



Co-funded by
the European Union



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

MODUŁ 3: Bezpieczeństwo i prywatność w sieci

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 3. Bezpieczeństwo i prywatność w sieci

Wprowadzenie

Moduł „Bezpieczeństwo i prywatność w sieci” został opracowany w formie interaktywnych materiałów online, dostępnych pod adresem: [Bezpieczeństwo i prywatność w sieci](#). Zasoby te można wykorzystywać w różny sposób – jako prezentację podczas zajęć stacjonarnych, jako element kursu e-learningowego lub w formule blended-learningu, łączącej pracę online i offline.

Celem modułu jest podniesienie świadomości uczestników w zakresie ochrony danych osobowych, bezpiecznego korzystania z mediów społecznościowych oraz minimalizowania ryzyka związanego z aktywnością w sieci. Materiały prowadzą uczestników krok po kroku od zrozumienia istoty bezpieczeństwa online, przez praktyczne umiejętności (m.in. tworzenie silnych haseł, konfiguracja ustawień prywatności, korzystanie z 2FA), aż po świadome publikowanie treści i reagowanie w sytuacji naruszenia prywatności.

Struktura modułu opiera się na lesson planie, który obejmuje:

- wprowadzenie do tematyki bezpieczeństwa i prywatności,
- zagrożenia związane z mediami społecznościowymi (kradzież danych, phishing, cyberstalking, spoofing, uzależnienie),
- zasady bezpiecznego logowania i korzystania z publicznych sieci Wi-Fi,
- skutki publikacji danych osobowych, zdjęć i informacji o lokalizacji,
- analizę przypadku (case study) i ćwiczenia grupowe,
- podsumowanie oraz dodatkowe źródła i narzędzia.

Materiały online zawierają filmy, grafiki, linki do zasobów zewnętrznych oraz opisane ćwiczenia, które można realizować indywidualnie lub w grupach. W przewodniku znajdują się także wskazówki, jak prowadzić dyskusje i analizę przypadków, aby angażować uczestników oraz pomagać im w przenoszeniu zdobytej wiedzy na własne doświadczenia w internecie.

Dzięki elastycznej formule materiał może być realizowany zarówno w pełnej wersji (ok. 120 minut), jak i w skróconej, dopasowanej do możliwości czasowych grupy. Edukator decyduje, które elementy włączyć, biorąc pod uwagę potrzeby i poziom kompetencji uczestników.



Bezpieczeństwo i prywatność w Internecie

Matryca kompetencji w zakresie bezpieczeństwa cyfrowego dla osoby aktywnej w mediach społecznościowych

Obszar kompetencji	Wiedza	Umiejętności	Postawy
Zarządzanie hasłami	- Zasady tworzenia silnych haseł - Rola menedżerów haseł - Znaczenie uwierzytelniania dwuskładnikowego (2FA)	- Tworzenie i zmiana silnych haseł - Konfiguracja uwierzytelniania dwuskładnikowego (2FA) na różnych platformach - Obsługa menedżera haseł	- Dbanie o stosowanie różnych haseł do różnych kont - Zaufane narzędzia do zarządzania hasłami - Ostrożność przy udostępnianiu haseł
Świadomość zagrożeń związanych z phishingiem i inżynierią społeczną	- Rodzaje ataków phishingowych - Techniki inżynierii społecznej stosowane przez cyberprzestępców	- Rozpoznawanie podejrzanych wiadomości i stron internetowych - Zgłaszanie phishingu - Ochrona danych osobowych	- Krytyczne podejście do otrzymanych wiadomości - Ostrożność w podawaniu danych - Czujność wobec nietypowych sytuacji
Bezpieczeństwo urządzeń	- Rola aktualizacji systemu - Znaczenie programów antywirusowych i zapór sieciowych - Zagrożenia związane z fizycznym dostępem do urządzeń	- Instalacja i konfiguracja programu antywirusowego - Regularna aktualizacja oprogramowania - Urządzenia zabezpieczające	- Aktualizowanie oprogramowania - Świadomość zagrożeń związanych z brakiem bezpieczeństwa - Odpowiedzialność za własne urządzenia
Zarządzanie danymi i prywatnością	- Ustawienia prywatności na platformach - Ochrona danych - Przepisy RODO (RODO)	- Skonfigurowanie ustawienia prywatności - Ograniczanie widoczności danych osobowych - Bezpieczne udostępnianie informacji	- Szacunek dla prywatności własnej i innych osób - Odpowiedzialność za przetwarzane dane - Świadomość prawna w zakresie ochrony danych



Bezpieczne korzystanie z sieci	- Zagrożenia związane z publicznymi sieciami Wi-Fi - Funkcje i zalety korzystania z VPN	- Konfiguracja VPN - Bezpieczne korzystanie z sieci Wi-Fi - Unikanie ryzykownych połączeń internetowych	- Należy zachować ostrożność podczas korzystania z sieci publicznych. - Proaktywność w zabezpieczaniu połączeń - Świadomość zagrożeń internetowych
Zarządzanie kontem i treścią	- Narzędzia do monitorowania kont - Rola polityki prywatności w mediach społecznościowych	- Regularny przegląd i analiza aktywności na koncie - Bezpieczna publikacja treści	- Odpowiedzialność za publikowane treści - Dbłość o przestrzeganie zasad polityki prywatności - Proaktywne monitorowanie działalności

Moduł 3. Bezpieczeństwo i prywatność w sieci

Efekty uczenia się:

Uczestnicy i uczestniczki warsztatów:

- rozumieją, dlaczego prywatność i bezpieczeństwo online są ważne;
- potrafią tworzyć silne hasła i korzystać z uwierzytelniania dwuskładnikowego;
- umieją ustawić odpowiednie poziomy prywatności na swoich profilach społecznościowych;
- są świadomi zagrożeń związanych z publikowaniem danych osobowych, zdjęć i lokalizacji;
- potrafią bezpiecznie korzystać z publicznych sieci Wi-Fi i obcych urządzeń;
- wiedzą, jak reagować w przypadku naruszenia prywatności lub przejęcia konta;
- potrafią ocenić, jakie treści można bezpiecznie publikować w mediach społecznościowych.

Czas trwania: 120 minut

Działania	Cel	Wskazówki metodyczne	Materiały	Czas	Inne zasoby / link do zasobów
1. Wprowadzenie: Dlaczego prywatność online jest ważna?	Podniesienie świadomości zagrożeń w sieci i ich konsekwencji.	Krótkie wprowadzenie trenera + przykłady z życia .	Treści ze strony Bezpieczeństwo i prywatność - historia Magdy, Krzysztofa, przykłady trenera.	15 minut	Bezpieczeństwo i prywatność

2. Silne hasła i 2FA	Uczestnicy nauczą się tworzyć silne hasła i rozumieją znaczenie uwierzytelniania dwuskładnikowego.	Pokaz krok po kroku Sugerowane materiały filmowe, które są w języku angielskim można tłumaczyć za pomocą ustawień w Youtube. Proponowane materiały w postaci stron internetowych można tłumaczyć na dowolny język przy użyciu tłumacza w przeglądarce np. Chrome. Aby uzyskać najlepsze tłumaczenie sugeruje się użycie strony przygotowanej w projekcie w języku angielskim.	Tablica/flipy, marker, aplikacje mobilne	15 minut	Instrukcje dotyczące tworzenia silnych haseł i konfigurowania 2FA  How to protect...  What Is Two-F... Co to jest uwierzytelnianie Definicja uwierzytelniania Malwarebytes Uwierzytelnianie dwuskładnikowe 2FA: Zabezpiecz swoje cyfrowe życie Menedżer Haseł
3. Ustawienia prywatności profilu	Uczestnicy samodzielnie sprawdzają i zmieniają ustawienia swoich kont.	Praca indywidualna z telefonem/laptopem + wsparcie trenera.	Dostęp do Internetu, instrukcje YouTube	20 minut	How to configure privacy in Instagram
4. Świadome udostępnianie treści	Uczestnicy potrafią rozróżnić, które treści są bezpieczne do publikacji.	Dyskusja kierowana, analiza przykładów.	Treści ze strony https://sites.google.com/view/bezp-pryw-re-mcread	15 minut	Privacy and Social Media

5. Bezpieczne logowanie i korzystanie z Wi-Fi	Uczestnicy znają zagrożenia związane z publicznym Wi-Fi i wiedzą, jak ich unikać.	Prezentacja + pytania do grupy	Treści ze strony https://sites.google.com/view/bezp-pryw-re-mcread/	15 minut	Centrum zasobów cyberbezpieczeństwa
6. Co robić w przypadku naruszenia prywatności?	Uczestnicy znają kroki, które należy podjąć po przejęciu konta.	Dyskusja, analiza procedur	Opisy procedur (Facebook, Instagram, Twitter X)	15 minut	https://help.instagram.com/
7. Case study: Maria i bezpieczeństwo uchodźczyń	Refleksja nad bezpieczeństwem wrażliwych użytkowników.	Praca w grupach + prezentacja wniosków	Opis przypadku Marii https://sites.google.com/view/bezp-pryw-re-mcread/	20 minut	
8. Podsumowanie i pytania	Podkreślenie najważniejszych zasad i rozwianie wątpliwości.	Otwarte pytania, zebranie wniosków		5 minut	