**Дитяча безпека в інтернеті. Що слід знати про загрози віртуального життя.**

В середньому українські діти починають користуватися інтернетом з 8 років. Згодом мережа стає частиною середовища їх існування. Як забезпечити безпеку в інтернеті для дітей? Що чекає в мережі і як боротися з загрозами віртуального світу?

Інтернет пропонує дітям масу корисних можливостей і безліч загроз. Оберігаючи своє чадо, батьки прагнуть виключити всесвітню павутину з життя малюка. Це нерозумно, адже так дитина обмежується в сучасних засобах навчання, спілкуванні та розвитку. Які загрози таяться в онлайн-світі і як забезпечити безпеку в інтернеті для дітей? Давайте розбиратися разом.

**Загрози для дітей в інтернеті**

Безпеці дітей в інтернеті загрожують ризики трьох типів:

* контент;
* небажане спілкування;
* вірусні програми.

**Контент**

Сайти «для дорослих». За різними дослідженнями, до 70% світового трафіку займає порнографічний контент. Середній вік дитини, яка вперше стикається з порнографією – 11 років!

Пропаганда жорстокості, сцени агресії та насильства. Сюди ж відноситься пропаганда вступу в секти, екстремізм і т.д.

Інструкції суїцидів. Діти в інтернеті можуть знайти по-справжньому жахливі речі. Наприклад, деякий час в мережі поширювалася «методичка» про те, як стати феєю з мультика «Winx». Фактично, текст пропонував дитині вбити себе і підірвати будинок.

**Небажане спілкування**

Кібербулінг, або віртуальний терор. Простіше кажучи, це цькування з боку однолітків і знайомих через зовнішність, віросповідання, стать і т.д. На перший погляд, це здається не таким і страшним. Але не забуваємо, що онлайн-світ жорстокий. Те, що не скажуть в очі, в соціальних мережах або чаті напишуть запросто. А дитині з цим жити.

Мережева педофілія. Часто педофіли ховаються за фальшивим аккаунтом, з ніби нормальною сторінкою в соціальних мережах. Вони втираються в довіру, а потім можуть попросити непристойні фото, домовиться про зустрічі і т.д.

Фішинг, тобто спроба шахраїв роздобути особисту інформацію – паролі, дані карток і т.д. Вони ховаються під маскою надійних організацій, і потрапити «на вудку» можуть як діти, так і дорослі.

Кіберсуїцид, або узгоджені самогубства. Чи варто згадувати про «групи смерті» в мережі «ВКонтакті». До слова, саме ця мережа визнана найбільш небезпечною для дітей.

**Вірусні програми**

Віруси (шкідливі програми, що викликають збій в роботі комп’ютера). Шкідливе програмне забезпечення може ховатися в безкоштовних, доступних для скачування програмах, у вкладеннях до підозрілих електронних листів, на шкідливих сайтах, куди користувачів заманюють за допомогою спам-оголошень і т.д.

Спам. Наприклад, масова розсилка листів, які містять віруси. Ще один варіант – розсилка листів зі зворушливою історією про потерпілого малюка і проханням переслати лист. Нібито, за кожну пересилку інтернет-провайдер перерахує потерпілому певну суму грошей. Насправді, це трюк для збору емейл-адрес.

Фішингові атаки. Шахраї масово розсилають листи з гіперпосиланням на фальшивий сайт (зазвичай банку або іншої авторитетної організації), де користувачеві пропонують ввести конфіденційні дані. Таким способом виманюють паролі, PIN-коди і т.д.

**Безпека в інтернеті для дітей: правила для батьків**

Розкажіть дитині, які бувають небезпеки в мережі. Якщо самі не знаєте – подивіться разом навчальне відео або прочитайте статтю.

Помістіть комп’ютер в загальній кімнаті, якщо це можливо. Якщо малюк користується планшетом, то хоча б цікавтеся, чим він займається в мережі.

Встановіть чіткі правила поведінки в інтернеті:

* в яких соціальних мережах і чатах можна реєструватися, а в яких ні;
* який контент можна завантажувати, а який не можна (музика, ігри і т.д.);
* забороніть робити покупки в інтернет-магазинах без Вашої участі;
* забороніть використовувати сервіси з GPS, які фіксують розташування;
* домовтеся про те, скільки часу може дитина проводити в мережі.
* Забороніть передавати особисті дані стороннім в соціальних мережах під будь-яким приводом. Наведіть приклади фішингу.
* Будьте зразком. Не заходьте у присутності дитини на небезпечні для неї сайти.
* Встановіть надійну антивірусну програму і батьківський контроль.
* Будьте своїй дитині другом. Якщо у вас довірчі відносини, Ви з більшою ймовірністю дізнаєтеся, що хвилює малюка, з ким він спілкується в мережах і чим цікавиться. Це правило стосується не тільки життя «онлайн», але і реального.