Безпека в Інтернеті

Викладач інформатики
Яремій С.І.

Інтернет-залежність

Її симптоми:

- непереборне бажання зайти в Інтернет;
- нездатність контролювати свій час в Інтернеті;
- розумове або фізичне виснаження;

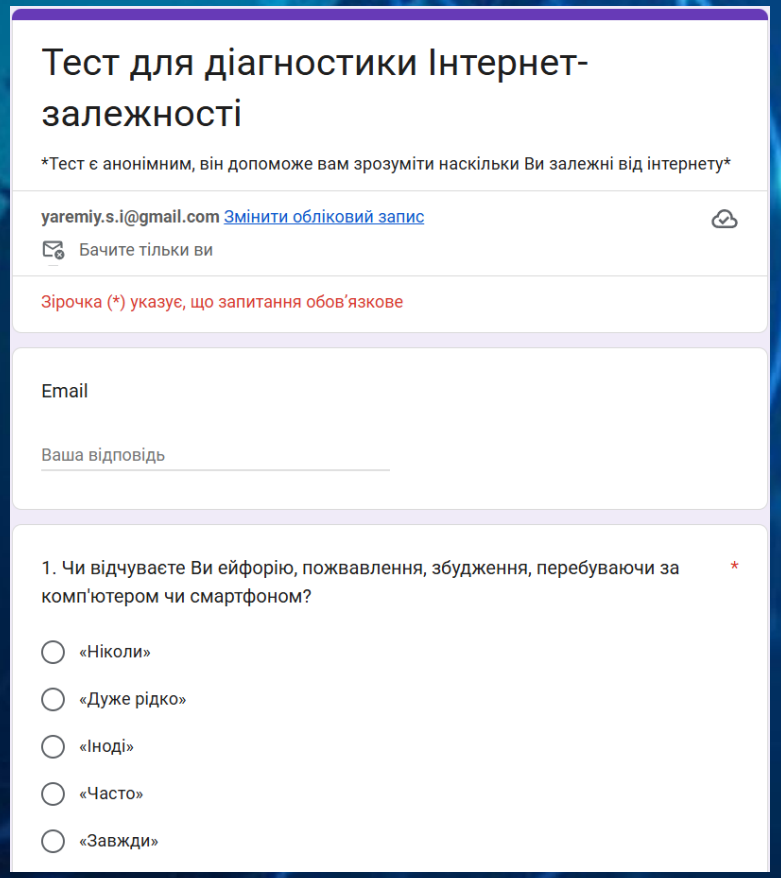
- порушення сну або концентрації уваги;
- дратівливість, депресія, нерви, замкнутість.
- Вся енергія віддається спілкуванню в Інтернеті.

Тест для діагностики Інтернет-залежності

запропонований Кімберлі Янгом, професором психології Пітсбурзького університету.

Тест є інструментом самодіагностики патологічної пристрасті до інтернету.

ТЕСТ
НА ІНТЕРНЕТ-ЗАЛЕЖНІСТЬ



Тест для діагностики Інтернет-залежності

Тест є анонімним, він допоможе вам зрозуміти наскільки Ви залежні від інтернету

yaremiy.s.i@gmail.com Змінити обліковий запис

Бачите тільки ви

Зірочка (*) указує, що запитання обов'язкове

Email

Ваша відповідь

1. Чи відчуваєте Ви ейфорію, пожвавлення, збудження, перебуваючи за комп'ютером чи смартфоном? *

- «Ніколи»
- «Дуже рідко»
- «Іноді»
- «Часто»
- «Завжди»

https://forms.gle/UmpJG3htJrMNGqK3A

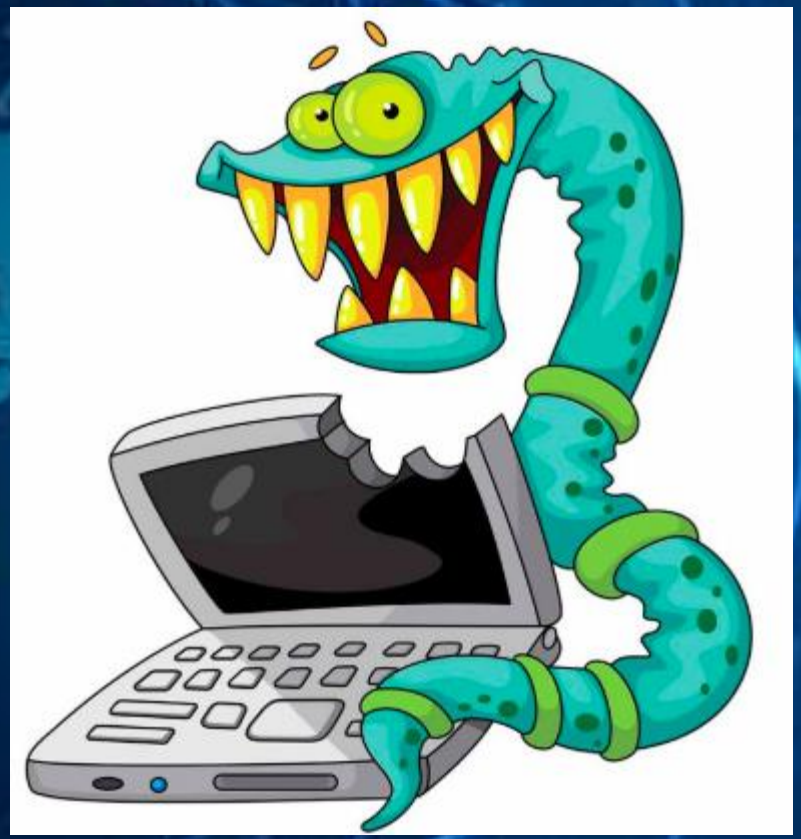
Інтерпретація результатів:

20 - 49 БАЛІВ – у вас **немає інтернет-залежності** – ви звичайнісінький інтернет-користувач. Часом ви, звичайно, затримуєтеся трохи довше в мережі, ніж збиралися, але ви абсолютно в змозі самостійно контролювати використання Інтернету, з урахуванням своєї потреби.

50 - 79 БАЛІВ – час від часу, а можливо останнім часом і часто, ви стикаєтеся з певними проблемами через надмірне використання Інтернету. Вам слід звернути увагу на те, який вплив робить Інтернет на ваше життя і постаратися його контролювати.

80 - 100 БАЛІВ – у вашому житті однозначно відбуваються значні проблеми, які породило надмірне використання Інтернету. У вас **явна інтернет-залежність**. Вам просто необхідно усвідомити, наскільки сильно і згубно впливає Інтернет на ваше життя, постарайтеся відмовитися від нього на час і зайнятися проблемами, які накопичилися, поки ви «пропадали» у мережі Інтернету.

ХРОБАКИ



Окремий вид шкідливих програм, головним завданням яких є розмноження серед комп’ютерів в мережі.

КЛАВІАТУРНИЙ ШПИГУН

Програма, що відстежує введення користувачем паролів і пін-кодів.

Keylogger - програма клавіатурний шпигун

розповість, хто і на що витрачає час в Інтернеті, може використовуватися для крадіжки паролів.

АДВАРЕ

Рекламні модулі. Ці програми, мабуть найменш небезпечні, але через дуже широку розповсюдженість останній час вони стали досить неприємними. Завдання рекламного модуля – показати вам рекламу (відкривання певних сторінок в браузері, які ви не відкривали)

СПАМ

Це масова розсилка реклами або іншого виду повідомлень.

КІБЕР-БУЛІНГ

Одна із форм переслідування дітей та підлітків за допомогою інформаційних технологій. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину

ОН-ЛАЙН-ХИЖАКИ

«Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою.

КІБЕР-ГРУМІНГ

Входження у довіру до дитини з метою використання її у сексуальних цілях.

ШАНТАЖ

Виманювання інформації про дитину та її сім’ю з метою подальшого пограбування, шантажу.

ГРИФЕРИ

Інтернет-шахраї, які заважають учасникам он-лайн ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

ФАРМІНГ

Різновид шахрайства в Інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів.

Потім відбувається зараження комп’ютера вірусами та шпигунським програмним забезпеченням.

ФІШИНГ

Технологія Інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації.

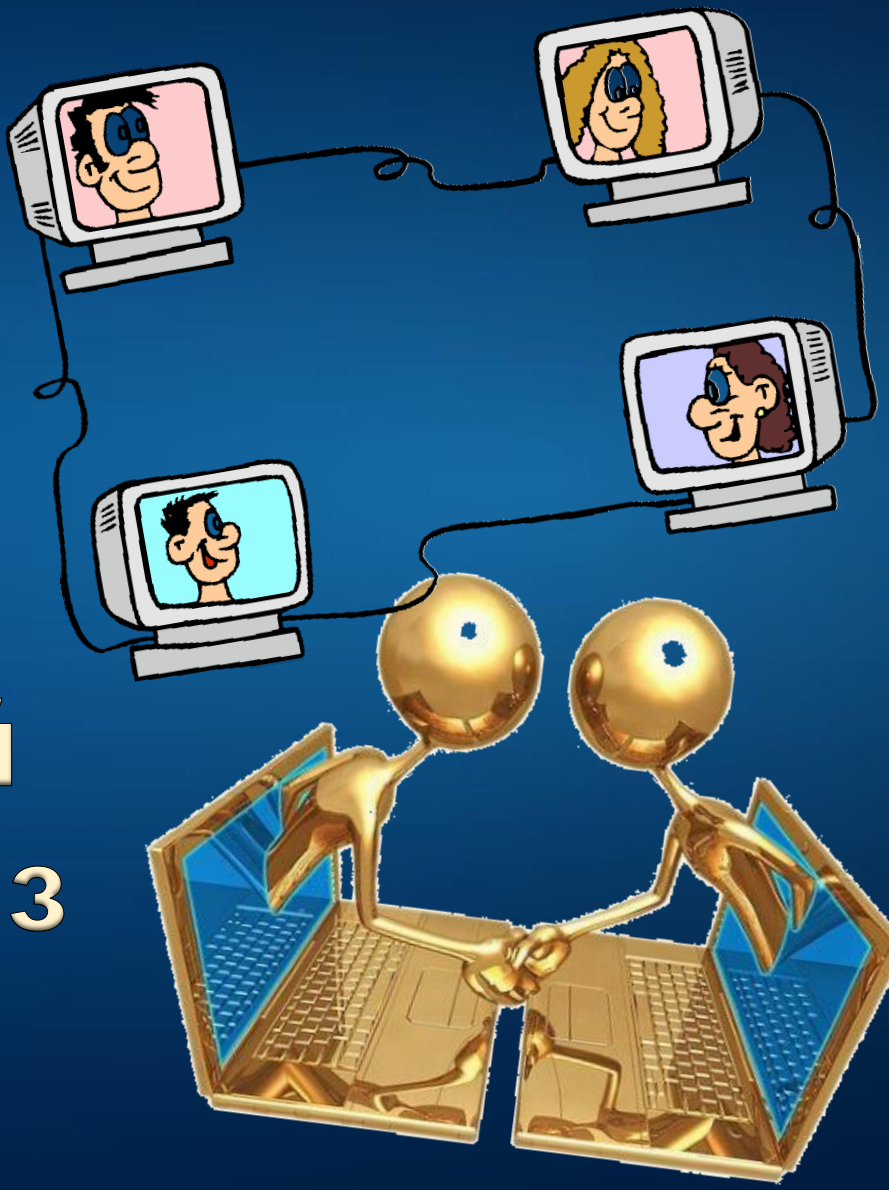
НЕДОСТОВІРНА ІНФОРМАЦІЯ

В Інтернеті на різноманітних форумах досить легко знайти інформацію, яка є життєво небезпечною, якщо нею скористатися.

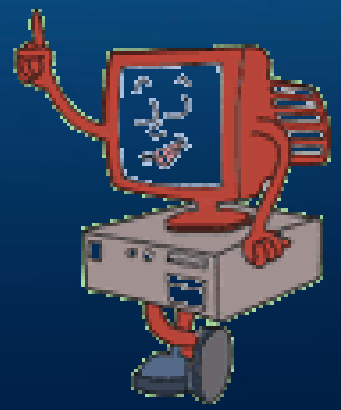
ПРАВИЛА ІНТЕРНЕТ БЕЗПЕКИ

Обмежте доступ до особистої інформації в соцмережах!

Використовуйте надійний пароль та не діліться ним з іншими.



Встановіть антивірус одразу після встановлення операційної системи і постійно його оновлюйте.



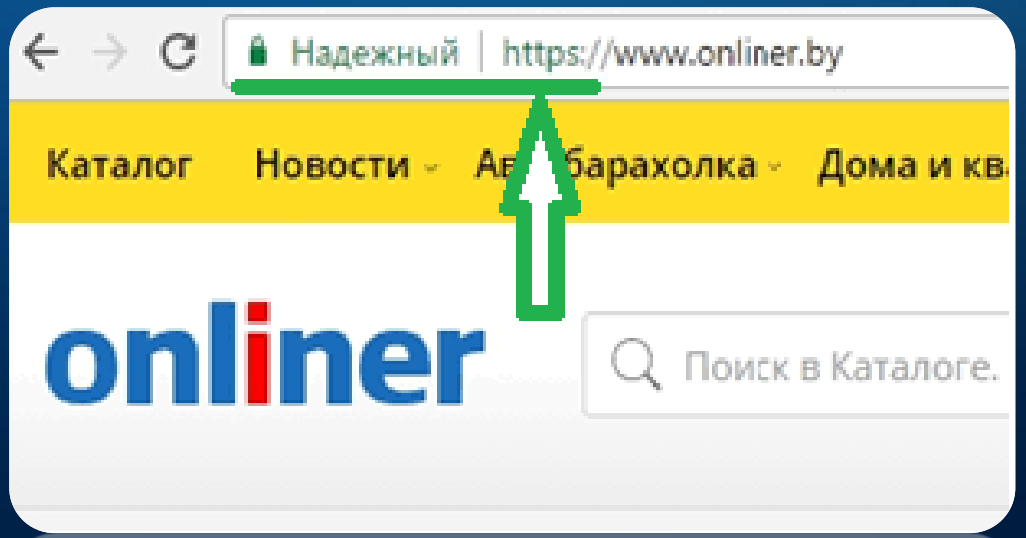
Не додавайте у друзі в соцмережах нікого, кого не знаєте в реальному житті

Не переходьте за жодними посиланнями, якщо ви не впевнені в їх безпечності

Використовуйте складні паролі,
не користуйтесь одним паролем для всіх
акаунтів, періодично змінюйте паролі.

Увімкніть двофакторну автентифікацію
Вашого облікового запису

При проведенні будь-якої фінансової операції через Інтернет уважно дивіться на протокол з’єднання. Потрібно щоб сайт мав 'https://' протокол. Сайти, які можуть викрадати дані працюють використовуючи протокол з’єднання 'http://'.

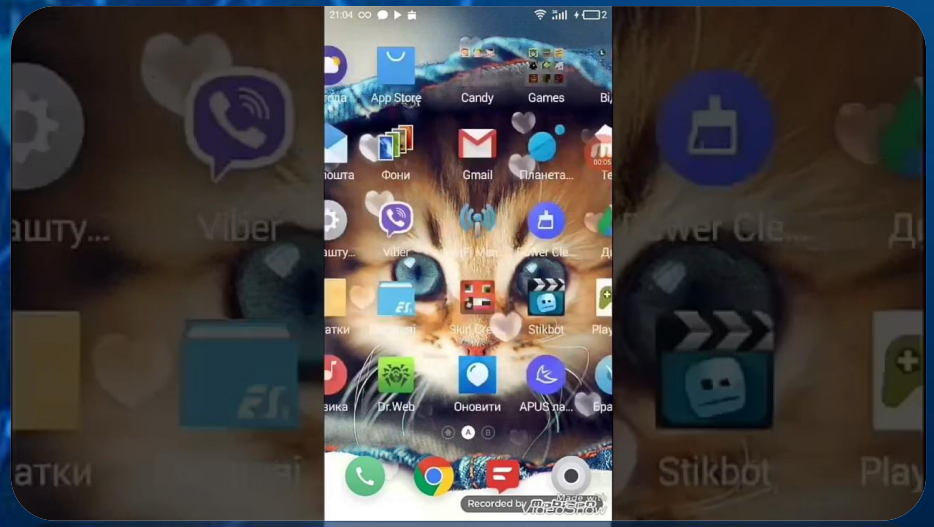


Нікому і ніколи не повідомляйте персональні дані

Ніколи не публікуйте та не поширюйте конфіденційні фотографії себе чи інших, які можуть бути використані для шкоди Вам у майбутньому!

Цифровий слід– дописи, “вподобайки”, коментарі, переглянуті вебсторінки, відповіді на електронні листи.

Періодично перевіряйте Ваші мобільні пристрої на предмет додаткових програм, можливо Ви помітите незнайомі іконки на головному екрані чи в меню смартфона.



Періодично робіть резервне копіювання важливої інформації.

В умовах воєнного часу забороняється висвітлювати в соцмережах:

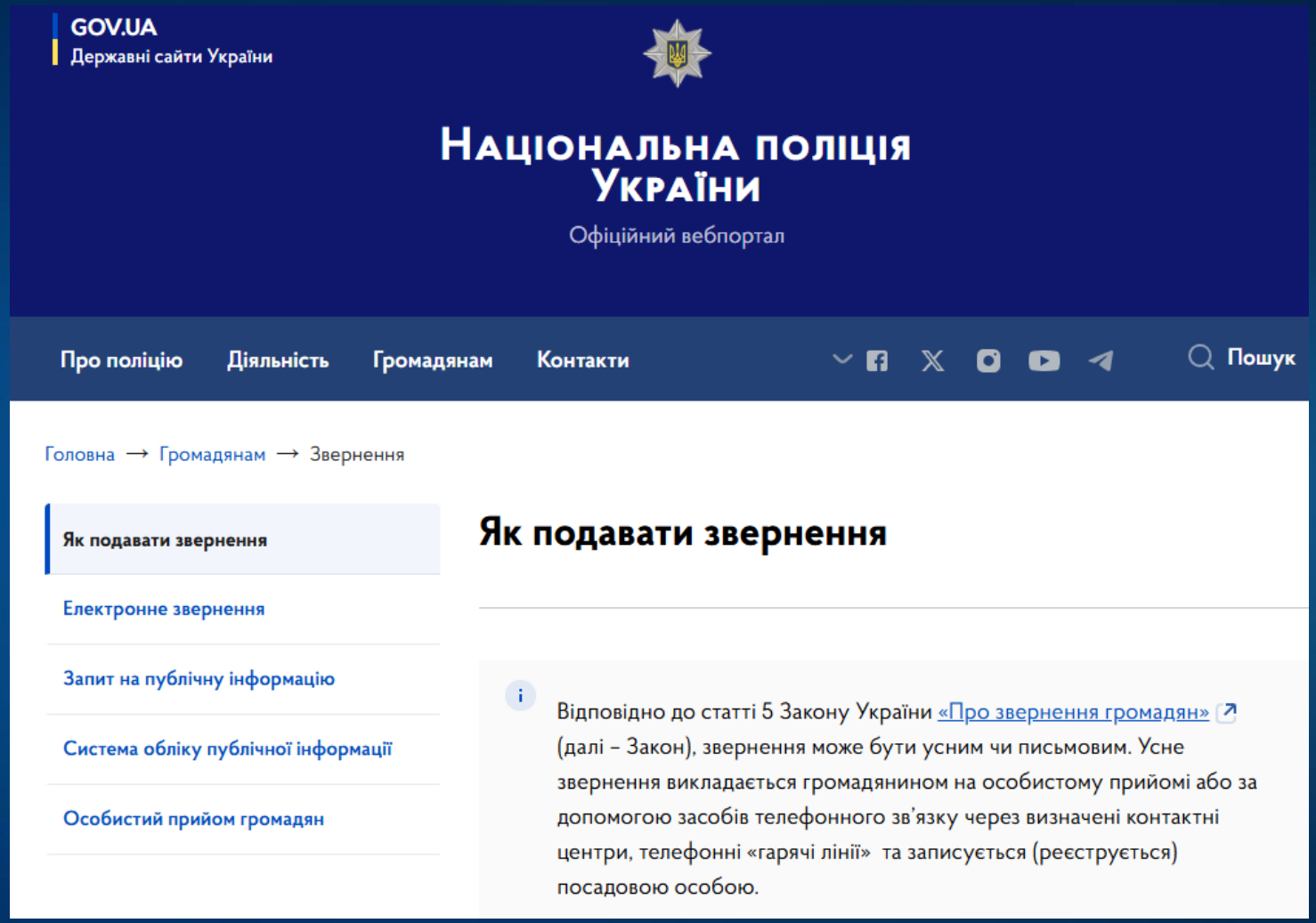
- інформацію про пересування техніки та особового складу українських військ!!!
- персональні дані та світлини, що містять обличчя військових;
- фіксування геолокаційної прив’язки до місць виконання завдань військовими;
- фото та відеофіксацію з місць вибухів та місць укриття цивільного населення (бомбосховищ).

Запам’ятайте чітке правило: виявивши будь-яку загрозу для цифрової безпеки чи проблему в мережі, дійте за принципом, що звучить як

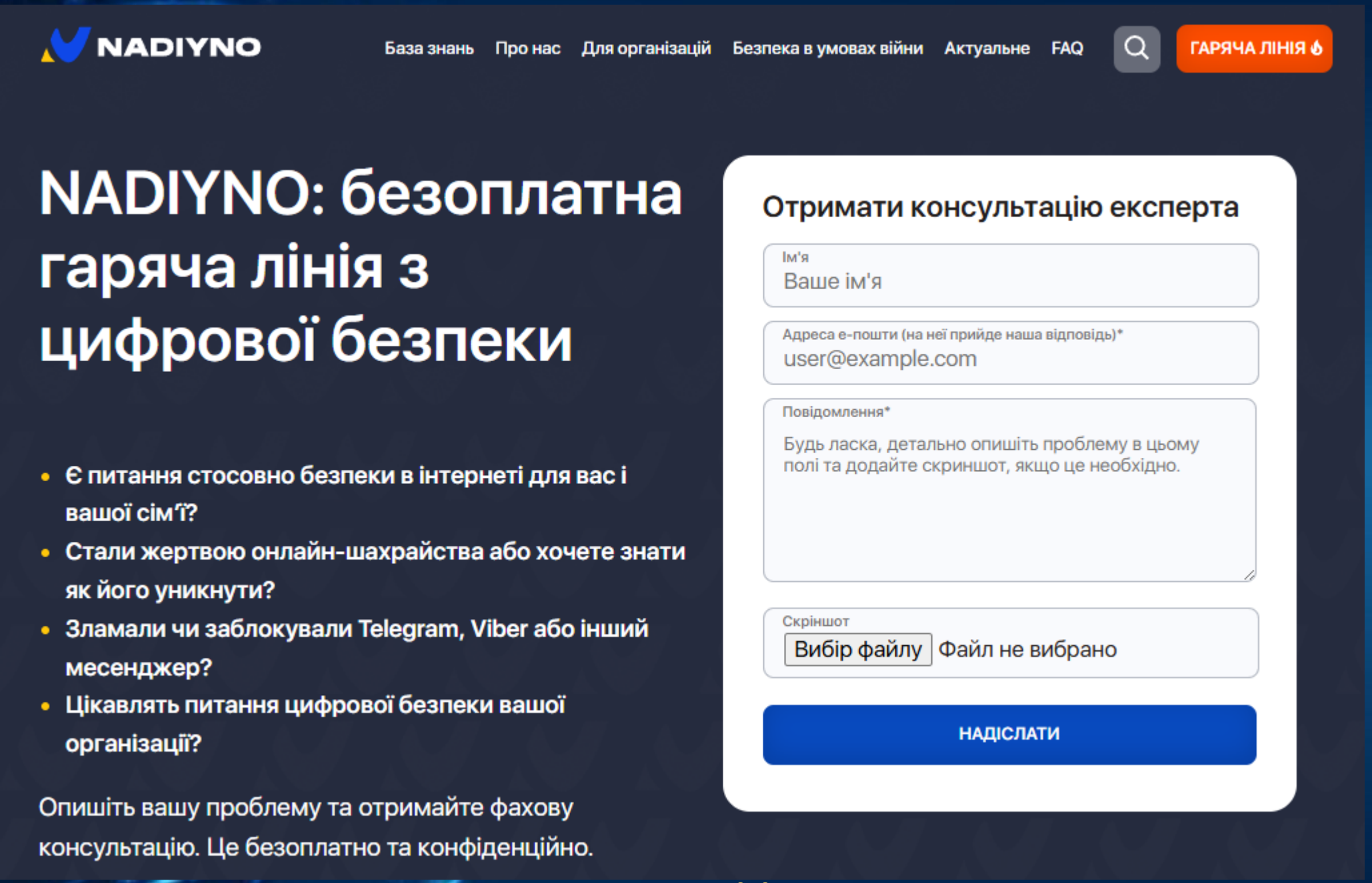
«Зафіксуй та повідом»!

Якщо ви стали жертвою порушення авторського права та суміжних прав онлайн, шахрайства чи інших злочинів у сфері використання комп’ютерів, систем, комп’ютерних мереж і мереж електрозв’язку, звертайтеся до поліції.

Це можна зробити, зателефонувавши на лінію **102** або написавши на офіційний вебсайт Національної поліції України.



https://npu.gov.ua/gromadyanam/zvernennya



https://nadiyno.org

Будьте обережні в Інтернеті!