



MODUŁ 5

CYBERBEZPIECZEŃSTWO I BEZPIECZNE KORZYSTANIE Z INTERNETU



erasmediah.eu



**Co-funded by
the European Union**



Lekcja 5.2

Ochrona danych osobowych i prywatności w internecie



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

Lekcja 5.2

Ochrona danych osobowych i prywatności w internecie

Cele:

- Podniesienie świadomości na temat ryzyka związanego z udostępnianiem danych osobowych w Internecie i możliwości ich niewłaściwego wykorzystania.
- Wyposażenie uczestników w praktyczne strategie kontrolowania ich cyfrowego śladu, w tym ustawień prywatności danych, bezpiecznej komunikacji i unikania nadmiernego udostępniania informacji.
- Zbadanie przykładów naruszeń prywatności, pokazanie ich wpływu na osoby fizyczne i sposobów, w jakie można było im zapobiec.
- Inspirowanie do aktywnej postawy poprzez budowanie nawyków, takich jak sprawdzanie uprawnień aplikacji, rozumienie warunków świadczenia usług i korzystanie z narzędzi ochrony prywatności.

Kluczowe przesłanie:

- Każda informacja, którą udostępniasz online - od zdjęć i polubień po dane o lokalizacji - może zostać wykorzystana przez cyberprzestępców lub firmy. Wiedza o tym, jak ograniczyć im dostęp, jest pierwszą linią obrony.
- Ochrona prywatności nie polega na unikaniu Internetu; chodzi o bycie świadomym i konkretnym. Proste narzędzia i decyzje mogą zapewnić bezpieczeństwo danych bez poświęcania swojego cyfrowego życia.



RODZAJ LEKCJI:





Przegląd lekcji

Przez to, że tak wiele z naszego życia dzieje się w internecie, dbanie o bezpieczeństwo danych osobowych nigdy nie było ważniejsze. Ta lekcja pokazuje, dlaczego ochrona prywatności ma znaczenie. Zbadamy, w jaki sposób proste nawyki, takie jak nadmierne udostępnianie w mediach społecznościowych lub akceptowanie uprawnień aplikacji bez zastanowienia, mogą narazić twoje dane na niebezpieczeństwo. Rozpoznając te zagrożenia i przyjmując praktyczne strategie, zyskasz narzędzia do ochrony swojej cyfrowej tożsamości i przejmiesz kontrolę nad swoim bezpieczeństwem online.

Warsztaty podzielone są na 4 etapy:

- 1: Wprowadzenie do zagrożeń prywatności w internecie (15 min)
- 2: Analiza rzeczywistych przypadków naruszenia prywatności (10 min)
- 3: Praktyczne strategie ochrony danych osobowych (10 min)
- 4: Podsumowanie i wnioski (5 min)



Krok 1

Wprowadzenie do zagrożeń prywatności w internecie

Czy kiedykolwiek pobrałeś nową aplikację, zaakceptowałeś jej uprawnienia i nigdy nie zastanawiałeś się, jakie informacje gromadzi? Kiedy korzystamy z internetu, nasze dane osobowe - takie jak lokalizacja, hasła i nawyki przeglądania - mogą łatwo zostać ujawnione. Teraz zbadamy, jakie zagrożenia dla prywatności istnieją i jak mogą one wpłynąć na ciebie.

Jako pierwszy krok, **przeczytaj fragment “Typowe zagrożenia dla prywatności w internecie” z tego artykułu: builtin.com/articles**

Podczas czytania zapisz w kilku słowach na kartce papieru:

- Zagrożenie prywatności, które uważasz za najbardziej niepokojące i dlaczego to zagrożenie wyróżnia się dla ciebie lub wydaje się niebezpieczne.



Krok 1

Wprowadzenie do zagrożeń prywatności w internecie

Gdy skończysz czytać, porozmawiajmy o tym:

- Które zagrożenie dla prywatności zaskoczyło cię najbardziej i dlaczego?
- W jaki sposób te zagrożenia wpływają na nasze codzienne życie?
- Co może się stać, jeśli je zignorujemy?

Zachęcamy do podzielenia się krótkim przykładem z własnego doświadczenia - niezależnie od tego, czy chodzi o słabe hasła, śledzenie danych, czy coś innego, co widziałeś lub słyszałeś. Jeśli nie masz pewności, samo słuchanie innych może podsunąć ci pomysły!



Krok 2

Analiza rzeczywistych przypadków naruszenia prywatności

Przyjrzyjmy się rzeczywistemu przykładowi tego, co dzieje się, gdy nie jesteśmy ostrożni z naszymi danymi osobowymi w internecie.

Wyobraź sobie, że: Sarah uwielbia dzielić się swoim życiem w mediach społecznościowych. Publikuje zdjęcia swojego nowego mieszkania, opowiada o codziennych czynnościach, a nawet udostępnia swoją lokalizację, gdy jest w ulubionej kawiarni. Pewnego dnia Sarah odkrywa, że jej konto bankowe zostało opróżnione. W jaki sposób? Cyberprzestępca zebrał jej dane osobowe z jej publicznych postów - jej lokalizację, nawyki związane ze stylem życia, a nawet wskazówki dotyczące haseł - aby uzyskać dostęp do jej kont. Wszystko z powodu nadmiernego udostępniania informacji!

Teraz zastanów się nad następującymi pytaniami:

- Co poszło nie tak? Jakie działania lub nawyki doprowadziły do naruszenia prywatności?
- Jak można było zapobiec tej sytuacji? Jakie proste zmiany mogłyby coś zmienić?

Zapisz swoje odpowiedzi i przygotuj się do podzielenia się nimi z grupą.



Krok 2

Analiza rzeczywistych przypadków naruszenia prywatności

Porozmawiajmy o tym razem:

- Co poszło nie tak w sytuacji Sarah?
- Dlaczego naruszenia prywatności tego typu są tak częste?

Na koniec, rozważ przez chwilę:

- Czy ty lub ktoś, kogo znasz, miał kiedykolwiek do czynienia z kwestią prywatności w internecie? Może to być podejrzana wiadomość email, włamanie się na konto lub incydent nadmiernego udostępniania informacji w mediach społecznościowych.
- Jak do tego doszło i jaki był rezultat?

Jeśli czujesz się z tym komfortowo, podziel się swoją historią z grupą. Jeśli nie, nic nie szkodzi - samo słuchanie da ci cenne spostrzeżenia.



Krok 3

Praktyczne strategie ochrony danych osobowych

Teraz, gdy zapoznaliśmy się z zagrożeniami dla prywatności i rzeczywistymi przykładami, skupmy się na praktycznych krokach, aby chronić siebie (i nasze dane) online.

Rozpocniemy od krótkiego filmiku: <https://youtu.be/6WQzMAAd6mJs>

Zwróć uwagę na zawarte w nim wskazówki.

Po obejrzeniu filmu zapisz **trzy konkretne działania**, które możesz podjąć, aby poprawić swoją prywatność w internecie. Zastanów się nad:

- Dostosowaniem ustawień prywatności na swoich kontach w mediach społecznościowych.
- Sprawdzeniem uprawnień aplikacji na telefonie.
- Zachowaniem ostrożności przy udostępnianiu danych osobowych online, zwłaszcza na platformach publicznych.



Krok 3

Praktyczne strategie ochrony danych osobowych

A teraz, podziel się **jedną strategią** którą planujesz wdrożyć. Na przykład:

- „Dziś wieczorem przejrzę wszystkie aplikacje na moim telefonie i usunę te, których nie używam”
- „Ograniczę liczbę osób, które mogą zobaczyć moje posty na Facebooku/Instagramie i wyłączę publiczną widoczność mojego profilu”

Podyskutujmy o:

1. Co sprawia, że te nawyki dotyczące prywatności wydają się łatwe lub trudne do wdrożenia?
 - Czy nie czujemy się zbyt komfortowo udostępniając informacje online?
 - Czy uważamy, że ustawienia prywatności i uprawnienia są skomplikowane lub czasochłonne?
2. Dlaczego tak wiele osób ignoruje proste praktyki dotyczące prywatności, nawet jeśli są świadome występującego ryzyka?
 - Czy dzieje się tak dlatego, że nie sądzą, że dojdzie do naruszenia ich prywatności?
 - Czy uważasz, że dzieje się tak dlatego, że ludzie nie są świadomi narzędzi lub nawyków, których powinni używać?
3. Jak można zmotywować się do przestrzegania tych nawyków?
 - Na przykład poprzez ustawienie przypomnienia o aktualizacji haseł lub regularnie sprawdzając ustawienia mediów społecznościowych.

Krok 4

Podsumowanie i wnioski

Podsumowując te warsztaty, poświęćmy chwilę na refleksję nad tym, czego się nauczyliśmy i zastanówmy się, jak możemy to zastosować w naszym codziennym życiu.

Zadaj sobie pytanie: *Jaki jest jeden nawyk, który możesz dziś zmienić, aby zwiększyć swoją prywatność w internecie? Może to być coś prostego, na przykład wyłączenie udostępniania lokalizacji, sprawdzenie ustawień prywatności w mediach społecznościowych lub ostrożniejsze publikowanie treści. Teraz zastanów się, jak możesz pomóc innym: W jaki sposób podzielisz się tym, czego się dziś nauczyłeś z przyjacielem, członkiem rodziny lub współpracownikiem? Nawet małe wskazówki, takie jak wyjaśnienie, dlaczego silne hasła mają znaczenie lub pokazanie komuś, jak sprawdzić uprawnienia aplikacji, mogą mieć znaczny wpływ.*





Podsumowanie kluczowych wniosków

- **Uważaj na to, co udostępniasz online:** Drobne szczegóły, takie jak lokalizacja lub nawyki, mogą zostać niewłaściwie wykorzystane, jeśli wpadną w niepowołane ręce.
- **Sprawdź i dostosuj ustawienia prywatności:** Regularnie sprawdzaj swoje media społecznościowe, uprawnienia aplikacji i ustawienia konta, aby ograniczyć niepotrzebne udostępnianie danych.
- **Ogranicz publicznie publikowane dane osobowe:** Unikaj udostępniania wrażliwych danych, takich jak adresy, procedury lub osobiste identyfikatory w mediach społecznościowych lub na innych platformach.
- **Zachowaj ostrożność przy korzystaniu z aplikacji i linków:** Zastanów się przed klikaniem linków, pobieraniem aplikacji lub udzielaniem uprawnień - ufaj tylko zweryfikowanym źródłom.
- **Zacznij od małych kroków:** Proste nawyki, takie jak wyłączenie śledzenia lokalizacji lub ograniczenie publicznych postów, mogą mieć duży wpływ na ochronę prywatności.



Instrukcje dla osób pracujących z młodzieżą, edukatorów i nauczycieli

Cel:

Celem tej lekcji jest zapewnienie uczestnikom praktycznych umiejętności i wiedzy w zakresie ochrony ich danych osobowych i zachowania prywatności w internecie. Dzięki interaktywnym ćwiczeniom, rzeczywistym przykładom i przemyślanym dyskusjom uczestnicy zidentyfikują typowe zagrożenia dla prywatności w internecie, uzyskują wgląd we wpływ naruszeń prywatności i opracują praktyczne strategie ochrony swoich danych. Pod koniec sesji uczestnicy poczują się bardziej świadomi, przygotowani i zaangażowani w przyjmowaniu nawyków, które zwiększają ich bezpieczeństwo cyfrowe.

Potrzebne materiały:

- Połączenie internetowe do odtwarzania filmów lub artykułów
- Projektor i ekran
- Głośniki
- Dostęp do zalecanych narzędzi cyberbezpieczeństwa
- Kartka papieru lub markery do tablicy
- Długopisy, ołówki i karteczki samoprzylepne





Krok 1: Wprowadzenie do zagrożeń prywatności w internecie (15 min)

1. Zaczniij od pytania związanego z tematem: "Kiedy ostatnio pobrałeś aplikację, zaakceptowałeś jej uprawnienia lub udostępniłeś post online? Czy zastanawiałeś się nad tym, jakie dane osobowe możesz przez to udostępniać?". Wyjaśnij, że te małe, codzienne działania mogą nieumyślnie ujawnić prywatne dane, takie jak lokalizacja, nawyki przeglądania lub osobiste nawyki osobom trzecim lub cyberprzestępcom.

2. Podkreśl, że ochrona danych osobowych jest niezbędna w dzisiejszym cyfrowym świecie. Podkreśl, że pozornie nieszkodliwe zachowania - takie jak udostępnianie zdjęć lub zezwalanie aplikacjom na dostęp do kontaktów - mogą mieć niezamierzone konsekwencje. Użyj prostego przykładu: "Twoje dane osobowe są jak elementy układanki. Pojedynczy element może wydawać się nieszkodliwy, ale w połączeniu z innymi może wiele o tobie wyjawiać".

3. Aktywność – czytanie artykułu i przemyślenia

Udostępniij fragment "Typowe zagrożenia dla prywatności w internecie" pochodzący z artykułu: Czym jest prywatność w internecie?.

Poproś uczestników o:

- Zidentyfikowanie zagrożenia prywatności, które uważają za najbardziej niepokojące.
- Zastanowienie się, dlaczego to zagrożenie wydaje się szczególnie niebezpieczne lub szokujące.

Zachęć ich do zanotowania krótkich przemyśleń w celu przygotowania się do dyskusji grupowej.





Krok 1: Wprowadzenie do zagrożeń prywatności w internecie (15 min)

4. Poprowadź krótką dyskusję, korzystając z poniższych sugestii:

- “Które zagrożenie dla prywatności było dla ciebie najbardziej wyróżniające się i dlaczego?”
- “Jak te zagrożenia wpływają na twoje zachowanie lub nawyki online?”

Poproś kilku uczestników, aby podzielili się swoimi przemyśleniami, podkreślając, że świadomość tych zagrożeń jest pierwszym krokiem do lepszej ochrony danych osobowych.

5. Na koniec - podsumuj kluczowy punkt dyskusji (na przykład: Rozpoznając te zagrożenia prywatności, przejmujesz kontrolę nad swoją obecnością online. Świadomość pozwala podejmować lepsze decyzje dotyczące tego, co udostępniasz i jak wchodzisz w interakcje online).





Krok 2: Analiza rzeczywistych przypadków naruszenia prywatności (10 min)

1. Zaczynij od udostępnienia związanego z tematem i istotnego scenariusza, aby zilustrować, w jaki sposób nadmierne udostępnianie online może prowadzić do poważnych naruszeń prywatności. Wyjaśnij uczestnikom, że ta historia nie jest czymś niespotykanym. Wiele osób nieświadomie udostępnia dane osobowe, które cyberprzestępcy lub złośliwe osoby mogą wykorzystać do śledzenia ich, włamania się na ich konta, a nawet kradzieży ich tożsamości. Podkreśl, że naruszenia prywatności często zaczynają się od małych, pozornie nieszkodliwych informacji.

2. Pokaż uczestnikom krótki scenariusz, oparty na historii Sarah lub innej przykładowej sytuacji:

Przykład innego scenariusza:

“Alex pobrał bezpłatną aplikację mobilną bez zapoznania się z jej uprawnieniami. Aplikacja miała dostęp do jego lokalizacji, kontaktów i plików multimedialnych. Wkrótce potem zauważył dziwne wiadomości wysyłane do jego znajomych. Okazało się, że aplikacja zbierała jego dane i wysyłała spam przy użyciu jego konta”.





Krok 2: Analiza rzeczywistych przypadków naruszenia prywatności (10 min)

3. Przekaż uczestnikom instrukcje:

Pracuj indywidualnie lub w małych grupach, aby przeanalizować sytuację.

- Co poszło nie tak? Jakie działania lub zachowania spowodowały naruszenie?
- Jak można było temu zapobiec? Zidentyfikuj proste kroki lub nawyki w celu ochrony danych osobowych.

Opisz krótko swoje przemyślenia.

4. Niech uczestnicy podzielą się swoimi przemyśleniami w następujący sposób:

- „Czy ty lub ktoś, kogo znasz, spotkał się z podobnym problemem, takim jak phishing, hakerstwo lub nadmierne udostępnianie informacji?”
- „Dlaczego ludzie udostępniają tak wiele danych osobowych, nie biorąc pod uwagę ryzyka?”
- Możliwe powody:
 - Zaufanie do aplikacji lub platform.
 - Niezdawanie sobie sprawy z konsekwencji.
 - Niezrozumiałe ustawienia prywatności.

Zachęcaj do otwartego, wspierającego dzielenia się doświadczeniami lub spostrzeżeniami.





Krok 3: Praktyczne strategie ochrony danych osobowych (10 min)

1. Projekcja filmu

Wyświetl film Jak chronić swoje dane w internecie. Zachęć uczestników do zwrócenia szczególnej uwagi na praktyczne, możliwe do zastosowania strategie przedstawione w filmie. Podkreśl, że te wskazówki są łatwe do wdrożenia, ale mogą znacznie poprawić prywatność w internecie.

2. Aktywność – “Plan ochrony prywatności”

Poproś uczestników o zapisanie trzech działań, które podejmą w celu ochrony swojej prywatności w internecie.

Zachęć ich do rozważenia:

- Dostosowania ustawień prywatności w mediach społecznościowych.
- Sprawdzenia uprawnień aplikacji na swoich urządzeniach.
- Zwracania uwagi na to, co publikują publicznie.

3. Dzielenie się w grupie

Poproś uczestników, aby podzielili się z grupą jednym działaniem, które planują wdrożyć. Skorzystaj z następujących podpowiedzi, aby poprowadzić dyskusję:

- „Która strategia wydaje ci się najłatwiejsza do rozpoczęcia dzisiaj i dlaczego?”
- „Jakie wyzwania możesz napotkać, próbując przyjąć te nawyki?”
- „Jak możemy pokonać częste bariery które napotykamy, takie jak zapominanie o dostosowaniu ustawień lub bycie niepewnym w stosowaniu narzędzi?”

Zachęć grupę do udzielenia praktycznych wskazówek lub podzielenia się osobistymi doświadczeniami na temat tego, jak pokonali podobne wyzwania. Podkreśl, że konsekwentne podejmowanie małych kroków może prowadzić do znacznej poprawy prywatności w internecie.

4. Dodatkowo możesz poprosić uczestników, aby zastanowili się, w jaki sposób mogą podzielić się tymi strategiami z przyjaciółmi lub rodziną.





Krok 4: Podsumowanie i wnioski:

1. Poproś uczestników o zastanowienie się:

- „Jaki jest jeden nawyk, który zmienisz, aby poprawić swoją prywatność w internecie, zaczynając od dzisiaj?”
- „Jak podzielisz się tym, czego się nauczyłeś z przyjaciółmi lub rodziną?”

2. Podkreśl główne założenia lekcji:

- Małe zmiany, takie jak dostosowanie ustawień lub ograniczenie tego, co udostępniasz, mają duży wpływ.
- Ochrona danych daje kontrolę nad tożsamością cyfrową.

3. Zakończ lekcję podsumowaniem. Na przykład: "Twoje dane osobowe są cenne. Podejmij małe, przemyślane kroki, aby je chronić, a będziesz bezpieczniejszy w internecie".

Kluczowe wnioski:

Pod koniec lekcji uczestnicy powinni wyraźnie zrozumieć, że prywatność w internecie zaczyna się od świadomości i małych, możliwych do podjęcia kroków. Proste zmiany, takie jak dostosowanie uprawnień aplikacji, przeglądanie ustawień prywatności w mediach społecznościowych i zwracanie uwagi na to, co jest udostępniane publicznie, mogą znacznie zmniejszyć ryzyko. Zachęcaj uczestników do przejęcia kontroli nad ich cyfrowym zachowaniem poprzez rozwijanie nawyków, takich jak sprawdzanie, kto ma dostęp do ich danych i zachowanie ostrożności w przypadku podejrzanych linków lub wiadomości. Wspieraj ideę, w której ochrona danych osobowych umożliwia jednostkom zachowanie kontroli nad ich cyfrową tożsamością i bezpieczeństwem.





Działania uzupełniające i zadanie domowe:

Poproś uczestników, aby w ciągu najbliższych dni wdrożyli co najmniej jedno działanie dotyczące prywatności, które zidentyfikowali podczas sesji. Może to obejmować sprawdzenie ustawień prywatności na jednej z platform mediów społecznościowych, usunięcie nieużywanych aplikacji lub podzielenie się wskazówkami dotyczącymi prywatności z przyjaciółmi lub członkami rodziny. Zasugeruj, aby udokumentowali swoje postępy i zastanowili się, w jaki sposób te zmiany sprawiają, że czują się bezpieczniej w internecie. Ponadto zachęć uczestników do zapoznania się z narzędziami takimi jak DuckDuckGo (prywatna wyszukiwarka) lub Google Privacy Checkup, aby zobaczyć, jak łatwo mogą zwiększyć swoje bezpieczeństwo w internecie. Rozważ zorganizowanie spotkania podsumowującego, podczas którego uczestnicy będą mogli podzielić się swoimi doświadczeniami i omówić napotkane wyzwania.

Wskazówki dla nauczycieli:

Zalecane jest uwzględnienie w dyskusji rzeczywistych przykładów, aby koncepcja prywatności w internecie była zrozumiała. Użyj scenariuszy obejmujących nadmierne udostępnianie informacji w mediach społecznościowych, naruszenia danych lub uprawnienia aplikacji, aby pokazać, jak małe nawyki mogą mieć duże konsekwencje. Stwórz wspierającą przestrzeń dla uczestników, aby mogli dzielić się swoimi doświadczeniami bez osądzania. Aby zapewnić ciągłe zaangażowanie, uwzględnij w lekcjach krótkie, praktyczne zadania, takie jak pokazanie, jak dostosować ustawienia prywatności lub rozpoznać podejrzane linki. Regularnie poruszaj ten temat, aby utrzymać świadomość prywatności i zachęcić uczniów do postrzegania ochrony swoich informacji jako nawyku na całe życie.





Narzędzia

DuckDuckGo



DuckDuckGo jest przeglądarką kładącą duży nacisk na prywatność użytkownika, która nie śledzi historii wyszukiwania ani nie gromadzi danych osobowych. Zapewnia prywatność wyszukiwań i pomaga zminimalizować cyfrowy ślad pozostawiony podczas przeglądania.

duckduckgo.com

Google Privacy Checkup



Google Privacy Checkup to wbudowane narzędzie, które pomaga zarządzać ustawieniami konta Google. Pozwala ono sprawdzić i dostosować, jakie dane osobowe są gromadzone, kto może zobaczyć twoje wyszukiwania oraz które aplikacje mają dostęp do twoich informacji.

myaccount.google.com/privacycheckup



Referencje

- DuckDuckGo (n.d.). Pozyskano z <https://duckduckgo.com>
- Farrier, E. (2024, Sierpień 21). A guide to protecting your personal information. Pozyskano z <https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online>
- Glover, E. (2024, Styczeń 24). What Is Online Privacy?. Built In. Pozyskano z <https://builtin.com/articles/what-is-online-privacy>
- Google Privacy Checkup (n.d.). Pozyskano z <https://myaccount.google.com/privacycheckup>
- Negrean, R. (n.d.). 10 Tips for Protecting Online Privacy: Strategies for Digital Security. Privacy Tutor. Pozyskano z <https://privacytutor.net/10-tips-for-protecting-online-privacy>
- Tech Implement Infra Pvt Ltd. (2024, Grudzień 8). Essential Tips on Protecting Personal and Professional Data Online. [Film]. YouTube. <https://youtu.be/6WQzMAd6mJs?si=cq1NFnjxu7i8NRk5>
- Webb, M. (2023, Listopad 26). How to Protect Your Online Privacy: 7 Best Practices to Implement Today. Techopedia. Pozyskano z <https://www.techopedia.com/how-to/how-to-protect-your-privacy-online>





QUIZ

1. Jakie jest jedno proste działanie, które można podjąć, aby ograniczyć niewłaściwe wykorzystanie danych osobowych w internecie?
 - A. Całkowite unikanie tworzenia kont w mediach społecznościowych
 - B. Wyłączanie wszystkich powiadomień na swoich urządzeniach
 - C. Akceptowanie uprawnień aplikacji bez ich sprawdzania
 - D. Regularne dostosowywanie ustawień prywatności w mediach społecznościowych

2. Które z poniższych działań jest przykładem nadmiernego udostępniania informacji, które może prowadzić do kradzieży tożsamości?
 - A. Udostępnianie zdjęcia z wakacji tylko bliskim znajomym
 - B. Publiczne publikowanie swojej lokalizacji i codziennych czynności
 - C. Wysyłanie zdjęć swoich zwierząt domowych za pośrednictwem prywatnych wiadomości
 - D. Używanie emotikonów do opisywania swojego nastroju w internecie

3. W jaki sposób przeglądanie uprawnień aplikacji może poprawić prywatność online?
 - A. Pozwala ograniczyć aplikacjom dostęp do niepotrzebnych danych osobowych
 - B. Pomaga szybciej pobierać aplikacje, pomijając sprawdzanie uprawnień
 - C. Zapewnia automatyczną aktualizację wszystkich aplikacji na urządzeniu
 - D. Pozwala aplikacjom działać płynniej na urządzeniu





QUIZ

4. Dlaczego wiele osób nie chroni swoich danych osobowych w internecie?

- A. Narzędzia ochrony prywatności są niedostępne dla zwykłych użytkowników
- B. Ludzie ufają firmom, że ich dane są bezpieczne
- C. Ustawienia i narzędzia ochrony prywatności są często pomijane lub postrzegane jako skomplikowane
- D. Większość ludzi uważa, że nie ma danych osobowych wartych ochrony

5. Jaki jest dobry nawyk, który należy wyrobić w celu ochrony danych osobowych?

- A. Używanie tego samego hasła dla wygody
- B. Zezwalanie aplikacjom na śledzenie twojej lokalizacji przez cały czas
- C. Ignorowanie warunków umów o świadczenie usług
- D. Ostrożność w udostępnianiu poufnych informacji na platformach publicznych





Rozwiązania

Pytanie 1: D

Pytanie 2: B

Pytanie 3: A

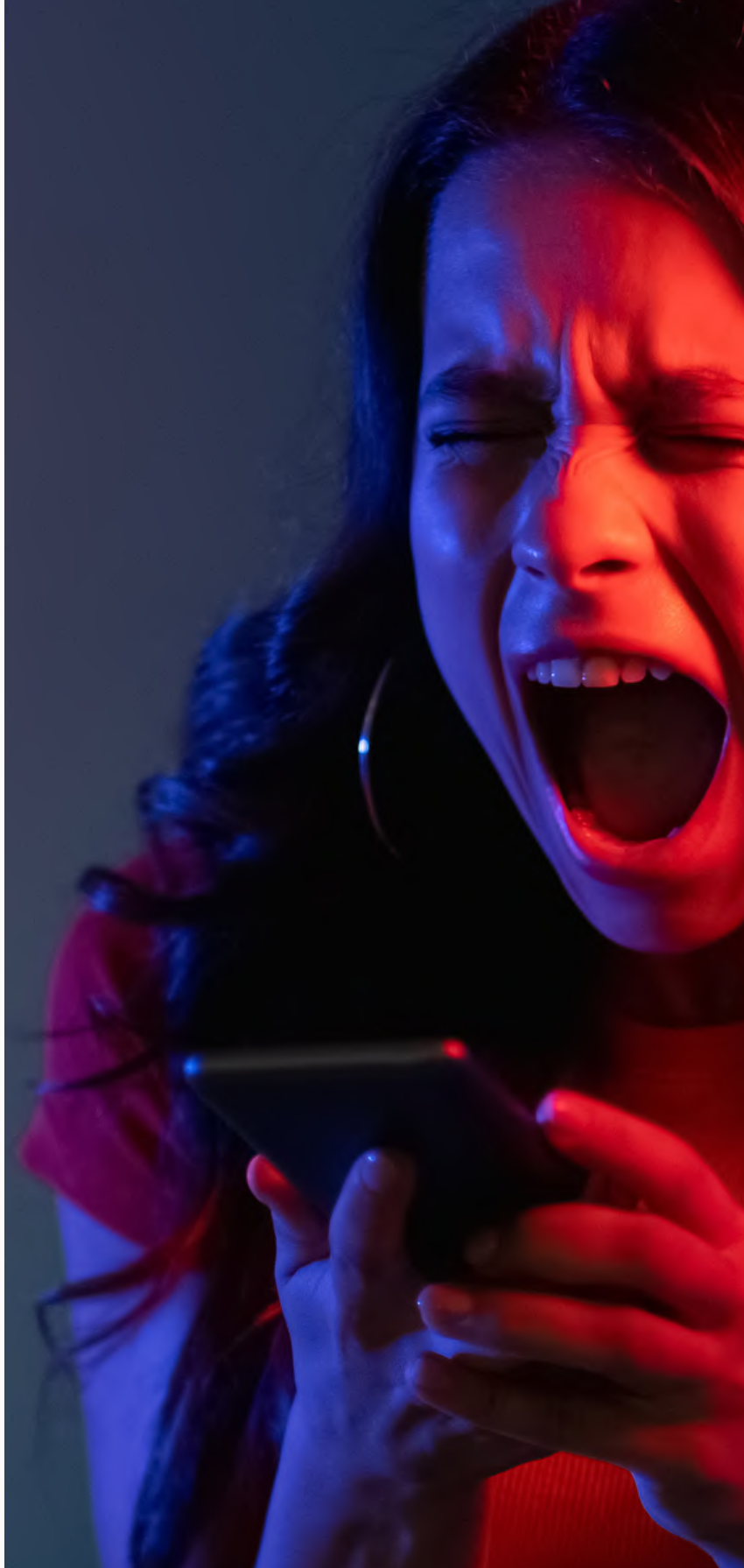
Pytanie 4: C

Pytanie 5: D





Centrum Wspierania
Edukacji
i Przedsiębiorczości



Co-funded by
the European Union

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie ponoszą za nie odpowiedzialności.