**ПАМ'ЯТКА ДЛЯ БАТЬКІВ:**

**КІБЕРБЕЗПЕКА**

В епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у ХХІ столітті будуть одними з найчисельніших.

В Україні та в усьому світі щороку вчиняються десятки тисяч злочинів з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. Щодня у людей та компаній крадуть персональні дані, кошти з рахунків, збирають безліч конфіденційної та комерційної інформації, блокують діяльність тощо.

#### З ЯКОГО ВІКУ ГОВОРИТИ З ДИТИНОЮ ПРО КІБЕРБЕЗПЕКУ ТА ЯКІ ПРАВИЛА ВСТАНОВИТИ

Починати говорити з дітьми про кібербезпеку треба одразу, коли ви даєте їм користуватися телефоном чи комп’ютером. У когось це може бути в 3 роки, у когось – у 7. Однак треба врахувати, що дитина, яка не має гаджета, може контактувати з тими, у кого він є. І тоді про це також треба говорити.

Залежно від віку, ми можемо розповідати дітям, які ризики є й чому вони саме такі. Кожен етап розповіді відповідатиме етапу розуміння дитини. Наприклад, коли дитина розуміє цінність грошей, можна говорити про інтернет-банкінг і чому треба ставити надійний пароль. Коли дитина розумітиме цінність приватної інформації, можна говорити з нею про це.

Як учителі, так і батьки можуть обговорити з дітьми такі правила в кіберпросторі:

* **Ти спілкуєшся не з пристроями, а все ж таки з людьми через пристрій.**На іншому боці може бути хто завгодно, навіть якщо тобі пише хтось, хто здається знайомим.
* **Те, що ти розмістиш в інтернеті чи відправиш у повідомленні, автоматично стає не твоїм**. Тому треба донести дитині, що таке цінна інформація та чому її не варто нікому надсилати.
* **Усе, що ти отримав, але не очікував отримати, – підозріло.** Тебе можуть обманути.
* **Безплатний сир – лише в мишоловці.**Гроші просто так не даються. Якщо в тебе є потреба в грошах, краще скажи про це дорослим, яким довіряєш.
* Якщо ти в чомусь сумніваєшся,**проконсультуйся зі мною**, дорослим.
* Ще одним правилом може бути, наприклад, не натискати (або не тицяти) на сайти з доменом “.ru”.

Найбільша проблема кіберпростору така: у пересічних громадян є відчуття, що у випадку загрози вони можуть просто розв’язувати цю проблему, вимкнувши цей-таки телефон чи комп’ютер. Утім, ця думка – хибна. Тож ми маємо розуміти правила поведінки в кіберпросторі та навчитися з цим жити.

Насправді **ми маємо перенести до кіберпростору ті самі правила, якими користуємося в житті.** Наприклад, мити руки, не спілкуватися з незнайомими людьми, прибирати за собою, бути ввічливими, перевіряти перед тим, як купувати тощо.

Єдина різниця між цими правилами у звичайному житті та кіберпросторі полягає в тому, що **доступність вас як об’єкта збільшилася.** Тобто, з одного боку, утворився новий цікавий простір, а з іншого – попри оманливе відчуття безпеки, ви стали доступними для всіх.

Коли ви купуєте дитині телефон, уявіть, що вона поринає в цей уявний простір, а там – цукерки перемішані з брудом, безліч поганців та вірусів. І це все треба вміти фільтрувати. Сучасна людина має значно більше викликів у кіберсвіті. Зокрема, в інтернеті діти можуть піддаватися трьом найголовнішим загрозам: ***шахрайству***, ***вимаганню*** та ***цькуванню***.

Пам’ятайте, що світ живе в еру інформаційних технологій, коли можливості мережі є не лише приємним джерелом можливостей, знань та спілкування, але й джерелом підвищеної небезпеки бути «відкритою книгою», якщо вами зацікавляться певні особи.

**ЩО РОБЛЯТЬ ПІДЛІТКИ В ОН-ЛАЙНІ**

Відомо, що підлітки у період заниженої самооцінки шукають підтримки серед своїх друзів, а не у родинному колі. Старші підлітки, бажаючи незалежності, мають потребу ототожнювати себе з певною групою й схильні порівнювати цінності своєї сім’ї та своїх товаришів.

В он-лайні підлітки завантажують музику, використовують обмін миттєвими повідомленнями, електронну пошту та грають в он-лайнові ігри. За допомогою пошукових серверів підлітки знаходять інформацію будь-якого змісту та якості в мережі Інтернет. Більшість підлітків реєструються у приватних чатах та спілкуються на будь-які теми, видаючи себе за дорослих. Хлопці в цьому віці надають перевагу всьому, що виходить за межі дозволеного: брутальний гумор, насильство, азартні ігри, еротичні та порно сайти. Дівчатам, які мають занижену самооцінку, подобається розміщувати провокаційні фото, вони схильні на фривольні розмови, видаючи себе за дорослих жінок, в результаті чого стають жертвами сексуальних домагань.

**ЯК ЗАБЕЗПЕЧИТИ БЕЗПЕКУ ДІТЕЙ В МЕРЕЖІ ІНТЕРНЕТ**

Пропонуємо декілька рекомендацій, які слід взяти до уваги:

* розміщуйте комп’ютери з Internet-з’єднанням поза межами кімнати Вашої дитини;
* розкажіть дітям про безпеку в Інтернеті. Ви не зможете весь час стежити за тим, що вони роблять в мережі. Їм необхідно навчитися самостійно користуватися Інтернетом безпечним і відповідальним чином;
* поговоріть зі своїми дітьми про друзів, з яким вони спілкуються в он-лайні, довідайтесь як вони проводять дозвілля і чим захоплюються;
* цікавтесь які веб сайти вони відвідують та з ким розмовляють;
* вивчіть програми, які фільтрують отримання інформації з мережі Інтернет, наприклад, Батьківський контроль в Windows\*;
* наполягайте на тому, щоб Ваші діти ніколи не погоджувалися зустрічатися зі своїм он-лайновим другом без Вашого відома;
* навчіть своїх дітей ніколи не надавати особисту інформацію про себе та свою родину електронною поштою та в різних реєстраційних формах, які пропонуються власниками сайтів;
* використовуйте налаштування конфіденційності та управління доступом до вашого розташування. На YouTube, Blogger, в соціальних мережах і на багатьох інших сайтах користувачі можуть розміщувати власний контент. Зазвичай автору надається можливість обмежити доступ до особистого блогу, фотографій, відео та інформації в профілі. Особливо важливо обмежувати доступ до таких даних, як ім’я, адреса або номер телефону, які дитина розміщує на загальнодоступних сайтах;
* зберігайте паролі в таємниці. Нагадуйте дітям, що паролі не можна нікому повідомляти. Також необхідно, щоб для дітей стало звичкою знімати прапорець «Запам’ятати мене» при вході в свій акаунт з комп’ютерів, встановлених, наприклад, у школі, Інтернет-кафе або бібліотеці;
* контролюйте інформацію, яку завантажує дитина (фільми, музику, ігри, тощо);
* цікавтесь чи не відвідують діти сайти з агресивним змістом;
* навчіть своїх дітей відповідальному та етичному поводженню в он-лайні. Вони не повинні використовувати Інтернет мережу для розповсюдження пліток, погроз іншим та хуліганських дій;
* переконайтеся, що діти консультуються з Вами, щодо будь-яких фінансових операції, здійснюючи замовлення, купівлю або продаж через Інтернет мережу;
* встановіть захист від вірусів. Використовуйте і регулярно оновлюйте антивірусне програмне забезпечення. Навчіть дітей не завантажувати файли з файлообмінних сайтів, а також не приймати файли і не завантажувати вкладення, що містяться в електронних листах від незнайомих людей;
* інформуйте дітей стосовно потенційного ризику під час їх участі у будь-яких іграх та розвагах;
* інтернет-залежність є актуальною проблемою, дослідження якої зумовлене запитами суспільства, що пояснюється швидким темпом розвитку комп’ютерних технологій, отриманням вільного доступу все більшої кількості людей до Інтернету. Але якщо батьки разом зі своїми дітьми будуть дотримуватись правил «Безпечного Інтернету» можна уникнути багатьох проблем;
* оцінюйте Інтернет-контент критично. Те, що міститься в Інтернеті, не завжди правда. Діти повинні навчитися відрізняти надійні джерела інформації від ненадійних і перевіряти інформацію, яку вони з находять в Інтернеті. Також поясніть дітям, що копіювання і вставка змісту з чужих веб -сайтів можуть бути визнані плагіатом;
* розмовляйте як з рівним партнером, демонструючи свою турботу про суспільну мораль.

Використовуючи ці рекомендації, Ви маєте нагоду максимально захистити дитину від негативного впливу всесвітньої мережі Інтернет. Але пам’ятайте, Інтернет, це не тільки осередок розпусти та жорстокості, але й найбагатша в світі бібліотека знань, розваг, спілкування та інших корисних речей. Ви повинні навчити свою дитину правильно користуватися цим невичерпним джерелом інформації.



Та найголовніше, дитина повинна розуміти, що Ви не позбавляєте її вільного доступу до комп’ютера, а насамперед, оберігаєте. Дитина повинна Вам довіряти.

#### ПРО ЗАБОРОНИ

Соцмережі та месенджери мають вікові обмеження, які батьки часто ігнорують. Наприклад, до 13 років діти мали б дивитися YouTube Kids, у Telegram можна реєструватися з 16 років, у Viber – з 13 тощо.

Є програми так званого батьківського контролю чи інші додатки, у яких батьки бачать активність дитини в інтернеті. Але батьківський контроль працюватиме, якщо дитина це сприйме та їй пояснять, чому це саме так і чому це треба. Адже діти можуть вигадати мільйон методів, як обійти батьківський контроль. Треба донести дитині важливість. Мовляв, дивись, ми не хочемо тебе обмежити – ми хочемо тебе попередити й убезпечити.

#### ЯКІ МАТЕРІАЛИ МОЖУТЬ ДОПОМОГТИ НАВЧИТИ ДІТЕЙ ПРАВИЛ КІБЕРБЕЗПЕКИ

У пригоді стануть:

1. **Блог *«***[**Хакер, що біжить**](https://styran.com/)», який веде експерт із кібербезпеки **Володимир Стиран**. Він ділиться досвідом і дає корисні поради, як не стати кібержертвою.

Ідеться про підозрілі посилання та пристрої, як вигадати надійний пароль, чому його варто тримати в секреті, навіщо потрібна двофакторна автентифікація, які месенджери безпечні, як працює шифрування даних, чому потрібно встановити антивірус, навіщо робити резервні копії, що таке мобільна безпека та як із нею бути тощо.

1. **Онлайн-курс «Основи кібербезпеки для школярів»**, створений CRDF Global в Україні у співпраці з ГО “Смарт Освіта” та Technomatix. Він повністю безплатний та є у відкритому доступі. Цей курс допоможе відрізнити правду від фейків, розкаже, з ким спілкуватися в інтернеті безпечно, а хто – насправді кіберзлочинець.

Джерело: <https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti/pamyatka-dlya-batkiv-diti-internet-mobilnij-zvyazok>