Рекомендації з онлайн-безпеки для учнів, які перебувають на тимчасово окупованих територіях

Якщо ти навчаєшся за українською програмою, але перебуваєш на тимчасово окупованій території (ТОТ), то, ймовірно, стикаєшся з ризиками – як у цифровому просторі, так і в реальному житті. Це непросто, і ми розуміємо, наскільки це сміливий вибір – продовжувати навчання попри загрози. Багато таких учнів, як ти, не здаються й вірять у своє українське майбутнє. І це дуже важливо.

Ми хочемо допомогти зробити твоє навчання безпечнішим – захистити твої особисті дані та зменшити ризики, з якими ти можеш зіткнутись. Тому створили ці поради, щоб підтримати тебе.

Щоб створити ці рекомендації, ми спершу зібрали основні поради з цифрової безпеки, а також окремо дослідили ситуацію на ТОТ: які сайти й сервіси там працюють, які – заблоковані, як збираються та зберігаються особисті дані в інтернеті, і які загрози можуть виникати. Завдяки цьому ми сформували прості, але важливі поради, які допоможуть тобі залишатися в безпеці під час навчання.

ЗМІСТ

1 **Користуйся VPN.** Коли ти під'єднуєш свій телефон або інший пристрій до інтернету — потрібно його додатково захисти за допомогою VPN. Також він допоможе тобі заходити на ті ресурси, які можуть блокуватися на ТОТ.
Радимо використовувати Proton VPN або Tunnel Bear (має обмеження на використання в безкоштовній версії).
! З міркувань безпеки краще користуватись VPN постійно.

2 **Використовуй безпечні веббраузери**

Google Chrome Opera Firefox Safari

Для того, щоб використовувати браузер для навчання, радимо використовувати анонімні вікна (або режим «інкогніто») й закривати їх, коли вони тобі більше не потрібні.
! Не можна в жодному разі користуватися **Yandex Browser**. Він може передавати твої дані й вони можуть не будуть захищеними.

3 **Використовуй безпечні програми та платформи для спілкування та навчання**

Gmail Google Meet ZOOM Discord*
WhatsApp Instagram facebook

* ***Discord*** *наразі є заблокованим на ТОТ та можливий для використання лише у веббраузері та у браузерній версії з мобільного з використанням VPN.*

! **Не використовуй** Signal
Хоч він і є безпечним для твоїх даних, однак може привернути небажану увагу, адже часто використовується військовими.

4 **Подбай про безпечні паролі.** Якщо ти маєш надто прості та однакові паролі всюди, то їх буде дуже легко зламати та отримати твої особисті дані.
Пароль має складатись з щонайменше 16 символів та містити малі й великі літери, цифри та символи.
Лайфхак: паролем можуть стати тексти улюблених пісень та улюблена цифра наприкінці (для кожного ресурсу окремий пароль).

Перевірити, наскільки міцний у тебе пароль, можна за посиланням: https://zillya.ua/check-password.

Також **рекомендуємо використовувати менеджер паролів,** адже запам'ятати 10-20-30 різних паролів складно, тому пропонуємо використовувати:

- Bitwarden (https://bitwarden.com/), з детальною інструкцією для безпечного використання можете ознайомитись за посиланням: https://yak.dslua.org/services/bitwarden/
- LastPass (https://www.lastpass.com/), з детальною інструкцією для безпечного використання можете ознайомитись за посиланням: https://yak.dslua.org/services/lastpass/.

5 **Налаштуй подвійний захист.** Щоб злочинцям було неможливо зламати твої акаунти — потрібно використовувати двоетапну перевірку всюди: в соціальних мережах, електронній пошті тощо.

Gmail	https://yak.dslua.org/services/gmail/2fa/
facebook	https://yak.dslua.org/services/facebook/2fa/
WhatsApp	https://yak.dslua.org/services/whatsapp/2fa/
Discord	https://support.discord.com/hc/en-us/articles/*
Instagram	https://yak.dslua.org/services/instagram/2fa/
ZOOM	https://support.zoom.com/hc/ru/article?id=zm_kb&sysparm_article=KB0066057

**Ця стаття подана англійською через відсутність перекладу українською. Ви можете скористатись функцією автоматичного перекладу сторінки від Google. Інструкція, як це зробити: https://support.google.com/chrome/*

6 Подбай про свою особисту інформацію.
Якщо ти перебуваєш на ТОТ, на заняттях тобі **НЕ МОЖНА казати своє прізвище, місце проживання, дані про батьків чи школу, або будь-яку іншу особисту інформацію.** Також не обов'язково на заняттях казати своє справжнє ім'я. Але не забудь домовитись з викладачами про це в особистих чатах.

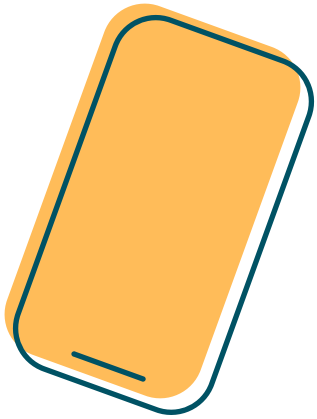
! Радимо утриматись від використання камери на заняттях. Вона також може видати зайву інформацію про тебе.
Дотримання цих правил убезпечить тебе на випадок, якщо стороння особа потрапить на урок, або ж хтось без твого відома зробить скриншот.

7 Не залишай вподобайки, реакції чи коментарі під публікаціями, а також не підписуйся на групи, канали чи акаунти в соціальних мережах, якщо вони можуть привернути увагу росіян.

! Уникай обговорень в публічних групах та чатах. Це може привернути зайву увагу до твоїх акаунтів й становити небезпеку для тебе.

8 Повідом, якщо твоїй безпеці в інтернеті щось загрожує. Якщо хтось намагатиметься зламати твій акаунт (тобі приходять невідомі посилання, смс-повідомлення) — повідом про це батькам/опікунам.

Радимо продумати та домовитись заздалегідь про альтернативні канали зв'язку з близькими та вчителем, на випадок зламу чи припинення роботи якогось з ресурсів.



Алгоритм приєднання до занять

Нижче ми поділимось універсальним алгоритмом безпечного онлайн-навчання, який ти зможеш адаптувати під себе залежно від платформ та пристроїв, якими користуєшся. Також нижче ти знайдеш посилання на детальні інструкції з приєднання на заняття з різних платформ.

Загальний алгоритм приєднання до занять:

1. Включи VPN.
2. Зайди на платформу/сайт/додаток для навчання без використання справжнього ім'я та прізвища та інших особистих даних (анонімно або з використанням нікнейму). Як це зробити розповідаємо нижче.
3. Будь без камери та не використовуй свої фотографії.
4. На самому занятті не ділись особистою інформацією.
5. По завершенню заняття та навчання закрий усі додатки та вкладки.

Детальні інструкції з приєднання на заняття в Google Meet, Zoom та Discord можна знайти за посиланням: https://drive.google.com/file/d/1TY-XsaX-NYX_Ute8nbs50D69Kk9BGci4/view?usp=sharing

Додаткові корисні ресурси

1. Пограти в гру від Google: https://beinternetawesome.withgoogle.com/uk_ua/interland
2. Пройти відеосимулятор про безпеку в інтернеті: https://osvita.diia.gov.ua/simulators/e-safety-teens-simulator
3. Подивитись онлайн курс про твої цифрові права та безпеку в інтернеті: https://minzmin.org.ua/onlinecourse/
4. Дослідити вебпортал «Кібер Брама» та ознайомитись з корисними рекомендаціями для безпечного користування Інтернетом: https://stopfraud.gov.ua/

ДЯКУЄМО, ЩО ДБАЄШ ПРО СВОЮ ОНЛАЙН БЕЗПЕКУ!