



# MODUŁ 5

## CYBERBEZPIECZEŃSTWO I BEZPIECZNE KORZYSTANIE Z INTERNETU



[erasmediah.eu](https://erasmediah.eu)



**Co-funded by  
the European Union**



## Lekcja 5.6

# Praktyczne narzędzia bezpieczeństwa online



**ERASMEDIAH**

Educational Reinforcement Against  
the Social Media Hyperconnectivity



**Co-funded by  
the European Union**

## Lekcja 5.6

# Praktyczne narzędzia bezpieczeństwa online

### Cele:

- Wyposażenie uczestników w praktyczne narzędzia i techniki identyfikacji i ograniczania powszechnych zagrożeń internetowych, w tym phishingu, złośliwego oprogramowania i oszustw.
- Budowanie biegłości w korzystaniu z zasobów cyberbezpieczeństwa, takich jak menedżery haseł, VPN i bezpieczne przeglądarki, przy jednoczesnym wspieraniu zrozumienia zarządzania prywatnością online.
- Promowanie bezpiecznych i odpowiedzialnych praktyk online poprzez krytyczną ocenę platform cyfrowych, rozpoznawanie znaków ostrzegawczych cyberzagrożeń i przyjmowanie nawyków ochronnych, takich jak zgłaszanie podejrzanych działań.

### Kluczowe przesłanie:

- Świadomość i przygotowanie to pierwsza linia obrony. Zrozumienie zagrożeń online i posiadanie odpowiednich narzędzi umożliwia bezpieczne poruszanie się po cyfrowym świecie.
- Twoje bezpieczeństwo jest w twoich rękach. Wykorzystanie praktycznych narzędzi, takich jak VPN, bezpieczne przeglądarki i ustawienia prywatności, pozwala chronić dane osobowe i zachować kontrolę nad swoją obecnością w internecie.



RODZAJ LEKCJI:





# Przegląd lekcji

Bezpieczeństwo online zależy w dużej mierze od umiejętności skutecznego korzystania z narzędzi zaprojektowanych w celu ochrony danych osobowych i zapobiegania zagrożeniom cyfrowym. Ta lekcja kładzie nacisk na praktyczne, praktyczne zaangażowanie w kluczowe narzędzia cyberbezpieczeństwa, takie jak menedżery haseł, VPN i ustawienia prywatności. Uczestnicy będą aktywnie badać, jak działają te narzędzia, testować ich funkcje i uczyć się strategii włączania ich do codziennej cyfrowej rutyny. Dzięki ćwiczeniom z przewodnikiem zbudują zaufanie do stosowania tych narzędzi w celu ochrony swojej obecności w internecie i reagowania na zagrożenia za pomocą praktycznych rozwiązań.

## **Warsztaty podzielone są na 4 etapy:**

- 1: Wprowadzenie do narzędzi bezpieczeństwa online (10 min)
- 2: Praktyczne zapoznanie się z narzędziami (15 min)
- 3: Zarządzanie ryzykiem w oparciu o scenariusze (10 min)
- 4: Końcowe przemyślenia (5 min)





## Krok 1

# Wprowadzenie do narzędzi bezpieczeństwa online

Czy kiedykolwiek natknąłeś się w sieci na coś, co wydało ci się podejrzane? Może dziwna wiadomość e-mail z prośbą o zresetowanie hasła, wyskakujące okienko oferujące darmową nagrodę lub strona internetowa prosząca o podanie zbyt wielu danych osobowych? Takie sytuacje mogą wydawać się ryzykowne - i często takie są.

Dobłą wiadomością jest to, że istnieją **praktyczne narzędzia**, których można użyć, aby chronić się w takich chwilach. Pod koniec tego ćwiczenia będziesz wiedział, jak rozpoznać te zagrożenia i korzystać z narzędzi, takich jak menedżery haseł, VPN i ustawienia prywatności, aby zachować bezpieczeństwo w internecie. Sprawdźmy, jak te narzędzia mogą ci pomóc!



## Krok 1

# Wprowadzenie do narzędzi bezpieczeństwa online

Oto trzy proste narzędzia, które mogą uczynić twoje życie online znacznie bezpieczniejszym:

- **Menedżery haseł:** Pomagają one tworzyć i przechowywać silne, unikalne hasła, dzięki czemu nie trzeba ich wszystkich zapamiętywać.
- **VPN (wirtualne sieci prywatne):** Chronią one aktywność online, zwłaszcza w publicznych sieciach Wi-Fi, zapewniając bezpieczeństwo połączenia.
- **Ustawienia prywatności przeglądarki:** Pozwalają one kontrolować, jakie informacje o użytkowniku mogą gromadzić witryny internetowe, takie jak lokalizacja lub nawyki przeglądania.

Skupimy się dziś na tych narzędziach, ponieważ mogą one mieć ogromny wpływ na bezpieczeństwo w internecie.

Pomyśl o tym, kiedy ostatnio natknąłeś się w sieci na coś, co wydało ci się niewiarygodne - może stronę internetową, która nie wydawała się godna zaufania. Jak sobie z tym poradziłeś? Zignorowałeś to, sprawdziłeś dalej, a może nawet kliknąłeś?

Zróbmy razem burzę mózgów:

- Jakiego rodzaju zagrożeń lub ryzyka online zauważyłeś wcześniej?
- Jakich narzędzi lub strategii już używasz, aby zachować bezpieczeństwo online?

Poświęcimy kilka minut na podzielenie się pomysłami w grupie. Nie martw się, jeśli nie doświadczyłeś tego na własnej skórze - historie twoich rówieśników mogą pobudzić cię do nowych przemyśleń.



## Krok 2

# Praktyczne zapoznanie się z narzędziami

Teraz nadszedł czas, aby zanurzyć się i zbadać, w jaki sposób proste narzędzia mogą uczynić twoją obecność w internecie bezpieczniejszą. W tym ćwiczeniu wypróbujesz ustawienia prywatności przeglądarki i przetestujesz swoje umiejętności tworzenia haseł za pomocą *The Password Meter*. Zaczynamy!

## Część 1: Ustawienia prywatności przeglądarki

Przeglądarka może kontrolować ilość informacji zbieranych o użytkowniku przez witryny internetowe. Sprawdźmy i dostosujmy ustawienia prywatności:

1. Otwórz ustawienia prywatności przeglądarki (poszukaj „Ustawienia” lub „Preferencje”, a następnie przejdź do „Prywatność” lub „Bezpieczeństwo”).
2. Sprawdź te kluczowe obszary:
  - **Zapobieganie śledzeniu:** Czy jest włączone?
  - **Pliki cookie:** Czy pliki cookie innych firm są zablokowane?
  - **Uprawnienia:** Które witryny mają dostęp do lokalizacji, kamery lub mikrofonu?



## Krok 2

# Praktyczne zapoznanie się z narzędziami

3. Dokonaj modyfikacji: Włącz wszystkie ustawienia prywatności, które twoim zdaniem pomogą chronić twoje dane.

Na przykład:

- Zablokuj śledzące pliki cookie.
- Wyłącz udostępnianie lokalizacji w witrynach, którym nie ufasz.

Szybka refleksja: Co zaskoczyło cię w twoich obecnych ustawieniach? Czy wprowadziłeś jakieś zmiany?

## Część 2: Testowanie siły hasła za pomocą *The Password Meter*

Tworzenie silnych haseł jest jednym z najprostszych sposobów ochrony kont. Sprawdźmy teraz, jak bezpieczne są twoje hasła:

1. Przejdź do [The Password Meter](#).
2. Wymyśl nowe hasło (nie używaj hasła, którego już używasz!)





## Krok 2

# Praktyczne zapoznanie się z narzędziami

3. Wprowadź hasło do *The Password Meter* i sprawdź informacje zwrotne:

- Jak silne jest twoje hasło?
- Jakie są sugestie, aby je wzmocnić?

4. Eksperymentuj, zmieniając hasło w oparciu o informacje zwrotne (np. dodając symbole, wydłużając je lub łącząc małe i wielkie litery). Zobacz, jak poprawia się wynik!

Szybka refleksja: Jak łatwe lub trudne było stworzenie silnego hasła? Jaka jest jedna rzecz, którą zrobisz inaczej podczas ustawiania haseł w przyszłości?

Pod koniec tego ćwiczenia poprawisz ustawienia prywatności swojej przeglądarki i nauczysz się tworzyć silniejsze hasła!



### Krok 3

## Zarządzanie ryzykiem w oparciu o scenariusze

Po zapoznaniu się z kilkoma praktycznymi narzędziami, zobaczmy, jak można je zastosować w rzeczywistych sytuacjach. Będziesz pracować w małych grupach, aby przeanalizować scenariusze, zidentyfikować ryzyko i zdecydować, jak sobie z nim poradzić za pomocą omówionych narzędzi. Przeczytaj scenariusz, który otrzymała twoja grupa. Oto kilka przykładów:

1. Otrzymujesz wiadomość e-mail z informacją, że wygrałeś nagrodę, ale link wygląda podejrzanie. Co powinieneś zrobić?
2. Aplikacja społecznościowa prosi o dostęp do lokalizacji, kamery i mikrofonu podczas instalacji. Czy należy na to zezwolić?
3. Korzystasz z publicznej sieci Wi-Fi w kawiarni i zostajesz poproszony o zalogowanie się do nieznanej witryny. Jak zachować bezpieczeństwo?

Porozmawiaj z grupą o zagrożeniach w tym scenariuszu. Zadajcie sobie pytania:

- *Co może pójść nie tak, jeśli nie będziesz działać ostrożnie?*
- *Dlaczego ta sytuacja wydaje się niebezpieczna?*

Zdecydujcie, w jaki sposób możecie użyć praktycznych narzędzi, aby poradzić sobie z ryzykiem. Na przykład:

- *Użyj ustawień prywatności przeglądarki, aby zablokować niepotrzebne uprawnienia.*
- *Unikaj klikania podejrzanych linków i sprawdzaj wiadomości e-mail pod kątem phishingu.*
- *Włącz VPN, aby zabezpieczyć połączenie w publicznej sieci Wi-Fi.*



### Krok 3

## Zarządzanie ryzykiem w oparciu o scenariusze

Po kilku minutach każda grupa podzieli się swoimi spostrzeżeniami:

- *Jakie zagrożenia zauważyliście w scenariuszu*
- *Jakich narzędzi lub kroków użyliście, aby zachować bezpieczeństwo*

**Zastanów się nad tym:** W jaki sposób te narzędzia mogą pomóc ci w twoich własnych działaniach online?

Praktyczne narzędzia, takie jak ustawienia prywatności przeglądarki, VPN i wykrywanie phishingu, mogą zmienić ryzykowne sytuacje w możliwe do opanowania. Regularne korzystanie z nich znacznie ułatwia zachowanie bezpieczeństwa online!

Zastanówmy się nad tym, czego się nauczyłeś i jak możesz to wykorzystać, aby zachować bezpieczeństwo w internecie.

## Krok 1: Zastanów się

Zastanów się nad tymi pytaniami:

- Które narzędzie (np. ustawienia prywatności przeglądarki, VPN, menedżery haseł) było dla ciebie najbardziej przydatne? Dlaczego?
- Jak zmienił się twój pogląd na bezpieczeństwo online po użyciu tych narzędzi?

## Krok 2: Zaplanuj następny krok

Zapisz jedno działanie, które podejmiesz, aby poprawić swoje bezpieczeństwo online.

- Co zamierzasz zrobić? (np. „Będę używać menedżera haseł do tworzenia silnych haseł.”)
- Kiedy to zrobisz? (np. „Do końca tygodnia.”)

Praktyczne narzędzia to twój pierwszy krok - bądź konsekwentny, aby zapewnić sobie bezpieczeństwo w sieci!

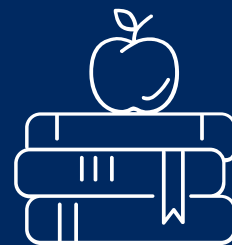






## Podsumowanie kluczowych wniosków

- **Ustawienia prywatności przeglądarki, menedżery haseł i sieci VPN to proste, ale potężne narzędzia zwiększające bezpieczeństwo online.**
- **Aktywnie zarządzaj informacjami, które udostępniasz online, dostosowując ustawienia prywatności i ograniczając niepotrzebne uprawnienia.**
- **Regularnie aktualizuj ustawienia prywatności, twórz bezpieczne hasła i sprawdzaj uprawnienia aplikacji, aby bezpieczeństwo online stało się rutynową częścią twojego cyfrowego życia.**
- **Bądź proaktywny - łączenie narzędzi z krytycznym myśleniem i byciem na bieżąco gwarantuje, że jesteś przygotowany na zmieniające się zagrożenia online.**
- **Spróbuj również przetestować inne praktyczne narzędzia online, aby zrozumieć i poprawić swoje bezpieczeństwo cyfrowe - im więcej narzędzi wiesz, jak z nich korzystać, tym bardziej zwiększysz swoje bezpieczeństwo!**



# Instrukcje dla osób pracujących z młodzieżą, edukatorów i nauczycieli

## **Cel:**

Ta lekcja koncentruje się na wyposażeniu uczestników w praktyczne umiejętności korzystania z podstawowych narzędzi bezpieczeństwa online. Poprzez indywidualne i grupowe ćwiczenia i dyskusje, zdobędą umiejętność identyfikowania i radzenia sobie z typowymi zagrożeniami online, wzmocnią swoją cyfrową ochronę za pomocą zasobów takich jak menedżery haseł, VPN i ustawienia prywatności oraz zintegrują bezpieczniejsze nawyki z codziennymi działaniami online.

## **Potrzebne materiały:**

- Dostęp do internetu w celu testowania narzędzi (np. VPN, menedżerów haseł)
- Laptopy, tablety lub smartfony do ćwiczeń praktycznych
- Tablica lub flipchart do burzy mózgów i podsumowywania dyskusji
- Puste kartki papieru do robienia notatek
- Długopisy, ołówki lub kolorowe markery





## **Krok 1: Wprowadzenie do narzędzi bezpieczeństwa online (10 min)**

1. Rozpocznij od zadania uczestnikom pytania, które można odnieść do ich sytuacji: „Czy kiedykolwiek natknąłeś się w Internecie na coś, co wydawało się podejrzane, na przykład dziwny e-mail, wyskakujące okienko oferujące nagrodę lub stronę internetową proszącą o podanie zbyt wielu danych osobowych?”. Krótko wyjaśnij, że takie sytuacje mogą wydawać się ryzykowne i często takie są, ale istnieją praktyczne narzędzia, aby sobie z nimi poradzić.
2. Przedstaw sesję skupiającą się na trzech podstawowych narzędziach: menedżerach haseł, sieciach VPN i ustawieniach prywatności przeglądarki. Podkreśl ich znaczenie, wyjaśniając, że menedżery haseł pomagają tworzyć i przechowywać silne, unikalne hasła, sieci VPN zabezpieczają aktywność online w publicznych sieciach Wi-Fi, a ustawienia prywatności przeglądarki kontrolują, jakie informacje mogą gromadzić strony internetowe, takie jak lokalizacja lub nawyki przeglądania.
3. Zachęć uczestników do zastanowienia się nad własnymi doświadczeniami związanymi z zagrożeniami online, pytając: „Pomyśl o tym, kiedy ostatnio spotkałeś się z czymś podejrzanym online. Jak sobie z tym poradziłeś?”.
4. Poprowadź krótką dyskusję, zadając pytania takie jak: „Jakie rodzaje zagrożeń online zauważyłeś?” i „Jakich narzędzi lub strategii już używasz, aby zachować bezpieczeństwo?”. Poproś uczestników, aby podzielili się swoimi historiami lub pomysłami, podkreślając, że uczenie się od siebie nawzajem może zaowocować nowymi spostrzeżeniami.
5. Zakończ, podkreślając znaczenie tych narzędzi w zarządzaniu zagrożeniami online, stwierdzając: „Korzystając z narzędzi takich jak menedżery haseł, sieci VPN i ustawienia prywatności, możesz pewnie poruszać się po cyfrowym świecie, jednocześnie chroniąc swoje dane osobowe”. Utrzymuj dyskusję interaktywną i wspierającą, upewniając się, że uczestnicy czują się zachęceni do dzielenia się swoimi przemyśleniami i uczenia się od grupy.





## **Krok 2: Praktyczne zapoznanie się z narzędziami (15 min)**

1. Rozpocznij od wyjaśnienia celu tego ćwiczenia: poznania praktycznych narzędzi, które zwiększają bezpieczeństwo online poprzez ustawienia prywatności przeglądarki i testowanie siły hasła.
2. Podziel ćwiczenie na dwie części, aby zapewnić ustrukturyzowane podejście.

### **Część 1: Ustawienia prywatności w przeglądarce (8 minut)**

1. Poproś uczestników, aby otworzyli ustawienia prywatności swojej przeglądarki (przejdź do „Ustawień” lub „Preferencji”, a następnie znajdź „Prywatność” lub „Bezpieczeństwo”). Poproś ich o przejrzanie kluczowych obszarów:

- Zapobieganie śledzeniu: Upewnij się, że jest włączone.
- Pliki cookie: Sprawdź, czy pliki cookie innych firm są zablokowane.
- Uprawnienia: Sprawdź, które strony internetowe mogą uzyskać dostęp do lokalizacji, kamery lub mikrofonu.

2. Zachęć uczestników do wprowadzenia zmian, takich jak zablokowanie śledzących plików cookie lub wyłączenie niepotrzebnego udostępniania lokalizacji.

3. Następnie poproś o krótką refleksję: „Co zaskoczyło cię w twoich obecnych ustawieniach? Czy wprowadziłeś jakieś zmiany?”. Pomoże to uczestnikom połączyć ich odkrycia z wartością tych narzędzi.

### **Część 2: Testowanie siły hasła (5 minut)**

1. Poproś uczestników o przejście do The Password Meter. Poproś ich o utworzenie nowego hasła (nie takiego, którego obecnie używają) i przetestowanie jego siły.

2. Zachęć ich do przeanalizowania informacji zwrotnych i eksperymentowania ze zmianami, takimi jak dodawanie symboli, mieszanie przypadków lub zwiększanie długości, aby zobaczyć, jak poprawia się wynik.

3. Zakończ refleksją: „Jak łatwe lub trudne było stworzenie silnego hasła? Jaką jedną rzecz zrobisz inaczej podczas ustawiania haseł w przyszłości?”

4. Zakończ ćwiczenie, podkreślając jego praktyczną wartość.

5. Utrzymuj sesję praktyczną i angażującą, oferując wskazówki w razie potrzeby, podczas gdy uczestnicy odkrywają i stosują te narzędzia.





### **Krok 3: Zarządzanie ryzykiem w oparciu o scenariusze (10 min)**

1. To ćwiczenie pomaga uczestnikom zastosować narzędzia bezpieczeństwa online w rzeczywistych scenariuszach. Podziel uczestników na małe grupy i przydziel każdej z nich scenariusz, np:

- Podejrzana wiadomość e-mail z linkiem do nagrody.
- Aplikacja społecznościowa żądająca nadmiernych uprawnień.
- Korzystanie z publicznej sieci Wi-Fi i spotkanie nieznanego monitu o logowanie.

2. Poinstruuuj grupy, aby omówiły ryzyko, zastanawiając się:

- „Co może pójść nie tak, jeśli nie będziesz działać ostrożnie?”
- „Dlaczego ta sytuacja wydaje się niebezpieczna?”

3. Niech określą, jak radzić sobie z ryzykiem za pomocą narzędzi, takich jak ustawienia prywatności przeglądarki, unikanie linków phishingowych lub włączenie VPN.

4. Następnie każda grupa dzieli się zidentyfikowanymi zagrożeniami i narzędziami, których użyła, aby im zaradzić.

5. Zakończ, podkreślając: „Narzędzia takie jak ustawienia prywatności, VPN i wykrywanie phishingu ułatwiają zarządzanie zagrożeniami online. Regularne korzystanie z tych narzędzi zwiększa bezpieczeństwo online”. Skoncentruj się na sesji i zachęcaj do praktycznych, użytecznych spostrzeżeń.





## **Krok 4: Końcowe przemyślenia (5 min)**

1. Zakończ sesję, prowadząc uczestników przez ćwiczenie refleksyjne w celu utrwalenia zdobytej wiedzy. Rozpocznij od poproszenia ich o zastanowienie się:

- „Które narzędzie (np. ustawienia prywatności przeglądarki, VPN, menedżery haseł) było dla ciebie najbardziej przydatne? Dlaczego?”
- „Jak zmienił się twój pogląd na bezpieczeństwo online po użyciu tych narzędzi?”

2. Zachęć uczestników do krótkiego podzielenia się swoimi przemyśleniami, tworząc sprzyjające środowisko do dyskusji.

3. Następnie zachęć ich do zaplanowania konkretnych działań mających na celu zwiększenie ich bezpieczeństwa w sieci, np:

- „Co zrobisz?” (np. „Będę używać menedżera haseł do tworzenia silnych haseł.”)
- „Kiedy to zrobisz?” (np. „Do końca tygodnia.”)

4. Zakończ, podkreślając znaczenie spójności, przypominając uczestnikom: „Praktyczne narzędzia to twój pierwszy krok - pozostań konsekwentny, aby zachować bezpieczeństwo online!”. Zachowaj motywujący ton i skup się na zastosowaniu wyciągniętych wniosków w codziennych praktykach online.

## **Kluczowe wnioski:**

Po ukończeniu lekcji uczestnicy zyskają jasne zrozumienie, jak korzystać z podstawowych narzędzi, takich jak menedżery haseł, VPN i ustawienia prywatności przeglądarki, aby zwiększyć swoje bezpieczeństwo online. Nauczą się identyfikować typowe zagrożenia, takie jak śledzenie danych, i podejmować proaktywne kroki w celu ochrony swoich danych osobowych. Włączając te narzędzia i strategie do swojej codziennej rutyny, będą mogli pewnie poruszać się po cyfrowym świecie, minimalizując potencjalne zagrożenia. Aby skutecznie przekazać te wnioski, należy użyć powiązanych scenariuszy i jasnych przykładów, aby zademonstrować rzeczywisty wpływ tych narzędzi na codzienne bezpieczeństwo online.



## **Działania uzupełniające i zadanie domowe:**

Zainspiruj uczestników, aby przyjrzeć się bliżej swoim obecnym praktykom online, przeglądając i dostosowując ustawienia prywatności przeglądarki, testując siłę swoich haseł za pomocą narzędzi takich jak The Password Meter i badając funkcjonalność VPN. Przydziel ich do oceny uprawnień często używanych aplikacji, zwracając uwagę na potencjalne zagrożenia i wdrażając bezpieczniejsze alternatywy. Na koniec poproś uczestników, aby podzielili się jedną nowo poznaną wskazówką dotyczącą bezpieczeństwa z przyjacielem lub członkiem rodziny, wzmacniając swoją wiedzę i szerząc świadomość na temat bezpieczeństwa cyfrowego.

## **Wskazówki dla nauczycieli:**

Możesz użyć praktycznych, rzeczywistych przykładów i innych interaktywnych ćwiczeń, aby zademonstrować, w jaki sposób narzędzia takie jak menedżery haseł, VPN i ustawienia prywatności mogą być skutecznie wykorzystywane w celu zwiększenia bezpieczeństwa online. Pokaż uczestnikom krok po kroku, jak nawigować i konfigurować te narzędzia, dzięki czemu sesja będzie konkretna i praktyczna. Stwórz otwarte i wspierające środowisko, w którym uczestnicy czują się komfortowo omawiając swoje doświadczenia z zagrożeniami online i zadając pytania. Podkreśl znaczenie regularnego korzystania z tych narzędzi i włączania ich do codziennych rutynowych czynności online w celu zapewnienia spójnej i proaktywnej ochrony cyfrowej.





## Narzędzia

### Get Safe Online



Wszechstronna strona internetowa oferująca bezpłatne, proste porady dotyczące szerokiego zakresu tematów związanych z bezpieczeństwem online. Zawiera praktyczne przewodniki dotyczące ochrony danych osobowych, unikania oszustw i bezpiecznej komunikacji online. Treść jest przyjazna dla użytkownika i przeznaczona dla osób o minimalnej wiedzy technicznej.

[www.getsafeonline.org](http://www.getsafeonline.org)

### The Password Meter



Bezpłatne narzędzie, które ocenia siłę haseł i dostarcza wskazówek, jak je poprawić. Uczniowie mogą eksperymentować z tworzeniem haseł i otrzymywać natychmiastowe informacje zwrotne na temat ich poziomu bezpieczeństwa, dzięki czemu jest to interaktywny sposób na zrozumienie znaczenia silnych haseł.

[passwordmeter.com](http://passwordmeter.com)





## Referencje

- Alice. (2022, Październik 3). 5 Tools That Help Keep People Safe Online. Ryadel. Pozyskano z <https://www.ryadel.com/en/5-privacy-data-protection-security-tools>
- Get Safe Online. (n.d.). Pozyskano z <https://www.getsafeonline.org>
- Goodwall Team. (2022, Marzec 24). 7 Best Online Safety Tools and Privacy Settings to Keep Yourself Protected. Pozyskano z <https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings>
- Lakhwani, S. (2024, Czerwiec 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Pozyskano z <https://www.knowledgehut.com/blog/security/cyber-security-fundamentals>
- The Password Meter. (n.d.). Pozyskano z <https://passwordmeter.com>
- Vodafone. (n.d.). Using online safety and wellbeing tools. Pozyskano z <https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools>





## QUIZ

1. Jaka jest podstawowa funkcja wirtualnej sieci prywatnej (VPN)?
  - A. Zapewnienie automatycznej ochrony antywirusowej
  - B. Zwiększenie prędkości internetu
  - C. Zapobieganie wyskakującym reklamom na wszystkich stronach internetowych
  - D. Szyfrowanie aktywności online, zwłaszcza w publicznych sieciach Wi-Fi
  
2. Które zachowanie może zagrozić bezpieczeństwu online?
  - A. Używanie silnych, unikalnych haseł dla każdego konta
  - B. Regularne dostosowywanie ustawień prywatności w przeglądarce
  - C. Używanie menedżera haseł do przechowywania danych logowania
  - D. Klikanie każdego linku w niechcianych wiadomościach e-mail
  
3. Jaki jest zalecany krok w celu ulepszenia ustawień prywatności przeglądarki?
  - A. Używanie domyślnych ustawień bez modyfikacji
  - B. Blokowanie śledzących plików cookie i wyłączanie niepotrzebnych uprawnień
  - C. Wyłączanie plików cookie dla wszystkich witryn
  - D. Zezwalanie wszystkim witrynom na dostęp do twojej lokalizacji





## QUIZ

4. Jaki jest cel ustawień prywatności przeglądarki?

- A. Aby przyspieszyć przeglądanie
- B. Aby bezpiecznie przechowywać hasła użytkownika
- C. Aby kontrolować, jakie informacje o użytkowniku mogą gromadzić strony internetowe
- D. Aby zapobiec wyskakującym reklamom na wszystkich stronach internetowych

5. Jak można poprawić siłę hasła?

- A. Włączając symbole, mieszając wielkości liter i zwiększając długość
- B. Używając popularnych fraz, które są łatwe do zapamiętania
- C. Unikając używania cyfr i znaków specjalnych
- D. Wielokrotnie testując to samo hasło





# Rozwiązania

Pytanie 1: D

Pytanie 2: D

Pytanie 3: B

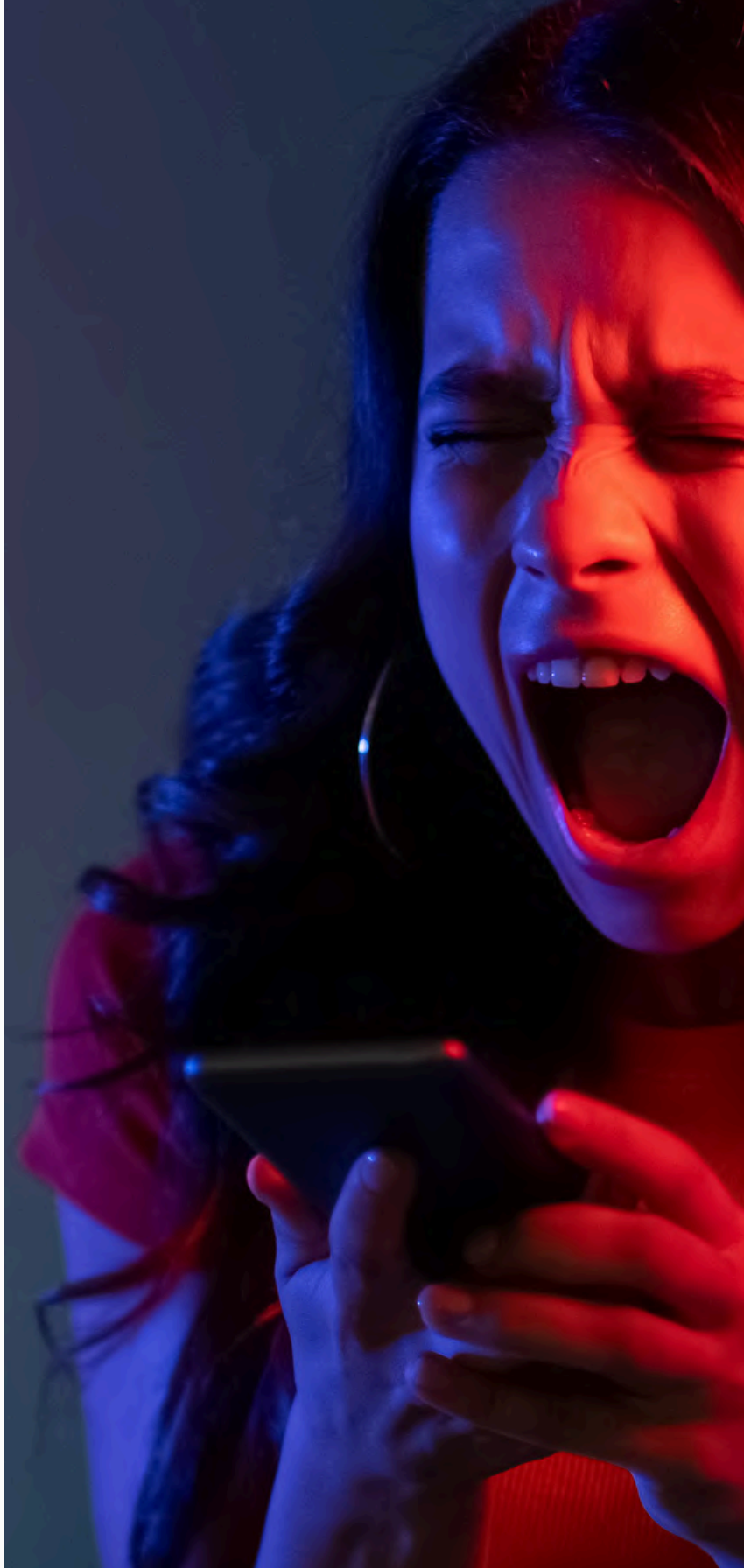
Pytanie 4: C

Pytanie 5: A





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.