***Діти в інтернеті:***

***загрози, які чекають підлітків,***

***правила безпеки в мережі,***

***способи контролю для батьків***

Для батьків

Інтернет ‒ благо чи зло для дитини? Мережа ‒ це чимало плюсів і безліч небезпек. На жаль, самостійно діти не вміють дозовано і правильно використовувати інтернет-ресурси для розвитку і навчання, а більше споживають розважальний контент, грають в ігри, спілкуються в соціальних мережах.

Що ж робити батькам? Розумно обмежувати перебування в мережі, цікавитися життям дитини, перевіряти, які ресурси відвідує підліток. Звичайно ж, мова не йде про постійне шпигунство і тотальні заборони, адже це тільки погіршить відносини. Як мінімум, потрібно просто знати, які загрози чекають на дитину в інтернеті, і якими правилами безпеки варто навчити своє підлітка. Це допоможе вам уникнути несподіваних проблем, котрі можуть звалитися, як сніг на голову.

*ЯКІ ЗАГРОЗИ МОЖУТЬ СПІТКАТИ ДИТИНУ В ІНТЕРНЕТІ?*

Зараз інтернет ‒ це свого роду допомога для батьків. Усе починається ще з дитинства: в дорозі можна зайняти малюка мультиками, дітям постарше можна запропонувати розвиваючі ігри на планшеті, більш старшим ‒ головне забезпечити постійний доступ до соціальних мереж для спілкування з однолітками.

Батьки поступово перестають помічати, коли вони повністю припиняють контролювати перебування дитини в мережі. І ось тут починаються проблеми. Уже в більш усвідомленому віці на підлітка в інтернеті чекає ряд загроз:

***Загроза залежності.***

Проста гра може тільки спочатку не нести ніякої небезпеки, але з часом у дитини може сформуватися ігрова залежність. Це поведе за собою погіршення успішності, відсутність контакту з однокласниками, небажання соціалізуватися. Дитина подумки буде жити в іншому, віртуальному, світі, і все життя буде «застрягати» у вигаданій кимось грі.

Загроза познайомитися в соціальних мережах з шахраями, булерами, соціально небезпечними елементами (маніяками і т.п.).

Постійне спілкування в соціальних мережах рано чи пізно призводить до того, що дитина починає листуватися з незнайомими людьми, розширюючи своє вузьке коло однокласників новими знайомствами. У довіру може втертися як дитина одного віку, так і дорослий, який буде використовувати в листуванні всі відомі маніпулятивні методи, для того щоб:

* витребувати у підлітка гроші або будь-які інші матеріальні цінності;
* викликати на особисту зустріч;
* викрасти підлітка і вимагати у батьків викуп і т.п.

Як відомо, неприємні історії зустрічаються досить часто. І саме від них дитину потрібно захищати.

Загроза знайти в інтернеті матеріали, які негативно впливають на психіку підлітка. Йде мова про усім відомий «Синій кит» і йому подібні «організації». В інтернеті дитина може вступити в товариство, яке, за своєю суттю, буде мати сектантську / расистську / суїцидальну спрямованість. Ну а що буде далі ‒ це вже питання часу. Підлітки піддаються впливу, тому трапитися може будь-що.

***Загроза порушення конфіденційності.***

Випадково вказаний номер телефону, адреса, зайва відвертість на своїй сторінці в соціальній мережі ‒ все це дає шахраям і булерам достатньо інформації, якою можна скористатися в своїх цілях. Кожне слово може бути використане проти вашої дитини, кожне невдале фото може бути насмішкою, а конфіденційною інформацією можуть скористатися з метою шантажу.

Як бачите, може трапитися чимало неприємностей, якщо підліток буде проводити занадто багато часу в інтернеті. Особливо, якщо буде використовувати ресурси не за прямим призначенням.

***ЯКИМ БАЗОВИМ ПРАВИЛАМ БЕЗПЕКИ В МЕРЕЖ***

***І СЛІД НАВЧИТИ ПІДЛІТКА?***

Незважаючи на те, що вся реальність зараз постійно взаємодіє з віртуальністю, немає ніякого шкільного предмета, який би вчив школярів правилам безпеки в мережі. Так і виходить, що якщо батьки не розкажуть, то не розкаже ніхто. Дорослі повинні самі ознайомитися з правилами безпеки і, звичайно ж, навчити ним дітей:

* ніколи не розміщувати на сторінках в соціальних мережах свій номер телефону та адресу. Дитині 12-14 років і в голову не прийде, що цією інформацією можуть скористатися шахраї, але дорослі повинні обов'язково про це попередити;
* краще використовувати нік, а не своє справжнє ім'я. Припустимо, якщо за дитиною полюють шкільні булери, то просто по імені і прізвищу знайти школяра не вийде. А ось нік буде відомий тільки близьким друзям, родичам і знайомим. І вбереже від спроби «вистежити» невдалу фотографію;
* не варто загострювати увагу на негативі, який може бути адресований дитині в коментарях або в особистому листуванні з незнайомими людьми. Скажіть підлітку, що він має право блокувати всіх людей, які викликають у нього хоч найменшу негативну емоцію;
* попередьте дитину, що вона не повинна виносити на обговорення в інтернеті теми особистого характеру (сімейні проблеми, любовні переживання, майбутню подорож, велику покупку). Цієї інформації тільки й чекають шахраї і різнопланові спільноти (секти, молодіжні організації неформального характеру);
* розкажіть, що на зустріч з незнайомцем відправлятися не можна. Підліток може думати, що спілкується з віртуальним другом свого віку, але за привітною фотографією може ховатися доросла людина, яка ставить перед собою небезпечні цілі;
* попередьте, що інформацію про кредитні картки батьків ні в якому разі нікому передавати не можна. Та й самі намагайтеся зробити так, щоб кредитні карти дітям на очі не попадалися;
* скажіть дитині, що вона може звернутися до вас за допомогою в разі виникнення якоїсь неприємної ситуації, надходження погроз, булінгу або шантажу. Скажіть підлітку, що він може на вас розраховувати в будь-який момент, і він завжди може розраховувати на вашу допомогу та захист.

***ПРОГРАМИ ДЛЯ БАТЬКІВ, ЯКІ ДОПОМОЖУТЬ КОНТРОЛЮВАТИ ПРОВЕДЕННЯ ЧАСУ ДИТИНИ В ІНТЕРНЕТІ***

Безумовно, постійно лізти в особистісний простір дитини ‒ не найкраща ідея. Але як тільки підліток починає користуватися інтернетом, ви повинні проконтролювати, скільки часу він проводить у віртуальному світі, які сайти відвідує, з ким спілкується. Чи немає чого підозрілого? Поспостерігати за школярем слід і тоді, коли ви помітили явні зміни в його поведінці: не властиву йому замкнутість, агресивність, заляканість, надмірну обережність. На жаль, не всі діти на всі 100% довіряють батькам. Не всі своєчасно діляться з ними своїми проблемами, тому відтягують висвітлення проблеми на «потім». На цьому етапі, як тільки підліток почав користуватися соціальними мережами і інтернетом, потрібно простежити за тим, скільки часу він там проводить і який контент споживає. Візьміть собі в помічники програми, які можна встановити на домашній комп'ютер:

**«Adult Blocker»** ‒ не програма, а розширення в браузері «Google Chrome». Цей плагін допомагає заблокувати сайти потенційно небезпечного змісту: сайти порнографічної спрямованості, форуми, сайти, які реагують на «блок-слова». До «блок-слів» можуть належати: «зброя», «самогубство», «вбивство», «наркотики» і т.п. Від небезпечного контенту ваша дитина застрахована!

**«Child Web Guardian Pro»** ‒ ця програма виконує той самий набір функцій, що і попередня, але тут є ще одна корисна функція ‒ контроль часу. Батьки можуть встановити ліміт, наприклад, 2 години на день. Після чого комп'ютер вимкнеться. Можна обирати різні варіанти стандартного графіка, який пропонується програмою, а можна встановити вручну.

**«Kids Control 1.6»** ‒ у цій програмі об'єднані функції обмеження перебування в інтернеті за часом, а також блокування сайтів із забороненим контентом. Примітним в «Kids Control 1.6» є те, що можна контролювати гаджети дітей. Наприклад, встановлювати контроль на планшет або смартфон.

**«Кібер Мама»** ‒ програма для встановлення графіку роботи за комп'ютером. Дисципліна ‒ фундамент усвідомленості. Якщо у дитини є чіткий графік життя, в якому вона навчається, розвивається, приділяє час спорту та хобі, то навряд чи вона буде занадто довго сидіти в інтернеті. За допомогою програми «Кібер Мама» ви зможете встановити графік роботи за комп'ютером, і підліток буде витрачати певну кількість часу в мережі для підготовки до навчання.

*Інтернет ‒ це, безумовно, чудовий винахід суспільства, адже дозволяє людям зробити життя комфортнішим, надаючи можливості для постійного розвитку, особистісного зростання, освіти. Але головне дозовано і вибірково споживати інформацію. Навчити підлітка основам безпеки в мережі і головним принципам користування інтернетом ‒ це прямий обов'язок батьків. Адже саме вони зацікавлені в тому, щоб розвиток дитини був гармонійним, щоб підліток менше стикався з негативом ззовні, щоб школяр не витрачав весь вільний час на сидіння біля комп'ютера. Турбота про дитину ‒ завжди на плечах батьків! Пам'ятайте про це, вибудовуйте довірливі відносини, вислухайте скарги дитини і м'яко контролюйте її вільне проведення часу.*

***Безпека дитини в інтернеті:***

***про що необхідно говорити***

Зараз в Україні майже 22 млн користувачів інтернету, питання безпеки в мережі більш ніж актуальне. У цьому контексті турбота про дітей набуває більших масштабів. Якщо раніше треба було говорити з дітьми про їх безпеку поза домом тощо, то вже давно має сенс застерігати їх від негараздів під час перебування в інтернеті.

*Від чого варто захищати дитину?*

Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально – суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду. Особливо вразливі у цьому контексті діти. Вони можуть не знати, яку інформацію можна викладати в мережу, а яку не варто.

І нколи школярі не можуть правильно зреагувати на матеріали з мережі з різних причин. Робота у цьому напрямку для вчителів та батьків дуже важлива. Безконтрольний доступ до інтернету може мати негативні наслідки для дитини.

**Типи загроз**

*Стосуються особистої безпеки:*

* Ознайомлення з порнографічними матеріалами, ненормативною лексикою, інформацією суїцидального характеру, расистського, ненависницького чи сектантського змісту.
* Загроза отримання недостовірної чи неправдивої інформації.
* Формування залежності (ігрової, комп’ютерної, інтернет).
* Спілкування з небезпечними людьми (збоченці, шахраї, грифери).
* Залучення до виконання протиправних дій (хакерство, порушення прав та свобод інших).

*Стосуються безпеки інших.*

* Матеріали, існування та використання яких може стати причиною посягання на безпеку оточуючих (наприклад, інформація про створення вибухівки).
* Свідоме та несвідоме введення в оману інших.
* Вчинення протиправних дій, що тягнуть за собою відповідальність згідно з чинним законодавством.
* Кібербулінг – свідоме цькування та приниження, передусім однолітків.
* Стосуються загрози витоку персональної інформації:
* Розголошення персональної та конфіденційної інформації (прізвища, імена, контакти, секретні дані кредитних карток, номери телефонів).
* Загроза зараження ПК вірусами різної категорії.
* Небезпека завантаження програм зі шкідливими функціями.

Це найбільш поширені типи загроз, з якими може зіштовхнутися дитина в інтернеті, викладаючи чи переглядаючи сумнівну інформацію. Від деяких з них можна захиститися технічними засобами, але більшість вимагають комплексного підходу.

***Пам'ятка***

*Основні правила безпечної роботи в інтернеті, про які варто сказати дітям:*

* Не давайте нікому своїх паролів.
* Не надавайте особистої інформації поштою чи в чатах без гострої на те потреби.
* Не реагуйте на непристойні та грубі коментарі, адресовані вам.
* Повідомляйте про ситуації в інтернеті, які вас непокоять (погрози, файли певного місту, пропозиції).
* Відмовляйтесь від зустрічей з випадковими людьми, з якими познайомились в онлайні.
* Не діліться своїми фото з незнайомцями.
* Не повідомляйте інформацію про кредитки батьків (номер картки, термін дії та таємний код).
* Не викладайте фото квитків, на яких видно штрих-код чи QR-код.
* Не скачуйте та не встановлюйте невідомі програми за посиланнями, навіть якщо їх надали друзі.
* Встановлюючи перевірені програми, контролюйте, щоб на ПК не додались небажані програми.
* Не переглядайте інформацію за невідомими посиланнями (друзі, які ними діляться можуть не підозрювати про загрозу).
* Не відкривайте листи-спам, вони можуть містити віруси.