

РЕКОМЕНДАЦІЇ ЩОДО ВВІЧЛИВОСТІ, ПРАВИЛ СПІЛКУВАННЯ, ЕТИКИ ТА БЕЗПЕЧНОГО СПІЛКУВАННЯ В МЕРЕЖІ ІНТЕРНЕТ

для студентів дніпровського фахового коледжу будівельно-монтажних технологій та архітектури

Шановні студенти!

Інтернет — це простір, де ви навчаєтесь, спілкуєтесь, будujete стосунки та формуєте свою репутацію. Але водночас це середовище, де є реальні загрози: кібербулінг, шахрайство, фішинг, грумінг та інші небезпеки.

Ці рекомендації розроблено на основі порад Кіберполіції України, UNICEF, Управління Верховного комісара ООН у справах біженців (UNHCR), психологів та фахівців із кібербезпеки (білих хакерів). Вони допоможуть вам поводитися відповідально та безпечно в цифровому просторі.

РОЗДІЛ 1. НЕТИКЕТ: ПРАВИЛА ВВІЧЛИВОСТІ В ІНТЕРНЕТІ

Нетикет (мережевий етикет) — це правила поведінки під час електронної комунікації. Вони базуються на тих самих принципах, що й звичайний етикет, але з урахуванням особливостей онлайн-середовища.

1.1. Основні правила ввічливості

Пам'ятайте, що ви спілкуєтесь з людиною. За екраном завжди є жива людина з почуттями та емоціями. Не дозволяйте собі писати те, чого б не сказали особисто.

Будьте ввічливими та доброзичливими. Завжди вітайтеся із співрозмовником, дякуйте за допомогу, використовуйте ввічливі формулювання.

Поважайте час і можливості інших. Не надсилайте повідомлення в пізній час, якщо це не терміново. Уникайте надмірно довгих повідомлень.

Уникайте фраз, які можуть стати причиною конфлікту. Намагайтеся формулювати думки так, щоб не образити співрозмовника.

Поважайте право на приватне листування. Не поширюйте в мережі інформацію про себе та інших (реальні імена, адреси, телефони, фотографії).

1.2. Правила спілкування в чатах і месенджерах

- **Вітайтеся на початку розмови.** Це елементарна ввічливість.
- **Представляйтеся,** якщо пишете незнайомій людині.
- **Пишіть по роботі у робочий час.**
- **Дотримуйтеся теми розмови.** Не відходьте від теми (офтопик).
- **Не надсилайте спам.** Не додавайте людей у групи без потреби та їхньої згоди.
- **Перевіряйте інформацію** перед тим, як ділитися нею.
- **Не переходьте на особистості** під час суперечок.
- **Вибачайтесь,** якщо помилилися.

1.3. Що є порушенням нетикету

До порушень нетикету належать :

- Образи та перехід на особистості.
- Зловмисний відступ від теми (офтопик).
- Реклама та самореклама у невідповідних місцях.
- Використання табуованої, непристойної ненормативної лексики або відразливих слів та висловів.

- Цькування та переслідування.

РОЗДІЛ 2. ЕТИКА СПІЛКУВАННЯ В ІНТЕРНЕТІ

2.1. Головне правило

Ставтеся до інших так, як хочете, щоб ставилися до вас. Це універсальне правило працює як у реальному житті, так і в інтернеті .

2.2. Принципи етичного спілкування

Принцип	Зміст
Повага	Поважайте думки, погляди та межі інших людей, навіть якщо вони відрізняються від ваших
Толерантність	Не дискримінують за статтю, віком, національністю, релігією, зовнішністю тощо
Чесність	Не видавайте себе за іншу людину, не створюйте фейкові акаунти
Відповідальність	Пам'ятайте, що ваші слова можуть мати реальні наслідки
Конфіденційність	Не розголошуйте особисту інформацію інших без їхньої згоди
Емпатія	Намагайтеся зрозуміти почуття іншої людини

2.3. Що не можна робити в інтернеті

- Погрожувати іншим людям.
- Цькувати когось (кібербулінг).
- Поширювати особисті дані інших без згоди.
- Використовувати чужі акаунти.
- Розповсюджувати незаконний контент.
- Порушувати авторські права.
- Вчиняти будь-які протиправні дії.

РОЗДІЛ 3. БЕЗПЕКА ОСОБИСТИХ ДАНИХ

3.1. Що таке особисті дані

Особисті дані — це будь-яка інформація, яка може ідентифікувати вас: прізвище та ім'я, дата народження, адреса, номер телефону, електронна пошта, номер картки, фото, геолокація.

3.2. Головне правило

Чим менше персональних даних ви виставляєте в мережі, тим важче шахраям отримати доступ до вашої особистої інформації. Кіберполіція України наголошує на необхідності мінімізувати ризики у віртуальному середовищі .

3.3. Практичні рекомендації

Оберігайте персональну інформацію :

- Не публікуйте повне ім'я та точну локацію.

- Не вказуйте адресу, номер телефону, номер школи/коледжу у відкритому профілі.
- Діліться тільки інформацією, необхідною та доречною .

Контролюйте налаштування конфіденційності :

- Налаштуйте профілі так, щоб вашу інформацію бачили лише друзі.
- Обмежте, хто може надсилати вам повідомлення.
- Регулярно перевіряйте ці налаштування.

Не переходьте за сумнівними посиланнями :

- Навіть якщо повідомлення надійшло від знайомого, переконайтеся, що його акаунт не зламано.
- Зателефонуйте цій людині та уточніть, чи дійсно вона надсилала повідомлення.

Не додавайте в друзі незнайомих:

- Перед підтвердженням запиту перевірте профіль: чи є реальна інформація, фотографії, який контент публікується.

Використовуйте окрему електронну пошту для соцмереж:

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

Пам'ятайте: будь-яка інформація, яку ви публікуєте в інтернеті, може залишитися там назавжди .

РОЗДІЛ 4. ПАРОЛІ ТА ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ

4.1. Як створити надійний пароль

Кіберполіція України та фахівці з кібербезпеки рекомендують :

- **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:

- K013g3#2026!Bd

4.2. Двофакторна автентифікація (2FA)

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

Де увімкнути 2FA:

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

Рекомендація: увімкніть двофакторну автентифікацію на всіх важливих акаунтах .

4.3. Що робити, якщо акаунт зламали

Ознаки зламу:

- З'являються публікації, яких ви не створювали.
- Друзі отримують від вас підозрілі повідомлення.

- Ви отримувате 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 5. ЯК РОЗПІЗНАТИ ФІШИНГ

5.1. 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 .

5.2. Ознаки фішингових повідомлень

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

5.3. Як розпізнати фішинговий сайт

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.

5.4. 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 6. ШАХРАЙСТВО В ІНТЕРНЕТІ

6.1. 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.

6.2. Як не стати жертвою шахраїв

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.

6.3. 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.

РОЗДІЛ 7. ГРУМІНГ ТА НЕБЕЗПЕЧНІ ЗНАЙОМСТВА

7.1. 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.

7.2. 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.

7.3. 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 8. КІБЕРБУЛІНГ: ЩО РОБИТИ

8.1. Що таке кібербулінг

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

8.2. 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.

8.3. Що робити, якщо ви стали жертвою

1. **Не відповідайте агресією на агресію.** Відповідь на образи лише розпалює конфлікт .
2. **Зберігайте докази.** Робіть скріншоти образливих повідомлень, коментарів, постів .
3. **Блокуйте кривдника.** У більшості соцмереж є функція блокування .
4. **Поскаржтеся на контент.** Використовуйте кнопку «Поскаржитися» на платформі .
5. **Розкажіть дорослим, яким довіряєте.** Батьки, викладач, психолог — усі вони можуть допомогти .

6. Не залишайтеся наодинці з проблемою.

8.4. 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.

8.5. 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 9. ПСИХОЛОГІЧНА ПІДТРИМКА

9.1. Якщо вам страшно або боляче

Зверніться по допомогу. Це не ознака слабкості, а прояв сили та відповідальності за себе .

Кому можна розповісти:

- Батьки або законні представники.
- Класний керівник.
- Практичний психолог Коледжу.
- Соціальний педагог.
- Національна дитяча гаряча лінія: **116 111**.
- Національна поліція: **102**.

9.2. Що казати собі

- «Це не моя провина.»
- «Я маю право на безпеку та повагу.»
- «Я не один. Є люди, які можуть допомогти.»
- «Я сильний. Я впораюсь.»

9.3. Підтримка друзів

Якщо ваш друг став жертвою кібербулінгу:

- Підтримайте його/її.
- Вислухайте без осудження.
- Допоможіть зібрати докази.
- Порадьте звернутися до дорослих.
- Не залишайте наодинці з проблемою.

РОЗДІЛ 10. 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 11. КОРИСНІ РЕСУРСИ ТА КОНТАКТИ

11.1. Офіційні ресурси

Ресурс	Посилання	Призначення
Кіберполіція України	cyberpolice.gov.ua	Офіційний сайт, корисні поради
Кібер Брама	stopfraud.gov.ua	Інформація про шахрайські схеми
Національний банк України	bank.gov.ua	Платіжна безпека

11.2. Гарячі лінії

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