**ВАЖЛИВО!!! БЕЗПЕКА В ЦИФРОВОМУ СЕРЕДОВИЩІ**

**Інтернет — це невід’ємна частина нашого життя.**

Він є глобальною системою взаємозалежних комп’ютерних мереж. Інтернет є мережею мереж, що дає можливість створення кіберпростору, де відбувається онлайнова комунікація. **Кіберпростір** ще називають віртуальною реальністю. **Віртуальна реальність** — це ілюзія дійсності, створена за допомогою комп’ютерних систем, які забезпечують зорові, звукові та інші органи чуття. Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні. **Офлайн-ідентичність** – це ви самі, особа, з якою ваші друзі та сім’я взаємодіють щодня вдома або на роботі. Оточуючі знають ваші персональні дані, а саме ваше ім’я, вік або місце проживання. **Ваша ідентичність в Інтернеті** – це ви у кіберпросторі. **Ваша онлайн-ідентичність** – це те, як ви представляєте себе іншим в Інтернеті. **Ця онлайн-ідентичність має розкривати лише мінімум інформації про вас.**

**Будьте обачні, обираючи ім’я користувача або псевдонім для себе в Інтернеті.** Ім’я користувача не повинно містити жодної особистої інформації. Це має бути щось доречне і прийнятне. Ім’я користувача не повинно давати привід стороннім людям подумати, що ви є легкою ціллю для кіберзлочинців або хочете привернути небажану увагу Питання збереження приватності в мережі Інтернет є актуальним, оскільки **віртуальне спілкування практично ніколи не буває приватним**. **Інформація, що поширюється в режимі онлайн електронною поштою, соцмережами тощо легко може бути доступна іншим. Від неї також неможливо повністю позбутися.** Недостатня захищеність інформації та своїх профілів створює ризик доступу до неї інших людей і її використання без дозволу. Користувачі Інтернету самі несуть відповідальність за захист відомостей про своє життя.

**Будь-яка інформація про вас може вважатися вашими персональними даними.** Ця персональна інформація може однозначно ідентифікувати вас як особистість. Ці дані містять фото та повідомлення, якими ви обмінюєтесь з родичами та друзями в Інтернеті. Інша інформація, така як ім’я, номер соціального страхування, дата і місце народження або дівоче прізвище матері, відома лише вам і використовується для встановлення вашої особистості. Такі відомості, як медична, освітня, фінансова інформація та дані про працевлаштування також можуть бути використані для ідентифікації вас в Інтернеті.

Комп’ютерні пристрої зберігають ваші дані та є порталом до вашого онлайн-життя. Навіщо та кому можуть знадобитися ваші особисті дані?

− Ними можуть скористатися рекламодавці (для збільшення кількості розсилок).

− Чужі особисті дані використовуються для отримання кредитів та крадіжок коштів із банків.

− Дані можуть бути викрадені з хуліганських спонукань (оприлюднити листування, наприклад).

− Дані можуть бути викрадені для подальшого перепродажу.

− Витік даних можливий з комп’ютера, ноутбука, мобільного пристрою. При цьому дані потрапляють до кіберзлочинців через Інтернет, електронну пошту.

− Цінність для зловмисників є і облікові записи електронної пошти. Адреса електронної пошти може бути використана для підтвердження реєстрації на інших вебсайтах.

Цікаво, що поняття «витік персональних даних» в англійській мові відповідає Identity theft (крадіжка особистості).

**Способи захисту особистих даних:**

1. Створення складних паролів.
2. Використання двофакторної аутентифікації.
3. Шифрування повідомлень.
4. Не підключатися до громадського WiFi.

**Як покращити безпеку браузера?**

Щоб запобігти потенційним загрозам для безпеки браузера та конфіденційних даних під час перегляду веб-сторінок, варто дотримуватись наступних порад.

1. Оновлюйте браузер та встановлені плагіни, щоб мінімізувати шанси використання вразливостей, а також видаліть усі застарілі плагіни.
2. Відвідуйте лише безпечні сайти з використанням протоколу HTTPS, про що свідчить замок в адресному рядку. У такому випадку хакери не зможуть перехопити трафік з браузера до веб-сервера.
3. Остерігайтесь фішингових загроз, які поширюються через електронну пошту та онлайн-повідомлення. Ніколи не відповідайте на небажані електронні листи, не перевіривши дані відправника, та не надсилайте конфіденційну інформацію незнайомцям.
4. Не завантажуйте підозрілі програми чи файли, а у випадку потреби використовуйте для цього виключно офіційні ресурси.
5. Використовуйте багатофакторну автентифікацію, щоб зменшити ризики викрадення облікових даних.
6. Застосовуйте VPN від надійного провайдера, а не безкоштовну версію. Це створить зашифрований тунель для Інтернет-трафіку та захистить від відстеження сторонніми особами.

**Більше інформаціїї за посиланнями:**

<https://www.unicef.org/ukraine/cyberbulling?fbclid=IwAR3m5HdVOwhspQW2fayyYEywK6B2hFjpyM1kbYi1lBjiQW_RL0uYRXndKmE>

**Про кібербулінг для підлітків**

**Освітній серіал.** Переглянувши 4 короткі відео, ви дізнаєтесь, як виглядає кібербулінг, які причини та потенційні наслідки кібербулінгу, як припинити кібербулінг і що робити, якщо хтось із друзів став жертвою кібербулінгу.

<https://www.unicef.org/ukraine/about-cyberbullying-for-teenagers?fbclid=IwAR0aqO-nbYyrFBX8IOD_4EHUlYmNaxlgawS0G-M-prNPk3MjF046Qeim2yc>