

РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕЧНОГО ПОВОДЖЕННЯ В ІНТЕРНЕТІ ТА КІБЕРБУЛІНГ

Методичний матеріал для студентів

Дніпровського фахового коледжу будівельно-монтажних технологій та архітектури

РОЗДІЛ 1. ВСТУП: ЧОМУ ЦЕ ВАЖЛИВО САМЕ ЗАРАЗ

Інтернет — це не просто розвага чи спосіб спілкування. Це простір, де ви навчаєтесь, працюєте, будujete стосунки та формуєте свою репутацію. Але водночас це середовище, де є реальні загрози: шахраї, кібербулінг, грумінг, фішинг.

За даними кіберполіції України, онлайн-шахрайство продовжує зростати, а кібербулінг залишається однією з найпоширеніших форм насильства серед молоді. Особлива небезпека кібербулінгу в тому, що він **не припиняється після занять** — він переслідує людину 24/7, адже телефон чи комп'ютер завжди поруч.

Цей матеріал допоможе вам:

- Розпізнавати небезпеки в інтернеті.
- Захистити свої акаунти та особисті дані.
- Правильно реагувати на кібербулінг.
- Не стати жертвою шахраїв.
- Поводитися відповідально в цифровому просторі.

РОЗДІЛ 2. ЩО ТАКЕ КІБЕРБУЛІНГ

2.1. Визначення

Кібербулінг — це систематичне приниження, цькування або переслідування людини з використанням цифрових технологій: телефону, комп'ютера, інтернету, соціальних мереж, ігор, форумів.

2.2. Форми кібербулінгу

Форма	Приклади
Образливі повідомлення	Принизливі коментарі, лайки, меми на адресу людини
Поширення чуток	Розповсюдження неправдивої інформації в чатах, групах
Виключення з груп	Ігнорування, видалення з чатів, бойкот в онлайн-спільнотах
Поширення фото/відео без згоди	Публікація компрометуючих матеріалів, монтажів
Шантаж	Погрози опублікувати особисту інформацію

Форма	Приклади
Сексуальне переслідування	Небажані повідомлення інтимного характеру, грумінг
Створення фейкових акаунтів	Профілі від імені жертви для знущань

2.3. Чим кібербулінг відрізняється від звичайного булінгу

- **Доступність 24/7:** на відміну від шкільного булінгу, кібербулінг не припиняється після занять .
- **Анонімність кривдника:** агресор може приховувати свою особу.
- **Швидке поширення:** образливий контент може стати вірусним за години.
- **Відсутність безпечного простору:** вдома людина не відчувається в безпеці, бо цькування продовжується в телефоні.

2.4. Ознаки, що ви можете бути жертвою кібербулінгу

- Ви отримуєте образливі або загрозливі повідомлення.
- Ваші фото або відео поширюються без вашої згоди.
- Вас виключають з онлайн-груп або ігнорують.
- Хтось створив фейковий акаунт від вашого імені.
- Ви відчуваєте тривогу, страх або сором після перебування в інтернеті.
- Ви почали уникати соціальних мереж через негативні коментарі.

2.5. Наслідки кібербулінгу для психіки

Постійне приниження в мережі формує почуття безпорадності, знижує самооцінку, змушує уникати спілкування. Можливі наслідки :

- Тривожність і депресивні стани.
- Безсоння, головний біль, біль у шлунку.
- Втрата інтересу до того, що раніше подобалось.
- Замкнутість, уникання соціальних контактів.
- Аутоагресія (самоушкодження).
- Суїцидальні думки.

Важливо! Якщо ви відчуваєте щось із цього — це не ваша провина. Зверніться по допомогу.

РОЗДІЛ 3. ЯК ЗАХИСТИТИ СЕБЕ ВІД КІБЕРБУЛІНГУ

3.1. Загальні правила

1. Не відповідайте агресією на агресію. Відповідь на образи лише розпалює конфлікт. Найкраща стратегія — **не годувати тролів**.

2. Зберігайте докази. Робіть скріншоти образливих повідомлень, коментарів, постів. Це допоможе, якщо потрібно буде звертатися до адміністрації або поліції .

3. Блокуйте кривдника. У більшості соцмереж є функція блокування. Скористайтеся нею без вагань .

4. Поскаржтеся на контент. Використовуйте кнопку «Поскаржитися» на платформі. Модератори можуть видалити образливий контент .

5. Не залишайтеся наодинці з проблемою. Розкажіть батькам, викладачу, психологу або другу, якому довіряєте.

3.2. Кому можна розповісти

- **Батьки або законні представники** — найперші люди, які можуть допомогти.
- **Класний керівник** — людина, яка координує вашу групу.
- **Практичний психолог Коледжу** — фахівець, який надає психологічну підтримку.
- **Соціальний педагог** — допомагає у складних соціальних ситуаціях.
- **Заступник директора з виховної роботи** — для офіційного реагування.
- **Національна дитяча гаряча лінія: 116 111** — безкоштовна конфіденційна допомога для дітей та молоді.
- **Національна поліція: 102** — якщо є погрози фізичною розправою або шантаж.

3.3. Що робити, якщо ви стали свідком кібербулінгу

- **Не залишайтеся осторонь.** Підтримайте постраждалого.
- **Не поширюйте образливий контент**, навіть «щоб показати друзям».
- **Повідомте постраждалому**, що ви на його/її боці.
- **Повідомте дорослим**, яким довіряєте.
- **Поскаржтеся на контент** модераторам платформи.

РОЗДІЛ 4. ЗАХИСТ ОСОБИСТИХ ДАНИХ В ІНТЕРНЕТІ

4.1. Що таке особисті дані

Особисті дані — це будь-яка інформація, яка може ідентифікувати вас:

- Прізвище та ім'я.
- Дата народження.
- Адреса проживання.
- Номер телефону.
- Електронна пошта.
- Номер банківської картки.
- Фото та відео.
- Геолокація.

4.2. Головне правило: менше даних — більше безпеки

Кіберполіція України наголошує: **чим менше персональних даних ви виставляєте в мережі, тим важче шахраям отримати доступ до вашої особистої інформації** .

4.3. Практичні рекомендації

1. Не публікуйте повне ім'я та точну локацію.

Save the Children рекомендує: **ніколи не діліться повними іменами або точною геолокацією** в інтернеті чи додатках .

2. Перевіряйте налаштування приватності.

Налаштуйте свої профілі так, щоб вашу інформацію бачили лише друзі, а не всі користувачі.

3. Не додавайте в друзі незнайомих.

Перед тим як підтвердити запит, перевірте профіль: чи є реальна інформація, фотографії, який контент публікується .

4. Не переходьте за сумнівними посиланнями.

Навіть якщо повідомлення надійшло від знайомого, переконайтеся, що його акаунт не

зламано. Кіберполіція радить: **зателефонуйте цій людині та уточніть, чи дійсно вона надсилає повідомлення** .

5. Обмежте публікацію фото.

Не публікуйте фото, які можуть бути використані проти вас. Особливо це стосується інтимних фотографій.

6. Використовуйте окрему електронну пошту для соцмереж.

Це допоможе захистити вашу основну пошту від спаму та фішингових атак .

РОЗДІЛ 5. ПАРОЛІ ТА ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ

5.1. Як створити надійний пароль

Кіберполіція України рекомендує :

- **Довжина:** щонайменше **12 символів**.
- **Складність:** великі та малі літери, цифри, спеціальні символи.
- **Унікальність:** кожен акаунт повинен мати **свій власний пароль**.
- **Оновлення:** змінюйте пароль, якщо є підозра на злам.

Приклади поганих паролів:

- 123456
- qwerty
- дата народження
- ім'я домашнього улюбленця

Приклад хорошого пароля:

- K0l3g3#2026!Bd
- M1j\$uP3r_P@rol

5.2. Двофакторна автентифікація (2FA)

Двофакторна автентифікація — це додатковий рівень захисту. Навіть якщо зломисник отримає ваш логін і пароль, без доступу до вашого телефону він **не зможе увійти в акаунт** .

Як це працює:

1. Ви вводите логін і пароль.
2. Система надсилає код на ваш телефон або використовує додаток-автентифікатор.
3. Ви вводите код і отримуєте доступ.

Де увімкнути 2FA:

- Google (Gmail, YouTube)
- Instagram, Facebook, TikTok
- Telegram, Viber, WhatsApp
- Банківські додатки

Рекомендація кіберполіції: увімкніть двофакторну автентифікацію на всіх важливих акаунтах .

5.3. Що робити, якщо акаунт зламали

Ознаки зламу :

- З'являються публікації, яких ви не створювали.
- Друзі отримують від вас підозрілі повідомлення.
- Ви отримуєте повідомлення про вхід з нового пристрою.
- Ви не можете увійти в акаунт.

Дії:

1. **Негайно змініть пароль.**

2. Завершіть усі активні сесії на інших пристроях.
3. Увімкніть двофакторну автентифікацію.
4. Попередьте друзів, що ваш акаунт був зламаний.
5. Зверніться до служби підтримки платформи.
6. Якщо постраждали фінанси — зверніться до банку та поліції.

РОЗДІЛ 6. ЯК РОЗПІЗНАТИ ФІШИНГ

6.1. Що таке фішинг

Фішинг — це метод шахрайства, при якому зловмисники створюють підроблені сайти або надсилають повідомлення, щоб виманити у вас особисті дані: логіни, паролі, номери банківських карток .

6.2. Ознаки фішингових повідомлень

За даними експертів з кібербезпеки, фішингові повідомлення часто мають такі ознаки :

Ознака	Приклад
Неперсоналізоване звернення	«Шановний клієнте!» замість вашого імені
Терміновість	«Негайно оновіть дані, інакше акаунт буде заблоковано!»
Погрози	«Якщо не підтвердите, ми змушені заблокувати ваш рахунок»
Запит конфіденційних даних	Прохання ввести пароль, номер картки, CVV-код
Підозрілі посилання	URL, який виглядає майже як справжній, але має зайву крапку або символ
Помилки в тексті	Граматичні помилки, дивні символи
Вкладення	Файли .exe або інші небезпечні формати

6.3. Як розпізнати фішинговий сайт

Кіберполіція України пояснює: **фейкові сайти можуть мати ідентичний інтерфейс, але в самому посиланні буде або граматична помилка, або додаткова крапка .**

Приклад:

- Справжній сайт: www.bank.gov.ua
- Фішинговий сайт: www.bank-gov.ua або www.bank.gov.ua.secure-login.com

Порада: завжди перевіряйте URL-адресу перед введенням будь-яких даних.

6.4. Що робити, якщо ви потрапили на фішинг

1. **Негайно змініть пароль** від акаунта, дані якого ви ввели.
2. **Якщо ввели дані картки** — негайно зателефонуйте до банку та заблокуйте картку.
3. **Запустіть антивірусну перевірку** пристрою.

4. Повідомте про інцидент кіберполіції.

РОЗДІЛ 7. ШАХРАЙСТВО В ІНТЕРНЕТІ

7.1. Найпоширеніші схеми шахрайства

1. Фейкові інтернет-магазини.

Зловмисники створюють сайти, які виглядають як відомі магазини. Товар продають за дуже низькою ціною, щоб заманити покупця .

2. Шахрайство на сайтах оголошень.

Шахраї видають себе за покупців або продавців, пропонують перейти для спілкування в месенджери, а потім надсилають фішингові посилання для оплати .

3. Дзвінки від «банку».

Шахраї телефонують, представляючись працівниками банку, і намагаються виманити код підтвердження з SMS .

4. Повідомлення від «друзів».

Шахраї зламують акаунт вашого знайомого і надсилають повідомлення з проханням позичити гроші .

5. Фейкові благодійні збори.

Зловмисники створюють фейкові сторінки для збору коштів на благодійність.

7.2. Як не стати жертвою шахраїв

Кіберполіція України радить :

При онлайн-покупках:

- **Обирайте післяплату.** Платіть тільки за те, що отримали.
- **Перевіряйте ціни.** Якщо пропозиція виглядає надто вигідною — це привід замислитися.
- **Перевіряйте продавця.** Шукайте відгуки, перевіряйте контакти.
- **Не переходьте в месенджери.** Спілкуйтеся лише через офіційний сайт або додаток.
- **Не вводьте платіжні дані на незнайомих сайтах.**

При отриманні повідомлень:

- **Перетелефонуйте** людині, від імені якої надійшло повідомлення .
- **Не переходьте** за сумнівними посиланнями.
- **Не вводьте** особисті дані на сайтах, які ви не перевірили.

При дзвінках:

- **Пам'ятайте:** справжні працівники банку **ніколи не запитують** паролі, CVV-коди або коди підтвердження.
- **Покладіть слухавку** і зателефонуйте до банку за офіційним номером.

7.3. Фінансова безпека

- **Використовуйте окрему картку** для онлайн-оплат. Поповнюйте її безпосередньо перед покупкою .
- **Увімкніть 3D Secure** — додаткову перевірку при оплаті .
- **Не здійснюйте оплату через публічні Wi-Fi мережі .**
- **Ніколи не повідомляйте реквізити картки** третім особам: нікому не потрібні ваш CVV-код або код з SMS, крім вас .

РОЗДІЛ 8. ГРУМІНГ ТА НЕБЕЗПЕЧНІ ЗНАЙОМСТВА

8.1. Що таке грумінг

Грумінг — це встановлення дорослою особою довірливих стосунків із дитиною або підлітком з метою сексуальної експлуатації. Це може відбуватися як в інтернеті, так і в реальному житті.

8.2. Ознаки грумінгу

- Доросла людина виявляє надмірну увагу до вас.
- Робить компліменти, дарує подарунки.
- Пропонує спілкуватися наодинці, подалі від батьків.
- Запитує особисту інформацію, фото.
- Пропонує зустрітися наодинці.
- Просить зберігати їхні стосунки в таємниці.
- Надсилає повідомлення інтимного характеру.

8.3. Що робити

- **Ніколи не погоджуйтеся на зустріч з онлайн-знайомим без дозволу батьків .**
- **Не надсилайте свої фото незнайомцям.**
- **Повідомте батькам або дорослим, яким довіряєте.**
- **Зabloкуйте цю людину.**

Важливо! Якщо ви стали жертвою грумінгу, це **не ваша провина**. Зверніться по допомогу негайно.

РОЗДІЛ 9. ПРАВИЛА СПІЛКУВАННЯ В ІНТЕРНЕТІ

9.1. Цифровий етикет

- **Будьте ввічливими.** Те, що ви пишете в інтернеті, може завдати реальної шкоди.
- **Поважайте інших.** Не принижуйте, не ображайте, не цькуйте.
- **Не поширюйте чужі фото без згоди.**
- **Перевіряйте інформацію** перед тим, як ділитися нею.
- **Не годуйте тролів.** Ігноруйте провокації.

9.2. Що не можна робити в інтернеті

- **Погрожувати** іншим людям.
- **Цькувати** когось.
- **Поширювати** особисті дані інших без згоди.
- **Використовувати** чужі акаунти.
- **Розповсюджувати** незаконний контент.
- **Вчиняти** будь-які протиправні дії.

9.3. Відповідальність за кібербулінг

В Україні булінг (цькування), у тому числі кібербулінг, є **адміністративним правопорушенням** згідно зі статтею 173-4 Кодексу України про адміністративні правопорушення.

Відповідальність:

- Штраф від 50 до 100 неоподатковуваних мінімумів доходів громадян.
- Або громадські роботи від 20 до 40 годин.
- За повторне порушення — більш суворе покарання.
- За дії неповнолітніх — відповідальність несуть батьки.

РОЗДІЛ 10. КОРИСНІ РЕСУРСИ ТА КОНТАКТИ

10.1. Офіційні ресурси

Ресурс	Посилання	Призначення
Кіберполіція України	cyberpolice.gov.ua	Офіційний сайт, корисні поради
Кібер Брама	stopfraud.gov.ua	Інформація про шахрайські схеми
Проект BRAMA	t.me/+FVp2IctBvfBiODY6	Протидія дезінформації та ворожим ресурсам
Національний банк України	bank.gov.ua	Платіжна безпека

10.2. Гарячі лінії

Служба	Телефон
Національна поліція	102
Національна дитяча гаряча лінія	116 111
Урядова гаряча лінія з питань протидії машиньому насильству	1547
Кіберполіція (заявка онлайн)	ticket.cyberpolice.gov.ua

10.3. Куди звертатися в Коледжі

Заступник директора з виховної роботи
Практичний психолог
Соціальний педагог
Класний керівник

РОЗДІЛ 11. ПАМ'ЯТКА: 10 ЗОЛОТИХ ПРАВИЛ БЕЗПЕКИ В ІНТЕРНЕТІ

1. Використовуй складні унікальні паролі (мінімум 12 символів).
2. Увімкни двофакторну автентифікацію на всіх важливих акаунтах.
3. Не діліться особистими даними з незнайомцями.
4. Перевіряй посилання перед тим, як клікнути.
5. Не переходь за сумнівними лінками навіть від друзів.

6. **Не надсилай інтимні фото** нікому.
7. **Не погоджуйся на зустрічі** з онлайн-знайомцями без дозволу батьків.
8. **Зберігай докази** кібербулінгу (скріншоти).
9. **Блокуй і скаржся** на кривдників.
10. **Розкажи дорослим**, яким довіряєш, якщо щось сталося.

РОЗДІЛ 12. ЩО РОБИТИ, ЯКЩО СТАЛАСЯ БІДА

Якщо ти став жертвою кібербулінгу:

1. **Не звинувачуй себе.** Це не твоя провина.
2. **Збережи докази** (скріншоти).
3. **Заблокуй кривдника.**
4. **Розкажи** батькам, викладачу, психологу.
5. **Звернися** до адміністрації Коледжу.
6. **За потреби** — до поліції (102).

Якщо ти став жертвою шахраїв:

1. **Заблокуй картку** (якщо ввів дані).
2. **Зміни паролі.**
3. **Звернися до банку.**
4. **Повідом кіберполіцію.**

Якщо тобі страшно або боляче:

- **Національна дитяча гаряча лінія: 116 111** — безкоштовно, конфіденційно, 24/7.
- **Практичний психолог Коледжу** — завжди готовий допомогти.

Пам'ятай: інтернет — це інструмент. Він може бути корисним і безпечним, якщо ти знаєш правила. Ти маєш право на безпеку та повагу — як в реальному житті, так і в цифровому.