7 порад для вчителів, як навчити учнів безпечної поведінки в інтернеті

<https://nus.org.ua/articles/7-porad-dlya-vchyteliv-pro-onlajn-bezpeku-ditej/>

*За даними UNESCO, пандемія вплинула на освіту орієнтовно 1,6 мільярда дітей і молодих людей із понад 190 країн. Із переведенням навчання в [дистанційний формат](https://nus.org.ua/tags/383/" \t "_blank) значно зросла кількість часу, який діти проводять онлайн. Це, відповідно, піддає дітей більшій кількості ризиків у цифровому середовищі.*

*Як навчити дитину безпечної поведінки в інтернеті і яких правил дотримуватися самим – читайте в статті “Нової української школи”.*

**НА ЯКІ РИЗИКИ НАРАЖАЮТЬСЯ ДІТИ В МЕРЕЖІ**

За класифікацією дослідницької мережі ЄС “Діти в цифровому середовищі”, є такі ризики для дітей:

* перегляд незаконного або шкідливого контенту;
* кібербулінг;
* неправомірне використання персональних даних дітей, [шерентінг](https://www.youtube.com/watch?v=65jQAeVG5jk&list=PL6RPqDSFS-kPld13DvBwbnsT7QDafw_YF&index=25&ab_channel=%D0%9C%D1%96%D0%BD%D1%96%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D1%97%D1%82%D1%80%D0%B0%D0%BD%D1%81%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8" \t "_blank);
* розсіювання уваги, брак критичного мислення.

Також не варто забувати про такий ризик, як сексуальні зловживання, формами якого є, наприклад, грумінг та секстинг.

[Грумінг](https://zakon.rada.gov.ua/laws/show/994_927#Text) – це умисна пропозиція про зустріч дитині до 18 років через інтернет задля вчинення сексуальних зловживань або виробництва матеріалів, що містять сцени сексуальних зловживань щодо дітей.

[Секстинг](https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti) – це пересилання за допомогою мобільних телефонів повідомлень або знімків сексуального характеру.

Перераховані ризики є реальною загрозою для безпеки дитини не лише в онлайн-середовищі, а й у реальному житті. Що ж робити, аби мінімізувати ризики для дітей у мережі та зробити онлайн-простір безпечнішим?

**ОСВІТНЄ СЕРЕДОВИЩЕ ТА БЕЗПЕКА ДІТЕЙ ОНЛАЙН: КОРОТКО ПРО ГОЛОВНЕ**

Освітянам важливо пам’ятати про два аспекти цифрової безпеки дітей.

**Перший аспект стосується шкільного середовища**. До нього відносять наявність безпечної шкільної мережі, політику школи з онлайн-безпеки дітей. Така політика має бути розроблена в кожній школі, адже адміністрація збирає дані про дітей і відповідає за них.

**Другий аспект стосується постійної комунікації вчителів із дітьми про їхню поведінку в інтернет-середовищі.** Якщо дитина стикається з проблемами або труднощами в інтернеті під час навчання, важливо, щоби вона не боялася розповісти про них учителю та знала, що може отримати допомогу в будь-якій ситуації.

Особливо це актуально, коли навчання відбувається в дистанційному форматі, і діти набагато частіше використовують інтернет для навчання.

Часом вважають, що лише вчителі інформаційних технологій мають турбуватися про безпеку дітей онлайн. Але це не так, адже інтернет використовують на різних уроках, і безпека в ньому має бути наскрізною. Вчителі, які хочуть, щоби як онлайн-, так і очний формати навчання для дітей були ефективними та безпечними з погляду використання технологій, мусять постійно підвищувати свої цифрові компетентності й бути прикладом для дітей, як доречно поводитися в цифровому середовищі.

Нещодавно в Україні за ініціативи Міністерства цифрової трансформації та підтримки Міжнародного союзу електрозв’язку громадська організація МІНЗМІН підготувала переклад українською рекомендацій МСЕ про захист дітей у цифровому середовищі. Ці рекомендації є міжнародними й були підготовлені експертами з усього світу для різних цільових аудиторій. Одна з них – освітяни.

Пропонуємо короткий огляд порад для освітян, як зробити навчання онлайн максимально безпечним для дітей.

**РЕКОМЕНДАЦІЇ ДЛЯ ВЧИТЕЛІВ**

Дотримуйтеся цих правил самі й розкажіть учням:

1. **Переконайтеся, що всі пристрої надійно захищені (паролями) і заблоковані тоді, коли ви ними не користуєтесь.** Якщо вам потрібно вийти з класу, заблокуйте всі пристрої, які використовували, або завершіть сеанс роботи чи вийдіть з облікового запису. Встановіть на всіх пристроях ліцензійну антивірусну програму та стежте за тим, щоби вона регулярно оновлювалася.
2. **Встановіть правила в школі, де й коли можна користуватися мобільними пристроями.**А також правила, що учнів можна фотографувати лише після отримання згоди батьків / опікунів / самих учнів на це. Ці правила мають бути закріплені в шкільній політиці щодо онлайн-безпеки. Така політика має встановлювати ще й порядок реагування на інциденти, пов’язані з безпекою дітей, зокрема, у цифровому середовищі. Так, у школі може бути призначений спеціальний координатор для обліку та реєстрації порушень та інцидентів, пов’язаних з онлайн-безпекою, задля формування цілісного уявлення про наявні в школі проблеми та тенденції, що вимагають уваги.
3. **Забезпечте фільтрацію й моніторинг даних, які передаються через шкільну мережу, встановивши необхідні програми.**Допомогти їх встановити можуть інтернет-провайдери. Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільну мережу. Такі системи фільтрації та контролю контенту допомагають звести до мінімуму передавання неприйнятного (наприклад, насильницького чи порнографічного) контенту в шкільній мережі. А системи фільтрації даних допомагають відстежувати, хто, що, коли й на якому пристрої завантажує. Такий механізм є одним зі способів запобігання кібербулінгу.
4. **Пам’ятайте, що ваші дії та слова в інтернеті можуть вплинути на вашу онлайн-репутацію, а також на репутацію навчального закладу.** Ви як користувач/-ка інтернету залишаєте свій цифровий слід – адже різні сайти, соціальні мережі, платформи, відповідно до своїх політик, збирають дані про вашу онлайн-активність. Перевіряйте інформацію, яку поширюєте в соціальних мережах. Перед тим як опублікувати інформацію, подумайте, хто може її побачити. Розповідайте дітям про важливість онлайн-репутації та як правильно її формувати.
5. **Слідкуйте за своєю професійною комунікацією**. Для будь-яких контактів між працівниками школи, учнями, батьками чи іншими зацікавленими сторонами завжди використовуйте шкільну електронну пошту замість особистої. У деяких випадках кодекс ділової етики, якщо він погоджений у школі, може передбачати заборону на контакти з учнями на платформах, які не мають стосунку до школи. Наприклад, у месенджерах чи соцмережах. Також рекомендується встановити в школі чіткі правила – як для працівників, так і для учнів – щодо проведення відеоконференцій чи занять у віддаленому режимі. Наприклад, правила, який вигляд має мати місце для проведення уроків, наявність фото профіля тощо.
6. **Сприяйте формуванню цифрових навичок та цифрової грамотності дітей.**Говоріть із ними про це на уроках. Намагайтеся включити до навчальних планів аспекти цифрової грамотності. Проводьте заходи в школі про онлайн-безпеку дітей. Водночас, показуйте високий рівень власної цифрової компетентності. І не забувайте проводити регулярну перевірку всіх заходів у школі на дотримання онлайн-безпеки дітей та її можливого удосконалення.
7. **Навчайтеся нового та постійно покращуйте навички цифрової грамотності**. Будьте в курсі того, які ризики на дітей можуть чекати в інтернеті, як діти проводять свій час у мережах. Це допоможе вам краще зрозуміти дітей та встановити з ними довірливі взаємини швидше й легше.

Пам’ятайте, що **інтернет – одночасно й ризик, і можливість для дітей**. Тому освітянам варто робити все можливе, щоби зробити цифрове освітнє середовище максимально безпечним для дітей.

Більше рекомендацій та інформації про безпеку дітей онлайн можна знайти в [рекомендаціях](https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines-for-Parents-Educators-UAfin.pdf" \t "_blank) Міжнародного союзу електрозв’язку.