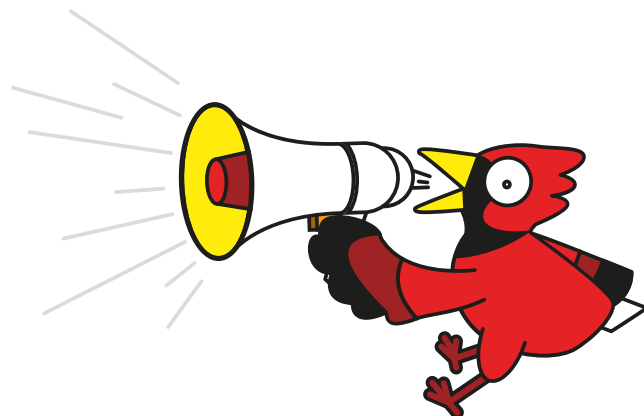


БЕЗПЕКА ОНЛАЙН І БУЛІНГ

СЛОВНИК ТЕРМІНІВ



Булінг — це форма поведінки людини чи групи осіб, що виявляється у постійному і навмисному агресивному ставленні до іншої людини в колективі.

Фішинг — використання повідомлень і дзвінків зловмисником, який видає себе за іншу особу й обманом спонукає жертву виконати певну дію, наприклад, натиснути на шкідливе покликання.

Кібербулінг — це цькування, образи чи погрози, що лунають на адресу дитини за допомогою засобів електронної комунікації (повідомлення у соціальних мережах, миттєві повідомлення, електронні листи, СМС).

Онлайн-грумінг — це побудова дорослим/групою дорослих осіб довірливих стосунків із дитиною з метою отримання її інтимних фото чи відео, щоб надалі шантажувати погрозами розповсюдити ці матеріали.

Секстинг — інтимне листування й обмін фото інтимного характеру.

Мобінг — цькування групою людей.

КОРОТКИЙ ЧЕКЛІСТ ІЗ ОНЛАЙН-БЕЗПЕКИ

☐ **Обмежте публічність особистої інформації**

Приберіть всю особисту інформацію з соціальних мереж. Якщо це неможливо, то приховуйте її від інших користувачів. До особистої інформації належать: ім'я та прізвище, вік, адреси дому та навчального закладу, номери телефонів, електронні пошти тощо.

☐ **Налаштуйте конфіденційність ваших акаунтів у соціальних мережах**

Зайдіть у налаштування своєї сторінки, оберіть дозвіл бачити дописи лише близьким друзям, а також залишати коментарі, робити відмітки на фото чи публікації тощо.



☐ **Додавайте до «друзів» лише друзів**

Додавання у «друзі» відкриває користувачам більше доступу до інформації про вас. Тому краще, аби в «друзях» були лише ті люди, яких ви реально знаєте: родичі, однокласники тощо.

☐ **Налаштуйте двофакторну автентифікацію на своїх акаунтах у соціальних мережах**

Це використання одразу двох різних способів підтвердження входу в акаунт.

Як встановити двофакторну автентифікацію?

- Увійдіть у потрібний акаунт (наприклад, Facebook, Telegram, Google чи інший).
- Зайдіть у розділ меню «налаштування», а потім «безпека».
- Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (зверніть увагу, може також називатися «двоетапна перевірка»).
- Виконайте всі необхідні дії за запропонованою інструкцією.



КОРОТКИЙ ЧЕКЛІСТ ІЗ ОНЛАЙН-БЕЗПЕКИ

☐ Вимкніть геолокацію

Якщо не використовуєте геолокацію на телефоні чи іншому ґаджеті, то вимкніть її. Відстежуйте, чи залишаєте ви геомітки на своїх публікаціях у соціальних мережах.

☐ Робіть перевірку питанням «Білборд»

Перш ніж щось опублікувати, уявіть, що ваш допис буде розміщено на великому білборді посеред міста. Якщо не проти, що це побачать всі, то публікуйте. Якщо ні — не варто.

☐ Фактчекайте та перевіряйте джерела інформації

Коли бачите якусь новину чи навіть просто публікацію, перевірте, хто її розповсюдив, чи можна довіряти цій людині. Спробуйте знайти інші джерела, які підтвердять, що це не вигадка.



ДЕ ДІЗНАТИСЬ БІЛЬШЕ?

- Брошура «Про кібербулінг для дітей»
- Гайд «Кібергігієна для дітей: правила безпеки в інтернеті»
- Освітній серіал «Обережно! Кібершахраї. Як захистити себе від шахраїв в інтернеті та у ґаджетах»
- Освітній серіал «Онлайн-безпека для дітей»
- Освітній серіал «Онлайн-безпека для підлітків»
- Настільна гра «Коло безпеки»

