Відокремлений структурний підрозділ
«Професійно-педагогічний фаховий коледж Глухівського національного педагогічного університету імені Олександра Довженка»

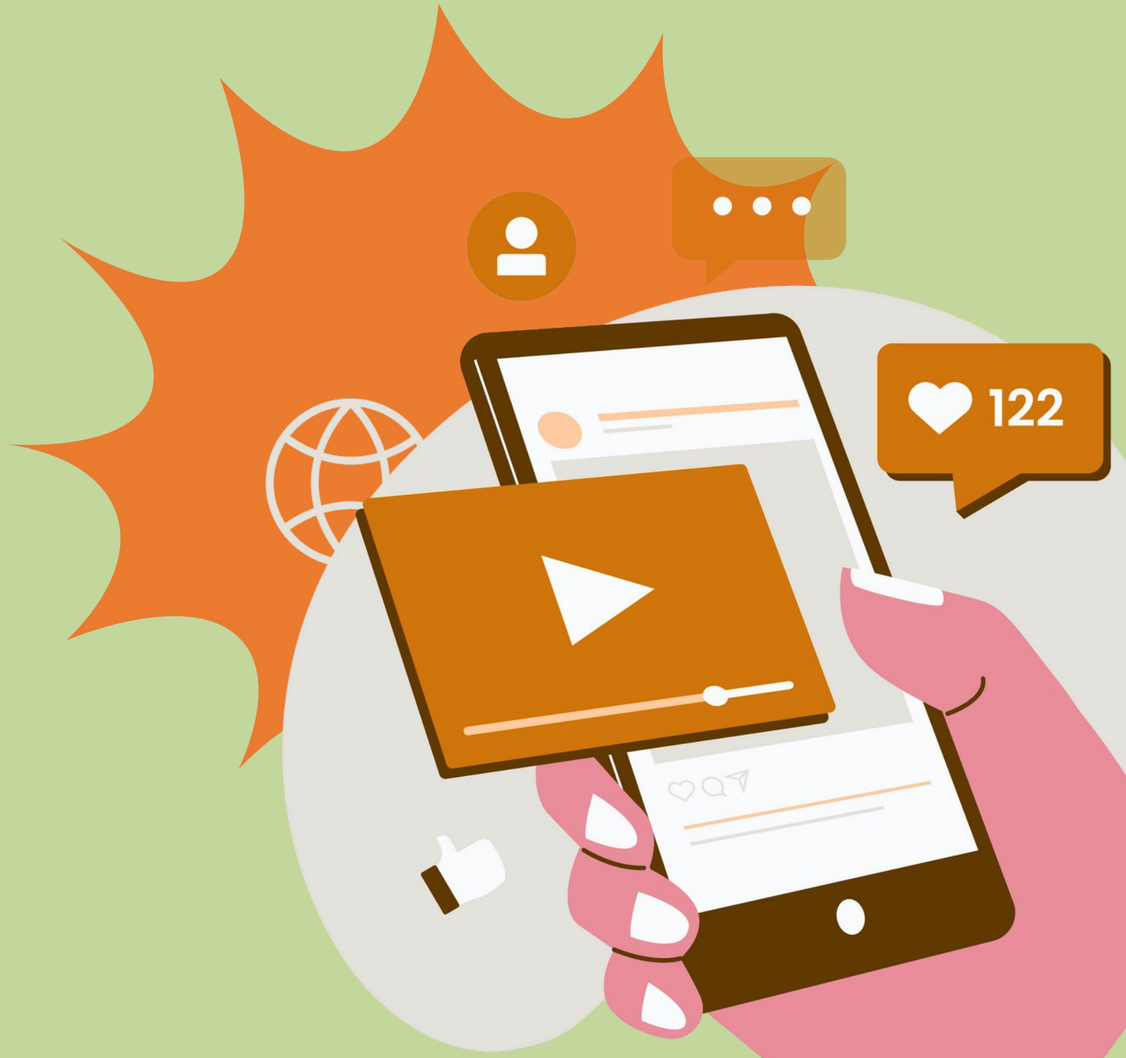
Кібербезпека під час війни: як не стати мішенню

 # ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ 2026

Ми користуємося мережею щодня, але не завжди помічаємо небезпеки. Сьогодні навчимося розпізнавати ризики та діяти грамотно. Інтернет дає доступ до знань, спілкування та можливостей, але водночас відкриває двері для шахраїв, маніпуляторів і агресії. Кожен підліток має знати, як захистити себе, свої дані та репутацію.

НАШІ ЦИФРОВІ СЛІДИ

Кожен лайк, коментар, фото та повідомлення залишають слід. За цими даними можна дізнатися про людину дуже багато: де вона живе, що любить, з ким дружить. Видалити інформацію повністю майже неможливо.



ГОЛОВНІ ЗАГРОЗИ 2026 РОКУ

- Фішинг і викрадення акаунтів;
- Шахрайство з оплатами;
- Віруси в додатках;
- Кібербулінг
- Небезпечні знайомства;
- Маніпуляції через ШІ та дипфейки.

ЦІ РИЗИКИ СТАЮТЬ ДЕДАЛІ РЕАЛІСТИЧНІШИМИ.

ОСОБИСТІ ДАНІ ПІД ЗАХИСТОМ

Не можна публікувати:

- адресу;
- номер телефону;
- документи;
- квитки;
- фото банківських карток.

Навіть звичайне фото з геолокацією може видати місце проживання.

ЯК ЗЛАМУЮТЬ АКАУНТИ

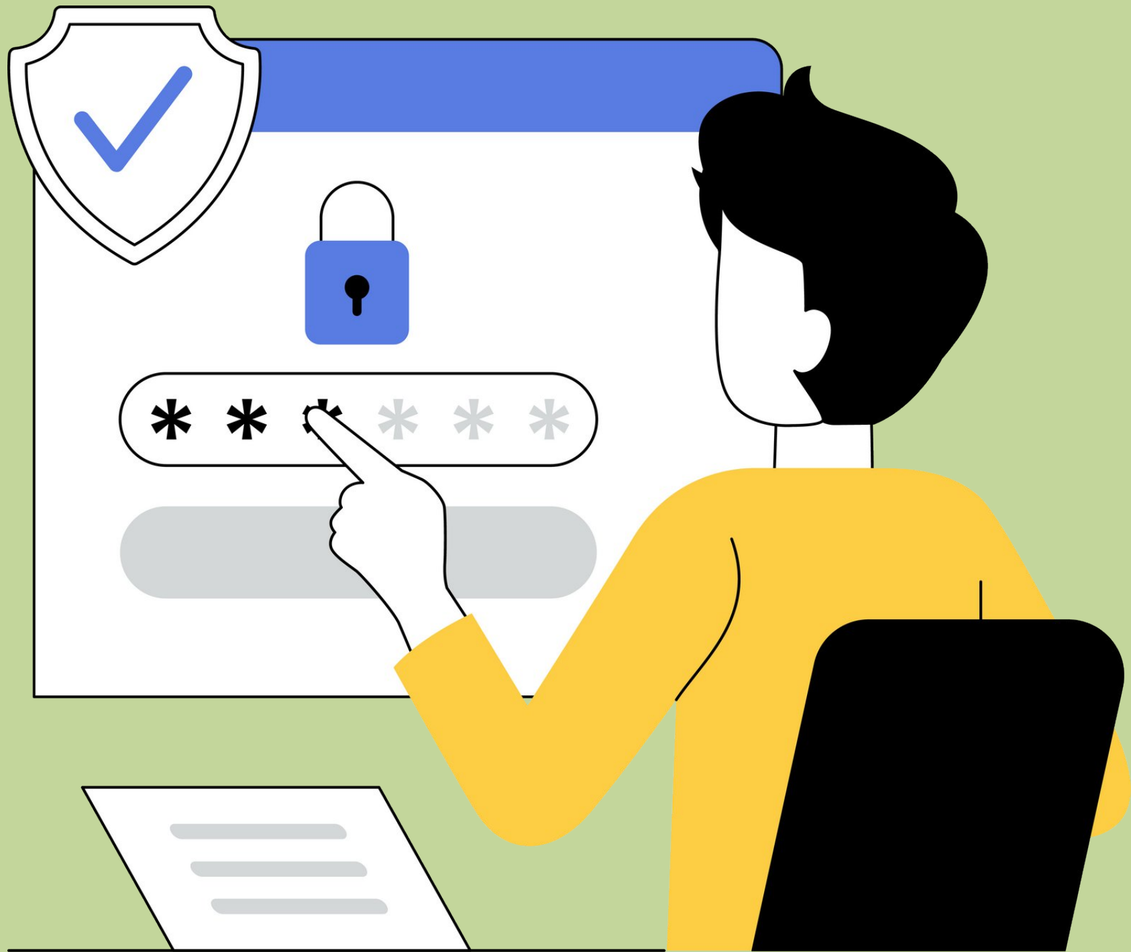
Підроблені сторінки входу, прохання проголосувати, «виграш призу», посилання на безкоштовні моди.

НАДІЙНИЙ ПАРОЛЬ

Пароль має бути довгим, без імен і дат, містити різні символи. Один пароль – один сервіс. **Найкращий захист** – двофакторна автентифікація через застосунок або SMS.

20_/pass26!wo=_rd

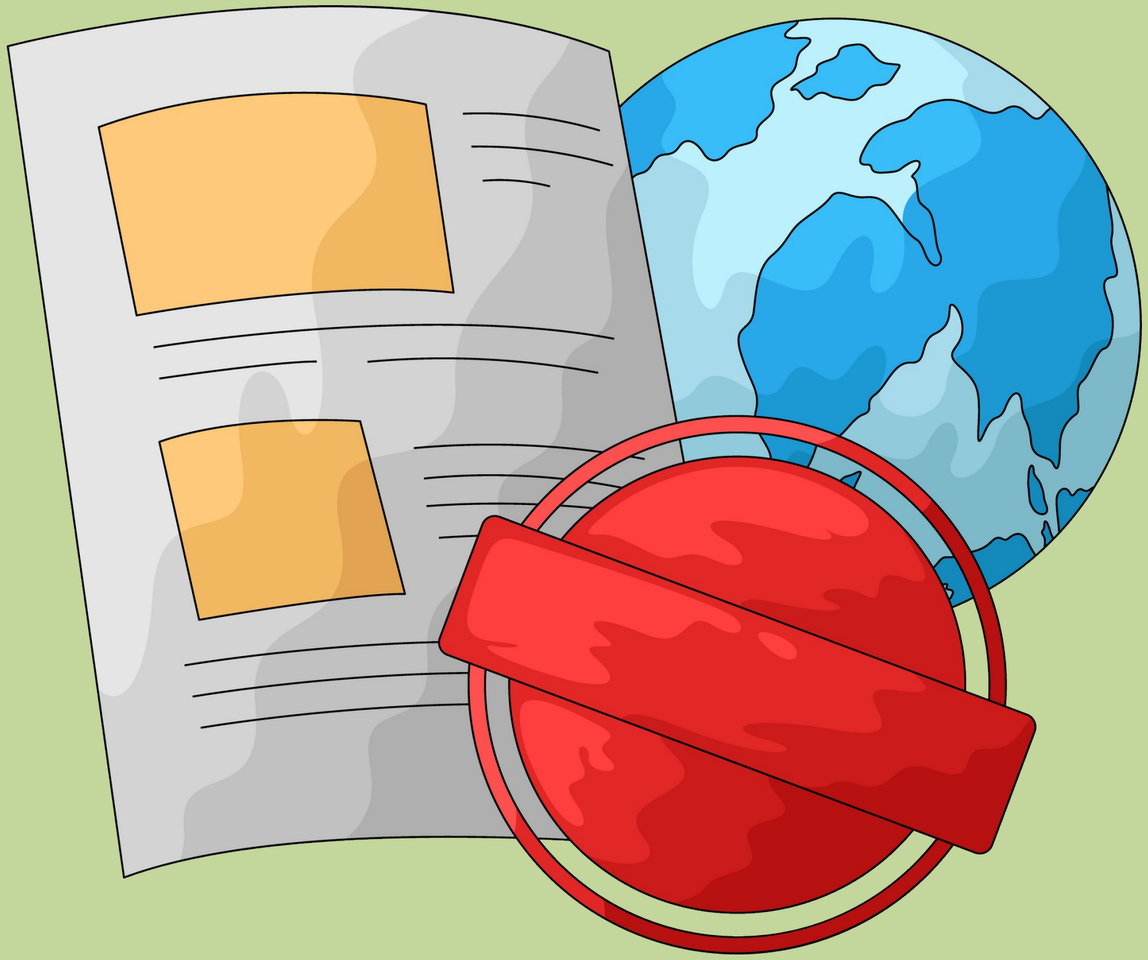
password



ФЕЙКИ В ІНТЕРНЕТІ

Неправдиві новини створюють паніку та маніпулюють людьми. Не все, що в мережі, є правдою.

Ознаки фейку: Емоційний заголовок, немає автора, прохання терміново переслати, невідомий сайт, багато помилок.



ЯК ПЕРЕВІРЯТИ ІНФОРМАЦІЮ:

- Порівняти у кількох джерелах;
- Перевірити дату;
- Прочитати повний текст;
- Знайти офіційне підтвердження.

Search

ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ 2026

КІБЕРБУЛІНГ

ЩО ТАКЕ КІБЕРБУЛІНГ?

Образи, погрози, створення фейкових сторінок, поширення чуток – це насильство в мережі. Що робити при кібербулінгу?

- Не відповідати агресією,
- Зробити скріншоти;
- Заблокувати кривдника
- Повідомити дорослим і платформі.

НЕБЕЗПЕЧНІ ЗНАЙОМСТВА

У мережі люди можуть видавати себе за інших. Не погоджуйся на зустріч без батьків і не надсилай особисті фото. Закритий профіль, мінімум особистої інформації, повага до інших, обдумані публікації.

ОНЛАЙН-ІГРИ

Не передавай паролі, не купуй сумнівні акаунти, завантажуй ігри тільки з офіційних магазинів.

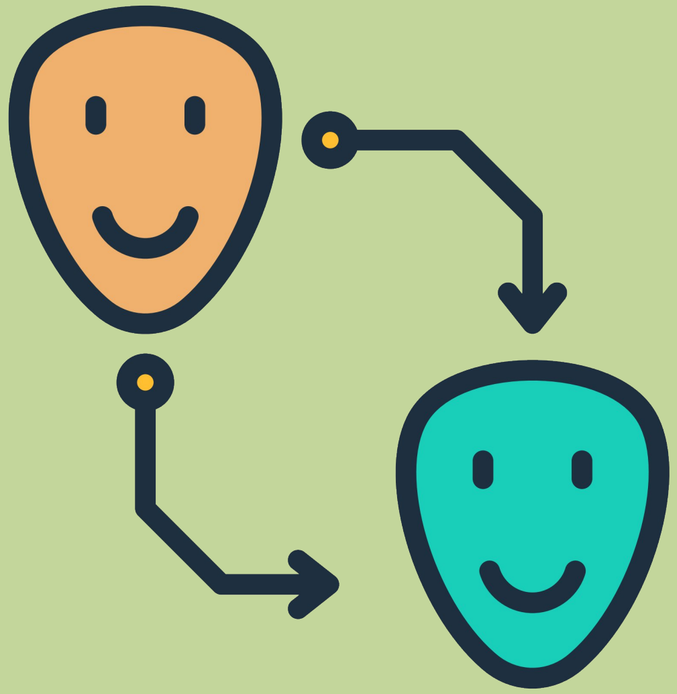
ШІ ТА ДИПФЕЙКИ

ШІ УВІЙШОВ У ПОВСЯКДЕННЕ ЖИТТЯ

Штучний інтелект уже створює тексти, картинки, музику, спілкується замість людей. Це корисно для навчання, але технології можуть використовувати й для обману. Сьогодні не все, що ми бачимо і чуємо в інтернеті, справжнє.

ЩО ТАКЕ ДИПФЕЙК

Дипфейк – це відео або аудіо, у якому обличчя чи голос людини підмінено за допомогою ШІ. Можна зробити, ніби відома людина сказала те, чого ніколи не говорила, або ніби ваш знайомий записав відео.



Шахраї створюють відео від імені блогерів із «розіграшами», підробляють голос родичів із проханням переказати гроші, роблять фейкові новини про події в країні. Мета – викликати довіру та змусити людину діяти швидко.

ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ 2026

ЖИТТЯ В МЕРЕЖІ – ВІДПОВІДАЛЬНІСТЬ І ЦИФРОВЕ ЗДОРОВ’Я

ВІДПОВІДАЛЬНІСТЬ ЗА СЛОВА В ІНТЕРНЕТІ

У мережі діють ті самі правила, що й у реальному житті. Образи, погрози, поширення чужих фото без дозволу, злам акаунтів – це не «жарт», а правопорушення. За такі дії людина може відповідати перед школою, батьками і навіть законом. Анонімність в інтернеті часто уявна, і кожну дію можна відстежити.

ЦИФРОВЕ ЗДОРОВ’Я ТА ЗАЛЕЖНІСТЬ

Постійне перебування онлайн впливає на сон, зір, настрій і навчання. Повідомлення та стрічка змушують повертатися до телефону знову й знову. Важливо робити перерви, вимикати сповіщення під час уроків і відпочинку, мати час без гаджетів щодня.

КУЛЬТУРА СПІЛКУВАННЯ В МЕРЕЖІ

Повага до інших – основа безпечного інтернету. Не варто писати те, чого не сказав би людині в очі. Підтримка друзів, ввічливий тон і вміння не піддаватися на провокації роблять онлайн-простір доброзичливішим.

Інструкція для здобувачів та батьків з безпеки в мережі Інтернет

Типи небезпечних ситуацій, у які можуть потрапити здобувачі освіти у мережі Інтернет:

1. Доступ до сайтів, що не призначені для перегляду підлітками.
2. Контакти з незнайомими людьми через чати, системи миттєвих повідомлень, електронну пошту.
3. Надання інформації особистого (конфіденційного) характеру.
4. Проблеми технологічного характеру.
5. Питання, пов’язані з покупками та фінансовими витратами.

Інструкція для здобувачів та батьків з безпеки в мережі Інтернет

Правила для здобувачів освіти з безпеки в мережі Інтернет

1. Не рекомендується розміщення особистої інформації в Інтернет мережі. Особиста інформація: номер вашого мобільного телефону, адреса електронної пошти, домашня адреса і ваші фотографії, фотографії членів вашої родини або друзів.
2. Якщо ви викладете фото або відео в Інтернеті - будь-хто може подивитися їх.
3. Ніколи не відповідайте на Спам (небажану електронну пошту).
4. Не можна відкривати файли, отримані від невідомих Вам людей. Ви ж не знаєте, що в дійсності містять ці файли - в них можуть знаходитися віруси або фото / відео з «агресивним» вмістом.
5. Ніколи не додавайте незнайомих вам людей у свій список контактів в Messenger.
6. Не забувайте, що віртуальні друзі і знайомі можуть бути не тими насправді, за кого себе видають.
7. Якщо біля вас або поблизу з вами немає родичів, ніколи не зустрічайтеся в реальності з людьми, з якими ви познайомилися в Інтернет мережі. Якщо ваш віртуальний друг насправді той, за кого себе видає, він з розумінням поставиться до вашої турботи про власну безпеку!
8. У будь-який час можна розповісти дорослим, якщо вас хтось образив.

Інструкція для здобувачів та батьків з безпеки в мережі Інтернет

Рекомендації для батьків щодо безпеки дітей у мережі Інтернет

1. Відвідуйте мережу разом з дітьми та закликайте дітей розповідати про свій досвід користування Інтернетом.
2. Привчіть дитину розповідати вам про все, що їх турбує в Інтернеті.
3. Якщо діти спілкуються в чатах, використовують програми миттєвого обміну повідомленнями, грають в он-лайн ігри чи використовують інші програми, що потребують реєстраційного імені, допоможіть дитині вибрати програму і переконайтесь, що вони не містять ніякої особової інформації.
4. Наполягайте на тому, щоб діти ніколи не надавали свою адресу, номер телефону або іншу особисту інформацію незнайомим людям.
5. Поясніть дітям, що різниця між правильним та неправильним однакова: як в Інтернеті, так і в реальному житті.
6. Навчіть дітей поважати інших в Інтернеті. Переконайтесь, що вони знають про те, що правила гарної поведінки діють всюди - навіть у віртуальному світі.
7. Наполягайте на тому, щоб діти поважали власність інших в Інтернеті. Поясніть, що незаконне копіювання чужої роботи - музики, комп'ютерних ігор та інших програм є крадіжкою.
8. Поясніть дітям, що їм не варто зустрічатися з людьми, з якими вони познайомилися в Інтернеті. Поясніть, що ці люди насправді можуть бути не тими за кого вони себе видають.
9. Поясніть дітям, що не все, що вони бачать в Інтернеті чи про що читають – є правдою. Привчіть їх запитувати у вас, якщо вони в чомусь не впевнені.
10. Контролюйте роботу дітей в Інтернеті за допомогою сучасних програм. Вони допоможуть відфільтровувати шкідливий вміст, визначити, на які сайти дитина заходить та що вона на них робить.

Практичні кейси із безпеки онлайн

Розподіли паролі.
Обери, який можна вважати надійним, а який – ні

Надійний пароль

Поганий пароль

Yujk_58_A

93%nk$ma

1234567

ivanov1965

anna2003

12&A@!Nn

22.05.1999

password

0987654

NB_yt_vgaV_)))

abcdef

00000

Практичні кейси із безпеки онлайн

З’ясуй, що робити, якщо отримав дивне повідомлення

«Голос у месенджері» (AI та дипфейки)

Скинути гроші негайно, адже ви бачите обличчя друга і чуєте його голос — це не може бути підробкою.

Задати уточнювальне запитання, відповідь на яке знаєте лише ви обоє, або зателефонувати другу на мобільний.

Написати у відповідь: «Доведи, що це ти», і чекати, поки він надішле фото паспорта.

Заблокувати друга назавжди, бо будь-яке прохання про гроші в інтернеті — це автоматично шахрайство. Кейс №2: «Тінь минулого лайк

Студенту в Telegram приходить кружечок (відеоповідомлення) від одногрупника. На відео той виглядає дуже схвильованим, каже, що потрапив у лікарню і йому терміново потрібно 2000 грн на ліки. Голос і обличчя — 100% його.

Тінь минулого лайка» (Цифровий слід)

Видалити всі акаунти в соцмережах, щоб роботодавець взагалі нічого не зміг знайти про вас.

Перейменувати всі профілі на вигадані нікнейми, наприклад «Кіт-Космонавт», щоб приховати свою особу.

Зробити аудит профілів: видалити суперечливі пости/фото та налаштувати приватність для «незнайомців».

Створити 10 нових порожніх акаунтів, щоб вони піднялися в пошуковій видачі вище за старі сторінки.

Студент претендує на круту посаду в міжнародній компанії. HR-менеджер знаходить його старі коментарі під скандальним постом, де студент у 16 років використовував нецензурну лексику та агресивно сперечався. Як можна «почистити» свій цифровий слід вже сьогодні?

«Мовчання у Telegram» (Кібербулінг)

Мовчати і не втручатися, адже якщо ви нічого не пишете, то ви не берете участі в булінгу.

Підтримати жертву особисто (в приватних повідомленнях) та повідомити про ситуацію куратору або адміністрації.

Написати в чаті агресорам: «Ви самі дурні!», щоб вони перемкнули свою увагу з жертви на вас.

Вийти з чату, щоб не бачити цього негативу і зберегти свій спокій.

У груповому чаті курсу кілька активних студентів почали жорстко висміювати одного з одногрупників за його помилку на лекції. Вони створюють образливі меми та «стікери» з його обличчям.
Решта 25 людей у чаті просто мовчать і спостерігають.

«Примарний залік» (Фішинг)

Перевірити адресу відправника та навести курсор на посилання, щоб побачити справжній домен сайту.

Ввести логін і пароль, але зробити це дуже швидко — хакери не встигнуть перехопити дані.

Спробувати ввести неправильний пароль: якщо сайт його прийме, значить це фішинг.

Відкрити посилання через режим «Інкогніто», оскільки цей режим повністю захищає від крадіжки паролів.

Всім студентам приходить лист на пошту (або повідомлення в бот коледжу) з текстом: «Терміново! Опубліковано списки тих, хто автоматично отримав залік. Перевір себе за посиланням». Посилання веде на сторінку, яка виглядає точно як Google-форма або портал коледжу, і просить залогінитися через свій Google-акаунт.

КУДИ ЗВЕРТАТИСЯ ПО ДОПОМОГУ

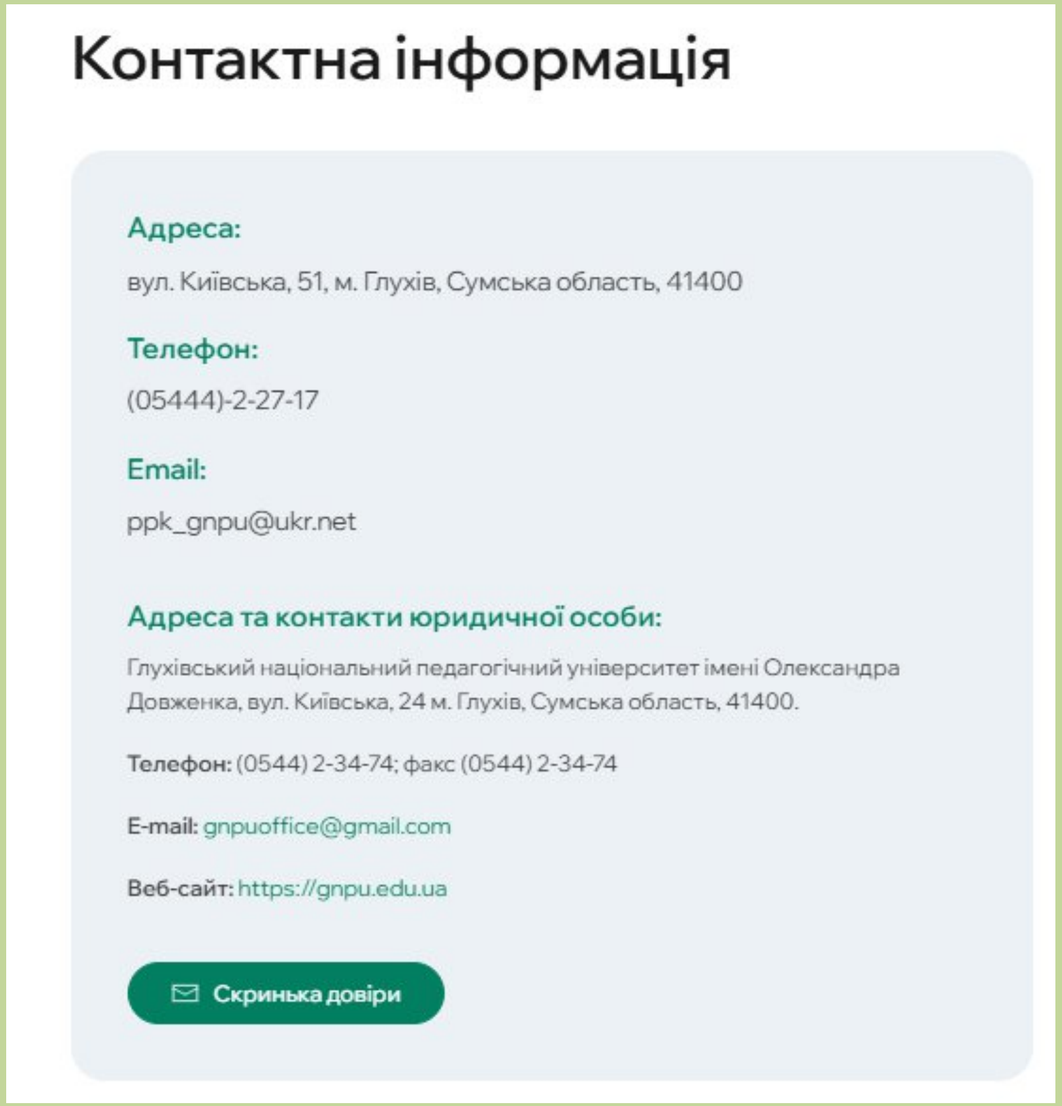
Якщо виникла небезпечна ситуація, не можна залишатися наодинці. Потрібно звернутися до батьків, вчителя, психолога закладу освіти, служби підтримки соцмережі або на спеціальні гарячі лінії для дітей. Просити про допомогу – це ознака сили, а не слабкості.

HELP

Куди звернутися по допомогу ?

До керівника закладу освіти

Керівник закладу освіти в межах наданих йому повноважень забезпечує створення безпечного освітнього середовища в закладі освіти, вільного від насильства та кібербулінгу. Повідомлення про випадок може бути подано керівнику закладу освіти в усній та (або) письмовій формі, в тому числі із застосуванням засобів електронної комунікації на сайті коледжу.



Контактна інформація

Адреса:

вул. Київська, 51, м. Глухів, Сумська область, 41400

Телефон:

(05444)-2-27-17

Email:

ppk_gnpu@ukr.net

Адреса та контакти юридичної особи:

Глухівський національний педагогічний університет імені Олександра Довженка, вул. Київська, 24 м. Глухів, Сумська область, 41400.

Телефон: (0544) 2-34-74; факс (0544) 2-34-74

E-mail: gnpuoffice@gmail.com

Веб-сайт: https://gnpu.edu.ua

Скринька довіри

Куди звернутися по допомогу ?

Телефони довіри

- Дитяча лінія **116-111** або **0 800 500-225** (з 12.00 до 16.00);
- Гаряча телефонна лінія щодо булінгу **116-000**;
- Гаряча лінія з питань запобігання насильству **116-123** або **0 800 500-335**;
- Уповноважений Верховної Ради з прав людини **0 800 50-17-20**;
- Уповноважений Президена України з прав дитини **044 255-76-75**;
- Центр надання безоплатної правової допомоги **0 800 213-103**.

ПІДСУМОК

Безпечний інтернет залежить від наших рішень: обережність, критичне мислення та повага.

- **Не довіряй незнайомцям.**
- **Не передавай паролі.**
- **Не поширюй сумнівну інформацію.**

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ