ЯК ПОДБАТИ ПРО ПРИВАТНІСТЬ ДИТИНИ В ІНТЕРНЕТІ?

ІНФОРМАЦІЯ ДЛЯ БАТЬКІВ

ПРЯМУЄМО РАЗОМ
ПРОЕКТ ФІНАНСУЄТЬСЯ ЄВРОПЕЙСЬКИМ СОЮЗОМ

БЛАГОПОЛУЧЧЯ ДІТЕЙ УКРАЇНСЬКИЙ ФОНД

ВОЛОНТЕР Всеукраїнський громадський центр

LHSI Соціальні ініціативи з охорони праці та здоров'я

Турбуватися про безпеку своєї дитини в інтернеті – це нормально. Інтернет пропонує дітям дуже багато можливостей вибору, але водночас онлайн-світ зі своєю вседоступністю та анонімністю містить низку небезпек та загроз. Дорослі можуть допомогти дитині опанувати необхідні навички та знання, які сприятимуть безпечному користуванню цифровим світом та ухваленню зважених рішень як у мережі, так і у реальному житті.

Що таке **КОНФІДЕНЦІЙНІСТЬ В ІНТЕРНЕТІ** та чому важливо дбати про персональні дані?

Конфіденційність в інтернеті – це можливість контролювати, скільки особистої інформації треті сторони (онлайн-платформи, веб-сайти, програми) можуть збирати, обробляти, використовувати під час того, як ми користуємося мережею.

Особиста інформація (або, як її ще називають, приватна інформація) – це інформація про конкретну людину:

- ім'я та прізвище;
- вік (скільки років);
- адреса проживання, навчального закладу;
- ПІБ близьких;
- місце роботи, номери телефонів, електронна адреса;
- номер банківської картки або банківського рахунку тощо.

Часто ми надаємо особисту інформацію в мережі, щоб зареєструвати обліковий запис на веб-ресурсах. Компанії запитують її, щоб підібрати контент, який відповідає інтересам і віку користувача, налаштувати рекламу і показувати те, що може його/її зацікавити. Водночас …

Важливо розуміти: будь-яку інформацію, яку ми розміщуємо в мережі, можуть використати з недоброчесними намірами на шкоду нам.

Все, що потрапляє в мережу, вже ніколи звідти не зникає. Навіть якщо ви видалили повідомлення, надіслане в приватній переписці, з нього могли зробити знімок (скриншот) та зберегти дані на інший носій, звідки воно може знову потрапити в мережу.

Перед тим як поділитися чимось у мережі, важливо оцінити, для чого ми хочемо розмістити таку інформацію, хто зможе мати до неї доступ. Поділитися особистою інформацією в інтернеті – це як розповісти її незнайомій людині особисто.

Що важливо враховувати, щоб дитина була в безпеці онлайн?

Безпека дітей в інтернеті включає три складові:

технічна безпека: застосування різних фільтрів, налаштування конфіденційності на пристроях і програмах, онлайн-активність;

довіра та інформування: відверті обговорення з дитиною поведінки та правил безпеки в мережі;

власний приклад.

Розглянемо кожну з цих складових.

ТЕХНІЧНА БЕЗПЕКА

Користуйтеся безпечною мережею (це домашня мережа або мобільний зв'язок) **та навчіть цьому дитину.** Не варто передавати персональні дані, фото, повідомлення тощо, використовуючи публічні мережі, не захищені паролем (wi-fi в кафе чи інших громадських місцях).

Регулярно оновлюйте програмне забезпечення ваших ґаджетів. Встановлюйте лише необхідні програми та контролюйте їх видалення. Звертайте увагу на надання дозволів, які просить програма (чи справді програмі для обробки фотографій потрібен доступ до контактів?). Переконайтеся, що на пристрої вашої дитини налаштування конфіденційності ввімкнено та налаштовано так, щоб мінімізувати збір даних.

Подбайте про надійний пароль. Різні акаунти – різні паролі. Що довший пароль – то він безпечніший. Наприклад, можна скористатися сервісом з генерації паролів від Кіберполіції (https://cyberpolice.gov.ua/generate-password/).

Налаштуйте додатковий рівень захисту (двоетапну перевірку). До прикладу, коли заходите в свій акаунт, налаштуйте функцію отримання підтвердження за допомогою смс чи дзвінка. Якщо дитина має власний акаунт, разом перегляньте, чи увімкнена двоетапна перевірка.

Налаштуйте безпечний пошук та скористайтеся функцією батьківського контролю, особливо для молодших дітей. До прикладу, це Google Safe Search, обмежений режим на YouTube і додаток YouTube Kids. Коли ваша дитина стає підлітком, швидше за все, технічні обмеження та заборони можуть не бути ефективними, тож переконайтеся, що він або вона може шукати інформацію на безпечних сайтах та знає, як поскаржитися на небезпечний контент.

Проведіть час зі своєю дитиною, щоб **знайти програми, ігри та інші онлайн-розваги, які відповідають її віку.** Наприклад, кожна соціальна мережа визначає мінімальний вік, необхідний для реєстрації. Більшість з них вимагають, щоб користувачі мали вік від 13 років для створення облікового запису самостійно. Поясніть, чому встановлена вікова межа та які ризики і небезпеки можуть очікувати на користувачів, якщо вказати неправдиві дані. Якщо дитина має власний акаунт, переконайтеся, що її профіль приватний і дописи бачать лише знайомі люди, яким дитина довіряє.

Дізнайтеся, як **скаржитися на неприйнятний контент** або на матеріали, які не відповідають віку дитини у соціальних мережах чи на онлайн-платформах.

ДОВІРА ТА ІНФОРМУВАННЯ

Відверто поговоріть зі своєю дитиною про її дії в мережі.

Щойно ваша дитина почне активно користуватися мережею, поговоріть з нею про те, що вона читає, дивиться, з ким спілкується в інтернеті, які сайти відвідує або якими застосунками користується. Дізнайтеся про хобі або інші інтереси дитини, пов'язані з мережею. Поясніть, що все, що потрапляє в інтернет – зображення, відео, коментарі, те, чим вона ділиться з іншими, а також те, що інші публікують і чим діляться з нею, – залишає за собою цифровий слід. Поясніть, що варто бути уважним/уважною до того, як ми висловлюємося в мережі – не варто поширювати чутки, ображати когось, ділитися приватними історіями чи фотографіями. Запевніть, що до вас можна звернутися, якщо трапиться щось непередбачуване, те, що засмутило або налякало.

Дізнайтеся, хто друзі ваших дітей в інтернеті.

Ми, дорослі, знаємо, що деякі люди в мережі можуть бути не тими, за кого себе видають. Розкажіть або нагадайте про це дитині та наголосіть на тому, що варто додавати у друзі лише тих, кого знаємо в реальному житті.

Навчіть дитину дбати про свою безпеку в мережі.

Розкажіть дитині, що перед тим як щось розмістити, важливо запитати себе: чи хочу я, щоб мою інформацію (ім'я, номер телефону, домашня адреса, електронна адреса, адреса навчального закладу) або фотографії отримали незнайомці? Якщо відповідь «ні» – краще не публікувати це. Це правило стосується і батьків/осіб, які їх замінюють, коли ви публікуєте власну інформацію або інформацію/зображення дитини.

Ви також можете навчити дитину користуватися правилом **«Запитай – Перевір – Подумай»**:

У кого ти можеш запитати, якщо в чомусь не впевнений(-а)?

Що маєш перевірити? (від кого надійшов лист/повідомлення – це знайома людина чи незнайомець?)

Про що варто подумати? (наприклад, що може статися, якщо перейду за лінком, який надіслала мені незнайома людина?)

Якщо ваша дитина ділиться фотографіями або публікаціями в інтернеті, попросіть її дозволити вам побачити, чим вона ділиться.

Розкажіть чому важливо зберігати конфіденційність свого місцезнаходження.

Більшість програм, мереж і пристроїв мають функції геотегування, які оприлюднюють місцеперебування та можуть привести когось безпосередньо до вас. Ці функції слід вимкнути.

Слідкуйте за часом онлайн.

Важливо стежити за часом, який дитина проводить в інтернеті. Обговоріть, скільки часу дитина може користуватися ґаджетами, і встановіть таймер на вимкнення. Якщо це можливо, відключіть екрани принаймні за годину перед тим, як лягати спати. Визначте конкретний час, коли дитина повинна припинити використання електронних пристроїв перед сном. Цей час може відрізнятися залежно від віку дитини, але зазвичай має бути принаймні за годину до сну.

Спробуйте зробити кілька днів «без екрану».

Пам'ятайте, що для здорового балансу в усіх аспектах життя потрібно поєднувати діяльність в інтернеті з активним способом життя та відпочинком поза мережею.

Ознайомтеся з соціальними мережами, щоб надавати найкращі поради з безпеки для дітей.

Зареєструйтеся в соціальних мережах і програмах, якими користується дитина, і дізнайтеся, як використовувати налаштування конфіденційності.

Якщо ваша дитина користується соціальними мережами, переконайтеся, що вона знає, як: повідомити про неприйнятний та/або образливий контент; заблокувати когось та зберігати інформацію конфіденційною.

Наголосіть, що не варто відповідати на електронні листи з погрозами чи повідомлення від незнайомих людей, а також **ніколи не можна погоджуватися зустрітися з незнайомцем**.

ВЛАСНИЙ ПРИКЛАД

Діти навчаються, копіюючи поведінку інших, тому будьте прикладом і поводьтеся в інтернеті так, як ви хотіли б, щоб поводилася ваша дитина.

Якщо ви самі порушуєте правила безпеки в мережі, дитина навряд чи прислухатиметься до ваших порад щодо поведінки в інтернеті.

Розкажіть дитині про те, **де можна знайти підтримку**, поділитися своїми переживаннями, а також отримати консультацію з питань, які хвилюють.

- Національна гаряча лінія для дітей та молоді:

childhotline_ua

t.me/CHL116111

- урядова консультаційна лінія з питань безпеки дітей в інтернеті:

  1545 (далі обрати «3»)

- бот kiberpes або чат-бот проєкту #stop_sextинг:

  t.me/kiberpes_bot

  stop-sexting.in.ua/chatbot

- чат-не-бот Unsee, в якому можна анонімно поскаржитися на небажаний контент у мережі:

  t.me/Unsee_nebot

- телеграм-канал з питань психологічного здоров'я для **підлітків**, а також онлайн та очні групи психологічної підтримки для підлітків та батьків «ПОРУЧ»:

  t.me/poruch_me

  https://poruch.me

Якщо трапилася небезпечна ситуація в інтернеті та є хвилювання за безпеку:

- єдина лінія Міністерства внутрішніх справ України – 112 (далі обрати «2»);
- поліція (телефон: 102 або звернення до відділку);
- кіберполіція: 0-800-505-170 або cyberpolice.gov.ua.

Дізнатися більше про безпеку дітей в інтернеті можна також на ресурсах:

- Практичні поради з цифрової безпеки. Сервіс з порадами з цифрової безпеки для кожного ґаджета та операційної системи:

  https://yak.dslua.org

- Цифрові права та безпека дітей. Приватність в інтернеті:

  https://minzmin.org.ua/projects

- Сервіс для звернень з питань онлайн-безпеки в режимі реального часу:

  https://nadiyno.org

- Дія.Освіта:

  https://osvita.diia.gov.ua/catalog/topic/cyber-security

Публікація підготовлена за фінансової підтримки Європейського Союзу. Її зміст є виключною відповідальністю Громадської організації «Всеукраїнський громадський центр «Волонтер» і не обов'язково відображає позицію Європейського Союзу.