Сучасний світ важко собі уявити без засобів мас-медіа – преси, телебачення, друкованих джерел, радіо, кіноматеріалів, Інтернету. Сьогодні без телевізора (або навіть декількох телевізорів), CD-плеєра, ноутбука або кабельного чи супутникового телебачення не обходиться жодна сім’я чи то в нашій країні, чи то за кордоном. Діти багато часу витрачають на перегляд фільмів, «надовго зависають» в Інтернеті або годинами готові слухати радіохвилі FM. Для того, щоб гідно орієнтуватися в просторі різноманітних засобів мас-медіа, було створено цікаву науку – медіаосвіту.

   Але медіаграмотними повинні бути не лише діти, а й батьки, які активно беруть участь в освітньому процесі. Медіаосвіта батьків, сьогодні, набуває все більшої актуальності, адже саме батьки повинні надати дітям можливість зрозуміти, як використовуються мас-медіа в суспільстваі, оволодіти навичками використання медіа в процесі комунікації з іншими людьми та забезпечити знаннями про те, як: аналізувати, критично осмислювати та створювати медіатексти.

   Перше, на що потрібно звернути увагу батькам це безпека з використання онлайну. Пропонуємо декілька підказок з безпеки, які слід взяти до уваги батькам, коли вони дають рекомендації з використання онлайну:

1.Створіть список  Правил користування Internet вдома за участю ваших дітей. Туди ви маєте включити типи сайтів з необмеженим доступом, години користування Internet та рекомендації зі спілкування з іншими в онлайні, включаючи чат-кімнати.

2.Тримайте комп'ютери з Internet-з'єднанням у відкритій зоні, поза межами кімнати вашої дитини.

3.Поговоріть зі своїми дітьми про їхніх онлайнових друзів та те, чим вони займаються так, як ви б говорили про будь-яких інших друзів або заняття. Це включає розмови з вашими дітьми про список миттєвих повідомлень і про те, щоб вони не спілкувалися з незнайомцями.

4.Вивчіть інструменти для фільтрування Internet (такі як Батьківський контроль в WindowsVista) як один із додаткових — але не замінюючих методів батьківського контролю.

5.Знайте, які чат-кімнати та дошки повідомлень вони відвідують та з ким розмовляють.

6.Рекомендуйте їм використовувати контрольовані чат-кімнати, та наполягайте на тому, щоб вони залишалися в публічних зонах чат-кімнат.

7.Наполягайте на тому, щоб ваші діти ніколи не погоджувалися зустрічатися зі своїм онлайновим другом.

8.Навчіть своїх дітей ніколи не давати про себе інформацію по електронній пошті, в чат-кімнатах, дошках оголошень, реєстраційних формах і персональних профілях, а також при участі в онлайнових конкурсах.

9.Навчіть своїх дітей не завантажувати програми, музику або файли без вашого дозволу. Спільний доступ до файлів, отримання текстів та картинок з Інтернету може порушувати закони про авторські права.

10. Скажіть своїй дитині розповідати вам про те, що або хто в онлайні примушує її почувати себе незручно або налякано. Будьте спокійними та нагадайте своїм дітям, що у них не виникне проблем, якщо вони про щось вам повідомлять. (Важливо, щоб ваша дитина не думала, що її позбавлять привілеї користуватися комп'ютером). Прочитайте більше про те, як діяти з онлайновими хижаками та кібер-хуліганами.

11.Поговоріть із своїми дітьми про онлайнову порнографію та направте їх на позитивні сайти про здоров'я та сексуальність.

12.Допоможіть дітям захиститися від спаму. Скажіть їм не давати свої адреса електронної пошти, не відповідати на "сміттєву" пошту та використовувати фільтри електронної пошти.

13.Знайте, які сайти відвідують ваші діти. Перевірте, щоб вони не відвідували сайти з агресивним змістом, або самі не розміщали персональну інформацію та фотографії.

14.Навчіть своїх дітей відповідальному та етичному поводженню в онлайні. Вони не повинні використовувати Internet для розповсюдження пліток, хуліганити або загрожувати іншим.

15.Переконайтеся, що ваші діти-підлітки консультуються з вами, перш ніж проводити в онлайні якісь фінансові операції, включаючи замовлення, купівлю або продаж.

16.Обговоріть  онлайнові азартні ігри та їхні потенційні ризики зі своїми дітьми-підлітками. Нагадайте їм, що їхні азартні розваги в онлайні є незаконними.

**Тролінг** — розміщення в Інтернеті (на форумах, у групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати флейм, конфлікти між учасниками, образи, війну редагувань, марнослів'я тощо.

**Флейм** — обмін повідомленнями в [інтернет-форумах](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%84%D0%BE%D1%80%D1%83%D0%BC) і [чатах](https://uk.wikipedia.org/wiki/%D0%A7%D0%B0%D1%82): словесна війна, яка не має жодного стосунку до початкової теми.  
Повідомлення флейму містять особисті образи, і часто направлені на подальше розпалювання суперечки, [сварки](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%BB%D1%96%D0%BA%D1%82). Іноді застосовується в контексті [тролінгу](https://uk.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D0%BB%D1%96%D0%BD%D0%B3), але частіше флейм спалахує просто через образу на віртуального співрозмовника.

**Фішинг** — це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію, наприклад паролі та номери соціального страхування. Вона зазвичай передбачає надсилання повідомлення спаму, яке справляє враження, ніби походить із довіреного джерела, наприклад із банку (це наживка).

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

**Мобінг** — систематичне цькування, психологічний терор, форми зниження авторитета, форма психологічного тиску у вигляді цькування співробітника у колективі, зазвичай з метою його звільнення.

**Кардинґ** — рід шахрайства, при якому проводиться операція з використанням банківської картки або її реквізитів, яка не ініційована або не підтверджена її власником. Реквізити платіжних карток, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також з персональних комп'ютерів  **Кібербулінг** — це новітня форма агресії, що має на меті жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж тощо.