БЕЗПЕЧНИЙ ІНТЕРНЕТ

Часто діти приймають все, що бачать по телевізору та в Інтернеті, за чисту монету… Вони повинні знати, які небезпеки підстерігають їх у мережі та як їх уникнути

Медіаграмотність визначається у міжнародному праві як грамотне використання дітьми та їх викладачами інструментів, що забезпечують доступ до інформації, розвиток критичного аналізу змісту інформації та прищеплення комунікативних навичок, сприяння професійній підготовці дітей та їх педагогів з метою позитивного та відповідального використання ними інформаційних та комунікаційних технологій та послуг. Розвиток та забезпечення інформаційної грамотності визнано ефективним заходом протидії посяганням на дітей з використанням мережі Інтернет.

Подолати небажаний вплив комп'ютера можливо лише спільними зусиллями вчителів, батьків та самих школярів. Наше завдання сьогодні – забезпечення безпеки дітей, не здатних іноді правильно оцінити ступінь загрози інформації, яку вони сприймають або передають, оскільки темпи інформатизації виявилися настільки швидкими, що й сім'я та освітній заклад виявилися не готовими до загроз нового типу, методи боротьби з якими ще тільки розробляються.

Як забезпечити безпеку дітей у мережі Інтернет

- Небажаний контент
- Інтернет-знайомства
- Кібербулінг
- Кібершахрайство
- Інтернет- та ігрова залежність
- Шкідливі програми
- Що робити, якщо дитина все ж таки зіткнулася з будь-якими ризиками
- Як захистити дитину від небажаного контенту в Інтернеті

Контентні ризики – це матеріали (тексти, картинки, аудіо, відеофайли, посилання на сторонні ресурси), що містять насильство, агресію, еротику та порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії та булімії, суїциду, і т.д.)

Як допомогти дитині уникнути зіткнення з небажаним контентом:

- Привчіть дитину радитися з дорослими та негайно повідомляти про появу небажаної інформації такого роду;
- Поясніть дітям, що не все, що вони можуть прочитати або побачити в Інтернеті, – правда. Привчіть їх запитувати, у чому вони впевнені;
- Намагайтеся запитувати дитину про побачене в Інтернеті. Найчастіше, відкривши один сайт, дитина захоче познайомитися з іншими подібними ресурсами;
- Увімкніть програми батьківського контролю та безпечного пошуку, які допоможуть захистити дитину від небажаного контенту;
- Постійно пояснюйте дитині правила безпеки у Мережі;
- Проте пам'ятайте, що неможливо завжди бути поруч із дітьми і постійно їх контролювати. Довірчі стосунки з дітьми, відкритий та доброзичливий діалог часто може бути набагато конструктивнішим, ніж постійне відстеження відвідуваних сайтів та блокування різноманітного контенту.
- Використовуйте спеціальні налаштування безпеки (інструменти батьківського контролю, налаштування безпечного пошуку та інше).
- Розробіть «сімейні правила» використання Інтернету. Орієнтуючись на них, дитина знатиме, як чинити при зіткненні з негативним контентом.
- Будьте в курсі того, що ваша дитина робить в Інтернеті. Частіше розмовляйте з дитиною про те, що вона робить у Мережі.

Як навчити дитину бути обережним при знайомстві з новими людьми в Інтернеті

Спілкування в Інтернеті може спричинити комунікаційні ризики, такі як незаконні контакти (наприклад, грумінг), кіберпереслідування, кібербулінг та ін. Навіть якщо більшість користувачів чат-систем (веб-чатів або IRC) мають добрі наміри, серед них можуть бути і зловмисники. У деяких випадках вони хочуть обманом змусити дітей видати особисті дані, такі як домашня адреса, телефон, паролі до персональних сторінок в Інтернеті та ін. В інших випадках вони можуть стати злочинцями у пошуках жертви. Фахівці використовують спеціальний термін «грумінг», що означає встановлення дружніх відносин із дитиною з метою вступу в сексуальний контакт. Знайомство найчастіше відбувається у чаті, на форумі чи соціальної мережі від імені ровесника дитини. Спілкуючись особисто («в приваті»), зловмисник входить у довіру до дитини, намагається дізнатися особисту інформацію та домовитися про зустрічі е.

Попередження грумінгу:

- Будьте в курсі, з ким контактує в Інтернеті ваша дитина, намагайтеся регулярно перевіряти список контактів своїх дітей, щоб переконатися, що вони знають усіх, з ким вони спілкуються;
- Поясніть дитині, що не можна розголошувати в Інтернеті інформацію особистого характеру (номер телефону, домашню адресу, назву/номер школи тощо), а також надсилати інтернет-знайомим свої фотографії;
- Якщо дитина цікавиться контактами з людьми набагато старшими за неї, слід провести роз'яснювальну бесіду;
- Не дозволяйте вашій дитині зустрічатися з онлайн-знайомими без вашого дозволу або без дорослої людини. Якщо дитина хоче зустрітися з новим інтернет-другом, слід наполягти на супроводі дитини на цю зустріч;
- Цікавтеся, куди і з ким ходить ваша дитина.
- Поясніть дитині основні правила поведінки у Мережі:
- Не можна ділитися з віртуальними знайомими персональною інформацією, а зустрічатися з ними у реальному житті слід лише під наглядом батьків.
- Якщо інтернет-спілкування стає негативним – таке спілкування слід перервати та не відновлювати.

Як уникнути кібербулінгу

Кібербулінг – переслідування повідомленнями, що містять образи, агресію, залякування; хуліганство; соціальне бойкотування за допомогою різноманітних інтернет-сервісів.

Попередження кібербулінгу:

- Поясніть дітям, що при спілкуванні в Інтернеті вони повинні бути дружелюбними з іншими користувачами, ні в якому разі не писати брутальних слів – читати грубості так само неприємно, як і чути;
- Навчіть дітей правильно реагувати на образливі слова та дії інших користувачів. Не варто спілкуватися з агресором і тим більше намагатися відповісти йому тим самим. Можливо, варто взагалі залишити даний ресурс та видалити звідти свою особисту інформацію, якщо не вдається вирішити проблему мирним шляхом;
- Якщо дитина стала жертвою буллінгу, допоможіть їй знайти вихід із ситуації – практично на всіх форумах та сайтах є можливість заблокувати кривдника, написати скаргу модератору або адміністрації сайту, вимагати видалення сторінки;
- Поясніть дітям, що не можна використовувати Мережу для хуліганства, поширення пліток чи загроз;
- Намагайтеся стежити за тим, що ваша дитина робить в Інтернеті, а також слідкуйте за його настроєм після користування мережею.

Як захиститися від кібербулінгу:

- Не провокувати. Спілкуватися в Інтернеті слід етично та коректно. Якщо хтось починає ображати дитину в Інтернеті – необхідно порекомендувати піти з такого ресурсу та пошукати зручніший майданчик.
- Якщо електронною поштою або іншими е-каналами хтось спрямовує дитині загрози та образи – найкраще змінити електронні контакти (завести новий email, Skype, ICQ, новий номер мобільного телефону).

- Якщо хтось виклав в Інтернеті сцену кіберзниження дитини, необхідно повідомити про це адміністрацію ресурсу. Також можна звернутися на гарячу лінію. Навіть при найдовірливіших стосунках у сім'ї батьки іноді не можуть вчасно помітити небезпеку, що загрожує дитині, і тим більше не завжди знають, як її запобігти.
- Ось на що слід звертати увагу батькам, щоб вчасно помітити, що дитина стала жертвою кібербулінгу:
- Неспокійна поведінка. Навіть самий замкнутий школяр переживатиме через те, що відбувається, і обов'язково видасть себе своєю поведінкою. Депресія і небажання йти до школи –перші ознаки того, що дитина зазнає агресії.
- Неприязнь до Інтернету. Якщо дитина любила проводити час в Інтернеті і раптово перестала це робити, слід з'ясувати причину. У дуже поодиноких випадках дітям справді набридає проводити час у Мережі. Однак у більшості випадків раптове небажання користуватися Інтернетом пов'язане із проблемами у віртуальному світі.
- Нервовість при отриманні нових повідомлень. Негативна реакція дитини на звук листа на електронну пошту має насторожити батька. Якщо дитина регулярно отримує повідомлення, які засмучують її, поговоріть з нею та обговоріть зміст цих повідомлень.

Як навчити дитину бути обережним у Мережі та не стати жертвою інтернет-шахраїв

Кібершахрайство – один із видів кіберзлочину, метою якого є заподіяння матеріальної чи іншої шкоди шляхом розкрадання особистої інформації користувача (номери банківських рахунків, паспортні дані, коди, паролі та інше)

Попередження кібершахрайства:

- Проінформуйте дитину про найпоширеніші методи шахрайства та навчіть її радитися з дорослими перед тим, як скористатися тими чи іншими послугами в Інтернеті;
- Встановіть антивірусні програми на комп'ютери або, наприклад, персональний брандмауер. Ці додатки спостерігають за трафіком і можуть бути використані для виконання множини дій на заражених системах, найчастішим з яких є крадіжка конфіденційних даних;
- Перш ніж здійснити покупку в інтернет-магазині, переконайтеся в його надійності і, якщо ваша дитина вже здійснює онлайн-покупки самостійно, поясніть їй прості правила безпеки та:
- Ознайомтеся із відгуками покупців
- Перевірте реквізити та назву юридичної особи – власника магазину
- Уточніть, як довго є магазин.
- Поцікавтеся, чи магазин видає касовий чек
- Порівняйте ціни у різних інтернет-магазинах.
- Зателефонуйте до довідкової крамниці
- Зверніть увагу на правила інтернет-магазину
- З'ясуйте, скільки точно вам доведеться заплатити
- Поясніть дитині, що не можна надсилати надто багато інформації про себе під час здійснення інтернет-покупок: дані рахунків, паролі, домашні адреси та номери телефонів. Пам'ятайте, що адміністратор або модератор сайту ніколи не вимагатиме повні дані вашого рахунку, паролі та пін-коди. Якщо хтось запитує подібні дані, будьте пильні – швидше за все це шахраї.

Як розпізнати інтернет- та ігрову залежність

Сьогодні все більш актуальними є проблеми так званої «інтернет-залежності» (синоніми: інтернет-адикція, віртуальна адикція) та залежності від комп'ютерних ігор («геймерство»). Першими з ними зіткнулися лікарі-психотерапевти, а також компанії, що використовують у своїй діяльності Інтернет і збитки, якщо у співробітників з'являється патологічний потяг до перебування онлайн.

Як виявити ознаки інтернет-залежності у дитини:

- Оцініть, скільки часу дитина проводить у Мережі, чи не нехтує вона через роботу за комп'ютером своїми домашніми обов'язками, виконанням уроків, сном, повноцінним харчуванням, прогулянками.
- Поговоріть з дитиною про те, чим вона займається в Інтернеті. Соціальні мережі створюють ілюзію повної зайнятості – що більше дитина спілкується, то більше в нього друзів, то більший обсяг інформації йому потрібно охопити – відповісти на всі повідомлення, простежити за всіма

подіями, показати себе. З'ясуйте, чи підтримується інтерес вашої дитини реальними захопленнями, чи вона просто намагається нічого не пропустити і стежить за оновленнями заради самого процесу. Намагайтеся дізнатися, наскільки важливе для дитини спілкування в Мережі і чи не замінює воно реальне спілкування з друзями.

- Спостерігайте за зміною настрою та поведінкою вашої дитини після виходу з Інтернету. Можливий прояв таких психічних симптомів як пригніченість, дратівливість, неспокій, небажання спілкуватися. З-поміж фізичних симптомів можна виділити головні болі, біль у спині, розлади сну, зниження фізичної активності, втрата апетиту та інші.

Якщо ви виявили можливі симптоми інтернет-залежності у своєї дитини, необхідно дотримуватись наступного алгоритму дій:

- Намагайтеся налагодити контакт з дитиною. Дізнайтеся, що йому цікаво, що його непокоїть і таке інше.
- Не забороняйте дитині користуватися Інтернетом, але постарайтеся встановити регламент користування (кількість часу, які дитина може проводити онлайн, заборона мережі до виконання домашніх уроків тощо). Для цього можна використовувати спеціальні програми батьківського контролю, що обмежують час у Мережі.
- Обмежте можливість доступу до Інтернету лише своїм комп'ютером або комп'ютером, що знаходиться в спільній кімнаті, – це дозволить легше контролювати діяльність дитини в мережі. Слідкуйте, які сайти відвідує дитина.
- Запропонуйте дитині протягом тижня докладно записувати, на що витрачається час, що проводиться в Інтернеті. Це допоможе наочно побачити і усвідомити проблему, а також позбавитися деяких нав'язливих дій, наприклад бездумного оновлення сторінки в очікуванні нових повідомлень.
- Запропонуйте своїй дитині зайнятися чимось разом, постарайтеся її чимось захопити. Спробуйте перенести кібердіяльність у реальне життя. Наприклад, для багатьох комп'ютерних ігор існують аналогічні настільні ігри, в які можна грати всією сім'єю або з друзями, при цьому спілкуючись один на одного наживо. Важливо, щоб у дитини були пов'язані з Інтернетом захоплення, яким він міг би присвячувати свій вільний час.

Діти з інтернет-залежністю суб'єктивно відчувають неможливість обходитися без Мережі. Постарайтеся тактовно поговорити з дитиною. Принагідно обговоріть з ним ситуацію, коли з якихось причин він був змушений обходитися без Інтернету. Важливо, щоб дитина зрозуміла – нічого не станеться, якщо вона на деякий час випаде з життя інтернет-спільноти.

У разі серйозних проблем зверніться за допомогою до фахівця.

Як навчити дитину не завантажувати на комп'ютер шкідливі програми

Шкідливі програми (віруси, черв'яки, «троянські коні», шпигунські програми, боти та ін.) можуть завдати шкоди комп'ютеру і даних, що зберігаються на ньому. Вони також можуть знижувати швидкість обміну даними і навіть використовувати ваш комп'ютер для поширення вірусу, розсилати від вашого імені спам з адреси електронної пошти або профілю будь-якої соціальної мережі.

Попередження зіткнення зі шкідливими програмами:

- Встановіть на всі домашні комп'ютери спеціальні поштові фільтри та антивірусні системи для запобігання зараженню програмного забезпечення та тері даних. Такі програми спостерігають за трафіком і можуть запобігти як прямим атакам зловмисників, так і атакам, що використовують шкідливі програми.
- Використовуйте лише ліцензійні програми та дані, отримані з надійних джерел. Найчастіше вірусами заражені піратські копії програм, особливо ігор.
- Поясніть дитині, як важливо використовувати лише перевірені інформаційні ресурси та не завантажувати неліцензійний контент.
- Періодично намагайтеся повністю перевіряти домашні комп'ютери.
- Зробіть резервну копію важливих даних.
- Намагайтеся періодично змінювати паролі (наприклад, від електронної пошти) та не використовуйте занадто прості паролі.
- Що робити, якщо дитина все ж таки зіткнулася з будь-якими ризиками

- Встановіть позитивний емоційний контакт з дитиною, розташуйте її до розмови про те, що сталося. Розкажіть про своє стурбованість тим, що з ним відбувається. Дитина повинна вам довіряти і знати, що ви хочете розібратися в ситуації та допомогти їй, а не покарати;
- Постарайтеся уважно вислухати розповідь про те, що сталося, зрозуміти, наскільки це сталося серйозно і наскільки серйозно це могло вплинути на дитину;
- Якщо дитина засмучена чимось побаченим (наприклад, хтось зламав його профіль у соціальній мережі) або потрапив у неприємну ситуацію (витратив вашу чи свою готівку в результаті інтернет-шахрайства та інше) – постарайтеся її заспокоїти і разом з нею розберіться в ситуації: що призвело до цього результату, які неправильні дії здійснила сама дитина, а де ви не розповіли їй про правила безпеки в Інтернеті;
- Якщо ситуація пов'язана з насильством в Інтернеті щодо дитини, то необхідно з'ясувати інформацію про агресора, з'ясувати історію взаємовідносин дитини та агресора, з'ясувати, чи існує домовленість про зустріч у реальному житті; дізнатися чи були такі зустрічі і що відомо агресору про дитину (реальне ім'я, прізвище, адресу, телефон, номер школи тощо), жорстко наполягайте на уникненні зустрічей з незнайомцями, особливо без свідків, перевірте нові контакти дитини останнім часом;
- Зберіть найповнішу інформацію про подію, як зі слів дитини, так і за допомогою технічних засобів: зайдіть на сторінки сайту, де була ваша дитина, перегляньте список її друзів, прочитайте повідомлення. При необхідності скопіюйте та збережіть цю інформацію – надалі це може стати вам у нагоді (наприклад, для звернення до правоохоронних органів);
- Якщо ви не впевнені в оцінці серйозності події з вашою дитиною, або дитина недостатньо відверта з вами або взагалі не готова йти на контакт, або ви не знаєте як вчинити в тій чи іншій ситуації – зверніться до фахівця, де вам дадуть рекомендації про те, куди і в якій формі звернутися, якщо потрібне втручання інших служб та організацій.