



Co-funded by
the European Union



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

МОДУЛЬ 3: Безпека та конфіденційність в Інтернеті ПЛАН УРОКУ



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project no. 2023-1-PL01-KA220-ADU-000156610

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



Модуль 3. Безпека та конфіденційність в Інтернеті

Вступ

Модуль «Безпека та конфіденційність в Інтернеті» розроблено як інтерактивний онлайн-ресурс, доступний за адресою: [Безпека та конфіденційність в Інтернеті](#). Ці ресурси можна використовувати різними способами – як презентацію під час занять у класі, як частину курсу електронного навчання або в форматі змішаного навчання, поєднуючи роботу в Інтернеті та поза ним.

Метою модуля є підвищення обізнаності учасників щодо захисту персональних даних, безпечного використання соціальних мереж та мінімізації ризиків, пов'язаних з онлайн-активністю. Матеріали покроково проводять учасників від розуміння сутності онлайн-безпеки до формування практичних навичок (створення надійних паролів, налаштування параметрів конфіденційності, використання двофакторної автентифікації), а також до усвідомленого розміщення контенту та реагування на порушення конфіденційності.

Структура модуля базується на плані уроку, який включає:

- вступ до питань безпеки та конфіденційності;
- ризики, пов'язані з використанням соціальних мереж (крадіжка даних, фішинг, кіберсталкінг, спуфінг, залежність);
- принципи безпечного входу в систему та використання публічних мереж Wi-Fi;
- наслідки оприлюднення персональних даних, фотографій та інформації про місцезнаходження;
- тематичне дослідження та групові вправи;
- підсумки, додаткові ресурси та інструменти.

Онлайн-ресурси містять відеоматеріали, графічні ілюстрації, посилання на зовнішні джерела, а також описані вправи, які можуть виконуватися індивідуально або в групах. Посібник також надає рекомендації щодо проведення дискусій та аналізу кейсів з метою активного залучення учасників і сприяння перенесенню набутих знань у їх власний досвід онлайн-діяльності.

Завдяки гнучкому формату матеріал може бути представлений як у повній версії (тривалістю орієнтовно 120 хвилин), так і у скороченому варіанті — відповідно до часових можливостей групи.

Викладач самостійно визначає, які елементи включити, з урахуванням потреб та рівня компетентності учасників.



**Co-funded by
the European Union**





Безпека та конфіденційність в Інтернеті

Матриця компетентностей у сфері цифрової безпеки для осіб, які активно використовують соціальні мережі

Область компетентності	Знання	Навички	Ставлення
Управління пароллями	- Принципи створення надійних паролів - Роль менеджерів паролів - Важливість двофакторної автентифікації (2FA)	- Створення та зміна надійних паролів - Налаштування 2FA на різних платформах - Підтримка менеджера паролів	- Слідкуйте за тим, щоб використовувати різні паролі для різних облікових записів. - Довіра до інструментів управління пароллями - Обережність при передачі паролів
Обізнаність щодо фішингу та соціальної інженерії	- Типи фішингових атак - Техніки соціального інжинірингу, що використовуються кіберзлочинцями	- Розпізнавання підозрілих повідомлень та сайтів - Повідомлення про фішинг - Захист персональних даних	- Критичний підхід до отриманих повідомлень - Обережність при наданні даних - Пильність до незвичайних ситуацій
Безпека пристроїв	- Роль оновлень системи - Важливість антивірусу та брандмауера - Загрози, пов'язані з фізичним доступом до пристроїв	- Встановлення та налаштування антивірусної програми - Регулярне оновлення програмного забезпечення - Захисні пристрої	- Оновлення програмного забезпечення - Усвідомлення ризиків, пов'язаних з відсутністю безпеки - Відповідальність за власні пристрої
Управління даними та конфіденційністю	- Налаштування конфіденційності на платформах - Захист даних - Положення RODO (GDPR)	- Налаштувати параметри конфіденційності - Обмеження видимості особистої інформації	- Повага до власної та чужої приватності - Відповідальність за обробку даних - Правова обізнаність щодо захисту даних



		- Безпечний обмін інформацією	
Безпечне використання мереж	- Небезпека публічних мереж Wi-Fi - Особливості та переваги використання VPN	- Налаштування VPN - Безпечне використання мереж Wi-Fi - Уникнення ризикованих підключень до Інтернету	- Будьте обережні при використанні громадських мереж - Проактивність у забезпеченні зв'язків - Усвідомлення онлайн-загроз
Управління обліковим записом та вмістом	- Інструменти моніторингу рахунків - Роль політики конфіденційності в соціальних мережах	- Регулярний перегляд та аналіз активності рахунку - Безпечна публікація контенту	- Відповідальність за опублікований контент - Дотримання політики конфіденційності - Проактивний підхід до моніторингу діяльності

Модуль 3. Безпека та конфіденційність в Інтернеті

Результати навчання:

Учасники семінару:

- розуміють, чому онлайн-конфіденційність та безпека є важливими;
- вміють створювати надійні паролі та використовувати двофакторну аутентифікацію;
- вміють налаштовувати відповідний рівень конфіденційності у своїх соціальних профілях;
- усвідомлюють ризики, пов'язані з оприлюдненням персональних даних, фотографій та інформації про місцезнаходження;
- знають, як безпечно користуватися публічними мережами Wi-Fi та сторонніми пристроями;
- знають, як діяти у випадку порушення конфіденційності або захоплення облікового запису;
- вміють оцінювати, який контент є безпечним для публікації у соціальних мережах.

Тривалість: 120 хвилин

Діяльність	Мета	Методологічні примітки	Матеріали	Час	Інші ресурси / посилання на ресурси
1. Вступ: Чому важлива конфіденційність в Інтернеті?	Підвищення обізнаності про ризики в Інтернеті та їх наслідки.	Короткий вступ від тренера + приклади з реального життя	Зміст з Безпека та конфіденційність в Інтернеті - Історія Магди, Крістофер, приклади тренера. -	15 хв	Безпека та конфіденційність в Інтернеті

2. Надійні паролі та двофакторна автентифікація (2FA)	Учасники дізнаються, як створювати надійні паролі та зрозуміють важливість двофакторної автентифікації.	Покрокова демонстрація Пропоновані відеоматеріали англійською мовою можна перекласти за допомогою налаштувань у Youtube. Пропонований матеріал у вигляді веб-сторінок можна перекласти будь-якою мовою за допомогою перекладача в браузері, наприклад Chrome. Для найкращого перекладу рекомендується використовувати сторінку, підготовлену в проекті англійською мовою.	Дошка/фліпчарт, маркер, мобільні додатки	15 хв	Instructions for creating strong passwords and configuring 2FA How to protect your accounts What Is Two-Factor Authentication? What is Authentication Two-Factor Authentication 2FA: Secure Your Digital Life What is Password Manager Do I need it
3. Налаштування конфіденційності профілю	Учасники самостійно перевіряють та змінюють налаштування своїх облікових записів.	Індивідуальна робота з телефоном/ноутбуком + підтримка тренера.	Доступ до Інтернету, інструкції на YouTube	20 хв	How to configure privacy in Instagram
4. Інформований обмін контентом	Учасники можуть розрізнити, який контент безпечно публікувати.	Керівництво дискусією, аналіз прикладів.	Зміст з	15 мін	Privacy and Social Media

			Безпека та конфіденційність в Інтернеті		
5. Безпечний вхід та використання Wi-Fi	Учасники знають про ризики, пов'язані з публічним Wi-Fi, та про те, як їх уникнути.	Презентація + питання до групи	Зміст з Безпека та конфіденційність в Інтернеті	15 хв	Cybersecurity Basics - Educate and protect yourself
6. Що робити у разі порушення конфіденційності?	Учасники знають, які кроки необхідно вжити після захоплення облікового запису.	Обговорення, аналіз процедур	Опис процедур (Facebook, Instagram, Twitter X)	15 хв	https://help.instagram.com/
7. Приклад з практики: Марія та безпека жінок-біженців	Роздуми про безпеку вразливих користувачів.	Групова робота + презентація висновків	Історія хвороби Марії Безпека та конфіденційність в Інтернеті	20 хв	
8. Підсумок та питання	Висвітлення основних принципів та вирішення проблемних питань.	Відкриті питання, збір висновків		5 хв	