Безпека дітей в Інтернеті - поради батькам

Інтернет технології стали природною складовою життя дітей і сучасної молоді. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку особистості.

Самостійне пізнання інформаційного світу дозволяє розширити коло інтересів дитини і сприяє її додатковій освіті, спонукає до кмітливості, привчає до самостійного розв'язання задач.

Всесвітня мережа також задовольняє потребу підлітків у лідерстві. Діти, які добре знають комп'ютер та Інтернет, більш адекватно оцінюють свої здібності та можливості, вони більш цілеспрямовані та кмітливі. Щоб повноцінно орієнтуватись у віртуальному просторі, дитині треба вчитися структурувати великі потоки інформації, дотримуючись основних правил безпеки в мережі.
Завдяки різним видам комунікації діти можуть виражати себе більш вільно та комфортно. Вони з цікавістю вивчають різні пропозиції у віртуальному просторі, однак часто виявляються досить незахищеними до негативних аспектів інформаційно-комп'ютерних технологій.

Основні небезпеки та ризики з якими діти можуть зіштовхнутися в мережі Інтернет. Діти і підлітки можуть наразитися на безліч ризиків: порнографія, порушення авторських прав, пропаганда екстремізму, наркотиків, нецензурні тексти (контентні ризики); віруси, трояни, спам, онлайн шахрайства; незаконні контакти, кіберпереслідування (погрози, сексуальні домагання з використанням інформаційних технологій) тощо.

Всі ці небезпеки та ризики з яким діти можуть зіштовхнутися поділено на чотири групи: контентні ризики, комунікативні ризики, електронні ризики, споживчі ризики.

Контентні ризики
"Контентні ризики — це матеріали (тексти, картинки, аудіо і відео файли, посилання на сторонні ресурси), що містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.д.

Як допомогти дитині уникнути зіткнення з небажаним контентом? Навчіть дитину радитися з дорослими і негайно повідомляти про появу небажаної інформації подібного роду.

Комунікативні ризики

Комунікаційні ризики – це знайомства і спілкування в Інтернеті під час яких на дитину можливий кібербулінг та кібергрумінг.
Кібербулінг — переслідування повідомленнями в Інтернеті, що містять образи, погрози та агресію; це підлітковий віртуальний терор, напад із метою завдати психологічної шкоди. Простіше кажучи — сучасний цифровий аналог дитячого знущання. Останнім часом основною платформою для кібербулінгу стали соціальні мережі.

Кібергрумінг – входження у довіру до дитини з метою використання її у сексуальних цілях. Шахраї дуже добре ознайомлені з особливостями вікової психології дитини і досить легко можуть встановлювати з нею контакт у соціальних мережах, форумах. Починаючи із віртуального спілкування та входячи у довіру до дитини, злочинці пропонують потоваришувати, а потім поступово переходять до розмов про зустріч у реальному житті та переводять тему спілкування у сексуальну площину. Як варіант, виділяють ще один вид кібергрумінгу - наполегливе чіпляння в мережі із сексуальними пропозиціями, розмови на теми сексу, насильства та (або) виготовлення, розповсюдження і використання матеріалів зі сценами насильства над дітьми (у більшості випадків – сексуального).

Електронні ризики.

Викрадання персональної інформації яке відбувається завдяки вірусам, шпигунським програмам, необдуманому висвітленню власної конфіденційної інформації.

Комп'ютерний вірус (англ. computer virus) — комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Приклади вірусів: Neshta, Staog, Archiveus.

Шпигунський програмний продукт (англ. Spyware) — це програмний продукт особливого виду, що встановлений і вживається без належного сповіщення

користувача, його згоди і контролю з боку користувача, тобто несанкціоновано встановлений.

Споживчі ризики.

Дану групу ризиків в мережі Інтернет відносять до кіберзлочинів: продаж товарів через мережу де часто вони не відповідають своїм характеристикам, про що порушується Закон України «Про захист прав споживача», перевід грошових потоків через банківські картки де не завжди конфіденційна інформація є незахищеною.

Отже, для того щоб запобігти всім тим негативним явищам та небезпекам, які очікують дітей в Інтернеті, необхідно їх навчити правильній поведінці та безпечному користуванню сучасними інтернет технологіями!

Поради для батьків:

1. Разом з дітьми розробіть правила користування Інтернетом. Особливо домовтеся з ними про прийнятий час роботи в Інтернеті і сайти до яких вони збираються заходити.
2. Знайдіть час для відвідування сайтів разом з дітьми та заохочуйте дітей ділитися з вами їх знаннями в Інтернеті.

3. Якщо діти спілкуються в чатах, використовують програми миттєвого обміну повідомленнями, грають або займаються чимось іншим, що вимагає реєстраційного імені, допоможіть дитині його вибрати і переконайтеся, що воно не містить ніякої особистої інформації.

4. Наполягайте на тому, щоб діти ніколи не видавали своєї адреси, номера телефону або іншої особистої інформації. Наприклад, місце навчання або улюблені місця для прогулянки.

5. Навчайте дітей не розміщувати свої чи сімейні фотографії.

6. Поясніть, що давати свої паролі не можна нікому, крім батьків, навіть найближчим друзям.

7. Поясніть, що не потрібно відповідати на невиховані й грубі листи. Якщо отримали такі листи, то потрібно сповістити про це батьків чи вчителів.

8. Скажіть дітям, що їм не слід зустрічатися з людьми, яких вони знають тільки з Інтернету. Поясніть, що ці люди можуть виявитися зовсім не тими, за кого себе видають. Якщо ж це необхідно, то спочатку треба спитати дозволу батьків. Зустріч у громадському місці та й у присутності батьків.

9. Скажіть дітям, що не все, що вони читають або бачать в Інтернеті, - правда. Привчіть їх запитувати вас, якщо вони не впевнені.

10. Навчіть дітей поважати інших в Інтернеті. Переконайтеся, що вони знають про те, що правила етикету діють скрізь – навіть у віртуальному світі.

11. Наполягайте, щоб діти не завантажували музику, комп'ютерні ігри та інших програми без вашого дозволу.

12. Поясніть наскільки небезпечно переходити на посилання, адреси яких вам невідомі.

13. Контролюйте діяльність дітей в Інтернеті за допомогою сучасних програм. Вони допоможуть відфільтрувати шкідливий вміст, з'ясувати, які сайти відвідує дитина і що вона на них робить.

В Інтернеті дійсно можна зустріти багато суб'єктів з недобрими намірами, але це не є приводом для того, щоб відмовитися від користування цією мережею. Дотримуйтесь цих простих правил, і ви будете впевнені, що жодна людина з нечесними намірами не отримає доступу до вашої персональної інформації.