub prostsze.



AI Skills, Powered by Values

values

Chcesz wybrać bardziej bezpieczne przepływy pracy AI – ten sam cel, mniej danych.

Gdy udostępniasz dane sztucznej inteligencji, mogą być one przetwarzane, przechowywane i powielane.

Kiedy wprowadzasz, wklejasz lub przesyłasz dane do narzędzia AI, system musi je przetworzyć, aby wygenerować odpowiedź. W zależności od usługi i ustawień, Twoje dane mogą również:

- Przechowywane lub rejestrowane (w celu podniesienia jakości usług, rozwiązywania problemów, zapewnienia bezpieczeństwa lub zgodności)
- W niektórych przypadkach poddane przeglądowi (np. w celu zwiększenia bezpieczeństwa lub jakości)
- Użyte do dostosowania Twojego doświadczenia (w niektórych narzędziach)
- Odzwierciedlone w rezultatach
- Udostępniane pośrednio podczas kopiowania i wklejania wyników do innych aplikacji lub przesyłania zrzutów ekranu.

Chcesz wiedzieć, dlaczego ograniczenie udostępniania danych jest istotne?

- Zmniejszasz ryzyko naruszenia prywatności (Twoje dane nie mogą zostać ujawnione, jeśli ich nie udostępniłeś).
- Redukujesz ryzyko wyrządzenia szkody innym (mniej danych osób trzecich, mniej identyfikatorów).
- Zmniejszasz ryzyko wyciągnięcia niesprawiedliwych lub mylących wniosków (mniej „szumu”, więcej informacji skoncentrowanych na celu).
- Posiadasz większą kontrolę nad swoimi danymi.

Chcesz zapoznać się z SAFE Workflow Ladder?

Zasada stopu:

Jeśli nie masz możliwości usunięcia elementów wrażliwych lub poufnych → nie przesyłaj!

Jeśli potrzebujesz wsparcia ze strony AI, nie rozpoczynaj od przesyłania wszystkiego. Wybierz najbezpieczniejszy poziom, który nadal funkcjonuje.

- **Poziom 1 (najbezpieczniejszy)**: Zadaj pytanie ogólne (bez informacji osobistych).
  Przykład: „Jak stworzyć CV?”
- **Poziom 2:** Skorzystaj z anonimowego podsumowania (role, bez identyfikatorów).
  Przykład: „Osoba A i Osoba B miały spór dotyczący terminów – w jaki sposób mogę zareagować?”
- **Poziom 3**: Wykorzystuj ograniczone, zanonimizowane dane jedynie w przypadku konieczności.
  Przykład: „Oto zestawienia według kategorii (bez nazw). Proszę o pomoc w interpretacji trendów.”

Jak uczynić niebezpieczne zapytanie bezpiecznym (przed → po)

Zapytanie przed:

„Oto moje kompletne CV. Proszę o jego poprawę.”

Co jest ryzykowne: zbędne identyfikatory, dane kontaktowe osób trzecich, informacje, które można skopiować lub wykraść.

Zapytanie po:

„Proszę o poprawę sformułowania i struktury tego CV. Usunąłem dane osobowe. Proszę skupić się na klarowności, osiągnięciach oraz zwięzłym wyrażeniu.”

Reguła

Udostępniaj wzorzec i cel, a nie informacje osobiste.

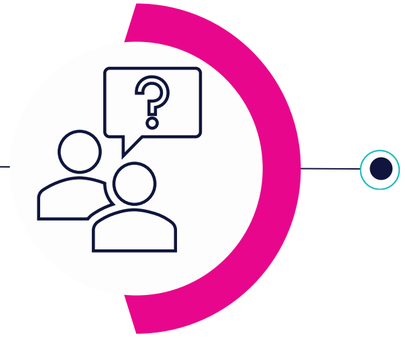
Bezpieczeństwo wyników: wyniki sztucznej inteligencji mogą również prowadzić do wycieku informacji.

Nawet jeśli udostępniasz informacje z ostrożnością, dane wyjściowe mogą wciąż zawierać poufne szczegóły, jeśli:

- Twój wkład zawierał informacje prywatne lub
- Sztuczna inteligencja powtarza to w podsumowaniu, na liście kontrolnej lub w projekcie wiadomości.

Bezpieczniejsze praktyki:

- Traktuj wyniki jako dokumenty: nie umieszczaj ich w publicznych czatach ani grupach.
- Przed udostępnieniem usuń nazwy, identyfikatory oraz unikalne szczegóły.
- Jeśli dane wyjściowe odnoszą się do konkretnej osoby, zachowaj je dla siebie lub przedstaw je w sposób bardziej ogólny.
- Przechowuj poufne dane wyjściowe w bezpiecznym miejscu lub usuń je, gdy przestaną być potrzebne.



Kluczowa aktywność: Przekształć niebezpieczne korzystanie ze sztucznej inteligencji w bezpieczne korzystanie ze sztucznej inteligencji (10 minut)

Będziesz doskonalić całą umiejętność, posługując się fikcyjnymi przykładami. Twoim celem jest formułowanie bardziej bezpiecznych żądań, które wciąż rozwiążą problem.

Dla każdego zapytania:

- Zidentyfikuj niebezpieczne elementy (Nigdy nie udostępniaj / Reguła zgody / Ryzyko integralności)
- Przepisz w sposób bezpieczny (minimalizuj, anonimizuj, streszczaj)
- Dodaj jeden wiersz FDC: „Czego może brakować lub co może być tendencyjne?”
- Wybierz przepływ pracy: Poziom 1 / Poziom 2 / Poziom 3 / Zatrzymaj

Rezultat:

- Krótki „Podręcznik bezpiecznego korzystania z danych”, który możesz wykorzystać w codziennym użytkowaniu sztucznej inteligencji.

Kluczowa aktywność: Przekształć niebezpieczne korzystanie ze sztucznej inteligencji w bezpieczne korzystanie ze sztucznej inteligencji (10 minut)

Ćwiczenie 1:

Zrzut ekranu rozmowy (prywatność + zgoda)

„Oto zrzut ekranu z rozmowy z moim znajomym [widoczne imiona]. Proszę, powiedzcie mi, kto ma rację i jak powinienem odpowiedzieć.”

Zadania etapowe:

- **NSL (Nigdy nie udostępniaj): Czego nigdy nie powinno się tutaj przesyłać?**
- **Reguła zgody: Czy posiadasz zgodę na udostępnianie tych danych?**
- **Bezpieczne przepisywanie (poziom 1 lub 2): Zasięgnij porady bez zrzutu ekranu.**
- **Granica sprawiedliwości: Czego może brakować w tej narracji?**

……. Linia FDC:……

Kluczowa aktywność: Przekształć niebezpieczne korzystanie ze sztucznej inteligencji w bezpieczne korzystanie ze sztucznej inteligencji (10 minut)

Ćwiczenie 2:

Lista osób (poufność + uczciwość)

„Proszę o przeanalizowanie tej listy wolontariuszy [z nazwiskami, numerami telefonów oraz problemami z frekwencją]. Oceń, kto zasługuje na zaufanie.”

Dlaczego to jest ryzykowne:

- Identyfikatory osobiste oraz dane osób trzecich
- Szkodliwy rezultat (klasyfikacja osób)
- Wysokie ryzyko integralności i oddziaływania
- **Twój bezpieczniejszy cel**: **zadaj pytanie dotyczące ulepszenia systemu, a nie oceniania jednostek.**

05

Niektóre informacje

(15 minut)

Kradzież danych i poświadczeń – zauważalny jest rosnący trend nielegalnego wykorzystywania danych przy użyciu sztucznej inteligencji.

„7% wzrost liczby ataków ransomware oraz innych destrukcyjnych incydentów. 23% wzrost liczby prób kradzieży danych uwierzytelniających.

Microsoft Threat Intelligence, „Raport Microsoft Digital Defense 2025: Oświetlanie ścieżki do bezpiecznej przyszłości" (Microsoft, 2025); https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

„Wielkość wycieku danych dla dziesięciu głównych rodzin ransomware wzrosła o 92,7%."

Zscaler ThreatLabz, „Raport Zscaler ThreatLabz 2025 dotyczący oprogramowania ransomware" (Zscaler, 2025); https://threatlabz.zscaler.com/

Kradzież danych i poświadczeń – zauważalny jest rosnący trend nielegalnego wykorzystywania danych przy użyciu sztucznej inteligencji.

„Liczba ataków ransomware na organizacje przemysłowe wzrosła o 87% w roku 2024.”

Dragos, ósmy coroczny przegląd cyberbezpieczeństwa OT jest już dostępny (2025); https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available.

Kradzież danych i poświadczeń – zauważalny jest rosnący trend nielegalnego wykorzystywania danych przy użyciu sztucznej inteligencji.

„Podmiot [...] w znacznym stopniu polegał na Claude w zakresie implementacji [złośliwego oprogramowania]”.

A. Moix, K. Lebedev, J. Klein, „Raport o zagrożeniach wywiadowczych: sierpień 2025” (Anthropic, 2025); https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pd

„Operatorzy ransomware APT INC zaimplementowali skrypt do niszczenia danych, prawdopodobnie autorstwa LLM.”

CrowdStrike, „Globalny raport o zagrożeniach CrowdStrike 2025” (CrowdStrike, 2025); https://www.crowdstrike.com/en-gb/global-threat-report/

Kradzież danych i poświadczeń – zauważalny jest rosnący trend nielegalnego wykorzystywania danych przy użyciu sztucznej inteligencji.

„[Google Threat Intelligence Group] zidentyfikowała rodzinę kodów, która wykorzystywała możliwości sztucznej inteligencji podczas wykonywania kodu, aby dynamicznie modyfikować zachowanie złośliwego oprogramowania. […] Atakujący wykraczają poza […] użycie narzędzi sztucznej inteligencji do wsparcia technicznego.”

Google Threat Intelligence Group, „GTIG AI Threat Tracker: Postępy w wykorzystaniu narzędzi AI przez podmioty stwarzające zagrożenie” (Google Threat Intelligence, 2025); https://services.google.com/fh/files/misc/advances-in-threat-actor-usage-of-ai-tools-pl.pdf

Kradzież danych i poświadczeń

Udział systemów sztucznej inteligencji w tym trendzie wydaje się być ograniczony i prawdopodobnie ma drugorzędne znaczenie w porównaniu do innych czynników. Jest jednak możliwe, że niektórzy złośliwi napastnicy nie przeprowadziliby ataków bez wykorzystania systemów opartych na sztucznej inteligencji.

Międzynarodowy raport dotyczący bezpieczeństwa sztucznej inteligencji 2026 (DSIT 2026/001, 2026); https://internationalaisafetyreport.org

Kradzież danych i poświadczeń

Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 r. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

Którym usługom internetowym najmniej ufasz w zakresie ochrony swoich danych osobowych?

Pamiętajmy, że sztuczna inteligencja jest obecnie szeroko wykorzystywana i często odgrywa kluczową rolę w świadczeniu usług oraz realizacji transakcji.

Kradzież danych i poświadczeń

Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 r. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

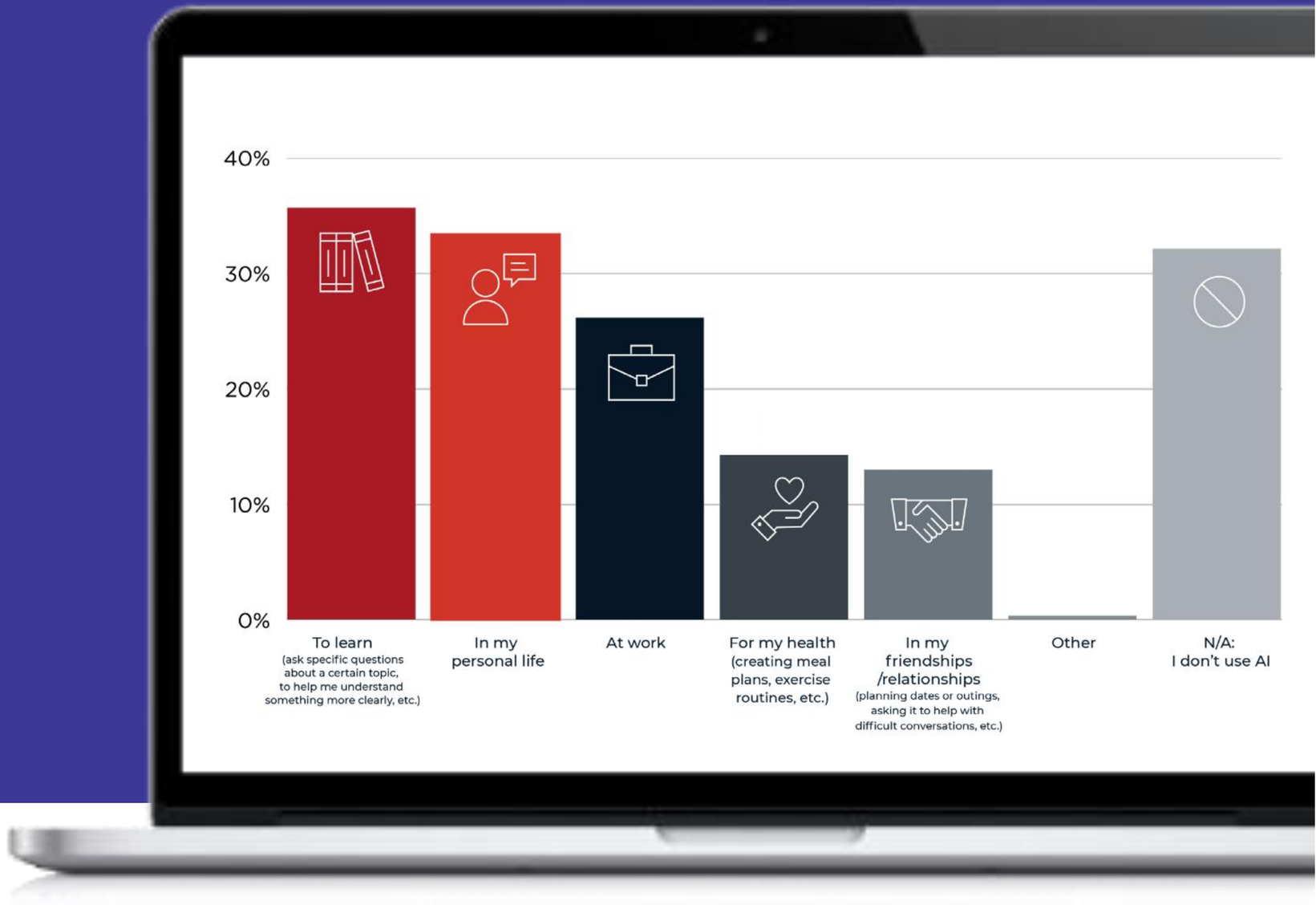
W jaki sposób aktualnie wykorzystujesz sztuczną inteligencję (AI)?

„Chociaż wiedza stanowi potęgę, rosnące zastosowanie sztucznej inteligencji w codziennym życiu uświadomiło wielu konsumentom jej potencjał. Doświadczają na własnej skórze, jak potężna może być ta technologia, gdy wykorzystują ją w swoich aplikacjach. Zauważają również coraz więcej informacji i danych dotyczących wzrostu zagrożeń bezpieczeństwa oraz cyberataków. W rezultacie zrozumiałe jest, że przyczynia się to do kryzysu zaufania wobec zdolności marek do ochrony danych osobowych konsumentów.”

Kradzież danych i poświadczeń

Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 r. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

W jaki sposób aktualnie wykorzystujesz sztuczną inteligencję (AI)?



Kradzież danych i poświadczeń - jakie masz obawy dotyczące sztucznej inteligencji w kontekście bezpieczeństwa tożsamości, jeśli takie występują?

Naruszenie mojej prywatności przez systemy sztucznej inteligencji.	27%
Phishing generowany przez sztuczną inteligencję.	27%
Sztuczna inteligencja jest wykorzystywana do nieautoryzowanego podszywania się pod mnie lub markę/osobę, z którą nawiązuję interakcję.	26%
Brak przejrzystości dotyczącej metod, w jakie systemy sztucznej inteligencji wykorzystują i przechowują moje dane osobowe.	25%
Zwiększone ryzyko cyberbezpieczeństwa – stanowiące zagrożenie dla bezpieczeństwa moich danych osobowych.	25%
Klonowanie głosu za pomocą sztucznej inteligencji	24%

Ciąg dalszy na kolejnym slajdzie

Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 roku. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

Kradzież danych i poświadczeń - jakie masz obawy dotyczące sztucznej inteligencji w kontekście bezpieczeństwa tożsamości, jeśli takie występują?

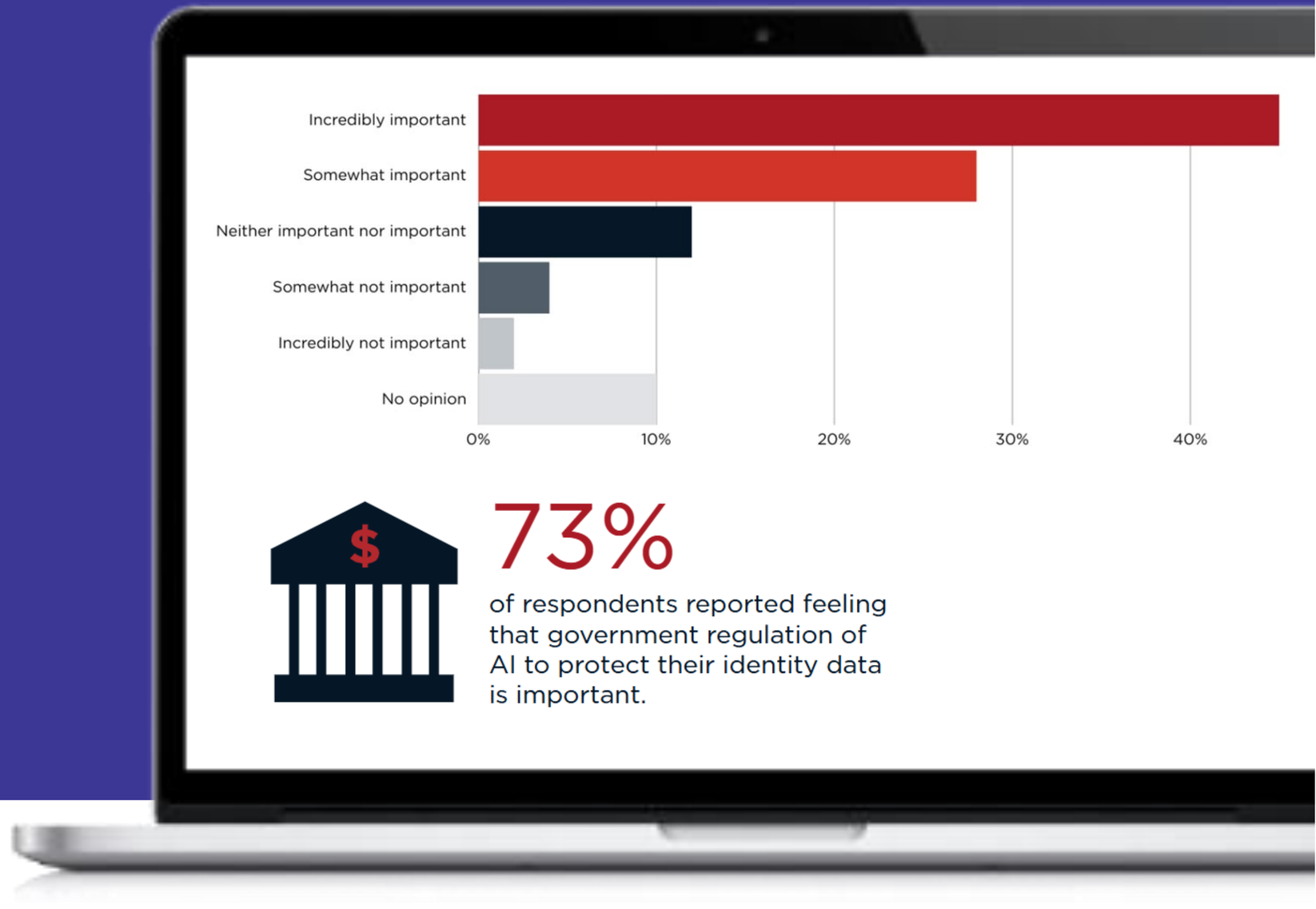
Deepfake’owe odwzorowania osób, które znam i którym ufam.	22%
Podszywanie się pod sztuczną inteligencję za pomocą chatbotów	20%
Brak precyzji/stronniczość w systemach sztucznej inteligencji	18%
Nie rozumiem, jakie mam zabezpieczenia prawne dotyczące sposobu, w jaki sztuczna inteligencja przetwarza moje dane.	18%
Autoryzacja sztucznej inteligencji do działania w moim imieniu	17%
Nie odczuwam żadnych obaw dotyczących sztucznej inteligencji oraz bezpieczeństwa tożsamości.	9%
Nie jestem pewien.	13%

Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 roku. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

Kradzież danych i poświadczeń

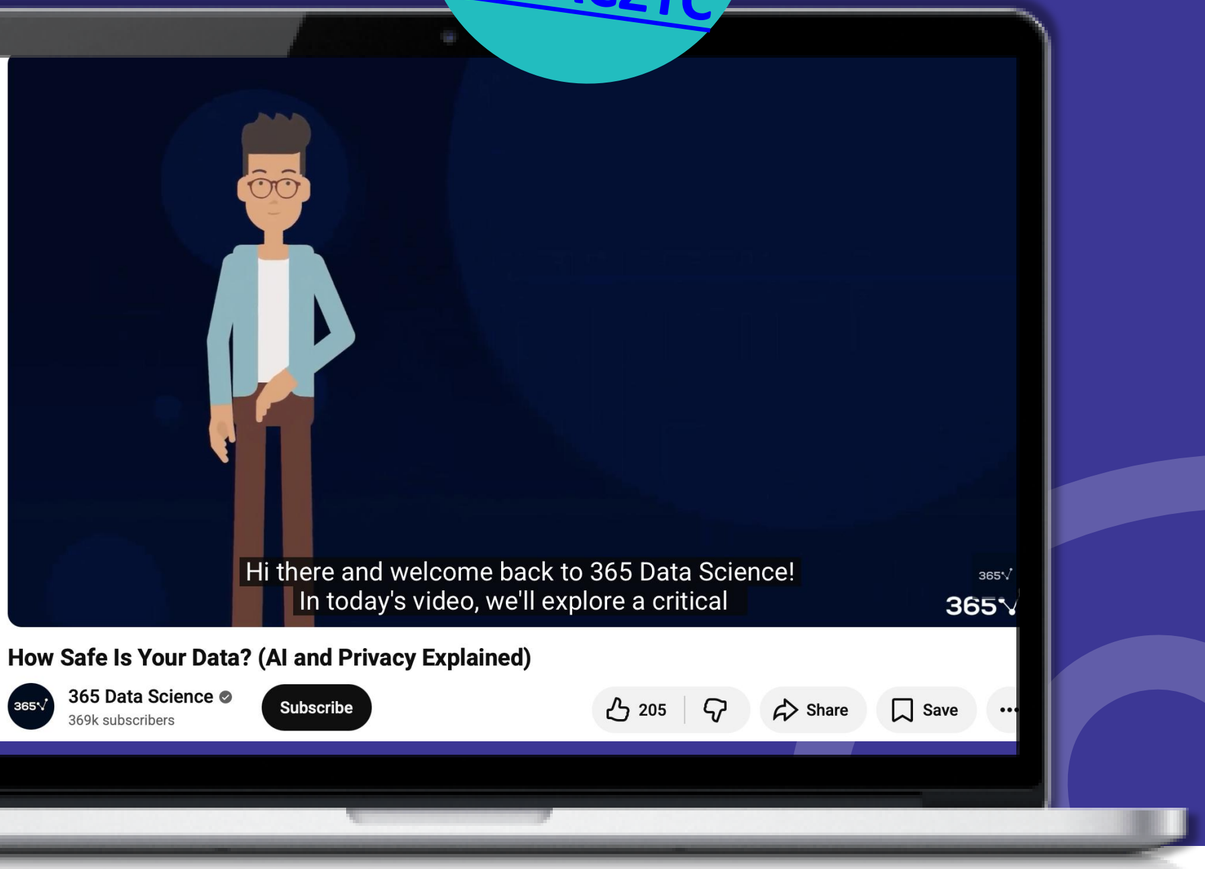
Ping Identity. (2024). Redukcja luki zaufania w erze sztucznej inteligencji: badanie konsumenckie z 2025 r. Ping Identity. https://www.pingidentity.com/en/lp/2025-consumer-survey.html

W jaki sposób aktualnie wykorzystujesz sztuczną inteligencję (AI)?



Kradzież danych i poświadczeń

KLIKNIJ, ABY ZOBACZYĆ



W dzisiejszej erze cyfrowej zabezpieczenie danych jest istotniejsze niż kiedykolwiek.

Film ten ukazuje skomplikowane interakcje między sztuczną inteligencją a danymi, którymi codziennie dzielimy się w sieci – od postów w mediach społecznościowych po nawyki zakupowe online.

AI Skills, Powered by Values

values

Śledź naszą wędrówkę

www.valuesai.eu

Co-funded by the European Union

Współfinansowane przez Unię Europejską. Wyrażone poglądy i opinie są wyłącznie poglądami i opiniami autora lub autorów i niekoniecznie odzwierciedlają stanowisko Unii Europejskiej ani Fundacji Rozwoju Systemu Edukacji. Ani Unia Europejska, ani instytucja przyznająca grant nie ponoszą za nie odpowiedzialności.