

MODUŁ 06

Sztuczna inteligencja oraz ślad
cyfrowy

Kontrola tego, co
pozostawiasz za sobą

Zawartość

01	Cyfrowy ślad (10 min)	3
02	Rodzaje śladów (15 min)	8
03	„Efekt domina”: konsekwencje dla Ciebie i innych (25 min)	15
04	Mój wybór: zwięzła lista kontrolna + mój plan działania (15 min)	25
05	Jak zabezpieczyć swój cyfrowy ślad (10 min)	35
06	Audyt, quiz oraz test (20 min)	39

Materiał dostępny na licencji Creative Commons CC BY 4.0
(<https://creativecommons.org/licenses/by/4.0/>).

by 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

Cyfrowy ślad (10 minut)

Czym jest cyfrowy ślad?

Cyfrowy ślad to zbiór informacji dotyczących osoby lub organizacji, które pozostają w sieci w wyniku ich aktywności online. Obejmuje on profile w mediach społecznościowych, posty, komentarze, historię przeglądania, zapytania wyszukiwania oraz dane automatycznie rejestrowane przez strony internetowe i aplikacje (np. pliki cookie, adres IP, dane lokalizacyjne).

Dlaczego Twój ślad cyfrowy ma znaczenie?

Twój ślad cyfrowy może wpływać na:



Prywatność



**kto i co wie o
tobie**



Reputację



**jak jesteś
postrzegany**



Bezpieczeństwo



**co może być
użyte w
niewłaściwy
sposób**



Inne osoby



**Twoje posty
mogą również
ujawnić innych**

Dlaczego Twój cyfrowy ślad jest istotny dla sztucznej inteligencji

Zadaj sobie pytanie:

Gdzie dostrzegam „decyzje algorytmiczne” w aplikacjach, których codziennie używam?



Sztuczna inteligencja integruje się z Twoim cyfrowym śladem, ponieważ:

- Sztuczna inteligencja często wykorzystuje dane behawioralne (kliknięcia, czas oglądania, polubienia, wyszukiwania) do przewidywania, czego będziesz pragnąć następnym razem.
- Twój bierny ślad (uprawnienia, sygnały lokalizacji, dane urządzenia) może wpływać na to, jakie wnioski systemy wyciągną na Twój temat.
- Sztuczna inteligencja ma zdolność wpływania na widoczność i zasięg (jakie treści są promowane, rekomendowane lub ukrywane).
- Twoje decyzje wpływają również na informacje dotyczące innych osób (tagowanie, udostępnianie zdjęć, zrzutów ekranu).

Wykorzystanie sztucznej inteligencji w zgodzie z wartościami

Pamiętaj:

Etyczna sztuczna inteligencja rozpoczyna się od codziennych decyzji cyfrowych.



Cztery pytania dotyczące wartości, którymi warto się kierować przy podejmowaniu decyzji cyfrowych (szczególnie w kontekście sztucznej inteligencji):

- **Decyzyjność:** Czy podejmuję świadomy wybór, czy też klikam automatycznie?
- **Prywatność:** Czy udostępniam więcej informacji (o sobie lub innych), niż jest to konieczne?
- **Sprawiedliwość:** Czy może to wyrządzić komuś szkodę lub zaszkodzić (teraz lub w przyszłości)?
- **Przejrzystość:** Czy jestem świadomy, kto ma dostęp do tych informacji i w jaki sposób mogą być one udostępniane?

02

Rodzaje śladów (15 minut)

Aktywny ślad w sieci

Aktywny ślad cyfrowy to informacje, które świadomie generujesz podczas korzystania z internetu.

Przykłady:

- Publikowanie informacji, komentarzy, zdjęć,
- Udostępnianie danych w formularzach i ankietach,
- Tworzenie oraz uzupełnianie profili na stronach internetowych, w przedsiębiorstwach lub na platformach.

Przy tym typie śladu posiadasz stosunkowo większą kontrolę nad tym, co udostępniasz.

Pasywny ślad cyfrowy

Pasywny ślad cyfrowy to dane gromadzone automatycznie, często bez pełnej świadomości użytkownika. Przykłady:

- Historia przeglądania oraz logi serwera,
- Informacje gromadzone przez pliki cookie oraz moduły śledzące,
- Dane dotyczące urządzenia, systemu oraz lokalizacji (np. adres IP),
- Interakcje rejestrowane przez platformy (kliknięcia, czas trwania wizyty, sesje).

Ślad ten jest zazwyczaj zbierany przez systemy analityczne, reklamowe i śledzące, co utrudnia użytkownikom jego usunięcie lub pełną kontrolę.

Aktywne i pasywne ślady cyfrowe tworzą kompleksowy cyfrowy ślad danej osoby, a zarządzanie nimi (czyszczenie historii, ograniczanie danych, dostosowywanie ustawień prywatności) znacząco wpływa na bezpieczeństwo oraz prywatność w Internecie.



• Szybka aktywność: Uporządkuj ślady

**Zadanie (2 minuty) i
wybierz jedną opcję:**

Aktywny

Pasywny

Obydwa?



- Oznaczanie znajomej osoby na zdjęciu
- Aplikacja prosi o dostęp do lokalizacji „zawsze”
- Polubienie postu publicznego
- Model Twojego urządzenia w metadanych fotografii
- Publikowanie opowieści z etykietą lokalizacji
- Pliki cookie śledzą Twoje kliknięcia.
- Zrzut ekranu z prywatnego czatu
- Platforma rekomendująca „osoby, które możesz znać”

Podsumowanie: Większość ludzi nie dostrzega swojego „pasywnego” śladu cyfrowego.

Rozważając swój cyfrowy ślad, prawdopodobnie koncentrujesz się głównie na postach, zdjęciach i komentarzach. Niemniej jednak znaczna część Twojego śladu powstaje bez Twojego aktywnego publikowania czegokolwiek, poprzez Twoje ustawienia, sygnały z urządzenia, uprawnienia oraz aktywność w sieci.

AI Skills,
Powered
by Values



Gdzie sztuczna inteligencja łączy się z Twoim śladem: codzienne przykłady

Nie musisz „tworzyć ani aktywnie korzystać ze sztucznej inteligencji”, aby na nią wpływać. Wiele usług internetowych wykorzystuje sztuczną inteligencję do personalizacji treści, klasyfikacji informacji oraz automatyzacji decyzji – często opierając się na sygnałach lokalizacyjnych.

Typowe sytuacje z wykorzystaniem sztucznej inteligencji, oparte na sygnałach śladowych:

- Ranking: co pojawia się jako pierwsze w wynikach wyszukiwania lub w Twoim strumieniu
- Targetowanie: reklamy spersonalizowane i „sugerowane treści”
- Filtrowanie i moderacja: treść oznaczona, ograniczona w zasięgu lub usunięta
- Wykrywanie wzorców: nietypowe powiadomienia logowania lub monity o „podejrzanej aktywności”
- Rekomendacje: kanały „Dla Ciebie”, proponowane filmy, muzyka lub produkty



03

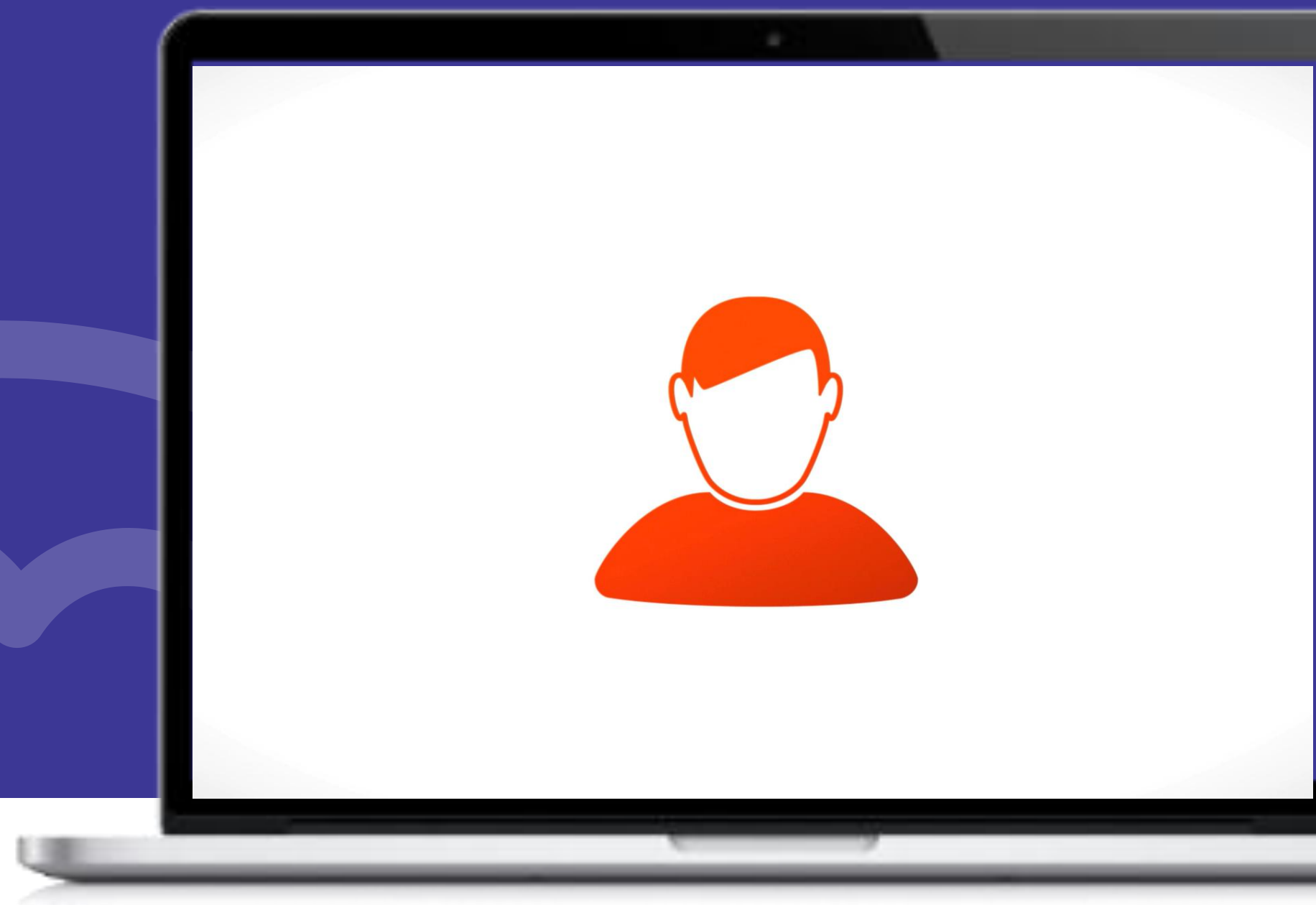


„Efekt domina”:
konsekwencje dla Ciebie i
innych

(25 minut)

„Efekt domina”: działania w sieci mają szerszy zasięg, niż się spodziewasz.

Treści online mogą szybko przemieszczać się między ludźmi i platformami. Nawet drobne działania (komentarz, tag, zrzut ekranu) mogą się rozprzestrzeniać, tracić kontekst i pozostawać dostępne dłużej, niż pierwotnie zamierzono.



„Efekt domina”:
działania w sieci
mają szerszy
zasięg, niż się
spodziewasz.



Jeden post może prowadzić do:

- **Kopie:** zrzuty ekranu, udostępnianie, pobieranie
- **Utrata kontekstu:** żarty lub emocje są niewłaściwie interpretowane bez wyjaśnienia.
- **Długa żywotność:** przestarzałe treści mogą się pojawić ponownie po miesiącach lub latach.
- **Szersza publiczność:** znajomi znajomych, grupy lub publiczne udostępnianie
- **Wpływ na innych:** osoby obecne w Twoich treściach mogą również zostać dotknięte (prawdopodobnie bez ich zgody).

Konsekwencje dla Ciebie: prywatność, wizerunek, bezpieczeństwo oraz samopoczucie

Cyfrowy ślad nie jest automatycznie „dobry” ani „zły”. Jego ocena zależy od kontekstu oraz dokonanych wyborów. Niemniej jednak, pewne wzorce (nadmierne udostępnianie, otwarte ustawienia, impulsywne publikowanie) mogą stwarzać zagrożenia dla Twojej prywatności, reputacji, a nawet bezpieczeństwa, których można uniknąć.



Prywatność (kto może się czegoś o tobie dowiedzieć)	Reputacja (jak jesteś postrzegany)	Bezpieczeństwo (co może być niewłaściwie wykorzystane)	Dobre samopoczucie. (stres i konflikt)
Publiczne profile, tagi, lokalizacja oraz uprawnienia mogą ujawniać więcej, niż pierwotnie zamierzano.	Posty można czytać bez kontekstu; pierwsze wrażenie może szybko się uformować i pozostać trwałe.	Nadmierne udostępnianie danych może prowadzić do oszustw, przejęć kont oraz niepożądanych kontaktów (nie tylko w kontekście życia cyfrowego).	Kłótnie, nękanie lub poczucie żalu po opublikowaniu posta mogą negatywnie wpływać na pewność siebie oraz nastrój.

**Konsekwencje dla CIEBIE:
prywatność, wizerunek,
bezpieczeństwo oraz
samopoczucie.**



Przykład:

Zdjęcie z widoczną lokalizacją oraz otwartymi ustawieniami profilu może ujawnić, gdzie się znajdujesz, z kim spędzasz czas i co robisz na co dzień – bez konieczności bezpośredniego podawania informacji.

Zadaj sobie pytanie: Które ryzyko jest dla mnie obecnie najistotniejsze: prywatność, reputacja, Bezpieczeństwo czy komfort psychiczny? Dlaczego?

Niewielkie modyfikacje (ustawienia odbiorców, uprawnienia, wstrzymanie publikacji) mogą znacząco zredukować te ryzyka.

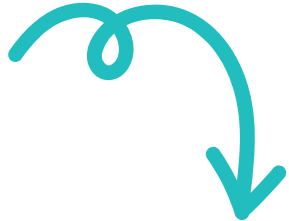
Konsekwencje dla INNYCH: szacunek, akceptacja i rzetelność

**Typowe metody, w
jakie narażamy
innych na
niebezpieczeństwo
w Internecie:**



- Publikowanie lub udostępnianie treści w lokalizacjach, w których obecni są inni użytkownicy.
- Oznaczanie lub wspomnianie kogoś (umieszczanie odnośników do treści)
- Udostępnianie zrzutów ekranu z prywatnych rozmów
- Ujawnianie czyjejś lokalizacji, harmonogramu lub danych osobowych.
- Udostępnianie treści, które mogą później prowadzić do konfliktów

Konsekwencje dla INNYCH: szacunek, akceptacja i rzetelność



Przykład

„Zabawny” zrzut ekranu z prywatnego czatu może zostać udostępniony, błędnie zinterpretowany i użyty przeciwko komuś – ponieważ pierwotny kontekst zanika.

Jak kontrolować

Zadaj sobie pytanie: Czy byłoby dla mnie akceptowalne, gdyby ktoś bez pytania udostępnił podobne treści na mój temat?

**Ochrona prywatności obejmuje także prywatność innych osób:
Zgoda i szacunek stanowią integralne elementy odpowiedzialnego działania w Internecie.**

Mini scenariusze: wybierz najbardziej odpowiednią opcję

Decyzje podejmowane w rzeczywistości często są podejmowane „na szybko”. To ćwiczenie pomoże Ci przećwiczyć wybór opcji, która chroni prywatność, minimalizuje szkody i szanuje innych ludzi, zwłaszcza gdy treść może być kopiowana lub udostępniana.



Scenariusz: Prywatny zrzut ekranu

Znajomy przesyła Ci zrzut ekranu z prywatnej konwersacji i stwierdza: „To jest niezwykle zabawne – podziel się tym z innymi”.

Opcja 1: Wyślij to natychmiast (to zabawne).

Opcja 2: Zachowaj prywatność i zapytaj znajomego, jakie cele ma na myśli, udostępniając tę wiadomość.

Opcja 3: Nie udostępniaj informacji, chyba że osoby zainteresowane wyrażą na to zgodę; w przypadku wątpliwości – nie udostępniaj.

Mini scenariusze: wybierz najbardziej odpowiednią opcję

Decyzje podejmowane w rzeczywistości często są podejmowane „na szybko”. To ćwiczenie pomoże Ci przećwiczyć wybór opcji, która chroni prywatność, minimalizuje szkody i szanuje innych ludzi, zwłaszcza gdy treść może być kopiowana lub udostępniana.



Scenariusz: Prywatny zrzut ekranu

Znajomy przesyła Ci zrzut ekranu z prywatnej konwersacji i stwierdza: „To jest zabawne – podziel się tym z innymi”.

Twoje zadanie (30–60 sekund): Wybierz 1 / 2 / 3 Napisz jedno zdanie:

„Wybrałem... ponieważ...”

Sztuczna inteligencja a prywatność – przykład

O czym mówi przykład:

- Systemy sztucznej inteligencji analizują dane pochodzące z codziennych aktywności (np. mediów społecznościowych, przeglądania stron internetowych, zakupów online).
- Dane osobowe są wykorzystywane jako dane wejściowe do szkolenia i doskonalenia modeli sztucznej inteligencji.
- Nawet podstawowe zachowania w sieci mogą być zintegrowane w szczegółowe profile użytkowników.



04



Mój wybór: zwieszła lista
kontrolna + mój plan
działania

(15 minut)

Moje narzędzie selekcji: ZATRZYMAJ SIĘ-POMYŚL- SPRAWDŹ-WYBIERZ

Ta lista kontrolna to prosty nawyk, który pomoże Ci podejmować bezpieczniejsze i bardziej sprawiedliwe decyzje w Internecie. Skorzystaj z niej przed opublikowaniem, udostępnieniem, oznaczeniem, przesłaniem zrzutu ekranu lub zaakceptowaniem uprawnień aplikacji, zwłaszcza gdy czujesz się pośpieszony lub zdenerwowany.



ZATRZYMAJ SIĘ	POMYŚL	SPRAWDŹ	WYBIERZ
(zatrzymaj się na 5 sekund)	(cel i odbiorcy):	(prywatność + ludzie + informacje)	(najlepszy kolejny krok)
Czy publikuję szybko, znużony, zdenerwowany, podekscytowany lub pod presją?	Jaki jest cel (informowanie, żartowanie, popisywanie się, prośba o pomoc)? Kto obecnie to zobaczy, a kto może to zobaczyć w przyszłości?	Czy ustawienia odbiorców są poprawne (publiczne / znajomi / bliscy znajomi / grupa)? Czy obejmują inne osoby (twarze, imiona, wiadomości, lokalizacje)? Czy ujawniają dodatkowe informacje (naklejkę z lokalizacją, szczegóły tła, metadane)?	Publikuj / edytuj / przycinaj / rozmywaj / ograniczaj odbiorców / pytaj o zgodę / nie udostępniaj.

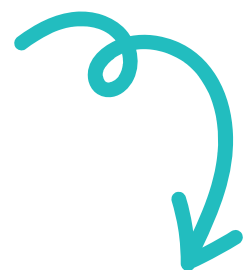
Scenariusz 1.

Ćwiczenie: wykorzystaj listę kontrolną przed publikacją

Tworzysz pasywny cyfrowy ślad nie tylko podczas przeglądania stron, ale również poprzez to, na co zezwalasz aplikacjom.

Ten scenariusz pozwoli Ci ćwiczyć w zakresie wyboru niezbędnych uprawnień oraz odrzucania tych, które gromadzą więcej danych, niż jest to konieczne.

Zobacz kolejny slajd



Scenariusz 1:

Instalujesz nową aplikację, taką jak edytor zdjęć, gra lub aplikacja edukacyjna.

Podczas konfiguracji prosi o:

- Lokalizacja
- Kontakty
- Mikrofon
- Zdjęcia

ZATRZYMAJ SIĘ

Czy klikając „Zezwól”, automatycznie przyspieszam zakończenie konfiguracji?

POMYŚL

Czego tak naprawdę potrzebuje aplikacja, aby realizować swoją podstawową funkcję? Czy mogę używać aplikacji z ograniczoną liczbą uprawnień?

SPRAWDŹ

Lokalizacja: czy lokalizacja jest niezbędna „zawsze”, „tylko podczas używania”, czy wcale? **Kontakty:** czy dostęp do nich jest rzeczywiście konieczny, czy jedynie „pożądany”? **Mikrofon:** czy jest wymagany do funkcji, z której zamierzam korzystać? **Zdjęcia/Media:** czy mogę wybrać „tylko wybrane zdjęcia” zamiast „wszystkich zdjęć”?

WYBIERZ

Udziel minimalnych wymaganych uprawnień. Preferuj opcję „tylko podczas używania” zamiast „zawsze”. Przejrzyj i dostosuj uprawnienia później, jeśli funkcjonalność rzeczywiście ich wymaga.

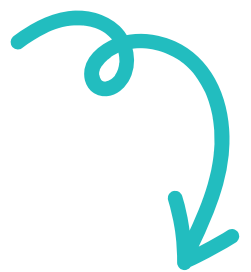
Scenariusz 2.

Ćwiczenie: zastosuj listę kontrolną, gdy zaangażowane są inne osoby

Jeżeli w Twoich treściach uczestniczą inne osoby, Twój wybór wpłynie również na nie.

Ten scenariusz umożliwi Ci ćwiczenie podejmowania decyzji z uwzględnieniem prywatności i zgody, ponieważ działania związane z udostępnianiem, tagowaniem i przekazywaniem mogą być trudne do odwrócenia.

Zobacz kolejny slajd



Scenariusz 2:

Masz grupowe zdjęcie z spotkania, wydarzenia lub wieczornego wyjścia. Chcesz je opublikować i oznaczyć znajomych. Jedna osoba na zdjęciu wcześniej zadeklarowała, że nie życzy sobie publikacji w internecie.

ZATRZYMAJ SIĘ

Czy zamierzam opublikować coś szybko, ponieważ pragnę podzielić się tą chwilą już teraz?

POMYŚL

Jaki jest cel publikacji? Czy tagowanie jest niezbędne? Kto zobaczy to teraz – a kto będzie mógł zobaczyć później?

SPRAWDŹ

Zgoda: Czy wszyscy wyrazili zgodę na wyświetlanie lub oznaczanie / Publiczność: Czy jest to dostępne publicznie, czy ograniczone do wąskiej grupy / Ryzyko: Czy to zdjęcie może w przyszłości kogoś skrzywdzić lub zawstydzić? Alternatywy: Czy mogę przyciąć, rozmyć lub wybrać inne zdjęcie?

WYBIERZ

Wybierz optymalny następny krok: najpierw zapytaj daną osobę / opublikuj, nie ujawniając jej treści / rozmyj lub przytnij / ogranicz liczbę odbiorców / nie publikuj.

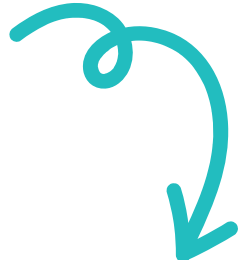
Scenariusz 3.

Ćwiczenie: wykorzystaj listę kontrolną uprawnień aplikacji

Tworzysz pasywny cyfrowy ślad nie tylko podczas przeglądania stron, ale również poprzez to, na co zezwalasz aplikacjom.

Ten scenariusz umożliwi Ci praktykę w zakresie wyboru niezbędnych uprawnień oraz odrzucania tych, które gromadzą więcej danych, niż jest to konieczne.

Zobacz kolejny slajd



Scenariusz 3:

Instalujesz nową aplikację, taką jak edytor zdjęć, gra lub aplikacja edukacyjna.

Podczas konfiguracji prosi o:

- Lokalizacja
- Kontakty
- Mikrofon
- Zdjęcia

ZATRZYMAJ SIĘ

Czy klikając „Zezwól”, automatycznie przyspieszam zakończenie konfiguracji?

POMYŚL

Czego tak naprawdę potrzebuje aplikacja, aby realizować swoją podstawową funkcję? Czy mogę używać aplikacji z ograniczoną liczbą uprawnień?

SPRAWDŹ

Lokalizacja: czy jest ona niezbędna „zawsze”, „tylko w trakcie użytkowania” czy w ogóle? **Kontakty:** czy dostęp do nich jest rzeczywiście niezbędny, czy też jedynie „pożądany”? **Mikrofon:** czy jest niezbędny do funkcji, z której zamierzam korzystać? **Zdjęcia/Media:** czy mogę wybrać „tylko wybrane zdjęcia” zamiast „wszystkich zdjęć”?

WYBIERZ

Bezpieczniejsze podejście domyślne: Przyznawaj jedynie minimalne wymagane uprawnienia. Preferuj opcję „tylko podczas używania” zamiast „zawsze”. Przejrzyj i dostosuj uprawnienia później, jeśli funkcjonalność rzeczywiście ich wymaga.

Trzy elementy o znaczącym wpływie: niewielkie zmiany, ogromny efekt

Nie musisz znać wszystkich ustawień prywatności, aby poprawić swój cyfrowy ślad. Te trzy elementy sterujące znacząco wpływają na większość platform i aplikacji – warto je zatem sprawdzić, nawet jeśli dysponujesz ograniczonym czasem.

Twój cyfrowy ślad rośnie najszybciej, gdy zarządzasz odbiorcami, lokalizacją i widocznością.

Trzy elementy o znaczącym wpływie: niewielkie zmiany, ogromny efekt

Podstawowa treść
(ogólny przewodnik do samodzielnej nauki)



- **Widoczność odbiorców** (kto ma dostęp do Twoich treści): Upewnij się, czy domyślnie jest to grupa publiczna, znajomi, bliscy znajomi czy prywatna. Pamiętaj: „znajomi znajomych” lub grupy otwarte mogą nadal obejmować szeroką publiczność.
- **Udostępnianie lokalizacji** (gdy Twoja lokalizacja jest widoczna): Unikaj publicznego udostępniania lokalizacji w czasie rzeczywistym. Preferuj dostęp do lokalizacji „tylko podczas korzystania” (lub wyłącz go, jeśli nie jest potrzebny). Zwracaj uwagę na ukryte wskazówki dotyczące lokalizacji na zdjęciach (w tle, w punktach orientacyjnych, popularnych miejscach).
- **Możliwość odnalezienia i synchronizacja kontaktów** (jak inni mogą Cię znaleźć): Zweryfikuj, czy Twój profil jest dostępny za pośrednictwem numeru telefonu lub adresu e-mail. Sprawdź czy aplikacje domyślnie synchronizują Twoje kontakty. Zdecyduj, czy pragniesz być wyszukiwany, czy też aby kontaktowały się z Tobą jedynie wybrane osoby.

05

Jak zabezpieczyć swój
cyfrowy ślad

(10 minut)

○ Praktyczne zasady.



01

Ograniczaj udostępnianie informacji w mediach społecznościowych.



02

Zaostrzenie ustawień prywatności w mediach społecznościowych



03

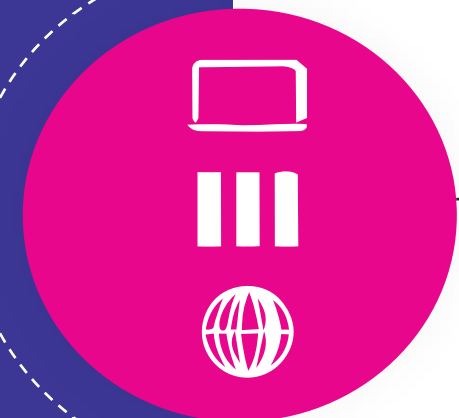
Ogranicz ilość danych przesyłanych do sieci.



05

Od czasu do czasu usuwaj pliki cookie przeglądarki oraz inne pliki śledzące z urządzeń osobistych.

Praktyczne zasady



06

Korzystaj z usług VPN, gdy to możliwe.



07

Anonimizuj, nie zezwalaj na dostęp do lokalizacji śledzenia przez aplikacje lub go ograniczaj.



08

Zainstaluj oraz zaktualizuj oprogramowanie antywirusowe na urządzeniach osobistych.



09

Okresowo weryfikuj informacje finansowe/kredytowe oraz medyczne/zdrowotne.

Praktyczne zasady



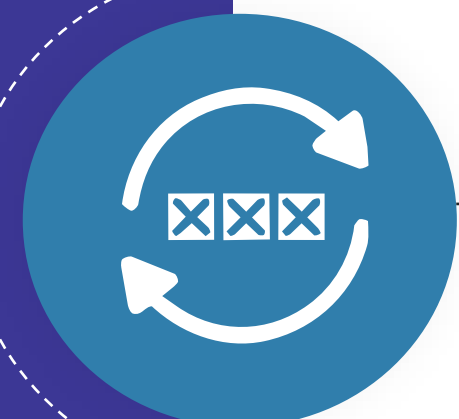
10

Nie otwieraj załączników ani nie klikaj w linki pochodzące z nieznanych lub wątpliwych źródeł.



11

Skonfiguruj powiadomienia o raportach kredytowych.



12

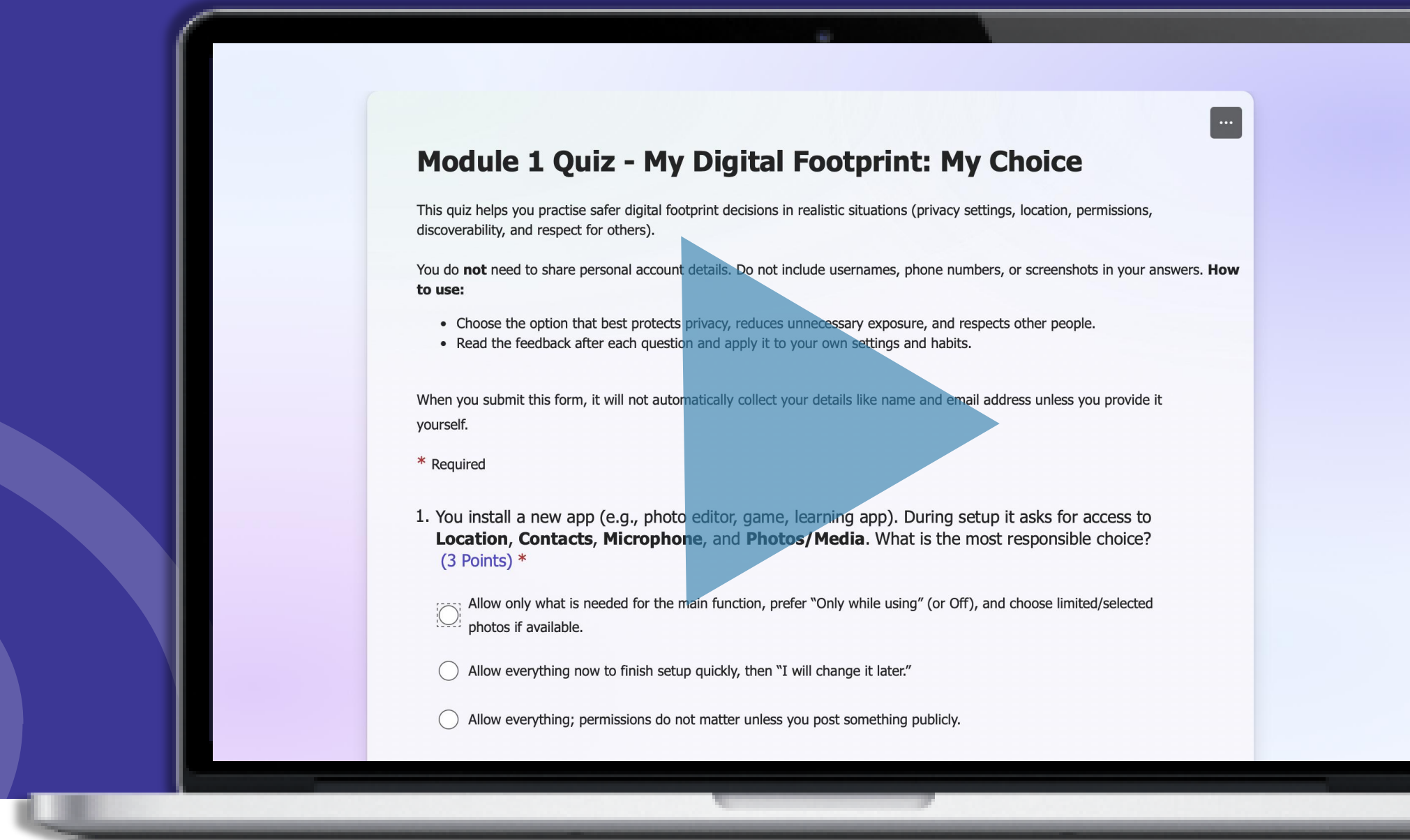
Ciągle aktualizuj hasła oraz zabezpieczenia haseł, szczególnie po uzyskaniu informacji o naruszeniu danych.

06

Audyt, quiz oraz test
(20 minut)

Quiz

Ten quiz pomoże Ci doskonalić umiejętność podejmowania bezpieczniejszych decyzji dotyczących cyfrowego śladu w realistycznych sytuacjach (ustawienia prywatności, lokalizacja, uprawnienia, wykrywalność oraz poszanowanie innych).



Test: Zbadaj swój cyfrowy ślad

Nie jesteś pewien swojego cyfrowego śladu? Odpowiedz „Tak” lub „Nie” na poniższe pytania, a następnie zsumuj łączną liczbę odpowiedzi „Tak”, aby ocenić złożoność swojego śladu.

Źródło: Cyfrowy ślad osoby wewnątrz organizacji oraz związane z nim ryzyko. Wsparcie w poszukiwaniu pracy, Agencja Kontrwywiadu i Bezpieczeństwa Obrony (CDSE), 2022
<https://www.cdse.edu/Portals/124/Documents/jobaid/insider/insiders-digital-footprint.pdf>

1. Czy dokonujesz zakupów online?
2. Czy zarejestrowałeś się na kupony, tworząc konto?
3. Czy zarejestrowałeś się lub subskrybowałeś newslettery lub aktualizacje bloga?
4. Czy pobrałeś i korzystałeś z aplikacji do zakupów?
5. Czy założyłeś nowe konto karty kredytowej?
6. Czy używasz aplikacji bankowości mobilnej?
7. Czy nabyłeś lub zbyłeś akcje?
8. Czy kiedykolwiek zarejestrowałeś swój adres e-mail w klubie fitness?
9. Czy korzystasz z opieki zdrowotnej?

Test: Zbadaj swój cyfrowy ślad

Nie jesteś pewien swojego cyfrowego śladu? Odpowiedz „Tak” lub „Nie” na poniższe pytania, a następnie zsumuj łączną liczbę odpowiedzi „Tak”, aby ocenić złożoność swojego śladu.

Źródło: Cyfrowy ślad osoby wewnątrz organizacji oraz związane z nim ryzyko. Wsparcie w poszukiwaniu pracy, Agencja Kontrwywiadu i Bezpieczeństwa Obrony (CDSE), 2022
<https://www.cdse.edu/Portals/124/Documents/jobaid/insider/insiders-digital-footprint.pdf>

10. Czy kiedykolwiek korzystałeś z aplikacji do monitorowania swojej aktywności i treningów?

11. Czy subskrybujesz czasopismo internetowe lub źródło informacji?

12. Czy kiedykolwiek zdarzyło Ci się ponownie publikować przeczytane artykuły i informacje?

13. Czy korzystasz z mediów społecznościowych na komputerze lub na urządzeniach mobilnych?

14. Czy nawiązujesz kontakt ze znajomymi w internecie?

15. Czy kiedykolwiek dzieliłeś się informacjami, danymi oraz zdjęciami ze swoimi znajomymi w internecie?

16. Czy kiedykolwiek zarejestrowałeś się w serwisie lub aplikacji randkowej?

•Test: Zbadaj swój cyfrowy ślad

WYNIKI

Mniej niż 5 odpowiedzi TAK

Cyfrowy ślad, który jest prostszy niż u większości użytkowników Internetu.

5 – 12 odpowiedzi TAK

Cyfrowy ślad, który jest typowy dla większości użytkowników Internetu.

Ponad 12 odpowiedzi TAK

Cyfrowy ślad, który jest bardziej skomplikowany niż większość użytkowników Internetu.

Audyt śladu cyfrowego

Teraz będziesz ćwiczyć identyfikację typowych zagrożeń związanych z odciskiem oraz wybieranie praktycznych uprawnień. Możesz to również zrealizować bez ujawniania danych osobowych, korzystając z fikcyjnego przykładu lub opcjonalnie, sprawdzając jedno ustawienie na swoim urządzeniu w trybie prywatnym.

Prywatne sprawdzenie własnego urządzenia – zweryfikuj jedno ustawienie prywatności lub uprawnień na swoim urządzeniu lub koncie. Jeśli pracujesz w zespole, wykonaj to bez udostępniania ekranu ani danych.

Audyt śladu cyfrowego – wybierz jedną z aplikacji mediów społecznościowych, które posiadasz.

Celem nie jest eliminacja Twojej obecności w sieci, lecz ograniczenie zbędnej ekspozycji oraz świadome zaznaczenie swojego śladu.

Uzupełnij wiersze:

Ryzyko 1 → Rozwiązanie 1: _____ → _____

Ryzyko 2 → Rozwiązanie 2: _____ → _____

Ryzyko 3 → Rozwiązanie 3: _____ → _____

Pierwsze działanie: _____

Krok 1: Zidentyfikuj trzy ryzyka związane z odciskiem

- Zbyt szeroka widoczność publiczna (posty/profile dostępne do odkrycia)
- Ujawniono lokalizację (miejsca w czasie rzeczywistym lub w ramach rutynowych działań)
- Tagowanie/wzmianki bez zgody użytkownika
- Zbyt szerokie uprawnienia (kontakty/mikrofon/lokalizacja „zawsze”)
- Widoczne dane osobowe (szkoła/praca, telefon, adres e-mail, rutyna)

Krok 2: Wybierz 3 usprawnienia (dopasuj jedno do każdego ryzyka)

- Ogranicz odbiorców / przełącz na tryb prywatny / sprawdź domyślną widoczność
- Usuń lub ogranicz udostępnianie lokalizacji.
- Zapytaj o zgodę przed oznaczeniem lub publikowaniem innych osób.
- Zredukuj uprawnienia do „minimum koniecznego”
- Usuń dane poufne z profilu

Krok 3: Określ, jakie będzie Twoje „pierwsze działanie”

- Jaką jedną zmianę wprowadziłbyś jako pierwszą, gdybyś dysponował jedynie 2 minutami?

Audyt śladu cyfrowego

Cyfrowy ślad poprawia się dzięki niewielkim, spójnym działaniom – nie dzięki jednemu idealnemu rozwiązaniu. Ten zwięzły plan pomoże Ci przekształcić dzisiejszy audyt w konkretne kroki, które możesz rzeczywiście zrealizować.

Uczyń to wykonalnym: Jeśli Twój plan wydaje się zbyt rozbudowany, ogranicz go do jednego celu i jednego nawyku. Twój cyfrowy ślad kształtuje się poprzez nawyki. Mały plan, którego się trzymasz, jest lepszy niż duży plan, o którym zapominasz.

1. Jedna zmiana, którą wprowadzę dzisiaj (5 minut)

Przykłady:

- Ogranicz widoczność profilu.
- Usuń udostępnianie lokalizacji.
- Zredukuj jedno uprawnienie.
- Sprawdź zdolność wykrywania

Napisz:

Dzisiaj zamierzam:

.....
.....
.....

Audyt śladu cyfrowego

Cyfrowy ślad poprawia się dzięki niewielkim, spójnym działaniom – nie dzięki jednemu idealnemu rozwiązaniu. Ten zwięzły plan pomoże Ci przekształcić dzisiejszy audyt w konkretne kroki, które możesz rzeczywiście zrealizować.

Uczyń to wykonalnym: Jeśli Twój plan wydaje się zbyt rozbudowany, ogranicz go do jednego celu i jednego nawyku. Twój cyfrowy ślad kształtuje się poprzez nawyki. Mały plan, którego się trzymasz, jest lepszy niż duży plan, o którym zapominasz.

2. Dwie zmiany, które wprowadzę w tym tygodniu (łącznie 10–20 minut).

Przykłady:

- Przejrzyj domyślne ustawienia ochrony prywatności.
- Wyczyść przestarzałe posty publiczne
- Sprawdź uprawnienia aplikacji.
- Zaktualizuj ustawienia dotyczące hasła (jeśli dotyczy)

Napisz:

W tym tygodniu zamierzam:

.....
.....
.....

Audyt śladu cyfrowego

Cyfrowy ślad poprawia się dzięki niewielkim, spójnym działaniom – nie dzięki jednemu idealnemu rozwiązaniu. Ten zwięzły plan pomoże Ci przekształcić dzisiejszy audyt w konkretne kroki, które możesz rzeczywiście zrealizować.

Uczyń to wykonalnym: Jeśli Twój plan wydaje się zbyt rozbudowany, ogranicz go do jednego celu i jednego nawyku. Twój cyfrowy ślad kształtuje się poprzez nawyki. Mały plan, którego się trzymasz, jest lepszy niż duży plan, o którym zapominasz.

3. Jedna zasada, której zamierzam przestrzegać w przyszłości (codzienny wybór)

Przykłady:

- „Zanim się podzielę, skorzystam z opcji ZATRZYMAJ–POMYŚL–SPRAWDŹ–WYBIERZ”
- „Złożę zapytanie o zgodę przed oznaczeniem”
- „Będę unikać lokalizacji w czasie rzeczywistym.”

Napisz:

Moja zasada jest następująca:

.....

.....

.....



Śledź naszą wędrówkę



www.valuesai.eu

AI Skills, Powered by 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.