Як захистити себе в застосунку ZOOM

Робота у мережі Інтернет пов’язана з певними ризиками !!!

- **Кібербулінг** – залякування, приниження, цькування, переслідування, компрометація людей з використанням цифрових технологій.
- **Кібергрумінг** – входження в довіру людини для використання її в сексуальних цілях.
- **Надмірне захоплення іграми в мережі** – може призвести до втрати реальності, комп’ютерної залежності.

ЗУМБОМБІНҐ

Ще у період пандемії й онлайн-навчання виникло таке явище, як «зумбомбінґ» (zoombombing). Це випадки, коли стороння людина приєднується до конференції й показує неналежні матеріали за допомогою камери або функції спільного перегляду.

Приєднатися до зустрічі в Зумі легко, однак це може бути й недоліком. Ідентифікатор зустрічі знайти не дуже складно, а тому зловмисники можуть її зіпсувати. І в часи онлайн-навчання учні нерідко використовують зумбомбінґ, щоб зірвати урок.

Зум посилив свою безпеку і включив опцію налаштувань за замовчуванням. Завдяки цьому кількість випадків зумбомбінґу зменшилась, але ця проблема все ще існує.

Правило 1

Встановіть пароль для конференцій, краще — на кожну подію!

Використовуйте можливість входу в конференцію за паролем, який надсилається учасникам заздалегідь. Можна ввести паролі для групи, облікового запису для всіх сеансів, користувача або окремої події. Щоб на зустріч не потрапили сторонні люди або пароль не вкрали, краще міняти це секретне слово для кожної онлайн-наради. Для цього на вкладці «Налаштування» увімкніть «Вимагати пароль при створенні нових зібрань». Сам пароль оберіть випадково згенерований. Не довіряйте своїй фантазії, адже є імовірність, що його підберуть жартівники або зловмисники.

Правило 2

Не пускайте сторонніх осіб!

На урок, конференцію чи нараду слід надсилати запрошення лише учням, запланованим учасникам, зареєстрованим користувачам. Не можна відкрито давати посилання на онлайн-уроки чи конференції. Також треба попередити учнів, що вони не можуть передавати посилання третім особам, розповісти, до чого це може призвести.

Правило 3

Першим заходить ведучий!

Не дозволяйте решті користувачів приєднатися раніше. Це можна передбачити у відповідному параметрі для групи «Налаштування облікового запису». Вимкніть функцію «Долучитися раніше за організатора». Саме ведучий відповідає за те, щоб на конференцію не потрапили сторонні особи.

Правило 4

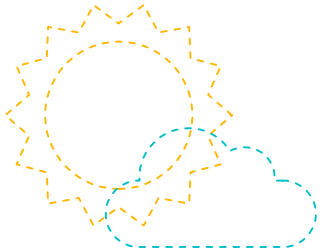
Використовуйте «кімнату очікування»

Ця функція дає змогу переглядати учасників, перш ніж додати їх до уроку, наради. Це збільшує контроль за безпекою сеансів, адже під час підтвердження легко виявити зайвих учасників. У всьому світі нині докучають так звані Zoom-бомбардування: хакери проникають у відеозустрічі та лякають або лають учасників. Звісно, навряд чи їх зацікавить заняття школярів, скоріше це стосується конференцій корпорацій та політиків, але краще перестаратися, ніж заспокоювати дітей.

Правило 5

«Зачиніть двері», коли всі на місці!

Після початку сеансу перейдіть на вкладку «Управління учасниками», натисніть «Ще» і виберіть «Заблокувати» збори, тільки-но з’являться всі очікувані учасники. Це ще один рівень безпеки, який не дасть приєднатися стороннім особам.



Правило 6

Вимкніть загальний доступ до екранів учасників!

Один з видів Zoom-хуліганств — продемонструвати якісь непристойні або такі, що лякають, знімки всім учасникам. Щоб цього не сталося, варто відключити можливість для учасників зустрічі ділитися змістом своїх екранів. Ця опція доступна на вкладці «Безпека» під час сеансів.

Правило 7

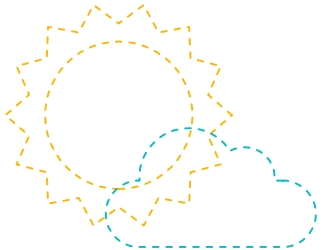
Ви маєте змогу видаляти порушників!

Звісно, це не для того, щоб «виганяти з класу» учнів. Ідеться про екстремальні випадки. Наприклад, за кордоном траплялося, що онлайн-заняття зривали брати чи сестри учнів або асоціальні батьки. Якщо хтось заважає та хуліганить, на вкладці «Учасники» наведіть курсор на ім’я, натисніть «Ще» і видаліть його. Ви також можете переконатися, що він не зможе повернутися на цю подію, відключивши параметр «Дозволити повернення віддаленим учасникам» на вкладці «Налаштування: Зустрічі — Основні».

Правило 8

Будьте обережними з обміном файлами!

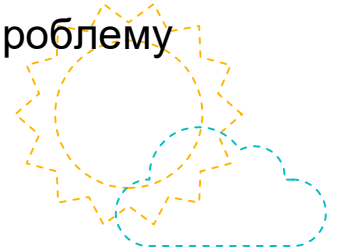
Дозволити передавати файли можна, лише коли впевнені в їхньому змісті. Це убезпечить від надсилання вірусних програм і зайвих файлів. Краще передавати їх через сервіс Google Drive або месенджери.



Правило 9

Перевіряйте оновлення!

Із кожним оновленням програми підвищується і рівень її безпеки. Тож використовуйте останню версію. Щоб перевірити, відкрийте додаток, натисніть на свій профіль у правому верхньому кутку і виберіть «Перевірити наявність оновлень». Якщо виникли проблеми, можна також перевстановити програму і повідомити про проблему службу підтримки Zoom.



Що учні можуть робити в Зумі

Крім голосового спілкування, Зум дає дітям безліч інструментів для взаємодії одне з одним і з учителем, для спільної роботи і роботи в малих групах. Якщо певні опції не потрібні на уроці, вчитель може їх вимкнути.

Ось лише декілька функцій Зум, які може використовувати вчитель:

- ділитися екраном – це дає можливість усьому класу переглядати екран комп'ютера одної людини і навіть коментувати документи, (викладачі можуть налаштувати обмеження, щоб лише вони могли ділитися екраном під час зустрічі);
- віртуальна дошка – це інструмент для мозкового штурму, де діти можуть залишати на дошці ідеї для групового проєкту, додавати зображення тощо;
- кімнати – учитель може об'єднати клас у менші групи для обговорення певного питання або виконання завдання, а потім зібрати весь клас разом;
- значки «піднести руку», «не погодитися», «аплодувати», «прискорити», «уповільнити» – учні використовують їх, щоб поставити запитання, відреагувати на репліку або попросити вчителя говорити швидше чи повільніше;
- груповий чат – учні можуть надсилати повідомлення всьому класу;
- приватний чат – також можна надсилати особисті повідомлення іншим учням (учитель не може переглядати повідомлення в приватних чатах).

Ось кілька порад щодо безпечної поведінки в Зумі:

- генерувати випадковий ідентифікатор зустрічі – хоча ви можете використовувати один ідентифікатор для всіх учнів одразу, Зум рекомендує вчителям використовувати випадкові ідентифікатори (таке налаштування вчитель може використати, коли створює запрошення – це менш зручно, але більш безпечно);
- вимкнути звук – учасники можуть (і повинні) вимикати звук, коли вони не говорять, але вчитель також може вимкнути звук будь-якому учаснику або всім одночасно.
- використовувати чат – учитель може контролювати, чи можуть учні писати в спільний і приватні чати;
- вимкнути відео – будь-який учасник може вимкнути відео до початку зустрічі і використовувати лише звук, а вчитель також може вимикати відео будь-якого учасника;
- налагоджувати невербальний зворотний зв’язок – використовуючи значки, учні можуть піднести руку, показати своє схвалення чи несхвалення і навіть інформувати вчителя, що їм потрібна перерва;
- заблокувати зустріч – як раніше в школі вчитель міг замкнути за собою двері після дзвінка, так і в Зумі викладач може так само заблокувати зустріч, щоб ніхто не зміг приєднатися без його дозволу;
- використовувати зали очікування – учасники, які хочуть увійти, перебувають у віртуальній кімнаті, і вчитель запускає їх одного за одним, щоб переконатися, що жоден зловмисник не отримав доступу;
- вимкнути передавання файлів – діти можуть надсилати один одному в чаті картинки і навіть відповіді на запитання, якщо вчитель не вимкнув цю функцію.

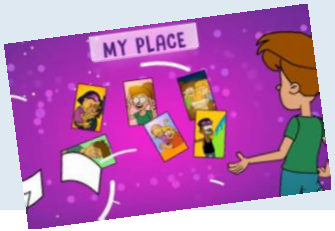
Правила безпеки у Інтернеті

Захистіть себе у соцмережах

- **Подумайте двічі, перш ніж поширити будь-яку інформацію.**

Пам'ятайте

Розмістивши інформацію в Інтернеті, ви втрачаєте контроль над нею і в більшості випадків вже ніколи не зможете видалити всі її копії.



Використані інтернет-джерела:

- https://osvitoria.media/experience/yak-zrobyty-onlajn-zanyattya-bezpechnymy-8-porad-dlya-pidvyshhennya-bezpeky-v-zoom/
- https://bzl.cprpp.org.ua/news/1643114720/