Рекомендації з онлайн-безпеки учнів, які перебувають на ТОТ та вчителів, які з ними працюють

Учні, які перебувають на тимчасово окупованих територіях (надалі ТОТ) України зіштовхуються з загрозами цифрової та фізичної безпеки під час навчання за українською програмою. Однак велика кількість таких учнів, попри ризик, продовжують навчання в українських школах та вірять у своє українське майбутнє. **Наша спільна мета – зробити все, щоб зберегти та посилити цей зв'язок**.

Ми розробили ці рекомендації для того, щоб допомогти зробити навчальний процес для учнів, які перебувають на ТОТ, безпечнішим, захистити їх особисті дані, а також подбати про безпеку вчителів.

Для розробки цих рекомендацій було проведене дослідження питання цифрової безпеки на ТОТ, аналіз доступних та заборонених сайтів та онлайн-сервісів на ТОТ, аналіз способів збору та збереження даних різними сайтами та онлайн-сервісами.

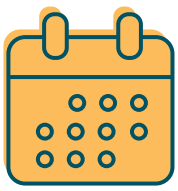
ЗМІСТ

ВИЗНАЧЕННЯ ТЕРМІНІВ

VPN — це послуга, яка дозволяє мати приватне з'єднання під час використання загальнодоступної мережі. VPN часто використовується для приховування вашого місцезнаходження, надаючи приватний шлях між комп'ютером та вебсайтами, які ви відвідуєте в інтернеті. Це означає, що ваше місцезнаходження не буде видно під час перегляду в інтернеті.

Двоетапна перевірка — це спосіб додаткового захисту, який забезпечує безпечніший захист даних, зокрема повідомлень електронної пошти та соціальних мереж. Зазвичай, використовується автоматичне надсилання SMS-повідомлень або окрема програма, яка генерує коди доступу.

Кібератака — це навмисна дія, здійснена через комп'ютерні мережі з метою порушити, пошкодити, знищити або отримати несанкціонований доступ до інформаційних систем, чужих даних чи інфраструктури. Кібератаки можуть бути спрямовані як на окремих користувачів, так і на організації, державні установи тощо.



ПРИНЦИПИ, ЗА ЯКИМИ СТВОРЕНІ ЦІ РЕКОМЕНДАЦІЇ

- ✓ Онлайн-захист як учня, так і вчителя.
- ✓ Надання доступу до платформ навчання тільки авторизованим користувачам з унікальними обліковими записами.
- ✓ Заборона публікації особистої інформації учасників у групових чатах або відеоконференціях.
- ✓ Проведення навчання та спілкування онлайн лише на платформах з високим рівнем кіберзахисту.
- ✓ Повідомлення про інциденти безпеки для швидкого реагування та розв'язання проблем.

ПРАВИЛА ДЛЯ ЗАБЕЗПЕЧЕННЯ ОНЛАЙН-БЕЗПЕКИ ВЧИТЕЛЯ

Учитель має подбати про захист власних особистих даних, зокрема про захист особистих та робочих акаунтів на цифрових платформах, у месенджерах та на електронній пошті. Це допоможе уникнути витоку даних та злому акаунтів.

Особливо це важливо, якщо на пристрої вчителя є будь-яка особиста інформація про учнів, які перебувають на ТОТ (номер телефону, прізвище, точна дата народження, документи учнів та їх батьків тощо).

1 **Створити безпечні паролі.** Учителі та тренери мають використовувати складні паролі для доступу до облікових записів, платформ чи месенджерів. Пароль має складатись з понад 16 символів, містити малі та великі літери, цифри та символи. Перевірити, наскільки міцний у вас пароль, можна за посиланням: https://zillya.ua/check-password.

Також **рекомендуємо використовувати менеджер паролів,** адже для кожного облікового запису у вас має бути пароль, який відрізняється від інших паролів. 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/.

2 Використовувати двоетапну перевірку на всіх цифрових акаунтах.

За посиланнями можна дізнатися, як це зробити:

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/*

3 Перевірте наявні активні сеанси у ваших месенджерах.

Активні сеанси — це всі випадки, коли ваш обліковий запис увійшов у систему на різних пристроях або в браузерах. Вони дозволяють бачити, де саме здійснено вхід до ваших облікових записів, і закривати небажані або підозрілі сеанси для підвищення безпеки. Саме активні сеанси, які показують відмінні від ваших пристрої чи розташування, будуть свідчити про злам ваших акаунтів.

Щоб **виявити та відреагувати на підозрілі сеанси** чи активність з місць, які не є знайомими – необхідно скористатися інструкціями нижче.

Gmail https://yak.dslua.org/services/gmail/vidkryty-sesii/

facebook https://yak.dslua.org/services/facebook/vidkryty-sesii/

Instagram https://yak.dslua.org/services/instagram/vidkryty-sesii/

У випадку наявності підозрілої активності необхідно натиснути «вийти з усіх акаунтів» та змінити паролі.

4 Перевірте, чи не було у вас витоків даних, або зламів електронної пошти.
Це можна зробити за посиланням: https://monitor.mozilla.org/.
Якщо було виявлено витік даних, пов'язаний з вашою електронною поштою — змініть ваш пароль.

5 Регулярно оновлюйте програмне забезпечення.
Важливо регулярно оновлювати програмне забезпечення на комп'ютерах, смартфонах та інших пристроях, що використовуються для онлайн-навчання, для забезпечення захисту від потенційних кіберзагроз.

6 Рекомендуємо покращити власні базові навички онлайн-безпеки за допомогою:

- Вебпорталу «Кібер Брама» з корисними рекомендаціями для безпечного користування Інтернетом, попередження та протидії злочинним діям онлайн: https://stopfraud.gov.ua/
- Відеосимулятора від Дія.Освіта про безпеку в Інтернеті: https://osvita.diia.gov.ua/catalog/topic/online-security
- Онлайн-курсу «Цифрові права та безпека дитини» (без отримання сертифікату): https://minzmin.org.ua/onlinecourse/
- Онлайн-курсу «Безпека в інтернеті під час війни» (із отриманням сертифікату): https://prometheus.org.ua/course/course

КОМУНІКАЦІЯ З УЧНЯМИ

Рекомендуємо використовувати такі програми та платформи:

Gmail Google Meet ZOOM Discord*

WhatsApp Instagram facebook

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

Як використовувати Discord на ТОТ: включити VPN → відкрити безпечний браузер → створити анонімну вкладку / приватний режим / приватний перегляд в браузері → перейти на сайт Discord й відкрити браузерну версію.

Для месенджерів рекомендуємо налаштувати автоматичне видалення повідомлень.

Як це зробити:

Відкрийте чат → натисніть на три крапки зверху → виберіть «Тимчасові повідомлення» → увімкніть функцію та задайте потрібний період (найкраще обрати варіант «24 години»).

Відкрийте чат з користувачем → проведіть пальцем вгору в чаті, щоб увійти в режим зникнення (Vanish Mode), у цьому режимі повідомлення автоматично зникають після закриття чату → щоб вимкнути цей режим, ще раз проведіть пальцем вгору або натисніть кнопку «Вимкнути».

facebook

Відкрийте чат із користувачем → натисніть на ім'я контакту у верхній частині екрана → у меню виберіть «Зникаючі повідомлення» → щоб повернутися до звичайного режиму, вимкніть режим зникнення у налаштуваннях чату.

Не рекомендуємо використовувати Viber та Telegram. Ці месенджери мають слід у співпраці з агресором та можуть становити **небезпеку для учнів**. Також з цієї причини не рекомендуємо надсилати листи на пошту учням, якщо вони мають адресу **mail.ru**

Категорично **не рекомендуємо використовувати Signal** для комунікації з учнями на ТОТ. Цей месенджер може становити загрозу, оскільки асоціюється з роботою на ЗСУ та привертає зайву увагу.

Якщо учні знаходяться на тимчасово окупованих територіях час від часу може переставати працювати той чи інший месенджер, або може бути відсутній мобільний зв'язок. **Тому рекомендуємо розробити альтернативні варіанти зв’язку з учнями заздалегідь.** Подумайте, який месенджер буде запасним та попередьте про це учнів.

БЕЗПЕКА УЧНІВ

1 **Рекомендуємо учням використовувати VPN** під час навчання. Рекомендуємо використовувати такий безкоштовний VPN, як Tunnel Bear - він інтерактивний, розроблений в ігровій формі (однак, зверніть увагу, що цей ресурс має обмеження використання в безкоштовній версії) та Proton VPN.

2 Для безпечного користування інтернетом рекомендуємо використовувати такі веббраузери, як:

Не рекомендуємо використовувати веббраузер Yandex. Це може становити небезпеку.

3 **Рекомендуємо**, щоб під час проведення навчання на групових онлайн-заняттях учні, які перебувають на ТОТ, **використовували нікнейми (псевдоніми) та не були підписані справжнім прізвищем**. Це необхідно для того, щоб навіть якщо під час заняття в приміщення до будь-кого з учнів зайде стороння людина та побачить екран дитини, це не видало інформації та імен інших учнів, які беруть участь в зустрічі. Також це убереже від витоку особистої інформації у випадку, якщо хтось із учасників онлайн-зустрічі зробить скріншот та покаже його стороннім людям.

Наприклад, можна рекомендувати учням створили **альтернативну електронну пошту без використання прізвищ** (kit_murkit@gmail.com, Lysy4k@gmai.com). Якщо для комунікації обрано Discord, WhatsApp або інші месенджери – важливо створити акаунт, який не містить справжнього прізвища.

Всі акаунти учнів мають бути закритим, а всі персональні дані прихованими або не вказаними. Це такі дані, як номер телефону, адреса, електронна адреса, геолокація тощо.

Детальніше про **приватність дітей в Інтернеті** рекомендуємо прочитати на вебпорталі «**Кібер Брама**»: https://stopfraud.gov.ua/cybersecurity-in-education/.

Якщо заняття проходять в Google Meet, учні можуть приєднуватися до занять під нікнеймом.

Як це зробити з ноутбука чи стаціонарного комп'ютера:

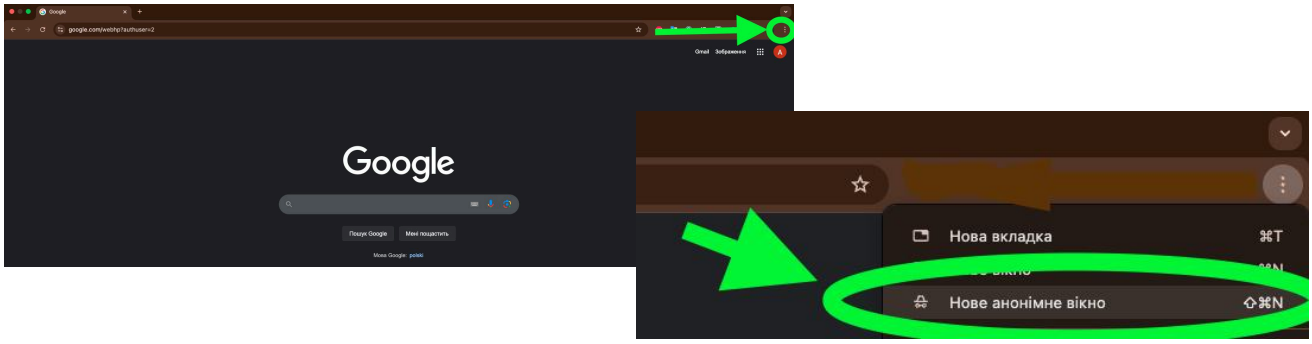
1) Відкрити безпечний браузер, створи анонімну вкладку / приватний режим / приватний перегляд в браузері.

Для відкриття анонімного вікна в браузері, можна скористатися наступними комбінаціями клавіш:

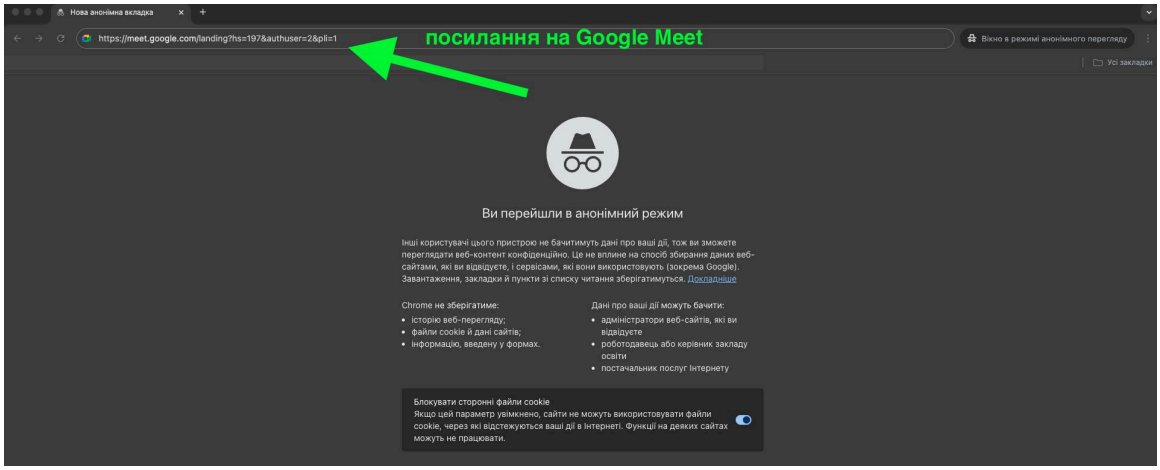
Ctrl + Shift + N (Windows, Linux, або ChromeOS)

⌘ **+ Shift + N** (macOS)

Також це можна зробити у правому верхньому куті, натиснувши на «меню» (зовнішній вигляд та назва можуть трохи відрізнятися залежно від браузера).

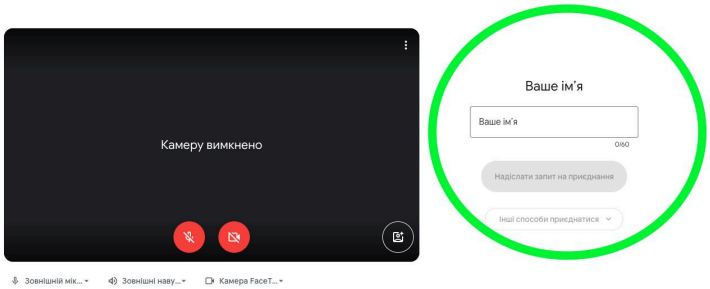


2) Скопіювати посилання на заняття в Google Meet та вставити його у командний рядок у браузері.



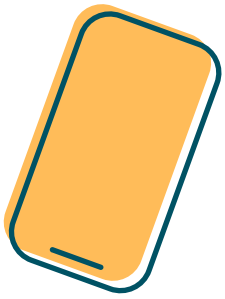
3) Для приєднання вписати своє ім’я (без прізвища) або нікнейм та надіслати запит на приєднання.

Якщо ви домовляєтесь з учнями про використання нікнеймів – домовтесь заздалегідь про те, який саме нікнейм це буде. Це необхідно для того, щоб ви впевнились, що це саме ваш учень приєднується до заняття.

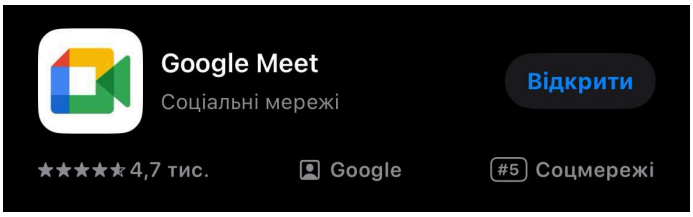


4) Після завершення заняття необхідно обов’язково закрити усі вікна.

Як це зробити з телефона чи планшета:

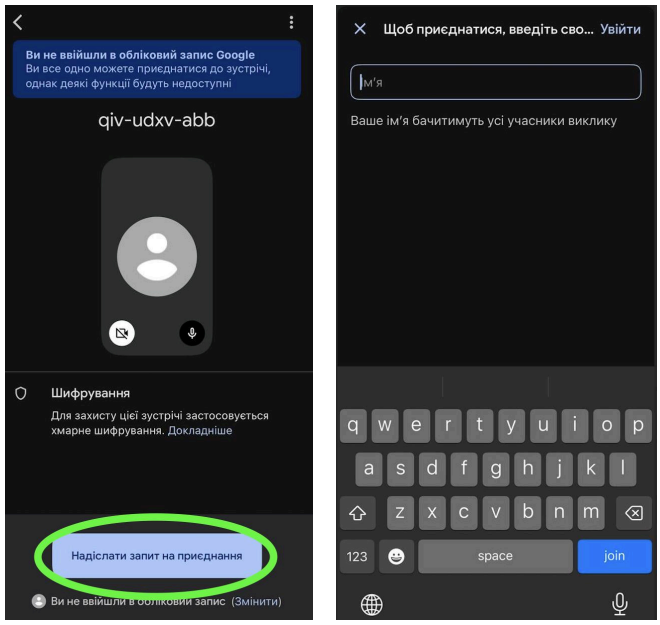


1) Встановити додаток **Google Meet**.

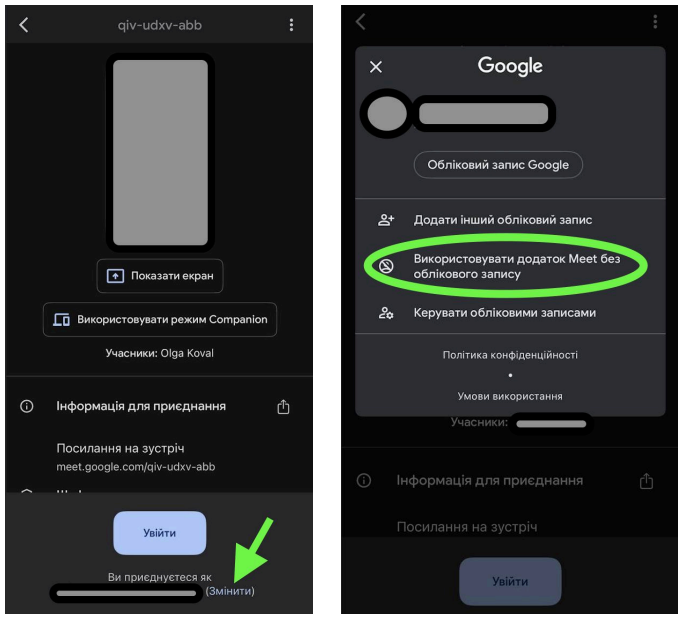


2) Натиснути на посилання на заняття в Google Meet. Після цього автоматично відкриється додаток Google Meet.

3.1) Якщо вхід в обліковий запис Google не було виконано в додатку Google Meet, то для приєднання необхідно натиснути «Надіслати запит на приєднання», після цього з’явиться можливість вписати своє ім’я (без прізвища) або нікнейм.



3.2) Якщо вхід в обліковий запис Google було виконано в додатку Google Meet, то необхідно натиснути «Змінити», далі обрати «Використовувати додаток Meet без облікового запису». Після цього вписати своє ім’я (без прізвища) або нікнейм та надіслати запит на приєднання.



Якщо заняття проходять в ZOOM, також рекомендуємо учням приєднуватися до занять під нікнеймом та без використання облікового запису.

Як це зробити з ноутбука чи стаціонарного комп'ютера:

1) Встановити додаток Zoom (це можна зробити на сторінці https://zoom.us/download) та відкрити його.

2) Не входити в обліковий запис та натиснути «Back» (назад) – *фото 1*. Якщо вхід в обліковий запис вже був виконаним, то потрібно спочатку вийти з нього – *фото 2*. Після цього натиснути «Back» (назад).

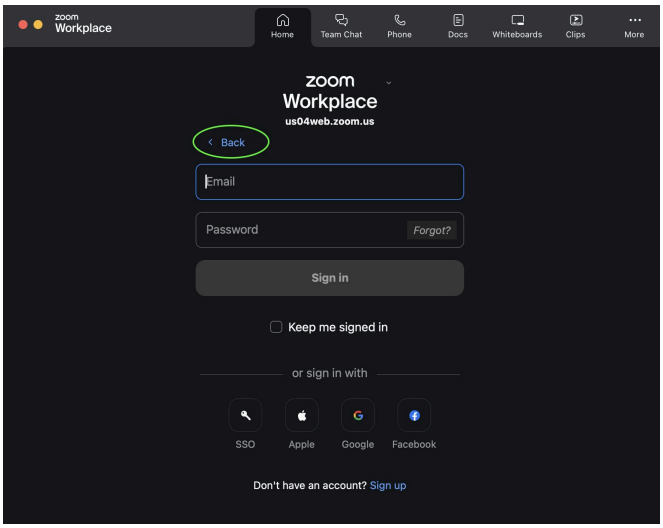


Фото 1

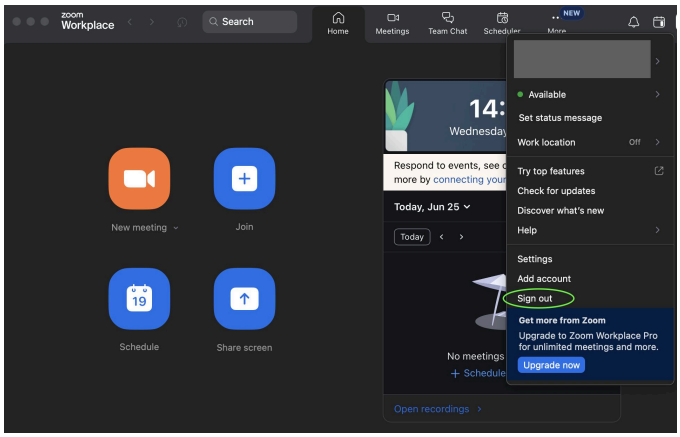
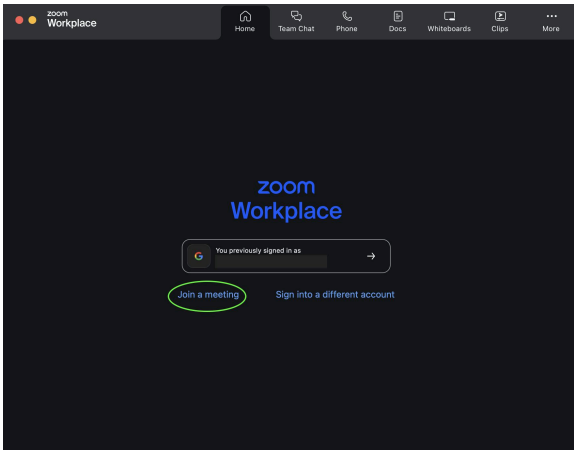
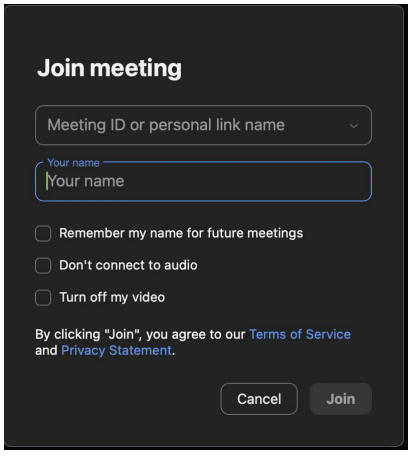
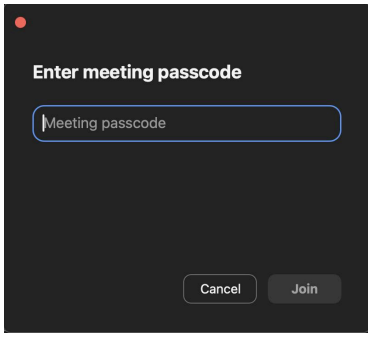


Фото 2

3) Обрати «Join a meeting» (приєднатися до зустрічі), ввести ID зустрічі (Meeting ID) або посилання на зустріч, нікнейм (Your name), натиснути «Join» (приєднатися), ввести пароль зустрічі (Meeting passcode). Після цього можна буде приєднатися до заняття, натиснувши кнопку «Join» (приєднатися).

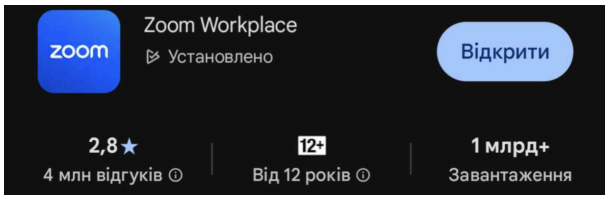






Як це зробити з телеофна чи планшетаа:

1) Встановити додаток Zoom та відкрити його.



2) Не входити в обліковий запис та натиснути «Join» (приєднатися) – *фото 1*. Якщо вхід в обліковий запис вже був виконаним, то потрібно спочатку вийти з нього (Sign out) – *фото 2*. Після цього натиснути «Join» (приєднатися).

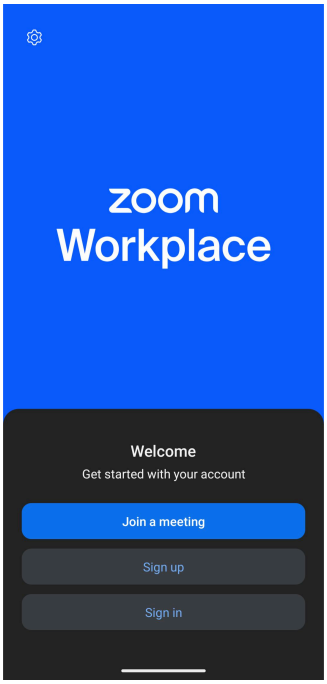


Фото 1

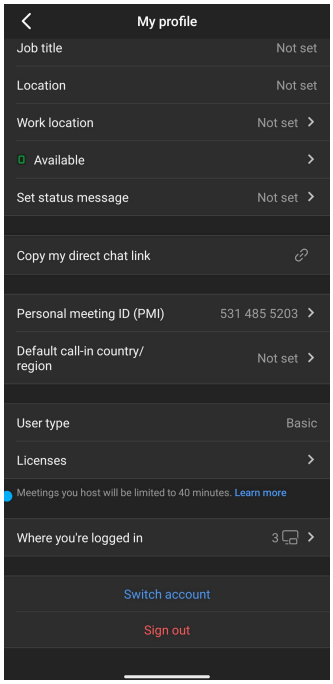
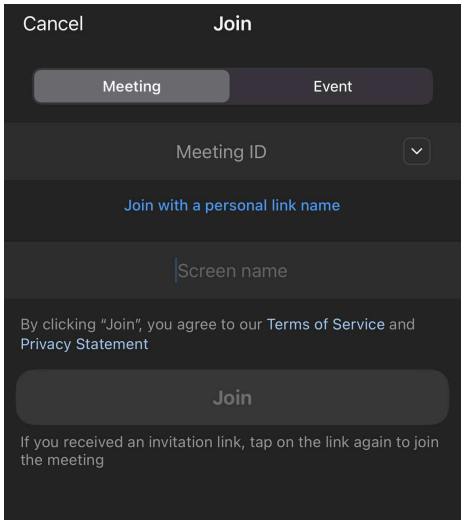
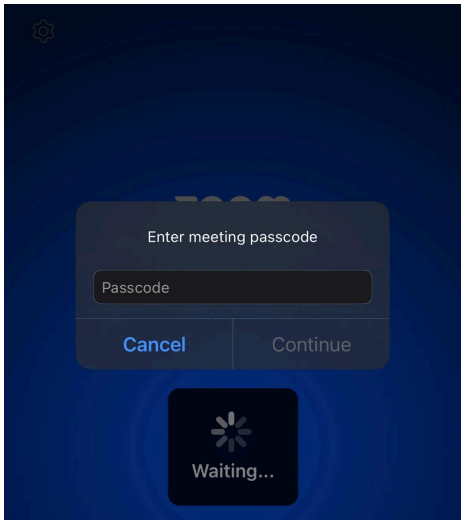


Фото 2

3) Ввести ID зустрічі (Meeting ID) або посилання на зустріч, ввести пароль зустрічі (Meeting passcode), нікнейм (Screen name), натиснути «Join» (приєднатися), ввести пароль зустрічі (Meeting passcode). Після цього потрібно натиснути «Continue» (продовжити). Далі необхідно вибрати налаштування відео та звуку і натиснути «Join» (приєднатися).





3 Необхідно **створити безпечні паролі на платформах, які використовують** (Gmail, Discord, WhatsApp, Instagram, Facebook тощо). Учні мають використовувати складні паролі для доступу до облікових записів, платформ чи месенджерів. Пароль має складатись з понад 16 символів та містити малі та великі літери, цифри та символи. Перевірити, наскільки міцний пароль, можна за посиланням – https://zillya.ua/check-password.

Лайфхак: паролем може стати текст улюбленої пісні та улюблена цифра наприкінці (для кожного ресурсу – окремий пароль).

4 **Учням важливо використовувати двоетапну перевірку на акаунтах.** Детальніше про те, як це зробити – на стор. 3 даних Рекомендацій.

5 Якщо хтось намагатиметься зламати акаунт учня у соціальній мережі, месенджері чи цифровій платформі, одразу необхідно повідомити про це вчителю та батькам.

6 Під час групових занять для кращого зв'язку та безпеки учням, які перебувають на ТОТ, категорично не рекомендується використовувати вебкамеру, а також приєднуватися під справжнім прізвищем. Найкраще використати для приєднання лише ім'я або нікнейм. Це допоможе уберегти учнів у випадках, якщо стороння людина побачить екран учнів під час заняття, або буде зроблений скріншот.

7 Рекомендуємо учням для безпечного використання інтернетом:

- дослідити **вебпортал «Кібер Брама»** та ознайомитись з корисними рекомендаціями для безпечного користування Інтернетом: https://stopfraud.gov.ua/
- пройти **відео-симулятор** про онлайн-безпеку: https://osvita.diia.gov.ua/simulators/e-safety-teens-simulator
- **подивитись онлайн-курс** «Цифрові права та безпека дитини»**:** https://minzmin.org.ua/onlinecourse/

8 В спілкуванні під час занять **необхідно уникати питань, які можуть видати особисту інформацію учнів** (наприклад, прізвище, місто проживання, інформація про батьків / опікунів, інформація про навчання у місцевій школі, дата народження тощо).

9 В спілкуванні **необхідно уникати чутливих тем**, пов'язаних із російсько-українською війною, життям на тимчасово окупованих територіях, втратами та травматичними ситуаціями тощо.

10 Викладачам **категорично не рекомендується розповсюджувати будь-яку інформацію про учнів** в особистому чи публічному спілкуванні, навіть якщо вона здається незначущою та, на вашу думку, не може загрожувати безпеці учнів.

ЩО РОБИТИ, ЯКЩО ВИ ПОМІТИЛИ ОЗНАКИ ЗЛАМУ ТА КІБЕРАТАКИ НА ВАШІ АКАУНТИ?

1. Зафіксуйте наявне порушення (зробіть фото, відео, скріншот).
2. Повідомте кіберполіцію. Це можна зробити за посиланням: https://ticket.cyberpolice.gov.ua/send.
1. Зверніться за безкоштовною консультацією на платформу Надійно (https://nadiyno.org/).

ДЯКУЄМО, ЩО ОЗНАЙОМИЛИСЬ З ЦИМИ РЕКОМЕНДАЦІЯМИ!

Ми закликаємо всіх дотримуватися цих правил і вживати всі необхідні заходи для забезпечення належного рівня кібербезпеки під час проведення навчання онлайн.