

Інститут психології ім. Г.С. Костюка Національної академії педагогічних наук України  
"Київстар" - національний лідер телекомунікацій

# ДІТИ В ІНТЕРНЕТІ: ЯК НАВЧИТИ БЕЗПЕЦІ У ВІРТУАЛЬНОМУ СВІТІ

ПОСІБНИК ДЛЯ БАТЬКІВ



З думкою про Вас



КИЇВСТАР

# ДІТИ В ІНТЕРНЕТІ: ЯК НАВЧИТИ БЕЗПЕЦІ У ВІРТУАЛЬНОМУ СВІТІ

Ігор Володимирович Литовченко,  
Сергій Дмитрович Максименко, Сергій Іванович Болтівець,  
Мирослав-Любомир Андрійович Чепа, Наталія Михайлівна Бугайова.  
– К.: Видавництво: ТОВ «Видавничий Будинок “Аванпост-Прим”», 2010.  
– с. – 48. (Посібник для батьків).

У посібнику розкрито можливості сучасних інформаційних технологій – інтернету, мобільного зв’язку та висвітлено способи безпечної поведінки дитини у віртуальному просторі, що убезпечать від негативного вплива на її психічне і фізичне здоров’я.

Посібник адресовано батькам, дідусям і бабусям, педагогам, працівникам соціальних служб для дітей і молоді.

Рецензенти:

**Биков В.Ю.**, доктор технічних наук, професор, директор Інституту інформаційних технологій і засобів навчання Національної АПН України.

**Жолдак М.І.**, доктор педагогічних наук, професор, завідувач кафедри інформаційних технологій Національного педагогічного університету ім. М.П. Драгоманова, академік Національної АПН України.

**Чепелєва Н.В.**, доктор психологічних наук, професор, заступник директора з наукової роботи Інституту психології ім. Г.С. Костюка Національної АПН України.

Рекомендовано Вченою радою

Інституту психології ім. Г.С. Костюка Національної АПН України,  
протокол № 8 від 27 серпня 2010 року.

© І.В. Литовченко, 2010

© С.Д. Максименко, 2010

© С.І. Болтівець, 2010

© М.-Л.А. Чепа, 2010

© Н.М. Бугайова, 2010

## ВСТУПНЕ СЛОВО

Вдосконалення інформаційних технологій створює умови для ефективного розвитку сучасного суспільства. Комуникаційні засоби стали невід'ємною складовою життя людей у всіх сферах діяльності. Мобільні телефони, комп'ютери та інтернет, розширивши комунікаційні, просторові й часові межі, розкрили нові можливості для спілкування, освіти, праці, відпочинку й творчої самореалізації особистості.

Кількість користувачів мобільних телефонів та інтернету щодня не-впинно збільшується. Більшою їхньою частиною є молодь.

Незважаючи на безумовно позитивну роль сучасних комунікаційних засобів та інтернету, існують певні ризики у використанні інформаційних технологій. Особливу небезпеку незахищений інформаційний простір приховує для дітей. Інтернет може містити інформацію агресивного чи соціально небезпечного змісту. А надання переваги віртуальному світу перед реальним спровокує негативний вплив на психіку і здоров'я дитини та може погіршити не тільки зір, поставу та сон, але й викликати тривожність, дратівливість, соціальну дезадаптованість і узалежнену поведінку.

За даними «Центру цифрових технологій майбутнього», 25% дорослих стурбовані тим, що їхні діти проводять в інтернеті забагато часу, 53% вважають кіберзлочинність реальною загрозою, а 63% висловлюють схвильованість через спілкування їхніх дітей у віртуальних співтовариствах, що лякають сучасних батьків так само, як попередні покоління бачили загрозу в негативному впливі «вулиці» на дітей. При цьому 46% користувачів всесвітньої мережі, які належать до молодіжної аудиторії, особисто зустрічалися зі своїми віртуальними знайомими. Для когось інтернет може бути єдиним джерелом спілкування, але слід враховувати те, що віртуальна реальність ніколи не замінить гармонійних взаємин і повноцінного спілкування між людьми.



Директор Інституту психології  
ім. Г.С. Костюка Національної АПН України,  
доктор психологічних наук, професор  
Сергій МАКСИМЕНКО

## ВСТУПНЕ СЛОВО

«Київстар» - соціально відповідальна компанія, ми дбаємо про те, щоб технології, які стають частиною життя українців, приносили максимум користі українським сім'ям і суспільству. Тому, як один з найбільших інтернет-провайдерів у країні, ми приділяємо значну увагу питанням безпеки використання Мережі, перш за все, дітьми. Наша мета - навчити наших клієнтів, батьків, дітей та вчителів правилам поведінки в інтернеті. Для цього «Київстар» впроваджує спеціальну програму, частиною якої є посібник, що Ви тримаєте в руках.

Діти блискавично освоюють усі останні новинки - соціальні мережі, ігри, програми. Інтернет допомагає їм розвиватися і читатися. При цьому інтернет – анонімний, його важко контролювати. Діти допитливі, у них ще немає того життєвого досвіду, який дозволив би їм визначити обман і маніпуляцію. Саме тому свідомість і підготовленість кожного користувача є основною запорукою його безпеки. Очевидно, що без сприяння дорослих, наші діти - можливо, більш «просунуті» в Мережі, але наївні у життєвих ситуаціях, - можуть потрапити до рук онлайн-шахраїв і кібер-злочинців.

У 2009 році «Київстар» ініціював проведення всеукраїнського соціологічного дослідження «Знання та ставлення українців до питання безпеки дітей в інтернеті». Його результати показали, що 76% батьків навіть не знають, які сайти відвідують їхні діти. До того ж більшість вчителів і батьків недостатньо розбираються в інноваційних технологіях і не знають про велику кількість можливостей та небезпек Мережі. Тому не завжди можуть передбачити ті загрози та ризики, з якими може зіткнутися дитина в онлайні. Головна шкода, на думку батьків, пов'язана з використанням інтернету - це загроза зниження зору. І як запобіжний засіб батьки або обмежують час проведення в Мережі, або зовсім забороняють дитині користуватися нею. Таким чином, старше покоління ігнорує той факт, що інтернет сьогодні став невід'ємною частиною життя та соціуму для наших дітей.

Наше завдання як дорослих і батьків - навчити дітей використовувати інтернет правильно. Так само, як ми вчимо дітей безпеки в реальному житті - на вулиці та дорозі, нам необхідно навчити їх безпечній поведінці у віртуальному житті - в інтернеті. Цей посібник покликаний допомогти батькам впоратися з цим завданням. У ньому просто та зрозуміло викладені основні правила та рекомендації, як створити у себе вдома територію безпечного інтернету.



президент «Київстар»  
Ігор ЛІТОВЧЕНКО

## ЗМІСТ

### Вступ

Інтернет сьогодні ..... 5

Інтернет і розвиток сучасної дитини ..... 6

### Інтернет-загрози для дітей

Чим займаються діти в інтернеті ..... 8

Відповідальність батьків: як розібратися у проблемі ..... 12

Як правильно організувати інтернет-життя дитини ..... 27

Технічні засоби захисту в інтернеті ..... 29

Експерти рекомендують: поради з інтернет-безпеки: ..... 31

якщо вашій дитині від 5 до 7 років ..... 32

якщо вашій дитині від 8 до 10 років ..... 34

якщо вашій дитині від 11 до 14 років ..... 37

якщо вашій дитині від 15 до 18 років ..... 39

Корисні ресурси: ..... 41

Гарячі контакти з інтернет-безпеки ..... 41

Дізнайтесь більше: корисні сайти для батьків ..... 42

Виноски ..... 43

Список використаних джерел ..... 44

Коротка пам`ятка для батьків ..... 46

# ВСТУП

## ІНТЕРНЕТ СЬОГОДНІ

1,8 млрд. людей у світі підключені до Мережі<sup>1</sup>. Щороку зростає кількість користувачів, серед яких дедалі більше дітей і підлітків. У розвитку інтернету виділяють три етапи:

1. Розвиток систем обробки інформації (*у цей час активізувалися пошукові системи – Yahoo, Google*).
2. Поширення комунікації та електронної комерції (*онлайн-магазини, Amazon, Ebay*).
3. Становлення інтернету як найбільшого середовища спілкування (*соціальні мережі та блоги (мережеві щоденники), Facebook, You Tube, Skype, Twitter, Blogger, MySpace та ін.*).

**Поширеність інтернету в Україні, за останніми дослідженнями<sup>2</sup>, становить близько 20%. Тобто майже кожен п'ятий українець користується Мережею<sup>3</sup>.**

Ще п'ять років тому користувачами інтернету були переважно мешканці великих міст, які використовували дротові технології та широкосмуговий доступ. Нині ж, завдяки розвитку мобільного інтернету за технологіями WAP і GPRS/EDGE, стрімке розширення Мережі відбувається<sup>4</sup> навіть у порівняно невеликих населених пунктах, а вік користувачів починається з 7-8 років.

Кількість інтернет-користувачів у країні збільшується за рахунок розширення кабельної мережі у великих містах, а також шляхом підключення до мобільного інтернету в селах і невеликих містах, де немає фіксованого доступу. Так, тільки за перший квартал 2010 року кількість користувачів стільникового інтернету від «Київстар» – провідного телеком-оператора країни – за технологією GPRS/EDGE зросла на 25%. А їхня загальна кількість – понад два мільйони людей, серед яких не тільки дорослі, а й молодь – студенти, школярі.

Податкові відрахування від надання інтернет-послуг і електронної комерції – це стаття прибутків до Держбюджету України, що постійно зростає. Ця індустрія розвивається, підтримує економіку і відкриває нові інформаційні можливості для українських громадян. Експерти знайшли цікаву залежність – зростання рівня проникнення фіксованого інтернету на 10% тягне за собою збільшення ВВП на 1,3%<sup>5</sup>.



Мобільний зв'язок робить інтернет більш доступним, а отже все більше людей відкриває для себе безмежний світ інформації. Так, щоденno пошукова машина Google обробляє близько 1 мільярда запитів, користувачі сервісів обміну повідомленнями (ISQ, Jabber та ін.) пишуть по 80 мільярдів повідомлень, аудиторія соціальних мереж (Facebook, MySpace, LinkedIn, ВКонтакте та ін.) перевищує 500 мільйонів людей! ■

## ІНТЕРНЕТ І РОЗВИТОК СУЧАСНОЇ ДИТИНИ

Інтернет-технології стали природною частиною життя дітей і сучасної молоді. Невміння працювати з комп'ютером і орієнтуватися в інтернет-просторі в сучасному суспільстві можна порівняти з невмінням писати й читати. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку. У кіберпросторі існує велика кількість спеціальних сайтів, адресованих дітям різного віку.

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.

### Чим приваблює інтернет дітей і підлітків?

Різноманітне спілкування.

Утамування інформаційного голоду.

Пошук нових форм самовираження.

Анонімність і віртуальна свобода (моделювання множинності «Я»).

Відчуття спільноті та принадлежності до групи.

Навчальні, розвиваючі та розважальні інтернет-ресурси орієнтовані на дітей будь-якого віку. За їх допомогою діти в цікавій ігровій формі засвоюють основи письма і лічби, вчаться малювати та моделювати, привчаються до самостійної роботи і складають уявлення про навколошній світ. Розв'язання цікавих задач формує у дошкільників навички навчальної діяльності. До завдань розвиваючих програм та ігор входить також удосконалення пам'яті, уваги, мислення, логіки, спостережливості, тренування швидкості реакції та ін. Існує багато ігор, що водночас мають виховну і освітню основу та здатні викликати інтерес дітей шкільного віку до економіки, соціології, історії, літератури.

Інтерактивні ігри на кшталт «розфарбуй сам» містять коментарі, що пояснюють і спрямовують дії дитини. Працюючи з такими програмами, дитина має можливість оцінювати, доопрацьовувати і виправляти результати власної праці. Логічні ігри розвивають мислення і просторову уяву (наприклад, дають



**Необхідно, щоб безпечні ділянки інтернет-простору, виконуючи всі функції щодо розвитку і освіти та дозвілля дітей не шодили психічному й фізичному здоров'ю підростаючого покоління.**



можливість дитині вчитися розпізнавати та запам'ятовувати різноманітні геометричні фігури й кольори).

Діти дошкільного і шкільного віку із задоволенням проходять етапи навчальної гри знову і знову. Численні повторення сприяють кращому засвоєнню навчального матеріалу та стимулюють до самостійного пошуку найбільш ефективних шляхів вирішення поставлених задач.

Мережеві освітні ресурси для підлітків допомагають прискорити й оптимізувати процес навчання, підвищують якість навчання завдяки максимальній структурованості та цікавій формі викладення навчального матеріалу. Діти засвоюють нові цифрові технології та вчаться вільно орієнтуватися в інформаційному просторі.

Отже, сучасний підхід дозволяє підвищити якість і швидкість усвідомлення, розуміння та запам'ятовування навчального матеріалу.



Майбутнє пред'являє нові вимоги до нового покоління, стає необхідним формування певних соціальних і професійних навичок, що дозволяють жити в сучасному цифровому суспільстві. ■

## ІНТЕРНЕТ-ЗАГРОЗИ ДЛЯ ДІТЕЙ

### ЧИМ ЗАЙМАЮТЬСЯ ДІТИ В ІНТЕРНЕТІ?

Діти, як найбільш активна й допитлива аудиторія, часто першими знаються з новими технологіями, такими як інтернет, випереджаючи в технічній освіченості батьків. У цьому є позитивний бік: підвищення рівня ерудиції, формування навичок спілкування з людьми. Але є й негативний: відсутність життєвого досвіду, як правило, підвищує ризик зіткнутися з онлайн-загрозами:

- онлайн-насилля;
- шахрайство;
- порнографія;
- отримання особистої інформації з метою злочинного використання



**76% батьків не знають, які сайти відвідують їхні діти. А ви знаєте?**



У 2009 році «Київстар» ініціював Всеукраїнське соціологічне дослідження «Знання і ставлення українців до питання безпеки дітей в інтернеті», яке провів Інститут соціології НАН України.



## ТРИВОЖНА СТАТИСТИКА:

- понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі.
- **17% без коливань діляться інформацією про себе і свою родину – адресу, професію, графік роботи батьків, наявність цінних речей у домі...** **Нащо незнайомцям така інформація, діти, як правило, не замислються.**
- **22%** дітей періодично потрапляють на сайти для дорослих.
- **28%** дітей, побачивши в інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а **11%** – спробували купувати наркотики.
- Близько **14%** опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і лише деякі звертають увагу на вартість послуги.

Дослідження «Київстар» також виявило: 87% батьків вважають, що саме вони повинні навчати дітей правилам безпеки користування інтернетом. Однак лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина. Причини різні – хтось не знає, які ресурси можуть бути небезпечними, а хтось не вміє користуватися журналом відвідування сайтів. Третина батьків (32%) – хвілюються, що у дитини погіршується зір від роботи з комп’ютером, тому за звичай обмежують дитині час користування Мережею. Тільки 11% батьків знають про такі онлайн-загрози, як «дорослий» контент, азартні ігри, онлайн-насилля, кіберзлочинність.



Результати дослідження підтвердили, що батьки недостатньо обізнані, як захистити дітей і навчити їх безпечному користуванню Мережею. Цей посібник створено «Київстар» у рамках соціальної програми компанії «Безпека дітей в інтернеті», і він допоможе Вам

- стати більш досвідченим інтернет-користувачем
- дізнатися, які сайти відвідує дитина, навчити її правильній онлайн-поведінці, показати безпечні й корисні дитячі інтернет-ресурси
- дізнатися, які програми потрібно встановити на комп’ютер, щоб захистити дитину від онлайн-загроз.

## ЩО РОБЛЯТЬ ДІТИ ТА ПІДЛІТКИ В ІНТЕРНЕТІ?



**Спілкуються** – знайомляться і шукають нових друзів у соціальних мережах, чатах, беруть участь у дискусіях і віртуальних форумах.

**Навчаються і розвиваються** – продивляються контрольні, реферати і курсові роботи, читають новини, підвищують рівень знань, технічної і медійної освіченості.

**Розважаються** – грають, слухають музику, дивляться фільми і відеоролики.

У віртуальному середовищі діти та підлітки прагнуть розслабитися і абстрагуватися від психологічних проблем реального світу, дати вихід емоціям, цікаво провести час.

Віртуальний ігровий простір дозволяє дітям реалізовувати низку базових потреб: у грі, розвагах, досягненні поставленої мети, саморозвитку, розвитку позитивних якостей, сміливості, вмінні долати перешкоди, поразки і невдачі; потреби у повазі та самоповазі, потреби в автономії, у протесті проти існуючих правил, знятті соціальних табу; потреби у домінуванні; потреби в агресії та запобіганні небезпеки і т. ін.<sup>6</sup>.





### За статистикою:

- Школярів цікавлять такі ресурси Мережі, як YouTube, Google и Facebook, Wikipedia, eBay и MySpace, а також фан-сайти.
- Хлопчики легше сприймають інформацію, що несеуть зображення, а дівчата надають перевагу текстам.
- Для дівчаток найбільша складність – це навігація сайтів і особливості користування ресурсами інтернет. Хлопчики швидше орієнтується в ресурсах сайтів і в навігації.
- Дівчата під час роботи з комп’ютером звертаються за допомогою до дорослих, а хлопчики намагаються самостійно розібратися у проблемі та знайти рішення.
- Хлопчики віддають перевагу інтернет-магазинам, іграм і «дорослим» ресурсам, а дівчата – музичним сайтам, розважальним ресурсам і сайтам, присвяченим відомим особистостям.
- До соціальних мереж хлопчики і дівчата виявляють одинаковий інтерес.
- Хлопчики частіше за дівчат відвідують порнографічні сайти і сайти з еротичним змістом<sup>7</sup>.

## ВІДПОВІДАЛЬНІСТЬ БАТЬКІВ: ЯК РОЗІБРАТИСЯ У ПРОБЛЕМІ

Діти проявляють підвищену зацікавленість до всього нового, яскравого, незвичайного, вони найбільше піддаються впливу зовнішнього середовища, більш допитливі, ніж дорослі, і використовують інтернет у якості одного з універсальних способів дослідження і пізнання навколошнього середовища. Проте такі психологічні особливості, як недостатня розвиненість саморегулятивних механізмів, слабкий вольовий і емоційний контроль, імпульсивність поведінки, роблять дітей найбільш вразливими для інформаційних і програмно-технічних загроз. Тому увага батьків до інтернет-безпеки дітей є дуже важливою.



**Діти не можуть реально оцінювати рівень достовірності й безпеки інформації, що містить інтернет-простір.** Веб-сайти агресивного спрямування становлять для них серйозну загрозу. Доступність інтернет-ресурсів для неповнолітніх диктує підвищені вимоги до якості, достовірності та безпеки інформації, що міститься в Мережі.

Незважаючи на загальні норми мережевого етикету (нетикет, сетикет), межі вседозволеності в інтернет-просторі ще достатньо широкі. Обмеження стосуються, перш за все, поведінки на форумах і в чатах (заборона використання ненормативного лексикону в ніках (іменах), заборона на пряму образу співрозмовника) і правил обміну інформацією (e-mail-етикет: обмеження обсягу надісланих файлів і т.ін.).

Батьки скаржаться, що їхні діти багато часу проводять в інтернеті, що погано позначається на інших видах дозвілля – вони майже не бувають на свіжому повітрі, мало рухаються, не встигають в школі. Порушення соціальної адаптації та недостатня увага з боку батьків роблять віртуальний світ найбільш бажаним для дитини. Відсутність реальних інтересів і цілей у житті викликає порушення балансу в сприйнятті дитини, і кіберпростір стає для неї важливішим за реальне життя.



Слід пам'ятати, що **ставлення дитини до комп'ютера та інтернета формують дорослі на власному прикладі.** Батьки повинні, перш за все, вирішити, для чого потрібен родині комп'ютер: для роботи, навчання, спілкування чи тільки для ігор. А, можливо, для того, щоб спрямувати інтереси дитини з небезпеки вулиці в «безпечний» кіберпростір?

Окрема тема – онлайн-ігри у Мережі та комп'ютерні ігри. Віртуальний ігровий світ, на відміну від реального, вирізняє керованість подій (можливість збереження у грі та можливість «переграти» подію), прогнозованість подій та можливості вибору складових (рівня складності, супротивника, зброї, місця дії), наявність здібностей, неможливих у реальному світі: декількох життів, інші фізичні закони (наприклад, гравітація чи швидкість) та фізіологічні особливості (здатність відчувати біль, втому), відсутність базових потреб (у сні, відпочинку, іжі). Комп'ютерні ігри навчають дітей жити за іншими правилами, де відсутня необхідність дотримуватися єдиних для всіх норм і законів, навіть законів природи.

У віртуальному світі знімаються заборони і обмеження морально-етичного і соціальних планів (зняття табу насилия, вбивств, руйнування; відсутність правових норм, що діють у реальності). Діти на підсвідомому рівні відсторонюються від фундаментальних речей: необхідності дотримання правил, неминучості покарання за агресивну поведінку і порушення закона, єдності просторово-часового континууму. Зацікавленість агресивними іграми призводить до того, що діти можуть спробувати застосовувати подібні методи рішення проблем у реальному житті.

Триває перебування за комп'ютером у статичному положенні викликає порушення кровообігу і провокує застійні явища в організмі дитини, що, в свою чергу, сприяє виникненню або загостренню захворювань опорно-рухового апарату, шлунково-кишкового тракту, судинним порушенням. Концентрація погляду на екран монітора і неправильне освітлення негативно впливають на зір.

Більшість батьків вважають комп'ютерні та онлайн-ігри абсолютно нешкідливими і навіть корисними. Вони, при користуванні ними у межах здорового глузду, дійсно можуть мати психотерапевтичний ефект, сприяють зняттю напруги, стресу, зниженню рівня тривоги і послабленню депресивних станів. Проте, у випадку зловживання, такі ігри призводять до прямо протилежного ефекту, викликаючи підвищення рівня тривоги, роздратування, агресивності, сприяючи повному відчуженню від реальності та створенню психологічної залежності.

## У ЧИСЛО ІНТЕРНЕТ-ЗАГРОЗ ВХОДЯТЬ:

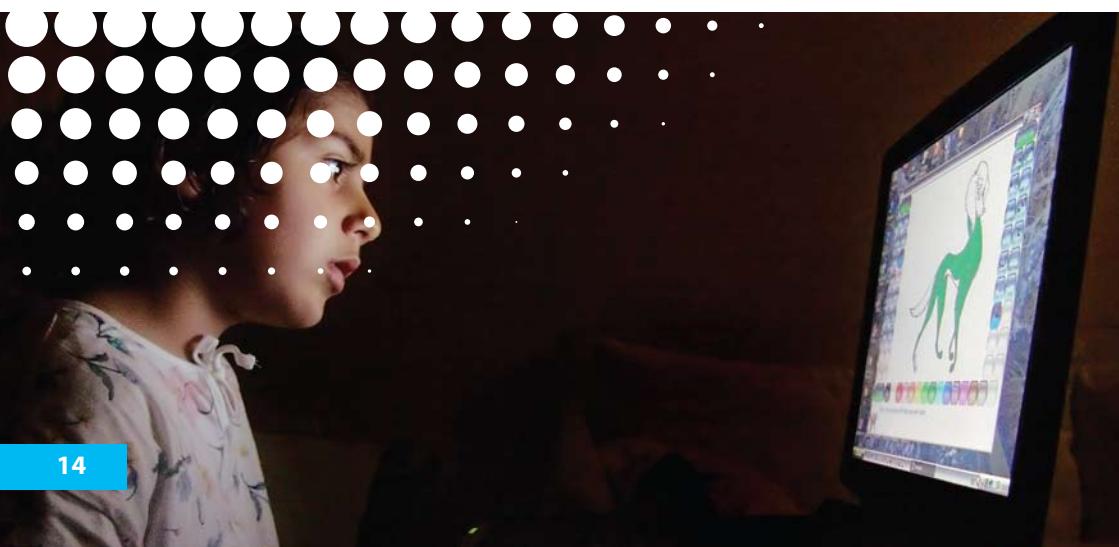
### КОМП'ЮТЕРНА ЗАЛЕЖНІСТЬ

До комп'ютерної залежності більш склонні підлітки 11-17 років. У них відбувається втрата відчуття часу, порушення зв'язків із навколошнім світом, виникає почуття невпевненості, безпорадності, страху самостійного прийняття рішень і відповідальності за них.

Комп'ютерна залежність негативно впливає на особистість дитини, викликаючи емоційну й нервову напругу, астеноневротичні та психоемоційні порушення, проблеми у спілкуванні та порушення соціальної адаптації.

Нічне використання інтернету спричиняє порушення режиму сну, внаслідок чого виникає хронічна втома, підвищується дратівливість, конфліктність. З метою подолання сонливості діти, які страждають залежністю, вдаються до підвищеного споживання кави, міцного чаю та інших тонізуючих речовин, що також шкодить їх здоров'ю. Щоб придбати нові ігри чи пристрой для гри або для оплати користування інтернетом деякі діти вдаються до шахрайства.

За ступінню впливу на гравця найбільш потужними є рольові комп'ютерні ігри, які сприяють інтеграції свідомості з комп'ютером, що може привести до повного самоототожнення дитини з комп'ютерним героєм. У нормальному стані відбувається короткочасове поринання гравця у віртуальну реальність з метою зняття напруги, відволікання від побутових проблем. У випадку патологічного відхилення від норми, дитина повертається у реальний світ на короткий проміжок часу, тільки щоб поїсти, попити і трохи поспати. Перебування залежної дитини в кіберпросторі може сягати 18 годин на добу. Залежність, як правило, помічають рідні і близькі користувача за змінами у поведінці, інтересах і режимі дня.



## ПСИХОЛОГІЧНІ І ФІЗИЧНІ СИМПТОМИ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ<sup>8</sup>:

### **ПСИХОЛОГІЧНІ СИМПТОМИ:**

- гарне самопочуття або ейфорія під час роботи за комп’ютером;
- неможливість зупинитися;
- постійне збільшення кількості часу перебування в інтернеті;
- зневага родиною і друзями;
- відчуття спустошіння, тревоги, роздратованості в періоди перебування поза інтернетом;
- брехня про свою діяльність своїм близьким;
- проблеми з навчанням.

### **ФІЗИЧНІ СИМПТОМИ:**

- біль в області зап’ястя через тривалу перенапрругу м’язів;
- сухість в очах;
- головний біль;
- біль у спині;
- нерегулярне харчування;
- зневага особистою гігієною;
- порушення сну.

### **НЕБЕЗПЕЧНІ СИГНАЛИ - ПЕРЕДВІСНИКИ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ<sup>9</sup>:**

- нав’язливе прагнення постійно перевіряти електронну пошту;
- очікування чергового сеансу онлайн;
- збільшення часу, проведеного онлайн;
- зростання витрат на інтернет-послуги.

### **ОЗНАКАМИ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ є:**

- повне поглинання інтернетом;
- потреба у збільшенні часу онлайн-сеансів;
- наявність неодноразових, малоекективних спроб скорочення часу перебування в інтернеті;
- поява симптомів абстиненції при скороченні користування інтернетом (повторна тяга, виникнення і посилення напруги через певний час);
- виникнення проблем з оточуючим середовищем (однолітками, членами родини, друзями);
- намагання приховати реальний час перебування в інтернеті;
- залежність настрою від використання інтернету (виражається емоційним і руховим збудженням, тривогою, нав’язливими розмірковуваннями про те, що зараз відбувається в інтернеті, фантазіями і мріями про інтернет, вільними чи несвідомими рухами пальців, що нагадує друкування на клавіатурі).

## РОЗХОДЖЕННЯ МІЖ РЕАЛЬНИМ «Я» І СВОЇМ ІНТЕРНЕТ-ОБРАЗОМ

може бути наслідком неадекватного сприйняття дитиною себе і оточуючого світу. Ототожнюючи себе з героем гри, дитина отримує можливість своєрідної самореалізації у віртуальному світі. При цьому якості героя (сміливість, сила, надзвичайні здібності та ін.) вона автоматично приміряє на себе. Повернення в реальність позбавляє гравця багатьох можливостей і робить безпорадним перед проблемами, що існують в реальності.

Це призводить до погіршення психологічного стану дитини: зміни її емоційного стану, підвищення тривоги, роздратованності, зниження самооцінки, проявів невпевненості в собі, виникнення агресії до оточуючих, погіршення навчальних показників і порушення соціалізації.

**Існують часові норми перебування за комп’ютером для дітей різного віку:**

*Згідно з нормами, визначеними Міністерством охорони здоров’я України, неперервне перебування за комп’ютером впродовж доби не повинно перевищувати:*



1-2 клас	<b>– 10 хв.</b>
3-5 клас	<b>– 15 хв.</b>
6-7 клас	<b>– 20 хв.</b>
8-10 клас	<b>– 30 хв.</b>

Для дітей 1 класу загальний час використання комп’ютера з рідкоокри-сталичним монітором має обмежуватися 30-45 хвилинами на тиждень, 2-3 класів – 2 години на тиждень, але не більше 1 години на добу, 4-6 класів – 2 години на тиждень, але не більше 1 години на добу, 7-9 класів – 2,5 години на тиждень, але не більше 1 години на добу і учнів 10-11 класів – 7 годин на тиждень, але не більше 1 години на добу.

## ДОСТУП ДО НЕБАЖАНОГО КОНТЕНТУ

(матеріалам непридатного для дітей та протизаконного змісту – порнографічним, тим що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість і нерівність, асоціальну поведінку, насилля, агресію, суїцид,

азартні ігри, інтернет-шахрайство, та матеріалам, що містять образи, наклепи і неналежну рекламу).

Небезпека перегляду ресурсів з «дорослим» контентом полягає у тому, що, по-перше, дитина ще емоційно не готова до сприйняття відвертих матеріалів, що стосуються статевих відносин, та можуть завадити формуванню нормальної сексуальної та громадської поведінки, справити негативний вплив на уяву про здорові сексуальні стосунки, нівелювати сімейні цінності та сприяти ранньому початку інтимного життя, а по-друге - що дитина може стати жертвою злочинців, педофілів чи людей з порушенням психіки.

Перегляд матеріалів, що містять сцени насилия та жорстокості щодо людей і тварин, що пропагують протиправну і антисуспільну діяльність - перешкоджає нормальному формуванню моральних цінностей.



**Розкриття конфіденційної інформації у Мережі** – це повідомлення повного власного імені чи імен членів родини, адреси проживання і навчального закладу, номерів телефонів, місця відпочинку, часу повернення додому, періоду відсутності батьків чи інших членів родини, номерів банківських карток батьків чи інтернет-гаманця, повідомлення паролей до електронної пошти та акаунтів соціальних мереж.

При реєстрації в інтернет-сервісах у кодових фразах не слід повідомляти свідчення особистого характеру, наприклад, дівоче прізвище матері, оськільки дана інформація використовується при оформленні банківських документів у якості ключової фрази.

Іноді дорослі самі розповсюджують через соціальні мережі та форуми інформацію про себе і своїх дітей, включаючи розміщення фотокарток родини, інформації про місце роботи і час повернення додому, місця відпочинку і точні дати відсутності. Це може зацікавити злочинців та поставити під загрозу безпеку дитини. Фотокартки, що розміщаються вами на персональній сторінці, але закриті для загального доступу, все рівно можуть потрапити на інші сервіси, де стануть загальнодоступними.

Нерідко підлітки, які перебувають у романтических стосунках вимагають одне від одного паролі до комунікаційних сервісів. При цьому дівчата більш склонні до розголошення власних даних.

**Надмірна зацікавленість індивідуальними та/або мережевими онлайн-іграми.** Агресивні ігри здатні зашкодити психіці дитини. Не слід вводити в арсенал дитячих ігор агресивні ігри з деструктивним змістом, що закликають до насилля і руйнування. Такі ігри негативно впливають на психіку дитини, підвищують тривожність і дратівлівість, роблять її більш збудженою і неслухняною, вчать вирішувати проблеми з позиції сили.

Конфлікти, що виникають між гравцями, можуть привести до драматичних наслідків у результаті з'ясування стосунків у реальності.

**Надмірне захоплення азартними мережевими іграми, віртуальними казино** (онлайн-гемблінг).

**Кібероніоманія.** Неконтрольовані покупки в інтернет-магазинах, без необхідності їх придбання та урахування власних фінансових можливостей, постійна участь в онлайн-аукціонах.

**Кіберкомунікативна залежність** (надмірне спілкування у чатах, участь у телеконференціях).

**Кіберсексуальна залежність** (нездоланий потяг до обговорення сексуальних тем на еротичних чатах і телеконференціях, відвідування порнографічних сайтів і заняття кіберсексом).

### **Перехід від віртуальних стосунків до реальних**

- залучення неповнолітніх до сексуальних стосунків;
- залучення через інтернет дітей і підлітків до протизаконної діяльності;
- знайомства через інтернет з метою пошуку сексуального партнера

**Секстинг** – новий вид розваг: фотографування себе у роздягненому вигляді на камеру телефона чи комп’ютера, з метою пересилки знімків друзям. Частіше за все секстинг використовують закохані пари, ті, хто хоче вихвалитися перед знайомими романтичними стосунками або підлітки, які розраховують на взаємність.

**Нав’язливий веб-серфінг**, блукання по Мережі, пошук у віддалених базах даних (відвідування сайтів новин, читання інформації на форумах, блогах, пегляд і прослуховування інформації в різних форматах). Веб-серфінг затягує дитину, відволікаючи її від навчання та інших справ, оскільки, потрапивши в інформаційний потік, втрачається відчуття часу.

**Відвідування сайтів агресивної і аутоагресивної спрямованості** (що пропагують ксенофобію, тероризм) (кіберсуїцид, онлайн-суїцид, суїциdalні домовленності, інформаційні ресурси про застосування засобів для суїциду з описом їх дозування і вірогідності летального результату).

**Аддиктивний фанатизм** (релігійний – сектантство, політичний – партійний, національний, спортивний, музикальний і т.ін.).

### **Пристрась до роботи з комп’ютером – програмування, хакерство.**

Основні мотиви хакерства: допитливість, боротьба за вільне розповсюдження і доступність інформації, самоствердження, відчуття власної сили, захоплення процесом, недостатність пізнавальної активності при навчанні, належність до «хакерської культури», залежна поведінка.

**Гаджет-аддикція** (пристрасть до заволодіння конкретним мобільним обладнанням, пристроями, що має вихід у інтернет: стільниковим телефоном, смартфоном, комунікатором, міні-комп’ютером, КПК і залежність від його використання).

**Кібербулінг** – одна з форм переслідування дітей і підлітків з використанням цифрових технологій. Кібербулінгу підлягають діти, яких відштовхнули однолітки. Іноді для цього створюються сайти, де розміщаються компрометуючі матеріали на дитину, яку переслідують. Якщо ж раптом Ваша дитина отримала численні електронні повідомлення агресивного змісту від незнайомців, якщо її почали переслідувати й залякувати, це означає, що дитина потрапила під кібербулінг. Складність фільтрації подібних повідомлень, неможливість контролю, регулярність атак і анонімність переслідувачів роблять залякування особливо потужним, завдаючи психологічну травму дитині.

### **Для кібербулінгу використовуються:**

- мобільний зв'язок (використання фото і відео для дискредитації та залякування жертви, доставка текстових і мультимедійних повідомлень);
- сервіси миттєвих повідомлень (використання ICQ для відправки повідомлень, взламування акаунта із розсланням дискредитуючих повідомлень рідним і друзям жертви);
- електронна пошта (розсилання повідомлень і листів, що містять залякування, віруси, публікація в Мережі листів жертви особистого характеру);
- форуми і чати (розсилання агресивних повідомлень, розкриття анонімності акаунта жертви, розміщення на сторінках форуму інформації про жертву конфіденційного і особистого характеру);
- соціальні мережі (розміщення коментарів, що містять залякування і знушення, фото і відеоматеріалів, блокування акаунта жертви і розсилання масових скарг і претензій на володаря акаунта, створення акаунта від імені жертви з її подальшим використанням для дискредитації жертви);
- веб-камери (провокування жертви на відеозапис з подальшою публікацією в інтернеті);
- сервіси відеохостингу (розміщення відеороликів, що містять знушення або залякування);
- ігрові сайти та віртуальні світи (розміщення повідомлень, що принижують і залякують жертву або шкодять її ігровому персонажу з метою психологічного тиску).

**Зіткнення з гриферами.** Інтернет-хулігани заважають гравцям (особливо початківцям) спокійно грati, постійно наносять пошкодження їхнім персонажам, блокуючи функції гри і створюючи неможливі умови для всієї команди Мережі, переслідуючи окремих її гравців.

**Кібергрумінг.** Входження в довіру дитини з метою використання її у сексуальних цілях. Злочинці добре розуміються на психології дітей і підлітків та орієнтуються в їхніх інтересах. Встановлюючи контакти в соціальній мережі або на форумах з дітьми, що знаходяться у пригніченому психологічному стані, вони співчувають, пропонують підтримку, обговорюють з дитиною питання, які її турбують, поступово переводячи їх у сексуальну площину, а потім про-

понують перейти до стосунків у реальному світі.

### ***Виробництво, розповсюдження та зберігання дитячої порнографії.***

Слід пам'ятати, що незважаючи на згоду дитини на участь у порнографічних сесіях, відповідальність цілком покладається на дорослих. 20 січня 2010 року було прийнято Закон України №1819-VI «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії». Відповідно до статті 301 Кримінального кодексу України, виготовлення і розповсюдження порнографічної продукції або змущення неповнолітніх до участі у створенні зображенень, відеопродукції або комп'ютерних програм порнографічного характеру карається позбавленням волі від п'яти до десяти років<sup>10</sup>.

***Шахрайство в Мережі.*** Інтернет- чи мобільне шахрайство є способами здійснення злочину з використанням сучасних технологій. Відповідно до Кримінального кодексу України, шахрайство, в залежності від особливостей і складності здійсненого злочину карається позбавленням волі від трьох до дванадцяти років з конфіскацією майна<sup>11</sup>. Також в Особливій частині Розділу XVI є низка статей, що передбачають покарання «за злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж електрозв'язку»<sup>12</sup>.

## **ІНТЕРНЕТ-ШАХРАЙСТВО:**

***Генерування кодів для карток оплати мобільного зв'язку.*** Пропозиція програми генерування PIN-кодів для карток експрес-оплати за мобільний зв'язок. Запропонована програма виявляється генератором випадкових чисел.

***Налаштування безкоштовного використання послуг мобільного оператора.*** На безкоштовних хостингах розміщаються сайти-одноденки, працівники яких представляються співробітниками певного мобільного оператора та за певну суму пропонують повідомити налаштування для безкоштовного використання послуг.

***«Читай чужі SMS».*** Пропозиція придбати спеціальну програму, що «дозволяє» читати SMS у чужому телефоні, переглядати адресну книгу та історії дзвінків.

***Продаж продукту, що не існує*** (програм, аудіофайлів, товарів, інформації). Прохання відправити SMS-повідомлення для отримання коду виявляється

звичайним виманюванням коштів. Зазвичай «неможливість відправити повідомлення» призводить до численного зняття коштів з рахунку абонента.

**«Передзвони мені».** Дзвінок з незнайомого номера з проханням зателефонувати. При спробі з'єднання з рахунку абонента знімаються кошти.

**Фішинг** – технологія інтернет-шахрайства з метою крадіжки конфіденційної інформації (імен і паролей доступу, даних банківських карток і інтернет-гаманця й т.ін.). Поштовий фішинг – отримання листа з вимогою повідомлення особистих даних. Онлайн-фішинг – копіювання дизайну і доменних імен сайтів та інтернет-магазинів з метою обдурити покупця. Комбінований фішинг – створення підробного сайту, де жертва самостійно заповнює форми, повідомляючи шахраям конфіденційні дані, або використання програм-шпигунів key-loggers, що фіксують інформацію, введену з клавіатури та пересилають її шахраям.

**Вішинг** – технологія інтернет-шахрайства з метою крадіжки конфіденційної інформації за допомогою інтернет-телефонії і автонабирачів. Абоненту пропонується зателефонувати за міським номером, де звучить повідомлення про необхідність надання особистої інформації.

**Фармінг** – перенаправлення трафіку із завантаженого веб-вузла на клон сайту, що хотів відвідати користувач. Далі відбувається зараження вірусами або активація файлу, що може пошкодити комп’ютер.

Попередьте дитину про подібні види шахрайства та необхідність повідомляти про надходження таких пропозицій батькам.



## МОБІЛЬНЕ ШАХРАЙСТВО

### **За допомогою SMS-повідомлень**

**Перекажіть кошти на рахунок і отримайте вдвічі більше.** SMS-повідомлення зі змістом на кшталт: «Сервер мобільного оператора X. Перекажіть гроші на номер XXXXXXXX і отримайте вдвічі більше!».

**Прохання надіслати гроши.** SMS зі змістом: «Не можу тобі дозвонитися, немає грошей, надішли 5 гривень». Далі повідомляється номер телефону XXX-XXXXXXX. При спробі набрати номер абонент виявляється «поза зоною досяжності».

**На ваш рахунок помилково перераховані кошти.** Отримання SMS із текстом про помилкове перерахування незначної суми грошей на рахунок абонента і прохання про її повернення. Для переказу коштів пропонують відправити повідомлення на короткий номер, дуже схожий на службовий. У результаті «повернення боргу» з балансу відправника знімається значна сума.

**Відмовся від рекламної SMS-роздилки.** Отримання SMS з пропозицією відписатися від рекламної SMS-роздилки. Поступова виявляється платною.

**Близька людина потрапила у халепу.** SMS-повідомлення про те, що близька людина потрапила в халепу. Вказану суму пропонують перерахувати картками експрес-оплати мобільного зв'язку.

### **За допомогою телефонного зв'язку**

**Блокування номера і перереєстрація SIM-карти.** Надходження дзвінка начебто із сервісного центру оператора про збій в системі і блокування телефона абонента на кілька діб. Для «вирішення» проблеми пропонується переєструватися в системі, набравши певну комбінацію чисел. Насправді ця комбінація чисел є командою переказу грошей з одного рахунку на інший.

**Виграш призу.** Дзвінок начебто від представника call-центрі і повідомлення про перемогу в акції. Для отримання «призу» необхідно придбати вау-



чер поповнення рахунку на XXX гривень і повідомити код активації. Рахунок виявляється недійсним.

**Прохання зробити короткий дзвінок з вашого телефону.** Звернення з проханням про необхідність термінового дзвінка тяжко хворій людині з вашого мобільного телефону. У результаті з рахунку абонента знімається значна сума. Попередьте дитину не реагувати на подібні звернення, не порадившись з вами.

### ЗАРАЖЕННЯ КОМП'ЮТЕРА ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ:

програмами, програмами-шпигунами, хакерські атаки.

**За даними опитування компанії Symantec 48% найбільш небезпечних сайтів, що містять загрози розміщення програм-шпигунів – це сайти із додрослім змістом.** Тому потрібно обмежити доступ на подібні ресурси з сімейного ПК.



# ХТО ПОВИНЕН НАВЧАТИ ДІТЕЙ, ЯК ВИКОРИСТОВУВАТИ ІНТЕРНЕТ ПРАВИЛЬНО І БЕЗПЕЧНО

Саме в родині закладаються основи поведінки дитини в реальному світі, і віртуальний простір не має бути виключенням. Батькам слід приділяти серйозну увагу вихованню дітей і підвищенню їхньої обізнаності про загрози інформаційного середовища.

Необхідно пам'ятати, що комп'ютер для дітей є інструментом навчання і розвитку, а не тільки розваг та ігор. Незважаючи на широкі можливості віртуального спілкування, воно не може виключати і замінювати реальних стосунків між людьми.

Завданням вихователів і вчителів є проведення освітньої роботи серед батьків для сприяння онлайн-безпеці підростаючого покоління.

Навіть якщо дитина надмірно захоплюється грою і інтернетом, не слід забороняти їй користуватися комп'ютером. Заборона може викликати протилежну реакцію і привести до замикання дитини в собі. Перш за все, слід знайти альтернативу онлайн-інтересам дитини і перемкнути її увагу на досягнення успіхів у реальному житті.

## ЩО НЕОБХІДНО ЗНАТИ І ВМІТИ БАТЬКАМ В ІНТЕРНЕТІ

Через те, що діти і підлітки більш «розвинені» в технічному плані, вони легко можуть обійти заборони батьків і усунути засоби батьківського контролю. Тому дорослим спочатку необхідно самим засвоїти основи інтернет-грамотності, а вже потім навчати правилам нетикуту (етикует спілкування в інтернеті) і комп'ютерній безпеці свою дитину та зробити це відповідно до віку дитини і кола її інтересів. Дізнайтеся більше про можливості і загрози Мережі.

**Наши прості правила і поради допоможуть вам у цьому.**

- Підвищуйте власну комп'ютерну грамотність, щоб стати авторитетом для дитини і вміти надавати допомогу у вирішенні питань, пов'язаних з використанням комп'ютера.
- Користуйтесь інтернетом разом з дітьми. Заохочуйте дітей ділитися з вами своїми успіхами і невдачами в освоєнні Мережі.

- Не забувайте, що ваша дитина може користуватися інтернетом у школі, у знайомих або в інтернет-кафе, тому заборони можуть виявится малоекективними. Приділяйте більше уваги вихованню дитини, навчайте її комп’ютерній грамотності й правилам безпеки в Мережі.
- Будьте другом і порадником, щоб дитина не соромилася і не приховувала від вас свої проблеми в опануванні інтернету. Спілкуйтесь з дитиною, обговорюйте її досягнення, пропонуйте допомогу.
- Щоб у дітей не виникало бажання обходити програмні заборони, встановлені батьками, необхідно запропонувати дітям в якості альтернативи пізнавальні, цікаві і захоплюючі курси, де вони будуть захищені від ризиків віртуального світу.



# ЯК ПРАВИЛЬНО ОРГАНІЗУВАТИ ІНТЕРНЕТ-ЖИТТЯ ДИТИНИ

## СТВОРІТЬ ТЕРИТОРІЮ БЕЗПЕЧНОГО ІНТЕРНЕТУ

- По-перше, важливо домовитися з дитиною, встановити правила сімейного користування мережею, з'ясувати їхню значущість для безпеки. Поясніть дітям, що якщо в інтернеті їх щось турбує, то ім слід не приховувати це, а поділитися з вами.
- По-друге, необхідно визначитися з найбільш прийнятним способом технічного захисту: від регулярно оновлюваного антивірусу до встановлення спеціального програмного забезпечення батьківського контролю на ПК та мобільний телефон. Просувайтесь поступово, щоб створити максимальний захист.

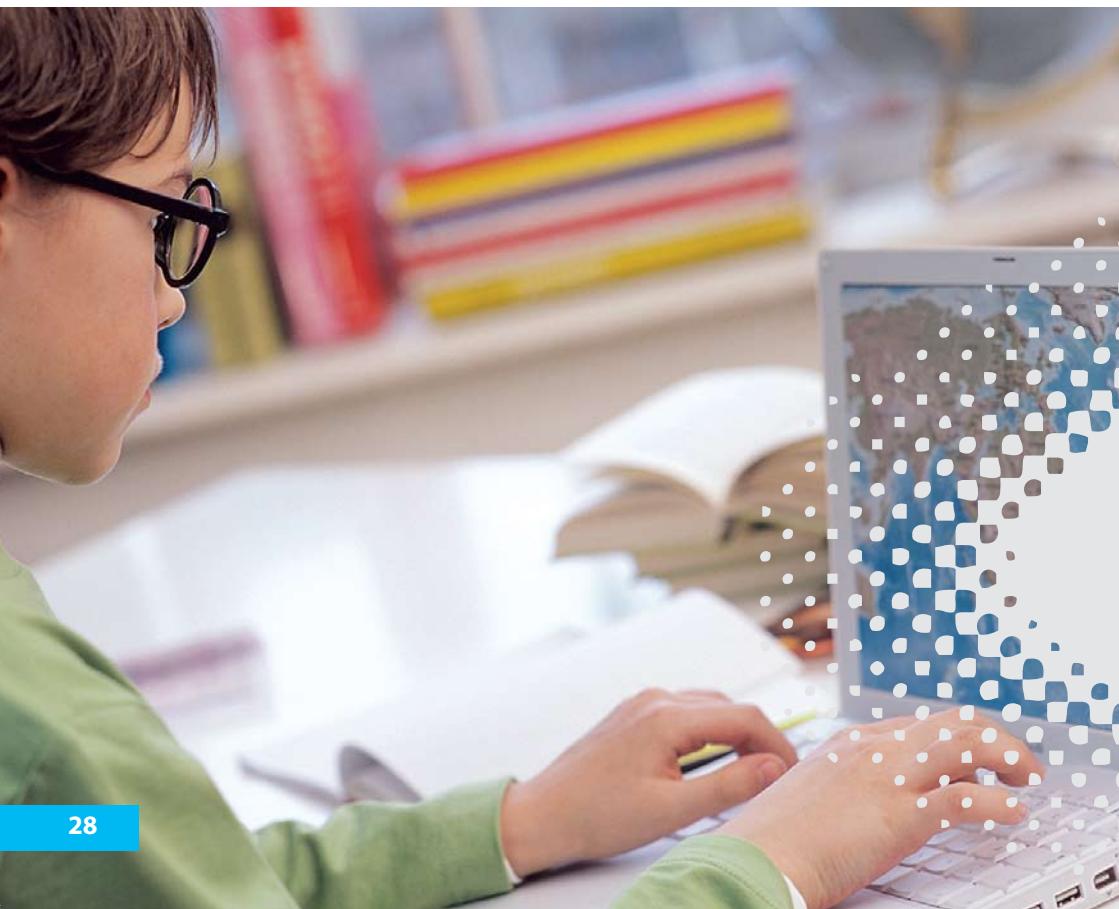
**Спочатку обговоріть з дитиною ці прості сімейні правила онлайн-безпеки.**

■ **Сімейна онлайн-безпека** – це відповідальність кожного. Роз'ясніть важливість збереження своєї та чужої конфіденційної інформації. Особистою інформацією можуть скористатися зловмисники. Тому не можна викладати в інтернеті інформацію про сім'ю, її фінансові справи, адреси мешкання і наявання, номери телефонів, коди банківських карток. Також небажано розміщувати особисті та сімейні фотографії на публічних форумах, сайтах. Ніколи ні кому, крім своїх батьків, не можна виказувати паролі інтернету, навіть найкращим друзям.

■ **Навчіть дітей поводити себе в онлайні як у реальному житті.** Так само, як у житті, у Мережі потрібно вести себе ввічливо, не робити того, що може образити інших людей чи входить у протиріччя з законом. Поясніть дітям, що в Мережі слід поводити себе коректно, з повагою ставитися до людей та до авторських прав. Незаконне копіювання і розповсюдження матеріалів, які є чиєюся власністю, вважається крадіжкою.

■ **Віртуальний співрозмовник може видавати себе за іншого.** Тому не можна призначати зустрічі з віртуальними знайомими без дозволу батьків. Поясніть дитині, що в Мережі можуть перебувати люди, які не є тими, за кого вони себе видають, тому не слід довіряти незнайомим людям і в жодному разі не можна повідомляти їм особисту інформацію.

- **Віртуальний світ іноді коштує реальних грошей.** Завжди необхідно з'ясовувати, скільки коштують SMS на окремі інтернет-сервіси, адже вартість SMS, наприклад, в онлайн-грах часто повідомляється без податків – тобто може бути більшою. Якщо така інформація незрозуміла, потрібно звертатися за порадою до батьків, які допоможуть розібратися, скільки насправді буде коштувати SMS і чи так вже необхідно його відправити.
- **Питати поради можна і потрібно.** Повідомте дитині, що вона може звернутися до вас у будь-якій ситуації, яка її турбує. Якщо в інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось незрозуміло, хвилює чи загрожує, завжди необхідно звертатися за допомогою до батьків. Інформація та послуги в інтернеті не завжди безпечні, тому раніше, ніж завантажувати, встановлювати або зберігати будь-що з інтернету, треба отримати дозвіл батьків. Навчіть дитину перевіряти інформацію з Мережі за допомогою додаткових запитів і звернення до перевірених джерел.



## ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ: ЯК УБЕЗПЕЧИТИ СВОЮ ДИТИНУ В ІНТЕРНЕТІ

*Відсутність комп'ютерної грамотності і компетентності в питаннях використання технологій у більшості випадків є основною причиною підвищеної інформаційної небезпеки.*

### Пам'ятка батькам – будьте уважними інтернет-користувачами!

- Слідкуйте за тим, щоб на загальному комп'ютері не було інформації, яка є небажаною для вашої дитини.
- Регулярно переглядайте електронну скриньку, не залишайте на робочому столі або в папках відкритого доступу документи і файли, призначенні тільки для дорослих.
- Налаштуйте запаролений вхід до комп'ютеру для різних користувачів.
- Завжди очищуйте журнал подій браузера від слідів перебування на сайтах небажаного змісту. Своєчасно видаляйте електронні повідомлення, фото-, відео- та аудіо-матеріали дорослого змісту, щоб виключити можливість їх випадкового перегляду неповнолітніми.
- Заборонені ресурси можуть завантажуватися автоматично під час відвідування сайтів з контентом, який не містить небезпеки для дітей. Згадайте про це перед тим, як сварити свою дитину за відвідання сайтів дорослого змісту після перегляду КЕШа браузера.

Необхідно навчитися правильно підбирати програмне забезпечення для захисту дитини від інформаційних загроз.

## АНТИВІРУСИ

Антивірусне програмне забезпечення (ПЗ) потрібно для захисту комп'ютера від вірусів, хакерів, спаму, шпигунського ПЗ, дозвонників і т.ін. Програму необхідно регулярно оновлювати з метою забезпечення максимального захисту.

### **Приклади антивірусів:**

- Kaspersky Internet Security [http://www.kaspersky.ru/kaspersky\\_internet\\_security](http://www.kaspersky.ru/kaspersky_internet_security) (можливо налагодити батьківський контроль, якщо створити окремий профіль для дитини та задати їйому параметри обмеження),
- Panda Internet Security 2009 <http://www.detionline.ru/ally.htm> (запобігає доступу до небажаного веб-контенту),

- ESET Smart Security 4 <http://eset.ua/products/home-computers/eset-smart-security> (можна налагодити персональний брандмауер).

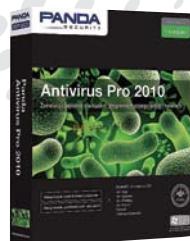
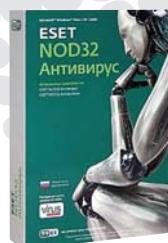
## **Батьківський контроль для ПК**

Будьте обізнатими батьками – встановлюйте спеціальні програми батьківського контролю, що пропонують розробники. Наприклад:

- Net Nanny <http://www.netnanny.com/>,
- Safe Eyes <http://www.internetsafety.com/safe-eyes-parental-control-software.php>,
- Crawler Parental Control <http://www.crawlerparental.com/>,
- CCT Internet Filter Home <http://www.controlchaostech.com/index2.php?menuid=20&prodid=53>,
- КіберМама <http://www.cybermama.ru/>,
- додаток для інтернет-браузерів Parental Control Bar <http://www.parentalcontrolbar.org/>.

В усіх цих прикладах йдеться про так званий «чорний список» заборонених ресурсів, що блокуються від відвідування. Проте прослідкувати за їх оновленнями та по-передити доступ до всіх небезпечних сайтів практично неможливо. Існує альтернатива – «білий список», тобто перелік безпечних, рекомендованих для дітей сайтів. Для того, щоб підібрати найпростіший й найбільш ефективний засіб захисту, можна спробувати як безкоштовні програми, так і демо-версії платних.

Спеціалісти «Київстар» разом з Інститутом психології ім. Г.С. Костюка Національної академії педагогічних наук України та за участі громадськості розробили список рекомендованих сайтів для дітей. Він враховує основні інформаційні потреби дітей різних вікових груп в освіті, розвитку, спілкуванні та розвагах. Спираєтесь на цей перелік, щоб створити для дитини територію безпечного інтернету. Наприклад, використовуйте безпечні пошукові системи для дітей: <http://www.gogul.tv>, <http://search.icensor.ru>, <http://quinturakids.com> (англійською мовою). Ресурси постійно проходять моніторинг й оновлення в режимі онлайн, тому ознайомитися з найбільш повною та актуальною версією списку можна на тематичному розділі <http://online-bezpeka.kyivstar.ua>.



# ЕКСПЕРТИ РЕКОМЕНДУЮТЬ: ПОРАДИ З ІНТЕРНЕТ-БЕЗПЕКІ

## ЯК ЗАХИСТИТИ ДИТИНУ

### **Загальні поради**

- Не встановлюйте комп’ютер у кімнаті дитини. Найкраще віддати перевагу розташуванню комп’ютера у кімнаті загального користування. Так буде легше здійснювати контроль за діяльністю дитини в інтернеті та обмежувати час її перебування за комп’ютером.
- Нормуйте час перебування дитини за комп’ютером. Не дозволяйте дитині довго засиджуватися за комп’ютером перед сном і вночі.
- Використовуйте програмне забезпечення, що відключає ПК після закінчення визначеного часу (Time-Scout). Якщо дитина багато часу проводить за комп’ютером, вона не отримує необхідних навичок для повноцінного розвитку, потрібних їй у реальному житті.
- Пам’ятайте – надмірне сплікування у Мережі може спричинити кіберкомунікативну залежність, а захоплення комп’ютерними іграми – перерости в ігromанію. Тому у дитини мають бути альтернативні інтереси та обов’язки (наприклад, догляд за тваринами, поливання квітів, прибирання своєї кімнати та ін.).

### **Онлайн-ігри**

- Уважно спостерігайте за тим, чим займається ваша дитина і слідкуйте за іграми, в які вона грає. Рольові ігри справляють найбільш сильний вплив на психіку. Надмірне захоплення рольовими іграми може негативно позначитися на формуванні особистості дитини, її соціалізації та рольовій ідентифікації. Тому не дозволяйте їй тривалий час грati в одну гру.
- Якщо дитина любить грati в комп’ютерні ігри, можна запропонувати їй цікаві навчальні та розвиваючі програми. У випадку, коли інтерес дитини зосереджено на рольових іграх, можна привабити її участю в шкільних театральних виставах або психологічних тренінгах для підлітків.
- Коли дитина продовжує надмірно захоплюватися комп’ютерними іграми та інтернетом і ви не взмозі самостійно впоратися з проблемою, зверніться до спеціаліста-психолога.

Безпека і правила поведінки в Мережі мають формуватися з урахуванням віку і психологічних особливостей дітей. Відсутність вольового та емоційного контролю, імпульсивність поведінки властиві дітям. Чим молодший вік, тим більше уваги слід приділяти спільному використанню інтернету. З підвищенням рівня самоконтролю дитини поступово знижується потреба в батьківському контролі.

## ЯКЩО ВАШІЙ ДИТИНІ ВІД 5 ДО 7 РОКІВ

**У дошкільному віці найважливішою потребою дитини є спілкування, завдяки якому вона засвоює соціальний досвід. Стосунки з дорослими та однолітками формують особистість. Спілкування відіграє важливу роль у житті дитини, адже саме так вона набуває досвід співпраці, взаєморозуміння і формує повагу до інших людей<sup>13</sup>.**

Потреба в зовнішніх враженнях сприяє розвитку пізнативальних здібностей та уяви. Діти цього віку намагаються виявляти самостійність і розширювати знання про оточуючий світ. Задаючи нескінчені питання, дитина, перш за все, хоче чути відповіді на них. Неуважне ставлення з боку дорослих може стати причиною появи впертості, неслухання і негативізму. Тому якщо ви не хотите, щоб важливу інформацію дитина дізналася з неперевірених джерел (у тому числі, з інтернету), приділяйте більше уваги своїй дитині.

Провідною діяльністю дошкільників є гра. Саме тому діти дуже люблять грati, зокрема, в комп'ютерні ігри. Незважаючи на користь ігор, особливо розвиваючих та навчальних, слід пам'ятати, що частка розважальних ігор у житті дитини не повинна превалювати, оскільки це може викликати нерівномірність розвитку, затримку формування готовності до навчання і навіть спричинити комп'ютерну залежність.



У дошкільному віці дитина засвоює правила поведінки і вчиться оцінювати власні вчинки та дії оточуючих крізь призму моральних норм, що формуються у спілкуванні з дорослими. Саме цей період є найважливішим для навчання правилам поведінки і безпеки в Мережі. При цьому слід пам'ятати, що, незважаючи на знання певних правил, діти можуть порушувати їх, тому необхідність батьківського контролю для дітей молодшого віку дуже висока.

**Маленькі діти повинні виходити в інтернет лише під наглядом дорослих ще й тому, що їм потрібна допомога в навігації під час пошуку сайтів і при спілкуванні.**

### Для підвищення безпеки Вашої дитини:

- Створіть список Вибраного з адресами перевіреніх сайтів.
- Навчіть дитину правилам конфіденційності і поведінки в Мережі.
- Роз'ясніть дитині те, для чого і як правильно створювати нікі. Придумайте разом з дитиною нік, у якому не міститься особиста інформація про неї, і bezpechnyj parol'.
- Розкажіть дитині, що в Мережі люди можуть видавати себе за кого завгодно, тому слід ставитися обережно до нових віртуальних знайомих і в жодному разі не повідомляти їм будь-яку особисту інформацію.
- Використовуйте пошукові сервіси, призначенні спеціально для дітей.
- Створіть спеціальне робоче середовище для дитини з обмеженим списком дозволених сайтів.
- Використовуйте спеціальне сучасне програмне забезпечення для контролю ресурсів, що відвідує Ваша дитина.
- Користуйтесь програмами батьківського контролю.
- Користуйтесь інформаційними фільтрами.
- Використовуйте засоби блокування небажаного контенту.
- Застосуйте функції блокування вікон, що вспливають.
- Виключіть можливість використання дитиною служб миттєвого обміну повідомленнями, електронної пошти та чатів.
- Не дозволяйте дитині користуватися голосовими службами для взаємодії з товаришами по мережевим іграм.
- Навчайте дитину відрізняти правду від брехні.
- Проявляйте зацікавленість до віртуального життя дитини і не ігнорируйте запитання, що вона ставить. Якщо не знаєте відповідей на якісь запитання, можете спільно пошукати їх в інтернеті.
- Хваліть дитину, якщо вона чинить правильно, і спокійно роз'яснююте, що потрібно робити і як себе вести, якщо вона помиляється.

- Довірливі стосунки дозволяють вам вжити своєчасних заходів у випадку виникнення ситуації, що загрожує безпеці вашої дитини.

## ЯКЩО ВАШІЙ ДИТИНІ ВІД 8 ДО 10 РОКІВ

У молодших школярів зберігається висока потреба в грі, русі та в зовнішніх враженнях. Саме остання є основною рушійною силою, завдяки якій виникають нові потреби: в оволодінні знаннями, вміннями та навичками.

**Діти цього віку прагнуть самостійно досліджувати навколошній світ, задовольняючи інтерес до пізнання, зокрема і за допомогою інтернету.**

У молодшому шкільному віці розвиваються мотиви поведінки, моральну складову яких формують ідеали. В якості таких ідеалів виступають герої фільмів, книг, ігор. Характерною особливістю наслідування є копіювання зовнішнього боку вчинків героїв, оскільки, незважаючи на правильний аналіз змісту цих вчинків, дитина може не співвідносити їх з власною поведінкою.



Контроль за діяльністю дитини в інтернеті має бути досить високим.

Основним видом діяльності у молодших школярів є учебова діяльність, головним авторитетом в якій виступає педагог. До десяти років на перший план виходять стосунки з товаришами та однокласниками, що підкріплюються моральною оцінкою їх поведінки. Створюються угруповання, що об'єднують дітей за інтересами. Спілкування в інтернеті стає для них важливим і сприяє соціалізації. Зазнає змін й емоційно-вольова сфера дитини, починають розвиватися інтелектуальні та естетичні почуття. У віковий період 8-10 років особливий інтерес викликають рольові та логічні ігри, а також ігри, що мають характер змагання. У цьому віці дитина легше засвоює складний навчальний матеріал. Допомогти тут може використання навчальних і розвиваючих програм.

### **З метою підвищення безпеки Вашої дитини:**

- Розташуйте комп’ютер у загальній кімнаті, щоб легше здійснювати контроль щодо по-водження дитини з комп’ютером.
- Користуйтесь програмами батьківського контролю.
- Вживаєте спеціальне сучасне програмне забезпечення для контролю ресурсів, що відвідує ваша дитина.
- Використовуйте інформаційні фільтри.
- Застосовуйте засоби блокування небажаного контенту.
- Застосовуйте функції блокування вікон, що вспливають.
- Встановіть програму, що обмежує час роботи за комп’ютером.
- Створіть профілі для всіх членів сім’ї за допомогою служби сімейної безпеки.
- Створіть список Вибраного з адресами перевірених сайтів.
- Проконтролюйте нік дитини, щоб виключити наявність у ньому особистої інформації та роз’ясніть, що в інтернет-просторі перебувають люди, які можуть використати особисті дані проти неї. Навчіть дитину вигадувати безпечний пароль і поясніть, що це дозволить їй захистити власну інформацію.
- Навчіть дитину правилам конфіденційності та поведінки в мережі і необхідності їх самостійного дотримання, оскільки діти цього віку вже можуть відвідувати інтернет у школі або у знайомих, де безпосередній контроль дорослих може бути відсутнім.
- Заходьте в інтернет разом з дитиною та навчайте її практичному застосуванню отриманих знань з безпеки в Мережі.
- Використовуйте пошукові сервіси, призначенні для дітей.
- Розповідайте дитині, що в Мережі досить часто знаходяться не ті особи, за яких вони себе видають, тому не слід довіряти новим знайомим, не можна повідомляти їм будь-яку особи-

сту інформацію, в жодному разі не можна зустрічатися з ними у реальному житті.

- Не дозволяйте дитині користуватися голосовими службами для взаємодії з мережевими ігроками.
- Якщо дитина спілкується в чатах і користується службами миттєвого обміну повідомленнями, розкажіть їй про те, які небезпеки очікують на неї, якщо вона не буде дотримуватися правил безпеки. Намагайтесь контролювати спілкування вашої дитини під час користування подібними службами.
- При зустрічі з гриферами навчіть дітей дотримуватися таких правил: ігнорувати атаки кібер-хуліганів, створити замкнену ділянку ігрового простору, змінити параметри гри та віддавати перевагу іграм з суворими правилами і функціями блокування небажаних повідомлень. Якщо ці методи не допоможуть, краще на деякий час змінити гру та повідомити адміністрацію сайта про кібер-хулиганів.
- Розкажіть дитині про ризики, які вона може зустріти у віртуальному просторі, зокрема про вірусі.
- Обмежуйте час перебування вашої дитини за комп'ютером.
- Виявляйте зацікавленість до віртуального життя вашої дитини та не ігнорируйте питання, що від неї надходять. У випадку, коли ви не знаєте відповіді, спробуйте разом з дитиною відшукати її в інтернеті.
- Привчайте дитину ділитися з вами враженнями про відвідання інтернету та розповідати вам про все, що викликало у неї хвилювання.
- Хваліть дитину, якщо вона вчиняє правильно, а якщо вона помилилася - спокійно поясніть, що потрібно робити і як себе поводити.
- Створіть альтернативні інтереси та обов'язки для вашої дитини:

– відвідання кружка за інтересами або спортивної секції;

– хобі;

– прибирання своєї кімнати;

– догляд за тваринами чи домашніми рослинами;

– допомога молодшим у виконанні домашніх завдань і т.ін.

- Довірливі стосунки допоможуть вам вжити своєчасних заходів у випадку виникнення ситуації, що загрожує безпеці дитини.



## ЯКЩО ВАШІЙ ДИТИНІ ВІД 11 ДО 14 РОКІВ

**Підлітковий період є перехідним: відбувається біологічне та статеве созрівання організму, психічний розвиток, виникає новий рівень самосвідомості, відбувається соціалізація особистості.**

Діти молодшого підліткового віку відрізняються гарним засвоєнням інформації, з цікавістю досліджують простір Мережі. Мотивами, що домінують у поведінці дітей даного віку, є: намагання до самостійності і визнання товарищів, розширення власних прав, бажання зайняти гідне місце в групі однолітків. Особливою ролі починає набувати самооцінка особистості. Відбувається формування власної ієрархії цінностей.

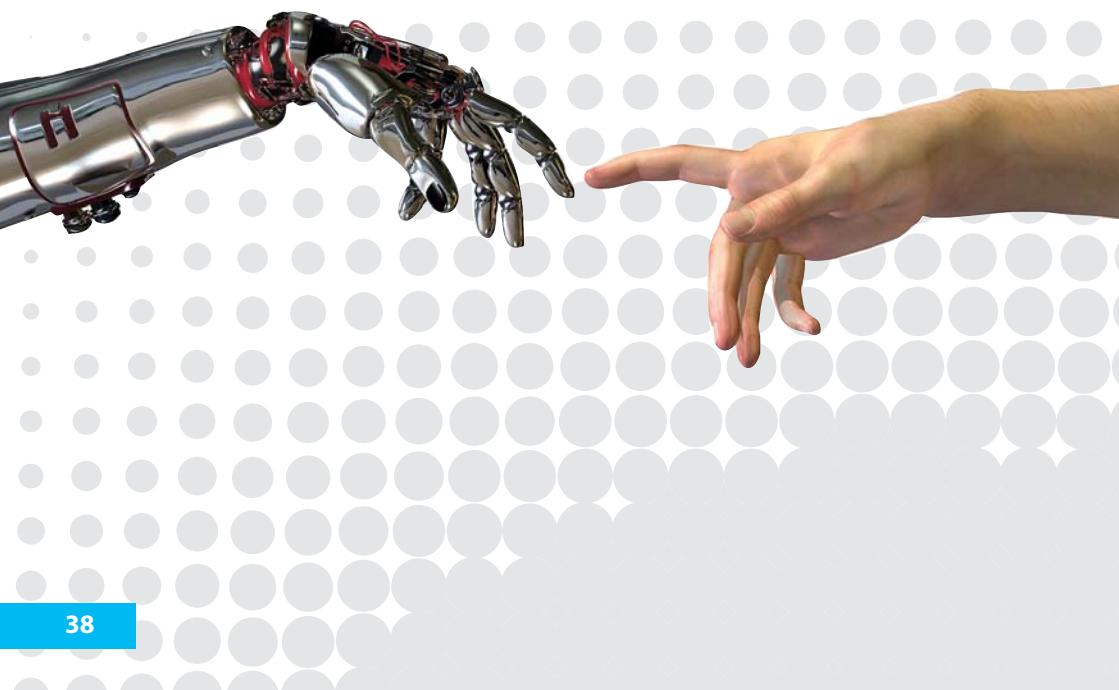
У даний період особливу зацікавленість викликають інтернет-ресурси, що дають змогу підлітку спілкуватися з реальними та віртуальними знайомими, а також розважальні і навчальні ресурси Мережі. Діти періоду дорослішання вже мають знання про те, яка саме інформація міститься в інтернет-просторі та нерідко намагаються дослідити ці ресурси в обхід заборонам батьків.

Прагнення до дослідження інтернету та надто суровий контроль з боку дорослих можуть викликати негативну реакцію дитини і стати причиною приховання її діяльності в інтернет-просторі.

**Діти 11-14 років потребують контролю батьків, але вже виявляють самостійність, тому дуже важливо навчити їх комп’ютерній грамотності та правилам безпечної роботи в Мережі, оскільки вони можуть входити в інтернет у школі, інтернет-кафе чи в товаришів, де зовнішній контроль відсутній. Необхідно розвивати внутрішній контроль дитини і привчати її до відповідальної поведінки в Мережі з метою особистої безпеки.**

- Не разміщуйте комп’ютер в ізольованій кімнаті. Якщо ви розташуете його в загальній кімнаті, легше буде контролювати поведінку дитини за комп’ютером.
- Створіть профілі для всіх членів родини, які користуються інтернетом із застосуванням служби сімейної безпеки.
- Утворіть список Вибраного з адресами перевірених сайтів.
- Створіть для дитини обліковий запис з обмеженими користувальними правами.
- Навчіть дитину правилам конфіденційності та поведінки в Мережі.
- Створіть сімейні правила безпеки і розкажіть, чому їх слід дотримуватися.
- Привчіть дитину з повагою ставитися до людей, яких вона зустрічає в інтернеті.
- Поясніть дитині, що її нік не має містити про неї особистої інформації.
- Навчіть дитину вигадувати безпечні паролі та поясніть, що це дозволить їй захистити власну інформацію й підвищити безпеку.

- Розкажіть дитині про ризики, які вона може зазнати виходячи в інтернет-простір, зокрема про віруси та програми-шпигуни.
- Поясніть, що в інтернеті, крім звичайних людей, можуть знаходитися авантюристи та злочинці, які здатні використати її особисті дані для злочинних дій.
- Розкажіть дитині, що зустрічатися з віртуальними знайомими в офлайні може бути небезпечним.
- Навчіть дитину розповідати вам про своїх знайомих у Мережі та обговорюйте з нею питання, що її зацікавили.
- Використовуйте спеціальне програмне забезпечення для контролю ресурсів, які відвідує дитина.
- Встановіть програму батьківського контролю.
- Використовуйте засоби блокування небажаного контенту. Застосовуйте функції блокування вікон, що вспливають.
- Обов'язково застосовуйте програми фільтрації веб-контенту.
- Встановіть програму, що обмежує час роботи на комп'ютері.
- Складши довірливі, дружні стосунки з дитиною, ви зможете краще контролювати її активність у Мережі, підвищивши, тим самим, рівень її безпеки.



## ЯКЩО ВАШІЙ ДИТИНІ ВІД 15 ДО 18 РОКІВ

**У цьому віці підліткам властива емоційна нестійкість, підвищена вразливість, необ'єктивне сприйняття дійсності, вони склонні до ідеалізації почуттів дружби, любові та сексуальних стосунків.** Для осіб цього віку характерні переживання, пов'язані з власною зовнішністю, прийняттям їх однолітками, визнанням оточуючими їх здібностей і вмінь. Зміни в поведінці викликані гормональною перебудовою організму та психологічними змінами, прагненням до самопізнання, самоствердження і самостійності. Криза інтересів є схожою та суттєвою проблемою підліткового віку. Дитина по-новому починає дивитися на навколишнє – предмети, явища, людей, світ у цілому. Відкриття нових сторін речей і процесів викликає нові потреби, мотиви, бажання, інтереси, цінності<sup>14</sup>.

Підлітки шукають себе, тому нерідко страждають від почуття самотності і не відчувають себе членами суспільства. Слід відзначити, що пошук власного кола спілкування підлітком йде паралельно його психологічному відокремленню від батьків. У кіберпросторі вони задовольняють свою потребу в спілкуванні і знаходять друзів<sup>15</sup>.

**Підлітки 15-18 років технічно освічені та добре орієнтуються в інтернеті. Незважаючи на самостійність і незалежність, вони все ж потребують нагадування про необхідність дотримання правил поведінки в Мережі та заходах безпеки.**

- Комп'ютер слід розташовувати в кімнаті загального користування.
- Розкажіть дитині про правила конфіденційності і поведінки в Мережі та її особисту відповіальність.
- Повідомте про ризики, яких вона може зазнати, відвідуючи інтернет.
- Дитина має вміти орієнтуватися у просторі Мережі, правильно користуватися пошуковими сервісами, відсіювати небажані електронні повідомлення і за жодних обставин не надавати про себе в Мережу особисту інформацію.
- Навчіть, як правильно себе поводити у випадках зустрічі з шахрайством та іншими фактами порушення закону.
- Привчіть поважати авторські права інших людей.
- Поясніть, що скачуючи з інтернету файли аудіо-, відео- або текстового форматів, вона може не тільки порушити закон, а й завантажити вірус чи програму-шпигуна на власний комп'ютер.
- Створіть сімейні правила безпеки і роз'ясніть причини необхідності дотримання встановлених внутрішніх правил.
- Виявляйте інтерес до віртуального життя дитини, обговорюйте з нею її інтернет-враження

та цікавтеся знайомими з Мережі.

- Обговорюйте з дитиною питання здорових статевих стосунків і сексу. Це дасть можливість дещо послабити її цікавість і підготувати до правильної реакції, якщо вона випадково потрапить на ресурси з дорослим змістом.
- Розкажіть дитині про ризики спілкування у приватному режимі.
- Навчіть дитину уважно ставитися до інформації, яку вона отримує з інтернету, щоб вона вміла відрізняти правду від брехні.
- Розповідайте про різноманітні способи перевірки інформації.
- Наполягайте на відвіданні модеруємих ресурсів інтернету.
- Привчіть дитину не зустрічатися зі знайомими по Мережі в офлайні, а якщо така проблема все ж таки виникне, проконтролюйте її нові контакти.
- Навчіть дитину радитися з вами перш ніж здійснити покупку через інтернет.
- Намагайтесь бути ознайомленими з сайтами, які відвідує ваша дитина. Це надасть можливість здійснювати певний контроль за діяльністю дитини в Мережі та зменшить вірогідність потрапляння до інтернету особистої інформації про неї та її близьких.



## КОРИСНІ РЕСУРСИ

### «ГАРЯЧІ» КОНТАКТИ З ІНТЕРНЕТ-БЕЗПЕКИ

#### **1. Спеціальний розділ сайту компанії «Київстар» із захисту дітей від негативного контенту.**

Проконсультуватися з експертом з онлайн-безпеки можна на сайті <http://online-bezpeka.kyivstar.ua>, де кваліфіковані спеціалісти дадуть відповіді на Ваші питання.

#### **2. Електронна гаряча лінія з протидії дитячої порнографії в інтернеті «Ла Страда-Україна».**

Повідомити про випадки дитячої порнографії в інтернеті можна за допомогою форми на головній сторінці [www.internetbezpeka.org.ua](http://www.internetbezpeka.org.ua)

Головною метою роботи ресурсу є блокування розповсюдження дитячої порнографії, особливо на серверах українських інтернет-провайдерів. Гаряча лінія функціонує на базі Міжнародного жіночого правозахисного центру «Ла Страда-Україна».

#### **3. Національна «гаряча лінія» з питань протидії домашньому насильству і захисту прав дітей.**

Звернувшись на гарячу лінію за телефоном 0 800 500 335 (безкоштовно для дзвінків із стаціонарних телефонів на території України), або 386 (безкоштовно для дзвінків з телефонів мобільних операторів «Київстар» і «МТС») чи електронною поштою на [info@lastrada.org.ua](mailto:info@lastrada.org.ua), [onlandia@live.com](mailto:onlandia@live.com), можна одержати такі консультації:

- Правила безпечної поведінки дітей під час користування інтернетом.
- Поради батькам з безпечної роботи дітей в інтернеті.
- Попередження комп'ютерної залежності і можливість отримання психологічної допомоги.
- Юридичні консультації стосовно злочинів проти дітей в інтернеті.
- Допомога у випадках або підозрах загрози дітям через інтернет.

Гаряча лінія працює на базі Міжнародного жіночого правозахисного центру «Ла Страда-Україна» за інформаційної підтримки проекту «Онляндія».

#### **4. Проект із протидії незаконним матеріалам в інтернет-просторі України Skarga.ua**

Кожний користувач українських інтернет-порталів може сповістити про мате-

ріали, що порушують законодавство країни та містять порнографію з участю неповнолітніх, прояви расової і національної нетерплячості, вияви тероризму, заклики до насильницької зміни конституційного ладу за допомогою форми на головній сторінці <http://skarga.ua/>

Проект створений Інтернет-Асоціацією України.

## **5. Телефон Довіри МВС України**

Телефон довіри Департаменту МВС: (+380 44) 254-76-04.

Повідомити про веб-сайти, що пропагують насильство і жорстокість або розпалюють ненависть, расову дискримінацію, займаються створенням чи розповсюдженням дитячої порнографії можна в Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми МВС України.

Дізнайтесь більше: корисні ресурси

### **Відвідайте українські та закордонні сайти для батьків з онлайн-безпеки:**

1. <http://online-bezpeka.kyivstar.ua/> «Безпека дітей в інтернеті» – спеціальний розділ сайту «Київстар»
2. <http://www.onlandia.org.ua/> Портал «Онляндія — безпека дітей в інтернеті».
3. <http://www.detionline.ru/> «Дитина в Мережі»
4. <http://saferunet.ru/> Російський сайт, присвячений безпеці дітей в інтернеті.
5. <http://www.icmec.org/> Міжнародний центр захисту дітей від експлуатації та викрадення.
6. <http://www.lastrada.org.ua/> Міжнародний жіночий правозахисний центр «Ла Страда-Україна»
7. <http://www.ecpat.net/> ECPAT (End Child Prostitution, Child Pornography and Child Trafficking for sexual purposes) International (англійською мовою)
8. <http://www.teachtoday.eu/> Teach Today (англійською мовою)
9. <http://www.make-it-safe.net/> Make-IT-safe Campaign (англійською мовою)
10. <http://www.thinkuknow.org/> Think U Know Initiative (англійською мовою)
11. <http://www.inhope.org/> INHOPE – Асоціація інтернет-провайдерів «гарячих ліній» (англійською мовою)
12. <http://www.nachalka.com/bezopasnost> Розділ сайту Началка.ру дає поради з онлайн-безпеки для батьків і вчителів.
13. <http://www.netpolice.ru/> Сайт NetPolice популяризує безпечний та ефективний доступ до інтернету для дітей і підлітків.

## ВИНОСКИ

<sup>1</sup> За підрахунками Internet World Stats.

<sup>2</sup> Результати дослідження gemiusAudience «Do you CEE? – Тенденції країн Центральної і Східної Європи у 2006-2009рр.»

<sup>3</sup> Інтерент-асоціації України (ІнАУ) використовують дані компанії InMind (12,6 млн. чол., другий квартал 2010р.), а Українська асоціація інтернет-реклами (УАІР) - дані Gemius і GFK(8,25 млн. чол., осінь 2009р.).

<sup>4</sup> В Україні спостерігається найбільший стрибок зросту у період з 2006 по 2009 роки – 84% (дані дослідження gemiusAudience).

<sup>5</sup> Координатор відділу Ради Європи з питань медіа і інформаційної спільноти Лі Хіббарда // «Кореспондент», 02.02.2010р.

<sup>6</sup> Бугайова Н.М. Ризики сучасних комп'ютерних технологій: ігрова залежність. //Інформаційні технології в наукових дослідженнях і навчальному процесі: Матеріали II Міжнародної науково-практичної конференції, м.Луганськ, 14-16 листопада 2006.

<sup>7</sup> Дослідження Symantec 2009р. Рейтинг дитячих пошукових запитів в інтернеті. Режим доступу: [http://www.infox.ru/hitech/internet/2009/12/21/Opublikovan\\_reyeting.shtml](http://www.infox.ru/hitech/internet/2009/12/21/Opublikovan_reyeting.shtml)

<sup>8</sup> Orzack M.H. Computer addiction: What is it?//Psychiatric Times. – August.-1998, V.15, N8.

<sup>9</sup> Young K.S. Internet addiction: The emergence of a new clinical disorder//CyberPsychology and Behavior.- 1998, V.1, P.237-244.

<sup>10</sup> Кримінальний Кодекс України, ст.301. Закон України №1819-VI, документ 1819-17 «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії».

<sup>11</sup> Кримінальний Кодекс України, ст.190.

<sup>12</sup> Особлива частина Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку», ст. 361, 361-1, 361-2, 363-1.

<sup>13</sup> Болтівець С.І. Педагогічна психогієна: теорія та методика: Монографія. — К.: Редакція «Бюлетеня Вищої атестаційної комісії України», 2000.

<sup>14</sup> Максименко С.Д. Генеза здійснення особистості. К.: Вид-во ТОВ «КММ», 2006.

<sup>15</sup> Чепа М.-Л. Пять великих тайн исторической психологии.– К.: «Школьный мир», 2005.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- Максименко С.Д. Генеза здійснення особистості. К.: Вид-во ТОВ «КММ», 2006.
- Максименко С.Д.. Загальна психологія. 3-е видання. Перероблене та доповнене. Навчальний посібник.– К.: «Центр учебової літератури», 2008.
- Максименко С.Д. Психологія у соціальній та педагогічній практиці. Методологія, методи, програми, процес– К., 1998.
- Максименко С.Д. Психологічне здоров'я дітей. В кн.: Авторські програми з психології.– К.: «Шкільний світ», 2002.
- Максименко С.Д., Чепа М.-Л.А., Бугаєва Н.М. Трансформационные механизмы нужды в зависимость: генетико-моделирующий метод прогнозирования аддикций в онтогенезе. Конференция «Экспериментальная психология в России: традиции и перспективы», Москва, 2010.
- Максименко С.Д., Максименко К.С., Папуча М.В. Психологія особистості.– К.: Вид-во ТОВ «КММ», 2007.
- Максименко С.Д., Кокун О.М. Теоретико-методологічні засади психологічного обґрунтування заходів пропагування серед молоді здорового способу життя / С.Д. Максименко // Практична психологія та соціальна робота. - 2009. - № 8. - С. 59-63.
- Болтівець С.І. Педагогічна психогігієна: теорія та методика: Монографія. — К.: Редакція «Бюлетеня Вищої атестаційної комісії України», 2000. — 302 с.
- Болтівець С.І. Теоретико-методичні основи психогігієнічного виховання молоді [Текст] // Практична психологія та соціальна робота : науково-практичний освітньо-методичний журнал. - 2009. - N 9. - С. 60-63.
- Болтівець С.І. Вікові особливості періодизації психорегуляційних норм розвитку учнів. // Проблеми загальної та педагогічної психології: 36. наук. пр. Ін-ту психології ім. Г.С.Костюка АПН України /За ред. С.Д.Максименка. – К., 2004. – Т. VI, вип. 8. – С. 33-43
- Болтівець С.І. Духовність і мораль у молодіжному середовищі. Дивосвіт. – 2003. – №2. – С. 24-26
- Болтівець С.І. Педагогічні аспекти психогігієни учня.- К.: Рад. школа. – 1990. – № 5. – С. 66-70
- Болтівець С.І. Как помочь подростку найти свой образ, или психогигиена собственного образа. // Зеркало моды – 2001. – №5 (23). – С. 66-67.
- Чепа М.-Л. Пять великих тайн исторической психологии.– К.: «Школьный мир», 2005.
- Чепа М.-Л.А. Від фізіології до духовності: якісні рівні вікового розвитку. Сборник трудов "Духовно-нравственное развитие личности в многокультурном славянском пространстве" Ростовский государственный педагогический университет. Дата розміщення 23.04.2003.
- Режим доступа: <http://rspu.edu.ru/conferences/religious/Chepa.htm>
- Чепа М.-Л.А. Психологічні особливості формування тютюнозалежності у підлітковому та юнацькому віці. Сучасні підходи до профілактики тютюнокуріння, алкоголізму, наркоманії та СНІДУ. Матеріали конференції. – К.: 2003. – С. 38–39.
- Чепа М.-Л.А., Рождественський Ю.Т. Психологія узалежнень (на прикладі формування тютюнозалежності. Проблеми загальної та педагогічної психології. Збірник наукових праць Інституту психології ім. Г.С. Костюка АПН України. – К.: 2003, Т.В, ч.4.–С. 347–353.

- Чепа М.-Л.А., Чайка Г.В., Пупцева Т.В. Тренування психічних функцій школяра комп'ютерними засобами. Науково-методичний посібник. За ред. М.-Л.А. Чепи. – К., Інститут психології АПН України, 1996.–99 с.
- Бугайова Н.М. Психологічні проблеми інтернет-адикції в умовах використання телекомунікаційних технологій. Розділ 4. Телекомунікаційні технології у навчальному процесі: методичні рекомендації.– Київ, НАП України, 2009.
- Бугайова Н.М. Ризики сучасних комп'ютерних технологій: ігрова залежність. // Інформаційні технології в наукових дослідженнях і навчальному процесі: Матеріали II Міжнародної науково-практичної конференції, м. Луганськ, 14-16 листопада 2006 р. Т.1.- Луганськ, 2006.
- Бугайова Н.М. Психологічні закономірності розвитку адикцій в онтогенезі. Збірник наукових праць Інституту психології ім. Г.С. Костюка НАПН України / За ред. С.Д. Максименка. Т. XII, част. 4. – К., «ГНОЗИС», 2010.
- Бугаєва Н.М. Глобальні риски использования современных телекоммуникационных технологий.– Актуальні проблеми психології: Психологічна теорія і технологія навчання.– К.: Міленіум, 2007.– Т.8, вип. 3.
- Бугайова Н.М. Віртуальні романтичні стосунки в Інтернеті, кіберсексуальна залежність..– Актуальні проблеми психології: Психологічна теорія і технологія.– К.: Університету ім. М.П. Драгоманова, 2008. – Т.8, вип. 5.
- Бугайова Н.М. Інтернет-адикція як форма залежності поведінки. // Теорія та методика навчання математики, фізики, інформатики.– Кривий Ріг, "НМетАУ", 2006. - Т.3, вип.VI. - 408 с. (7 стор. – 0,3).
- Бугайова Н.М., Цап В.Й. Профілактика Інтернет-залежності в перебігу електронного навчання: збірник наукових праць. Випуск I.– Кривий Ріг: Видавничий відділ НМетАУ, 2010.
- Войскунский А.Г. Психологические исследования феномена Интернет-аддикции. Режим доступа: <http://psynet.carfax.ru/texts/voysk4.htm>
- Егоров А.Ю. Нехимические зависимости.– СПб.: «Речь».- 2007.- 190°c.
- Котляров А.В. Другие наркотики или Homo Addictus: Человек зависимый.– М.: Психотерапия.- 2006.- 480 с.
- Старшенбаум Г.В. Аддиктология: психология и психотерапия зависимостей.– М., изд. "Когито-Центр", 2005.
- Marks I. Behavioural (non-chemical) addictions//British J. Addict.- 1990, V.85. - P.1389–1394.
- Orzack M.H. Computer addiction: What is it?//Psychiatric Times. – August.-1998, V.15, N8.
- Young K.S. Internet addiction: The emergence of a new clinical disorder//CyberPsychology and Behavior.- 1998, V.1, P.237-244.

# ДІТИ В ІНТЕРНЕТІ: ЯК НАВЧИТИ БЕЗПЕЦІ У ВІРТУАЛЬНОМУ СВІТІ

## КОРОТКА ПАМ'ЯТКА ДЛЯ БАТЬКІВ

- Підвищуйте власну комп'ютерну та інтернет-обізнаність.
- Станьте для своєї дитини другом і порадником, опановуйте інтернет разом.
- Оберіть найбільш прийнятний спосіб технічного захисту: від регулярно поновлюваного антивірусу до спеціального програмного забезпечення, що забезпечує батьківський контроль на комп'ютері та мобільному телефоні дитини.
- Створіть територію безпечного інтернету. Запропонуйте дітям пізнавальні, цікаві та захоплюючі інтернет-ресурси. Щоб захистити дітей від ризиків віртуального світу, використовуйте поновлюваний список рекомендованих сайтів для дітей на <http://online-bezpeka.kyivstar.ua/>

### *Сімейна онлайн-безпека – відповіальність кожного Навчіть дитину правилам безпечної роботи у Мережі:*

#### **1. Роз'ясніть дитині важливість захисту своєї та чужої конфіденційної інформації:**

- не можна викладати в інтернет інформацію про сім'ю та її фінансові справи, адреси проживання та навчання, номери телефонів, кредитної картки та банківські дані;
- нікому, крім батьків, не можна називати власні паролі до інтернет-сервісів (навіть найкращим друзям).

**2. Навчіть дітей поводитися в інтернеті так само, як у реальному житті.** У Всесвітній Мережі дитина має поводитися ввічливо, не робити нічого, що може образити інших людей або суперечити закону. Поясніть дітям, що в інтернеті також слід із повагою ставитися до людей та їх авторських прав. Незаконне копіювання та розповсюдження матеріалів, що є чиєюся власністю, вважається крадіжкою.

**3. Віртуальний співрозмовник може видавати себе за іншого.** Навчіть дитину не надто довіряти незнайомим людям у Мережі. Дитина повинна знати, що не можна призначати зустріч з віртуальними знайомими без дозволу батьків.

**4. Віртуальний світ іноді коштує реальних грошей.** Завжди потрібно з'ясовувати, скільки коштують спеціальні інтернет-сервіси: наприклад, якою є повна вартість SMS в онлайн-грі. Якщо така інформація не очевидна для дитини, вона має звертатися за порадою до Вас. Допомагайте дітям розібратися, скільки насправді коштують такі SMS-послуги та чи дійсно необхідно їх надсилати.

**5. Звертатися за порадою – необхідно.** Повідомте дитині, що вона може звернутися до Вас у будь-якій ситуації. Якщо в інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось не зрозуміло, хвилює або загрожує, дитина завжди має звертатися по допомозу до Вас. Інформація та послуги в інтернеті не завжди безпечні, тому перш ніж завантажувати, копіювати чи встановлювати будь-що з інтернету, дитина має отримати Ваш дозвіл. Навчіть перевіряти інформацію з Мережі за допомогою додаткових запитів і звернення до перевіреніх джерел.