



Co-funded by
the European Union



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

MODUŁ 1: Podstawy kompetencji cyfrowych

PLAN WARSZTATÓW

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Projekt nr 2023-1-PL01-KA220-ADU-000156610

Project website <https://www.remcreadwomen.eu/>



Moduł 1. Wprowadzenie do narzędzi cyfrowych. Kompetencje cyfrowe (Digital literacy).

Wprowadzenie

Kompetencje cyfrowe to zdolność do efektywnego i bezpiecznego korzystania z technologii cyfrowych, narzędzi, aplikacji i platform internetowych. Obejmuje ona takie umiejętności jak

1. **Obsługa urządzeń** (komputery, smartfony, tablety itp.).
2. **Zarządzanie informacjami** - wyszukiwanie, ocena i korzystanie z treści cyfrowych.
3. **Komunikacja online** - korzystanie z narzędzi takich jak poczta elektroniczna, media społecznościowe i wideokonferencje.
4. **Bezpieczeństwo online** - rozpoznawanie zagrożeń, ochrona danych osobowych i prywatności.
5. **Krytyczne myślenie** - ocena wiarygodności informacji i unikanie dezinformacji.

Kompetencje cyfrowe to zestaw podstawowych i kluczowych umiejętności niezbędnych w dzisiejszym społeczeństwie opartym na technologii do efektywnego uczestnictwa w życiu zawodowym, edukacyjnym i społecznym.

Warto uwzględnić też, że kompetencje cyfrowe (Digital Literacy) obejmują:

- Umiejętności techniczne, posługiwanie się technologią.
- Umiejętności poznawcze - wykorzystywanie mózgu do oceny, krytyki i stosowania wiedzy.
- Umiejętności społeczne - zdolność do interakcji z innymi.

DigComp Framework to ramy odniesienia, które tworzą uzgodnioną wizję tego, co jest potrzebne pod względem kompetencji, aby sprostać wyzwaniom stawianym przez cyfryzację w prawie wszystkich aspektach współczesnego życia. Ich celem jest stworzenie wspólnego zrozumienia przy użyciu uzgodnionego słownictwa, które można następnie konsekwentnie stosować, na przykład do planowania, oceny i monitorowania uczenia się.

Aktualne ramy DigComp 2.2 można znaleźć tutaj

<https://publications.jrc.ec.europa.eu/repository/handle/JRC128415>

Narzędzia do diagnozy kompetencji cyfrowych:

<https://mydigiskills.eu/index.php#header>

<https://europa.eu/europass/digitalskills/screen/home?referrer=epass&route=%2Fpl>



Na potrzeby tego projektu/szkolenia przyjęto następującą matrycę kompetencji:

Podstawy umiejętności cyfrowych - zakres kompetencji:

Kategoria	Wiedza	Umiejętności	Postawy
Podstawy technologii	Znajomość podstawowych urządzeń cyfrowych (komputer, smartfon, tablet). Znajomość systemów operacyjnych (Windows, macOS, Android, iOS).	Umiejętność korzystania z urządzeń cyfrowych i podstawowych aplikacji. Umiejętność rozwiązywania podstawowych problemów technicznych.	Otwartość na nowinki technologiczne, gotowość do samodzielnego rozwiązywania problemów technicznych.
<u>Wyszukiwanie informacji i zarządzanie nimi</u>	Znajomość metod wyszukiwania informacji online, różnych źródeł informacji. Zrozumienie pojęć jakości i wiarygodności źródeł.	Skuteczne wyszukiwanie informacji, filtrowanie wyników, krytyczna ocena źródeł. Umiejętność organizowania danych.	Krytyczne podejście do informacji, dążenie do rzetelności i wiarygodności w zdobywaniu wiedzy.
<u>Bezpieczeństwo cyfrowe</u>	Wiedza na temat ochrony danych, zagrożeń cyberbezpieczeństwa (phishing, złośliwe oprogramowanie, ransomware).	Umiejętności zabezpieczania swoich urządzeń i kont, używania haseł, uwierzytelniania dwuskładnikowego. Rozpoznawanie zagrożeń.	Świadomość zagrożeń, odpowiedzialność za ochronę danych i prywatności. Ostrożność wobec podejrzanych działań online.



Komunikacja cyfrowa	Znajomość narzędzi komunikacji (poczta elektroniczna, komunikatory internetowe, media społecznościowe). Znajomość zasad etykiety cyfrowej (netykiety).	Umiejętność skutecznej i odpowiedzialnej komunikacji online, stosowanie zasad etykiety w komunikacji.	Szacunek dla innych użytkowników, odpowiedzialność za swoje słowa i działania w środowisku cyfrowym.
Tworzenie treści cyfrowych	Znajomość narzędzi do tworzenia treści (edytory tekstu, grafiki, wideo, prezentacje). Znajomość podstawowych formatów plików.	Umiejętność tworzenia, edytowania i publikowania treści cyfrowych. Umiejętność pracy w zespole nad projektami cyfrowymi.	Kreatywność, chęć współpracy i dzielenia się wiedzą. Dbalność o jakość i rzetelność treści cyfrowych.
<u>Prawo i etyka w Internecie</u>	Znajomość praw autorskich, licencjonowania, prywatności i ochrony danych.	Umiejętność stosowania zasad prawa autorskiego, unikanie naruszeń prawa.	Poszanowanie własności intelektualnej, odpowiedzialność prawna i etyczna za treści publikowane online.
Rozwój kompetencji cyfrowych	Znajomość możliwości ciągłego doskonalenia swoich kompetencji cyfrowych, dostępnych kursów i narzędzi edukacyjnych.	Umiejętność samodzielnej nauki, korzystania z dostępnych kursów online, samodoskonalenia umiejętności cyfrowych.	Chęć ciągłego rozwoju, otwartość na nowe technologie i narzędzia. Inicjatywa w poszukiwaniu nowych rozwiązań cyfrowych.



Warsztaty: Wprowadzenie do narzędzi cyfrowych/ kompetencje cyfrowe

Opracowane i zamieszczone poniżej materiały koncentrują się na trzech kluczowych blokach tematycznych:

- 1.1 Wyszukiwanie informacji i zarządzanie nimi
- 1.2 Bezpieczeństwo cyfrowe
- 1.3 Prawo i etyka w Internecie

Materiały przygotowane dla każdej sekcji zawierają plan lekcji, linki do prezentacji i załączniki z materiałami, które mogą być wydrukowane lub w inny sposób udostępnione uczestnikom przez trenera (np. listy kontrolne, studia przypadków). Dostępne są również linki do proponowanych ćwiczeń cyfrowych.

Wskazówki dla edukatorów pracujących z dorosłymi uczącymi się

Prowadząc zajęcia w ramach Modułu 1, warto pamiętać o poniższych aspektach metodycznych i praktycznych:

- **W części 1.1 „Wyszukiwanie informacji i zarządzanie nimi”** szczególnie ważne jest połączenie teorii z praktyką. Uczestnicy mogą znać wyszukiwarki, ale nie wykorzystywać ich w pełni. Zwróć uwagę na różnorodne przykłady zapytań i ćwiczenia z operatorami logicznymi. Warto pokazać różnicę między wynikami w Google i w narzędziach AI, takich jak ChatGPT czy Perplexity – i omówić, jak oceniać ich przydatność i wiarygodność.
- Część dotycząca oceny źródeł może być trudna bez kontekstu – pracuj na przykładach stron prawdziwych i fałszywych, korzystając z checklisty do oceny wiarygodności. Zachęcaj do wspólnej analizy w parach lub grupach.
- Podczas omawiania narzędzi do organizowania informacji (Wakelet, Google Sites, zakładki w przeglądarce) warto zaprezentować je w praktyce – pokazując, jak wygląda tworzenie kolekcji lub dodawanie zakładek w czasie rzeczywistym. Jeśli uczestnicy mają swoje urządzenia, niech wykonają te czynności samodzielnie.
- **W części 1.2 „Bezpieczeństwo cyfrowe”** duże znaczenie ma odniesienie do codziennych doświadczeń uczestników – np. otrzymywania podejrzanych wiadomości, smsów czy reklam. Scenariusz przewiduje pracę na przykładach – dopasuj je do grupy wiekowej i doświadczenia uczestników. Jeśli to możliwe, pokaż aktualne przypadki z lokalnych źródeł lub mediów.
- W module o bezpieczeństwie kont online warto krok po kroku przeprowadzić uczestników przez proces tworzenia silnych haseł i konfiguracji 2FA.



- **Część 1.3 „Prawo i etyka w Internecie”** warto zacząć od przykładów z życia uczestników (np. pobieranie obrazów z sieci, tworzenie prezentacji lub plakatów). Edukator powinien pokazać, jak szukać materiałów z licencją Creative Commons. Ćwiczenia ze studium przypadku najlepiej działają w małych grupach – zachęcaj do dyskusji i zadawania pytań.
- Tematyka netykiety i etyki cyfrowej może być okazją do rozmowy o doświadczeniach uczestników w mediach społecznościowych. Warto stworzyć bezpieczną atmosferę, w której można poruszyć tematy hejtu, prywatności, nieetycznych zachowań online.
- **Wszystkie treści i ćwiczenia zaprojektowane są tak, aby można je było wykorzystać również w formie blended learning – zachęcaj uczestników do samodzielnego powrotu do materiałów (filmy, checklisty, prezentacje), np. poprzez repozytoria na Wakelet lub Google Sites.**

Moduł 1.1 Wyszukiwanie informacji i zarządzanie nimi - materiały warsztatowe

Efekty uczenia się:

Po ukończeniu tego modułu uczestnicy będą umieć:

- **skutecznie wyszukiwać informacje w Internecie** przy użyciu zaawansowanych narzędzi i operatorów wyszukiwania w celu znalezienia precyzyjnych i istotnych danych.
- **efektywnie zarządzać i organizować informacje**, krytycznie oceniać ich jakość i wiarygodność oraz przechowywać je przy użyciu odpowiednich narzędzi.
- **krytycznie oceniać wiarygodność źródeł**, aby podejmować świadome decyzje dotyczące wiarygodności treści online.

Czas trwania: **105 - 120 minut**

Działania	Cel	Metodologia	Materiały	Czas	Inne zasoby / link do zasobów
1. Wprowadzenie do warsztatów Krótkie omówienie programu warsztatów, Refleksja uczestników: Jakie są Twoje doświadczenia związane z wyszukiwaniem informacji w Internecie?	Przedstawienie uczestnikom celów i programu warsztatów. Badanie oczekiwań.	Dyskusja grupowa, pytania otwarte		10 min	
2. Wyszukiwanie informacji	Prezentacja podstawowych pojęć:	Prezentacja, dyskusja, analiza przykładów.	Slajdy z przykładami	10 min	



	algorytmy wyszukiwarek, słowa kluczowe, operatory logiczne.	Do przygotowania prezentacji można użyć załączonych materiałów: Wyszukiwanie informacji: podstawowe pojęcia			
3. Ćwiczenie: Efektywne wyszukiwanie informacji	Nauka korzystania z zaawansowanych funkcji wyszukiwarek (operatory, filtrowanie wyników). Porównanie wyników wyszukiwarek i AI	Ćwiczenia praktyczne, praca w parach. Dostosuj ćwiczenia do poziomu grupy. Propozycje zadań	Komputery/ tablety/ smartfony z dostępem do Internetu. Wydrukowane zadania dla uczestników	20 min	
4. Ocena wiarygodności źródeł informacji	Prezentacja metod oceny wiarygodności stron internetowych (autorzy, domeny, źródła informacji).	Dyskusja, analiza wybranych stron internetowych. Studium przypadku: Przykładowe strony internetowe (informacje prawdziwe i fałszywe).	Prezentacja przykładowych stron internetowych. Wydrukowane materiały dla uczestników	20 min	Jak analizować i oceniać rzetelność i wiarygodność źródeł - poradnik Lista kontrolna do oceny wiarygodności stron internetowych
5. Zarządzanie informacjami: organizacja wyników	Omówienie metod organizacji danych (foldery, zakładki, narzędzia do	Prezentacja narzędzi, praktyczna demonstracja.	Slajdy z przykładami narzędzi, flipchart.	15 min	Zarządzanie informacjami: porządkowanie wyników



	przechowywania i zarządzania danymi).				Filmy instruktażowe Wakelet Tutor... Google Sites T... How To Use Pi...
6, Ćwiczenie: Stwórz własny system organizacji danych.	Uczestnicy przetestują sposoby zarządzania wynikami wyszukiwania (foldery, zakładki, narzędzia).	Praca indywidualna z krótką informacją zwrotną.	Komputery, flipchart do omówienia wyników pracy.	20 min	
7. Podsumowanie i sesja pytań	Powtórzenie kluczowych kwestii, odpowiedzi na pytania uczestników.	Dyskusja, pytania i odpowiedzi.	Flipchart	10 min	



Wyszukiwanie informacji: podstawowe pojęcia

1. **Algorytmy wyszukiwarek.** Algorytmy wyszukiwarek to złożone systemy, które przetwarzają zapytania użytkowników i decydują, które strony internetowe wyświetlić w wynikach wyszukiwania. Wyszukiwarki takie jak Google analizują zawartość stron internetowych, biorąc pod uwagę takie czynniki jak jakość treści, aktualność, autorytet strony czy liczbę linków (odnośników) prowadzących do danej strony. Algorytmy są stale aktualizowane, aby zapewnić bardziej trafne i wartościowe wyniki.
2. **Słowa kluczowe.** Słowa kluczowe to słowa lub frazy, które wpisujemy w wyszukiwarkę w celu znalezienia informacji. Wybór odpowiednich słów kluczowych jest podstawą do uzyskania trafnych wyników. Użytkownicy powinni używać zarówno ogólnych, jak i bardziej szczegółowych fraz, w zależności od tego, jak precyzyjnych informacji szukają.
3. **Operatory logiczne** Operatory logiczne pomagają uszczegółowić wyszukiwanie i uzyskać bardziej trafne wyniki. Najczęściej używanymi operatorami są
 - **AND:** wyniki muszą zawierać oba słowa (np. "AI AND education").
 - **OR:** wyniki mogą zawierać dowolne słowo (np. "AI OR machine learning").
 - **NOT:** wyniki muszą wykluczać określone słowo (np. "AI NOT marketing").
 - **""** (cudzysłów): wyszukiwanie dokładnej frazy (np. "krytyczne myślenie w edukacji").

Wyszukiwanie informacji z pomocą AI – co warto wiedzieć

W ostatnich latach, oprócz tradycyjnych wyszukiwarek internetowych (np. Google, Bing), coraz częściej korzystamy z narzędzi opartych na sztucznej inteligencji, takich jak ChatGPT, Copilot czy Perplexity. Warto znać ich możliwości i ograniczenia, by skutecznie i bezpiecznie wyszukiwać informacje.

Jak działa wyszukiwanie z pomocą AI?

- Narzędzia AI przetwarzają nasze pytania w języku naturalnym i generują odpowiedzi na podstawie dużych zbiorów danych.
- W przeciwieństwie do tradycyjnych wyszukiwarek, AI **nie zawsze pokazuje linki do źródeł** (chyba że zostało do tego zaprogramowane, jak np. Perplexity).
- Odpowiedzi AI są tworzone automatycznie i mogą zawierać **błędy, przestarzałe informacje** lub **brak odniesienia do źródła**.



Jak zadawać pytania (tzw. promptowanie)?

- Zadawaj precyzyjne pytania, np. zamiast „Zmiany klimatu” – napisz:
„Podaj trzy skutki zmian klimatu w Europie w 2024 roku wraz ze źródłami”
- Możesz dodać prośby typu:
 - „Wymień źródła informacji”
 - „Skróć to do 5 punktów”
 - „Podaj w języku prostym”
 - „W formacie PDF” (jeśli korzystasz z AI z dostępem do internetu)

Na co uważać, korzystając z AI do wyszukiwania?

- **Zawsze sprawdzaj źródła** – AI może „wymyślać” tytuły artykułów lub autorów.
- **Nie podawaj danych osobowych** – zapytania trafiają do chmury.
- **Używaj AI jako asystenta**, a nie jedyne źródła prawdy.
- **Sprawdzaj daty** – niektóre narzędzia nie mają dostępu do najnowszych danych.

Ćwiczenie praktyczne 1: Wyszukiwanie za pomocą różnych kombinacji słów kluczowych

Cel ćwiczenia:

Uświadomienie uczestnikom, jak precyzyjne formułowanie zapytań i używanie słów kluczowych wpływa na wyniki wyszukiwania.

Opis ćwiczenia:

- Uczestnicy otrzymują konkretne zapytania, które muszą znaleźć w Internecie przy użyciu różnych kombinacji słów kluczowych.
- Celem ćwiczenia jest pokazanie, jak niewielkie zmiany w zapytaniach mogą wpłynąć na wyniki wyszukiwania.

Przykłady zapytań:

- **Zapytanie 1: Znajdowanie konkretnego przepisu kulinarnego**
 - **Proste zapytanie:** "lasagna recipe".
 - **Zadanie dla uczestników:**
 1. Znajdź przepis na lasagne, ale tylko w wersji wegetariańskiej (dodaj do zapytania słowa kluczowe "wegetariańska" lub "bezmięsna").
 2. Znajdź przepis z blogów kulinarnych (dodaj "blog kulinarny" do zapytania).



3. Znaleźcie przepis wyłącznie z filmem instruktażowym (dodanie "video" do zapytania).
- **Zapytanie 2: Wyszukiwanie informacji o lokalnym wydarzeniu**
 - **Proste zapytanie:** "koncert w Warszawie wrzesień 2024".
 - **Zadanie dla uczestników:**
 1. Znajdź koncerty tylko w jednym gatunku muzycznym (dodaj np. "rock").
 2. Wyszukiwanie koncertów w określonym miejscu (dodaj nazwę lokalizacji, np. "Stodoła").
 3. Znajdź koncerty, na które wstęp jest bezpłatny (dodaj "bezpłatny").
- **Zapytanie 3: Znajdowanie informacji naukowych**
 - **Proste zapytanie:** "zmiana klimatu".
 - **Zadanie dla uczestników:**
 1. Znajdź artykuł naukowy (dodaj "artykuł naukowy" lub "PDF").
 2. Znajdź informacje z określonej witryny (dodaj do zapytania "site:.edu" lub "site:.gov").
 3. Znajdź informacje z ostatniego roku (użyj funkcji filtrowania wyników do 12 miesięcy).

Ćwiczenia praktyczne 2: Bardziej zaawansowane strategie zadawania pytań

1. Ćwiczenie: Znajdź wiarygodne źródło

- **Cel:** Nauka oceniania wiarygodności źródeł i wyjaśniania zapytań.
- **Instrukcja:**
 - Poproś uczestników o wyszukanie informacji na temat korzyści zdrowotnych wynikających z picia kawy.
 - Powinni użyć operatorów takich jak "health benefits of coffee" site:.edu OR site:.gov, aby znaleźć wiarygodne źródła (np. strony akademickie lub rządowe).
- **Dyskusja:** Po zakończeniu wyszukiwania uczestnicy omówią, które strony są najbardziej wiarygodne i dlaczego. Należy zwrócić uwagę na domeny stron (np. .edu, .gov) i użycie operatorów.

2. Ćwiczenie: Wyszukiwanie określonych dokumentów

- **Cel:** Praktyczne zastosowanie operatorów logicznych i zaawansowanych filtrów.
- **Instrukcja:**



- Poproś uczestników o znalezienie raportu ONZ na temat zmian klimatu w formacie PDF, opublikowanego w ciągu ostatnich 2 lat. Mogą użyć operatora **filetype:** i filtrować według daty.
- Wyszukiwane hasło: **climate change site:un.org filetype:pdf**, a następnie przefiltruj wyniki, aby ograniczyć je do ostatnich dwóch lat.
- **Dyskusja:** Po zakończeniu ćwiczenia omów, w jaki sposób użycie operatorów i filtrów pomogło znaleźć bardziej odpowiednie wyniki.

3. Ćwiczenie: Wyszukiwanie dokładnych fraz

- **Cel:** Nauczenie się używania cudzysłówów i operatorów wykluczania do precyzyjnego wyszukiwania.
- **Instrukcja:**
 - Poproś uczestników o znalezienie dokładnych wyników dla cytatu z książki. Na przykład: "Internet zmienia sposób myślenia ludzi".
 - Uczestnicy powinni użyć cudzysłowu, aby wyszukać dokładną frazę i operatora **NOT**, aby wykluczyć wyniki pochodzące z artykułów marketingowych (np. "Internet zmienia sposób myślenia ludzi" **NOT marketing**).
- **Dyskusja:** Omów, w jaki sposób użycie cudzysłówów i operatorów wpłynęło na jakość wyników. Czy udało Ci się znaleźć dokładne cytaty?

4. Ćwiczenie: Wyszukiwanie za pomocą AI (SI)

Cel: Porównać wyniki wyszukiwania w Google i za pomocą AI

Zadanie:

1. Wyszukaj w Google: „**Jakie są objawy wypalenia zawodowego**”.
2. Zadaj to samo pytanie w ChatGPT lub innym narzędziu AI.
3. Porównaj:
 - Jakie informacje się pokrywają?
 - Czy AI podało źródła?
 - Co było bardziej zrozumiałe lub praktyczne?
 - Czy zauważasz brakujące informacje?



Jak analizować i oceniać rzetelność i wiarygodność źródeł - poradnik

W dzisiejszym świecie mamy dostęp do ogromnej ilości informacji w Internecie, ale nie wszystkie z nich są wiarygodne. Oto kilka prostych zasad, jak ocenić, czy informacja pochodzi z wiarygodnego źródła:

1. Sprawdź autora

- **Kto to napisał?** Sprawdź, kto jest autorem artykułu lub informacji. Jeśli jest to znana osoba, specjalista w danej dziedzinie (np. lekarz, profesor, ekspert), źródło jest bardziej wiarygodne.
- **Jak to sprawdzić?** Szukaj informacji o autorze w stopce artykułu, na stronie "O nas" lub w biografii. Jeśli autor jest anonimowy, rozważ wiarygodność takiego źródła.

Przykład: Jeśli czytasz artykuł o zdrowiu, warto, aby jego autorem był lekarz lub specjalista medycyny, a nie przypadkowa osoba bez wiedzy w danej dziedzinie.

2. Zwróć uwagę na typ domeny

- **Czy domena jest zaufana?** Strony z rozszerzeniami **.gov** (strony rządowe), **.edu** (strony uniwersyteckie) i **.org** (organizacje non-profit) są często bardziej godne zaufania. Witryny **.com** i inne mogą mieć różną jakość, od wiarygodnej do czysto komercyjnej.

Przykład: Jeśli szukasz statystyk zdrowotnych, strona z domeną "gov.co.uk" będzie bardziej wiarygodna niż blog kończący się na ".com".

3. Sprawdź datę publikacji

- **Czy informacje są aktualne?** Sprawdź, kiedy artykuł został opublikowany lub ostatnio zaktualizowany. Informacje z przestarzałych źródeł mogą być już nieaktualne lub nieadekwatne do dzisiejszej sytuacji.

Przykład: Szukając informacji o nowych lekach lub technologiach, upewnij się, że artykuł pochodzi z ostatnich lat, a nie sprzed dekady.

4. Czy podano źródła informacji?

- **Skąd pochodzą informacje?** Najnowsze artykuły często odnoszą się do badań, statystyk lub innych uznanych źródeł. Sprawdź, czy artykuł zawiera linki do zewnętrznych badań naukowych, raportów lub publikacji.
- **Jak to zrobić?** Sprawdź, czy w artykule znajdują się linki lub przypisy do źródeł. Brak odnośników może oznaczać, że artykuł opiera się na opiniach, a nie faktach.

Przykład: Jeśli czytasz artykuł na temat diety, warto, aby zawierał on odniesienia do badań naukowych lub artykułów z renomowanych witryn medycznych, a nie tylko osobiste doświadczenia autora.



5. Sprawdź neutralność treści

- **Czy artykuł jest obiektywny?** Wiarygodne źródła starają się prezentować informacje bez silnej stronniczości lub promowania określonego punktu widzenia. Jeśli artykuł ma wyraźny ton promujący jedną stronę lub agresywnie krytykujący inne poglądy, może nie być obiektywny.

Przykład: Artykuł na temat zmian klimatycznych powinien przedstawiać dowody i fakty, a nie skupiać się na krytykowaniu tylko jednej grupy ludzi lub teorii.

6. Zwracaj uwagę na reklamy i sensacyjne nagłówki

- **Czy strona zawiera dużo reklam?** Strony przepełnione reklamami mogą być bardziej nastawione na zysk niż dostarczanie wiarygodnych informacji. Unikaj stron z sensacyjnymi, krzykliwymi nagłówkami, które za wszelką cenę próbują przyciągnąć uwagę.

Przykład: Strona z nagłówkiem "Ten lek na pewno cię wyleczy - ZOBACZ JAK!" może nie być zbyt wiarygodna. Wiarygodne strony mają bardziej wyważone tytuły, takie jak "Nowe badania nad skutecznością leku X".

7. Porównanie z innymi źródłami

- **Czy inne źródła podają te same informacje?** Jeśli znajdziesz jakąś informację, warto sprawdzić, czy inne zaufane strony podają to samo. Jeśli tylko jedno źródło podaje daną informację, warto podejść do niej z ostrożnością.

Przykład: Jeśli czytasz sensacyjny raport o przełomowym odkryciu, sprawdź, czy piszą o nim również renomowane serwisy (np. gazety, strony rządowe).

Podsumowanie

Ocena wiarygodności źródeł w Internecie jest kluczową umiejętnością. Zawsze sprawdzaj **kto** napisał artykuł, **jaką** ma domenę, **czy** informacje są aktualne, **czy** odnoszą się do źródeł, **czy** są obiektywne i **czy** inne źródła potwierdzają te same informacje. Pomoże to uniknąć fałszywych wiadomości i dezinformacji.

Lista kontrolna do oceny wiarygodności stron internetowych

Oto przykładowa lista kontrolna, którą można wykorzystać do oceny wiarygodności stron internetowych. Lista ta pomoże użytkownikom zidentyfikować potencjalnie wiarygodne lub podejrzane źródła.

1. Autor i źródło informacji

- Czy strona podaje autora tekstu?
- Czy autor ma kwalifikacje do wypowiedzania się na dany temat (np. ekspert, specjalista)?



- Czy autor jest powiązany z uznanym ośrodkiem, instytucją lub organizacją?
- Czy można znaleźć więcej informacji o autorze w innych źródłach?

2. Domena witryny

- Jaka jest domena witryny (np. **.gov**, **.edu**, **.org** - generalnie bardziej wiarygodne niż **.com**, **.info** itp.)
- Czy witryna jest powiązana z renomowaną instytucją, organizacją lub uniwersytetem?
- Czy nazwa domeny wskazuje na organizację non-profit lub rządową?
- Czy witryna ma zasięg lokalny lub międzynarodowy i czy zasięg ten odpowiada prezentowanym treściom?

3 Źródła i linki

- Czy informacje na stronie są dobrze udokumentowane?
- Czy strona zawiera linki do oryginalnych źródeł informacji (raportów, badań, publikacji)?
- Czy źródła są aktualne i pochodzą od wiarygodnych instytucji?
- Czy witryna cytuje uznane badania, raporty lub autorów?
- Czy źródła cytowane na stronie można zweryfikować?

4. Aktualność

- Czy widoczna jest data publikacji artykułu lub strony?
- Czy informacje są aktualne i zgodne z aktualnym stanem wiedzy?
- Czy strona jest regularnie aktualizowana?

5. Cel i przejrzystość witryny

- Jaki jest cel witryny (informacyjny, edukacyjny, sprzedażowy, rozrywkowy)?
- Czy strona jest wyraźnie subiektywna, czy też ma na celu przedstawienie obiektywnych faktów?
- Czy strona unika sensacyjnego lub emocjonalnego języka?
- Czy witryna ma ukryte intencje komercyjne, reklamowe lub polityczne?
- Czy na stronie znajdują się wyraźne oznaki materiałów sponsorowanych?

6. Wygląd i profesjonalizm

- Czy strona wygląda profesjonalnie (brak błędów ortograficznych, logicznie uporządkowana treść)?
- Czy strona jest łatwa w nawigacji i czy jej wygląd wzbudza zaufanie?



- Czy strona zawiera dużo reklam? (Nadmierna liczba reklam może sugerować komercyjny cel witryny).
- Czy strona używa prawidłowych linków i linków, które działają prawidłowo?

7. Recenzje innych osób

- Czy można znaleźć pozytywne recenzje lub opinie o witrynie w innych wiarygodnych źródłach?
- Czy inne źródła polecają witrynę jako wiarygodną?
- Czy witryna została polecona przez znane i uznane organizacje, np. akademickie, media, instytucje badawcze?

Podsumowanie

Korzystając z tej listy, użytkownik Internetu może łatwiej zidentyfikować wiarygodne źródła informacji i unikać tych, które mogą wprowadzać w błąd. Lista ta jest narzędziem do krytycznej oceny treści dostępnych online, a systematyczne korzystanie z tych pytań pomaga budować nawyk oceny wiarygodności informacji w Internecie.

Zarządzanie informacjami: porządkowanie wyników

Organizowanie danych online i na komputerze pomaga w łatwym dostępie do informacji, porządkowaniu plików i efektywnym zarządzaniu zasobami. Oto kilka popularnych metod i narzędzi, które mogą ułatwić ten proces:

1. Organizacja danych w folderach

- Prosta struktura folderów: zacznij od utworzenia głównych folderów odpowiadających różnym kategoriom, np. "Dokumenty", "Zdjęcia", "Muzyka", "Praca", "Szkoła". Wewnątrz tych folderów można tworzyć podfoldery, np. "Zdjęcia" -> "Wakacje 2023" -> "Grecja".
- Nazwy plików mają znaczenie: Nadawaj plikom i folderom jasne, opisowe nazwy. Na przykład "bill_for_current_August_2023.pdf" jest bardziej pomocne niż "document1.pdf".

2. Organizacja danych w przeglądarkach internetowych (zakładki)

- Zakładki w przeglądarce: Zakładki umożliwiają szybki powrót do ważnych stron. Zakładki można pogrupować w foldery, takie jak "Praca", "Rozrywka" i "Zakupy".



- Nazwa zakładki: nadaj zakładkom opisowe nazwy, aby ułatwić ich znajdowanie. Zamiast "Strona główna" można zmienić nazwę zakładki na "Planer podróży".
- Synchronizacja zakładek: Korzystaj z przeglądarek z funkcją synchronizacji, takich jak Google Chrome lub Firefox, aby zakładki były dostępne na wszystkich urządzeniach.
- Menedżer zakładek: Wiele przeglądarek ma wbudowane narzędzia do zarządzania zakładkami, dzięki czemu można łatwo przeglądać, zmieniać nazwy lub porządkować zakładki.

3. Narzędzia do przechowywania i zarządzania danymi w chmurze

- Dysk Google, Dropbox, OneDrive: Są to podstawowe narzędzia, które umożliwiają przechowywanie plików w chmurze i synchronizowanie ich z różnymi urządzeniami. Wystarczy utworzyć konto i można przechowywać dokumenty, zdjęcia, pliki bezpośrednio w chmurze, uzyskując do nich dostęp z dowolnego miejsca.
- Zarządzanie plikami w chmurze: Podobnie jak na komputerze, twórz foldery tematyczne (np. "Praca", "Osobiste", "Projekty"). Ułatwia to wyszukiwanie danych.
- Zaawansowane funkcje chmury: narzędzia takie jak Dysk Google i OneDrive umożliwiają udostępnianie folderów i dokumentów innym użytkownikom. Możesz nadać im różne uprawnienia (takie jak tylko do odczytu lub tylko do edycji), ułatwiając współpracę w zespole.
- Automatyczna synchronizacja plików: Korzystaj z aplikacji desktopowych (takich jak Dropbox lub OneDrive na komputerze), które automatycznie synchronizują pliki między komputerem a chmurą. W ten sposób zawsze masz aktualną wersję swoich plików, bez konieczności ich ręcznego przesyłania.

4. Narzędzia do zarządzania informacjami i notatkami

- Google Keep, Evernote: Narzędzia te umożliwiają tworzenie notatek, list rzeczy do zrobienia i przechowywanie krótkich informacji. Notatki można organizować w kategorie lub tagi.
- Notatki z przypomnieniami: Narzędzia takie jak Google Keep umożliwiają ustawianie przypomnień dla notatek, ułatwiając zarządzanie zadaniami.

5. Repozytoria cyfrowe

Repozytoria to platformy, na których można gromadzić linki do materiałów i zasobów cyfrowych oraz, co najważniejsze, łatwo udostępniać je innym. Przykłady repozytoriów: Wakelet, Padlet, Pinterest.

Wakelet to darmowe (dla użytkowników indywidualnych) narzędzie, które może być bardzo przydatne do gromadzenia materiałów cyfrowych. Można w nim:



- tworzyć kolekcje zasobów cyfrowych, w różnych formatach: linki do stron internetowych, filmy z YouTube, materiały zapisane wcześniej w innych kolekcjach Wakelet (zakładki), zdjęcia i grafiki, pliki PDF
- dostosować wygląd każdej kolekcji do naszych potrzeb poprzez dodanie grafiki tła i okładki, a także wybór układu wyświetlania materiałów wchodzących w skład kolekcji;
- zarządzać zapisanymi materiałami i kolekcjami z poziomu strony internetowej, rozszerzenia przeglądarki i aplikacji mobilnej, czyli bardzo łatwy sposób na dodawanie do kolekcji materiałów znalezionych w sieci;
- zapraszać do współpracy osoby posiadające własne konta na Wakelet, a także osoby nieposiadające własnych kont
- dzielić się naszymi kolekcjami wyłącznie w celu ich wyświetlania lub edytowania i wspólnej pracy nad nimi.

Padlety to wizualne tablice do organizowania i udostępniania treści.

W swojej podstawowej wersji Padlet jest darmowy dla użytkownika, ale z ograniczeniami dotyczącymi liczby utworzonych padletów.

To proste narzędzie - wirtualna tablica, na której można umieszczać dokumenty tekstowe, grafiki, zdjęcia, filmy, nagrania dźwiękowe i prezentacje. Może to być również miejsce do wspólnej pracy: dyskusji, edycji udostępnionych dokumentów i otrzymywania informacji zwrotnych.

Udostępnianie zasobów odbywa się poprzez udostępnienie linku lub kodu QR i nie wymaga od odbiorcy posiadania konta ani logowania się do platformy. Padlet może być używany zarówno na komputerach, jak i urządzeniach mobilnych.

Pinterest to platforma społecznościowa służąca do odkrywania, gromadzenia i udostępniania inspiracji w postaci obrazów, grafik, filmów i treści wizualnych. Użytkownicy tworzą tzw. tablice, na których przypinają ("pinują") znalezione treści związane z różnymi tematami, takimi jak moda, kulinaria, wystrój domu, projekty DIY, podróże, a także inspiracje zawodowe związane np. z projektowaniem czy marketingiem. Pinterest działa jak cyfrowa tablica korkowa, na której można gromadzić pomysły z różnych źródeł. Jest to narzędzie zarówno do użytku osobistego (szukanie inspiracji), jak i dla marek i twórców, którzy mogą promować swoje produkty i treści w atrakcyjny, wizualny sposób.

Google Sites to proste narzędzie do tworzenia stron internetowych, które może być z powodzeniem wykorzystywane do gromadzenia zasobów cyfrowych i łatwego udostępniania ich innym osobom. Witryny Google mogą być automatycznie tłumaczone przez przeglądarki. Witryny Google to bezpłatne narzędzie dla wszystkich użytkowników. Kilka sposobów wykorzystania Witryn Google w praktyce:



- Repozytorium materiałów edukacyjnych: prezentacje, filmy, artykuły i inne materiały edukacyjne.
- Portfolio - prezentacja pasji lub kompetencji zawodowych.

Podsumowanie

Dobre zarządzanie danymi to kluczowa umiejętność dla każdego użytkownika Internetu. Początkujący mogą zacząć od prostej struktury folderów i korzystania z zakładek, podczas gdy średnio zaawansowani użytkownicy mogą korzystać z zaawansowanych narzędzi do zarządzania plikami, synchronizacji i tworzenia kopii zapasowych w chmurze. Ważne jest, aby regularnie organizować swoje pliki, aby były łatwiejsze do znalezienia i bezpieczne.

Zasoby

<https://youtu.be/Jv0KulFyLpI?si=X1M7zLI6MbwCDWrF>

https://youtu.be/4yrDF4JaZzI?si=-Z-kcejWv_U487H7

<https://youtu.be/mCxyblU5AY8?si=j9bEw8B112qyRHda>



Moduł 1.2 Bezpieczeństwo cyfrowe

Sprawdź DigComp 2.2, aby dowiedzieć się, jakie kompetencje (wiedzę, umiejętności i postawy) warto rozwijać w obszarze bezpieczeństwa.

<https://publications.jrc.ec.europa.eu/repository/handle/JRC128415>

Bezpieczeństwo

- Ochrona urządzeń, treści cyfrowych, danych osobowych i prywatności w środowisku cyfrowym.
- Ochrona zdrowia fizycznego i psychicznego, świadomość wpływu technologii na dobre samopoczucie i integrację społeczną.
- Świadomość wpływu technologii i ich wykorzystania na środowisko.

Uwaga:

Materiały (linki) dołączone do planu lekcji mogą być również wykorzystywane do samodzielnej nauki lub do pracy w trybie mieszanym.

Z doświadczeń trenerskich wynika, że dobrym sposobem na zwiększanie kompetencji w obszarze bezpieczeństwa cyfrowego jest praca metodą blended-learning.

Tu sugerujemy wcześniejsze udostępnienie uczącym się materiałów i analizy oraz refleksje w czasie spotkania grupowego.

Moduł 1.2 Bezpieczeństwo cyfrowe - materiały warsztatowe

Efekty uczenia się:

Po ukończeniu tej lekcji uczestnicy:

- będą w stanie rozpoznać i zrozumieć najczęstsze zagrożenia bezpieczeństwa online.
- będą wiedzieć, jak zabezpieczyć swoje urządzenia i konta za pomocą silnych haseł i weryfikacji dwuetapowej (2FA).
- będą w stanie rozpoznać podejrzaną aktywność online i wiedzieć, jakie działania należy podjąć w przypadku wykrycia zagrożenia.
- będą bardziej świadomi znaczenia ochrony danych osobowych i poczują się odpowiedzialni za swoje bezpieczeństwo cyfrowe i prywatność online.

Czas trwania: 90-120 minut

Działania	Cel	Metodologia	Materiały	Czas	Inne zasoby / link do zasobów
1. Wprowadzenie do warsztatów Krótkie wprowadzenie, Refleksje uczestników: jakie są Twoje doświadczenia z oszustwami internetowymi?	Prezentowanie uczestnikom tematu i celów warsztatów			10 min	
2. Ryzyko i zagrożenia w środowisku cyfrowym Podział uczestników na małe grupy	Uczestnicy poznają typowe zagrożenia cyfrowe i dowiadują się, jak się przed nimi chronić.	Praca w małych grupach - 3 osoby Edukator udostępnia (np. za pomocą QR kodów) strony z	Laptopy, tablety z dostępem do internetu	35 min	Linki do stron z zasobami Bezpiecznie w internecie

1. Każda grupa wybiera z materiałów obszar do zbadania (trener sprawdza powtarzalność). 2. Grupa przygotowuje mini-prezentację zagadnienia (charakterystyka zagrożenia, sygnały niebezpieczeństwa, jak się zachować). 3. Grupa opracowuje wspólną prezentację w chmurze (np. Canva, Google Presentation) 4. Prezentacja wyników pracy grup		zasobami, z których będą korzystać uczestnicy. Można też te materiały udostępnić wcześniej do zapoznania się przed zajęciami.			Centrum zasobów cyberbezpieczeństwa
3. Ćwiczenie: Rozpoznawanie zagrożeń	Nauka rozpoznawania podejrzanych e-maili, wiadomości i stron internetowych	Praca w grupach: analizowanie e-maili, stron i wiadomości pod kątem zagrożeń	Komputery z dostępem do Internetu, przykładowe wiadomości e-mail i strony internetowe	10 min	Tutaj znajdziesz quiz Samoobrona w sieci mBank Zmierz się z cyberprzestępcą
4. Bezpieczne zarządzanie hasłami Demonstracja tworzenia bezpiecznych haseł i	Uczestnicy dowiedzą się, jak tworzyć silne hasła i korzystać z uwierzytelniania dwuskładnikowego,	Prezentacja	Slajd z przykładami silnych haseł	10 min	Instrukcje dotyczące tworzenia silnych haseł i konfigurowania 2FA  How to protect y...  What Is Two-Fac...

uwierzytelniania dwuskładnikowego	poznają menedżera haseł				Co to jest uwierzytelnianie Definicja uwierzytelniania Malwarebytes Uwierzytelnianie dwuskładnikowe 2FA: Zabezpiecz swoje cyfrowe życie Menedżer Haseł
5. Ochrona prywatności online Prezentacja ustawień prywatności na kontach w różnych mediach społecznościowych Ćwiczenie: Sprawdzanie ustawień prywatności Uczestnicy sprawdzają ustawienia prywatności na swoich kontach w mediach społecznościowych	Prezentacja zasad ochrony danych i prywatności w Internecie, takich jak konfiguracja ustawień prywatności	Demonstracja, dyskusja, praca indywidualna, ćwiczenie praktyczne	Urządzenia z dostępem do Internetu, konta w mediach społecznościowych	10 min	Lista kontrolna ustawień prywatności dla serwisów Facebook, X (Twitter), Instagram i TikTok <i>(należy sprawdzić aktualność podanych informacji)</i>
6. Podsumowanie i sesja pytań Podsumowanie zasad bezpieczeństwa cyfrowego, Ćwiczenie:	Powtórzenie kluczowych informacji i	Dyskusja, pytania i odpowiedzi	Flipchart, podsumowanie kluczowych kwestii	5 min	Aplikacja »  CyberAlerty -- Niebezpiecznik.pl --



Co-funded by
the European Union



Wejdź na stronę swojego banku Znajdź sekcję bezpieczeństwa Sprawdź, jakie aktualne informacje o zagrożeniach online możesz tam znaleźć.	odpowiedzi na pytania uczestników				
---	--------------------------------------	--	--	--	--



Przykłady silnych haseł:

1. **W8#pL!rT93z**
 - Kombinacja małych i wielkich liter, cyfr i symboli.
2. **9fT#4kL!2&Q7**
 - Długość powyżej 10 znaków, brak porządku logicznego, różne typy znaków.
3. **!Lm7tR#xQ9Z8**
 - Używanie symboli, cyfr i losowych liter w różnych przypadkach.

Silne hasła powinny być długie (co najmniej 12 znaków), losowe i zawierać kombinację wielkich i małych liter, cyfr i symboli. Ważne jest również, aby używać unikalnych haseł dla różnych kont.

Lista kontrolna ustawień prywatności dla serwisów Facebook, X (Twitter), Instagram i TikTok

1. Facebook

- Profil i posty:
 - Ustaw widoczność swojego profilu (publiczny, znajomi, tylko ja).
 - Określ, kto może zobaczyć Twoje przyszłe posty (publicznie, znajomi).
 - Przeglądanie i dostosowywanie widoczności starych postów.
 - Wyłączanie tagowania przez inne osoby bez Twojej zgody.
 - Ograniczenie widoczności informacji osobistych (np. wieku, lokalizacji, adresu e-mail).
- Znajomi i kontakty:
 - Kontroluj, kto może wysłać zaproszenia do znajomych.
 - Dostosuj, kto może Cię wyszukać na podstawie adresu e-mail lub numeru telefonu.
- Aplikacje i witryny:
 - Sprawdź, które aplikacje mają dostęp do Twojego konta i co mogą zobaczyć.
 - Wyłącz udostępnianie swojej aktywności w aplikacjach Facebooka.
- Reklamy i śledzenie:
 - Ograniczenie personalizacji reklam na podstawie aktywności online użytkownika.
 - Wyłączenie udostępniania danych użytkownika zewnętrznym reklamodawcom.



2. Platforma X

- **Widoczność i aktywność:**
 - Ustaw swój profil jako prywatny, aby Twoje tweety były widoczne tylko dla zatwierdzonych obserwatorów.
 - Dostosuj, kto może wysyłać ci bezpośrednie wiadomości (wszyscy, tylko obserwatorzy).
 - Kontroluj, kto może oznaczać Cię na zdjęciach.
- **Lokalizacja:**
 - Wyłącz udostępnianie swojej lokalizacji w tweetach.
- **Dostęp do konta:**
 - Zabezpiecz swoje konto za pomocą uwierzytelniania dwuetapowego (2FA).
 - Sprawdź aplikacje z dostępem do konta i usuń te, których już nie używasz.
- **Reklamy i dane:**
 - Dostosuj personalizację reklam na podstawie aktywności na Twitterze.
 - Wyłącz opcje udostępniania danych partnerom reklamowym.

3. Instagram

- **Widoczność i interakcje:**
 - Ustaw swoje konto jako prywatne, aby Twoje posty były widoczne tylko dla zatwierdzonych obserwatorów.
 - Kontroluj, kto może komentować Twoje posty (wszyscy, tylko obserwatorzy, wybrane osoby).
 - Ogranicz, kto może wysyłać bezpośrednie wiadomości (wszyscy, tylko obserwatorzy).
- **Tagi i oznaczanie:**
 - Zdecyduj, kto może oznaczać Cię na zdjęciach i filmach (wszyscy, tylko obserwujący).
 - Ręcznie zatwierdzaj tagi, zanim pojawią się na Twoim profilu.
- **Reklamy i dane:**
 - Wyłącz personalizację reklam na podstawie Twojej aktywności na Instagramie i poza nim.
 - Sprawdź, które aplikacje mają dostęp do Twojego konta i usuń te, których już nie używasz.

4. TikTok

- **Widoczność konta i postów:**
 - Ustaw swoje konto jako prywatne, aby tylko zatwierdzeni obserwatorzy mogli oglądać Twoje filmy.
 - Dostosuj, kto może komentować Twoje filmy (wszyscy, znajomi, nikt).



- **Określ, kto może oglądać Twoje polubienia (wszyscy, tylko Ty).**
- **Zdecyduj, kto może odpowiadać na Twoje filmy (wszyscy, znajomi, nikt).**
- **Interakcje:**
 - **Kontroluj, kto może wysyłać Ci bezpośrednie wiadomości (wszyscy, znajomi, nikt).**
 - **Zablokowanie opcji duetu i zszywania (tworzenia filmów z Twoich treści) dla wszystkich lub ograniczenie jej do znajomych.**
 - **Wyłącz możliwość publikowania przez innych pytań lub reakcji na Twoje filmy.**
- **Lokalizacja:**
 - **Sprawdź, czy TikTok nie udostępnia Twojej lokalizacji w tle.**
 - **Wyłącz opcję oznaczania geograficznego w filmach.**
- **Dane i śledzenie:**
 - **Wyłącz personalizację reklam na podstawie aktywności użytkownika w serwisie TikTok.**
 - **Przeglądanie aplikacji z dostępem do konta i usuwanie tych, które nie są już potrzebne.**
- **Zarządzanie kontem:**
 - **Skonfiguruj uwierzytelnianie dwuetapowe (2FA), aby zwiększyć bezpieczeństwo konta.**
 - **Regularnie sprawdzaj, jakie urządzenia są zalogowane do Twojego konta i wyloguj te, których nie rozpoznajesz.**

Podsumowanie

Dostosowanie ustawień prywatności na Facebooku, Twitterze i Instagramie pozwala mieć większą kontrolę nad tym, kto widzi Twoje treści i jakie dane są udostępniane. Regularne sprawdzanie i aktualizowanie ustawień jest kluczem do zachowania prywatności w mediach społecznościowych.



Moduł 1.3 Prawo i etyka w Internecie

W tym module skupimy się na podstawowych zagadnieniach z zakresu prawa i etycznego zachowania w Internecie, które dotyczą twórców cyfrowych, czyli osób publikujących online.

Warsztaty koncentrują się na najważniejszych zagadnieniach z zakresu prawa autorskiego, licencjonowania treści, ochrony dóbr osobistych i wizerunku oraz zasad etycznych w komunikacji cyfrowej. Uczestnicy zdobędą praktyczną wiedzę na temat zgodnego z prawem korzystania z treści cyfrowych.

Moduł 1.3 Prawo i etyka w Internecie - materiały warsztatowe

Efekty uczenia się:

- Uczestnicy zrozumieją podstawowe zasady prawa autorskiego i znaczenie etycznego postępowania w Internecie, w tym ochrony danych i netykiety.
- Uczestnicy będą w stanie zidentyfikować różne naruszenia, takie jak nielegalne kopiowanie lub plagiat.
- Uczestnicy będą wiedzieć, jak stosować licencje Creative Commons i wybrać odpowiednią licencję dla różnych rodzajów treści.
- Zdobędą wiedzę na temat ochrony wizerunku i danych osobowych w kontekście cyfrowym.

Czas trwania: 120 minut

Działania	Cel	Wskazówki metodyczne	Materiały	Czas	Inne zasoby / link do zasobów
1. Wprowadzenie do warsztatów Krótkie wprowadzenie, Runda: jakie znasz przypadki naruszenia praw autorskich? Co dotknęło ciebie i twoją pracę? O	Przedstawienie uczestnikom celów i tematów warsztatów. Krótka dyskusja na temat znaczenia prawa i etyki w sieci.		Slajdy z programem warsztatów	10 min	

jakich przypadkach słyszałeś?					
2. Podstawowe zasady prawa autorskiego	Prezentacja podstawowych zasad prawa autorskiego.	Prezentacja i dyskusja Sprawdź swoją wiedzę https://learningapps.org/display?v=p6wsp2gp201 https://learningapps.org/display?v=pbexgjs9a01	Prezentacja Prawo autorskie Prawo autorskie i etyka Slajdy 3-13	20 min	Informacje o prawach autorskich Prawo autorskie i etyka
3. Ćwiczenie: Analiza przypadków naruszenia praw autorskich	Uczestnicy analizują przypadki naruszenia praw autorskich, np. nielegalne kopiowanie, plagiat.	Praca w grupach, studium przypadku	Przykłady naruszeń praw autorskich	15 min	Przykłady naruszenia praw autorskich. zadania do analizy
4. Creative Commons i inne licencje	Omówienie alternatywnych licencji, takich jak Creative Commons, które umożliwiają udostępnianie treści.	Prezentacja oparta na https://creativecommons.org/share-your-work/cclicenses/ , analiza narzędzi	Slajdy z opisami licencji, flipchart	10 min	Przykłady licencji Creative Commons i innych, instrukcje użytkowania



		Sprawdź siebie https://learningapps.org/display?v=pkwoxdhkt16			https://creativecommons.org/share-your-work/cclicenses/
5. Tworzenie treści zgodnych z prawami autorskimi.		Prezentacja Tworzenie treści zgodnie z prawem autorskim Trener może wykorzystać tę prezentację podczas warsztatów lub udostępnić ją uczestnikom do samodzielnej nauki.	Prezentacja Tworzenie treści zgodnie z prawem autorskim	10 min	Tworzenie treści zgodnie z prawem autorskim
6. Prawa do wizerunku i ochrona danych osobowych	Przedstawienie zasad ochrony wizerunku i danych osobowych w Internecie.	Prezentacja, analiza przepisów Prawo do wizerunku i ochrona danych osobowych	Prezentacja Prawo autorskie i etyka Slajdy 14-23	15 min	Prawo autorskie i etyka
7. Etyka w świecie cyfrowym	Dyskusja na temat etyki online, w tym netykiety i odpowiedzialności za publikowane treści.	Dyskusja, analiza przypadków	Prezentacja Prawo autorskie i etyka Slajdy 24-29	25 min	Prawo autorskie i etyka Etyka cyfrowa w praktyce – studia przypadków
8. Podsumowanie i sesja pytań	Powtórzenie kluczowych kwestii związanych z prawem autorskim i etyką cyfrową.	Dyskusja, pytania i odpowiedzi	Flipchart, summary of key issues	15 min	



Przykłady naruszenia praw autorskich, zadania do analizy

Studium przypadku 1: Paul, deweloper internetowy

Historia:

Paul, początkujący twórca stron internetowych, który prowadzi popularny kanał na YouTube, postanowił stworzyć zabawny filmik. W tym celu wykorzystał fragment popularnego filmu, który przerobił, dodając własne komentarze i efekty dźwiękowe. Wideo szybko stało się bardzo popularne, ale po kilku dniach Paul otrzymał wiadomość od prawnika reprezentującego studio filmowe, które posiadało prawa do wykorzystanego fragmentu. Został oskarżony o naruszenie praw autorskich i groziły mu poważne konsekwencje prawne.

Pytania do dyskusji:

- Jakie błędy popełnił Paul?
- Czy Paul mógł wykorzystać fragment filmu w inny sposób, aby uniknąć naruszenia praw autorskich?
- Jakie są konsekwencje naruszenia praw autorskich dla twórców internetowych?
- Jakie narzędzia mogą pomóc twórcom uniknąć naruszeń praw autorskich?

Studium przypadku 2: Ola, projektantka graficzna

Historia:

Ola, początkująca graficzka, stworzyła piękny plakat promujący lokalne wydarzenie muzyczne. Aby dodać plakatowi oryginalności, użyła czcionki, którą znalazła w Internecie i pobrała za darmo. Organizatorzy wydarzenia byli zachwyceni plakatem i wykorzystali go do promocji wydarzenia. Niestety okazało się, że użyta przez Olę czcionka jest chroniona prawami autorskimi i nie może być wykorzystywana komercyjnie. Organizatorzy wydarzenia zostali zmuszeni do zapłacenia wysokiej grzywny za naruszenie praw autorskich, a Ola poniosła straty finansowe.

Pytania do dyskusji:

- Czy Ola mogła uniknąć tej sytuacji?
- Jakie są różnice między czcionkami darmowymi a chronionymi prawem autorskim?
- Jakie są konsekwencje naruszenia praw autorskich dla grafików?
- Gdzie szukać darmowych zasobów graficznych, które można legalnie wykorzystać?



Studium przypadku 3: Kuba, muzyk

Historia:

Kuba, młody muzyk, nagrał własną wersję popularnej piosenki i zamieścił ją na swojej stronie internetowej. Piosenka szybko stała się bardzo popularna, ale po kilku tygodniach Kuba otrzymał wiadomość od wytwórni muzycznej, która posiadała prawa do oryginalnego utworu. Został oskarżony o naruszenie praw autorskich i musiał usunąć swoją wersję piosenki ze strony internetowej.

Pytania do dyskusji:

- Jakie są różnice między coverem a plagiatem?
- Jakie są prawa artystów do ich własnych dzieł?
- Jakie są możliwości legalnego korzystania z utworów innych artystów?
- Jakie są konsekwencje naruszenia praw autorskich dla muzyków?

Dodatkowe pytania do dyskusji w całej grupie:

- Jakie są najczęstsze błędy popełniane przez początkujących twórców cyfrowych związane z prawami autorskimi?
- Jakie są najważniejsze zasady, o których należy pamiętać, aby uniknąć naruszenia praw autorskich?
- Jakie narzędzia i platformy ułatwiają legalne korzystanie z materiałów chronionych prawem autorskim?

Etyka cyfrowa w praktyce - studia przypadków

Przypadek 1: Przemysłane udostępnianie treści

Janek jest aktywnym użytkownikiem Twittera. Pewnego dnia widzi emocjonalny wpis o rzekomych nielegalnych działaniach znanego polityka, który szybko udostępnia, chcąc poinformować znajomych. Później okazuje się, że informacja była nieprawdziwa, a udostępnienie jej naraziło Janka na krytykę.

Pytania do dyskusji:

1. Jakie kroki mógł podjąć Janek, aby upewnić się, że udostępniane przez niego informacje są prawdziwe?
2. Jakie są konsekwencje udostępniania fałszywych informacji online - zarówno dla jednostek, jak i społeczeństwa?
3. Jaką etykę cyfrową należy stosować, aby uniknąć takich sytuacji?



Przypadek 2: Prywatność w mediach społecznościowych

Marta regularnie publikuje zdjęcia swojej rodziny na Instagramie, w tym zdjęcia swoich dzieci podczas codziennych czynności. Pewnego dnia ktoś, bez jej zgody, wykorzystuje jedno ze zdjęć do stworzenia mema, który staje się popularny, a Marta zaczyna otrzymywać nieprzyjemne wiadomości od nieznajomych.

Pytania do dyskusji:

1. W jaki sposób Martha mogła lepiej chronić prywatność swojej rodziny w mediach społecznościowych?
2. Jakie są granice etycznego wykorzystywania zdjęć innych osób dostępnych publicznie?
3. Jakie narzędzia i ustawienia prywatności w mediach społecznościowych mogą pomóc w takich sytuacjach?

Przypadek 3: Netykieta i komunikacja online

Anne bierze udział w dyskusji na forum internetowym na temat szczepień. Jej post, wyrażający poparcie dla szczepień, spotyka się z falą agresywnych komentarzy i trollingu. Ostatecznie Anna decyduje się usunąć swoje konto, zniechęcona poziomem dyskusji.

Pytania do dyskusji:

1. Jakie zasady netykiety mogłyby zapobiec takiej sytuacji?
2. Jak użytkownicy i administratorzy platform mogą reagować na trolling i agresywne komentarze?
3. Jak dbać o kulturę dyskusji online, zwłaszcza na kontrowersyjne tematy?

Przypadek 4: Korzystanie z treści innych osób

Tom prowadzi blog poświęcony modzie. Aby zwiększyć zainteresowanie, publikuje zdjęcia znanych projektantów znalezione w Internecie, nie podając źródła ani nie uzyskując pozwolenia. Po pewnym czasie otrzymuje wiadomość z żądaniem usunięcia zdjęć i groźbą podjęcia kroków prawnych.

Pytania do dyskusji:

1. W jaki sposób Tom mógłby etycznie i legalnie wykorzystywać treści innych osób na swoim blogu?
2. Jakie są prawne i wizerunkowe konsekwencje naruszenia praw autorskich w Internecie?
3. Jakie praktyki i narzędzia pomagają przestrzegać praw autorskich podczas tworzenia treści?