ЗБІРНИК КОРИСНОЇ ІНФОРМАЦІЇ

ІНФОРМАЦІЙНА ВІЙНА

- Правила інформаційної гігієни
- Дезінформація
- Інформаційна війна
- Яку інформацію не можна поширювати
- Як допомогти в інформаційній війні
- Як допомогти знайти російських убивць
- Як захистити чат будинку
- Як перевірити людей, які пишуть у приват
- Якщо Ви поширили фейк...
- Чи можуть мене підслухати окупанти

Правила інформаційної гігієни

Далі

Під час війни критично важливо фільтрувати інформацію. Ворог поширює дезінформацію (часто — соцмережами), яка може загрожувати вашому життю.

Якщо ви отримали будь-яку інформацію...

① **Визначте, чи джерело надійне.** Плітки у місцевих чатиках, великі телеґрам-канали, які поширюють новини без покликань, експерти на телеефірах — це не надійні джерела. Навіть якщо вам щось схвильовано повідомляє мама — уточніть, звідки взято інформацію, та загляньте в першоджерело.

② Знайдіть підтвердження в державних джерелах.

Усі активні посилання на ресурси шукайте в описі нашого профілю

Як розпізнати дез-інформацію?

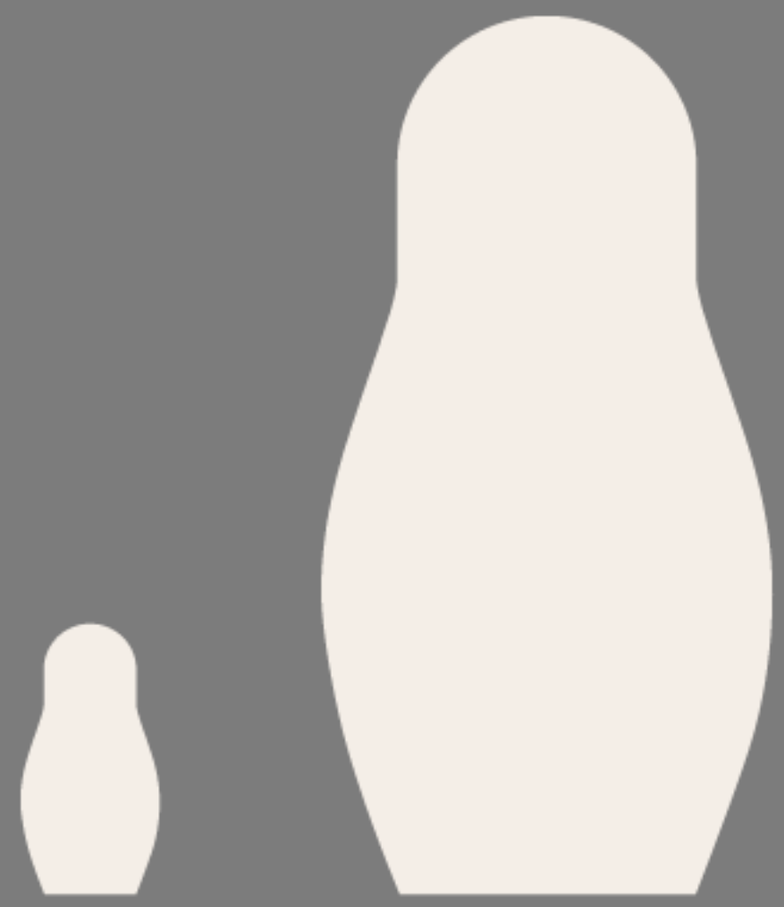
Далі →

Є 4 типові **стратегії** створення **дезінформаційних** меседжів.

Якщо ви бачите схожі риси у повідомленнях чи новинах, **не поспішайте їм вірити**. Усі ці елементи наявні в більшості офіційних виступів російських політиків.

Зневажай та принижуй опонента (dismiss)

Що **емоційніше принижен**ня опонента в новині, то ретельніше треба перевіряти факти. На думку путіна: «Украина никогда и не имела традиций собственной государственности».



Перекрути факти (distort)

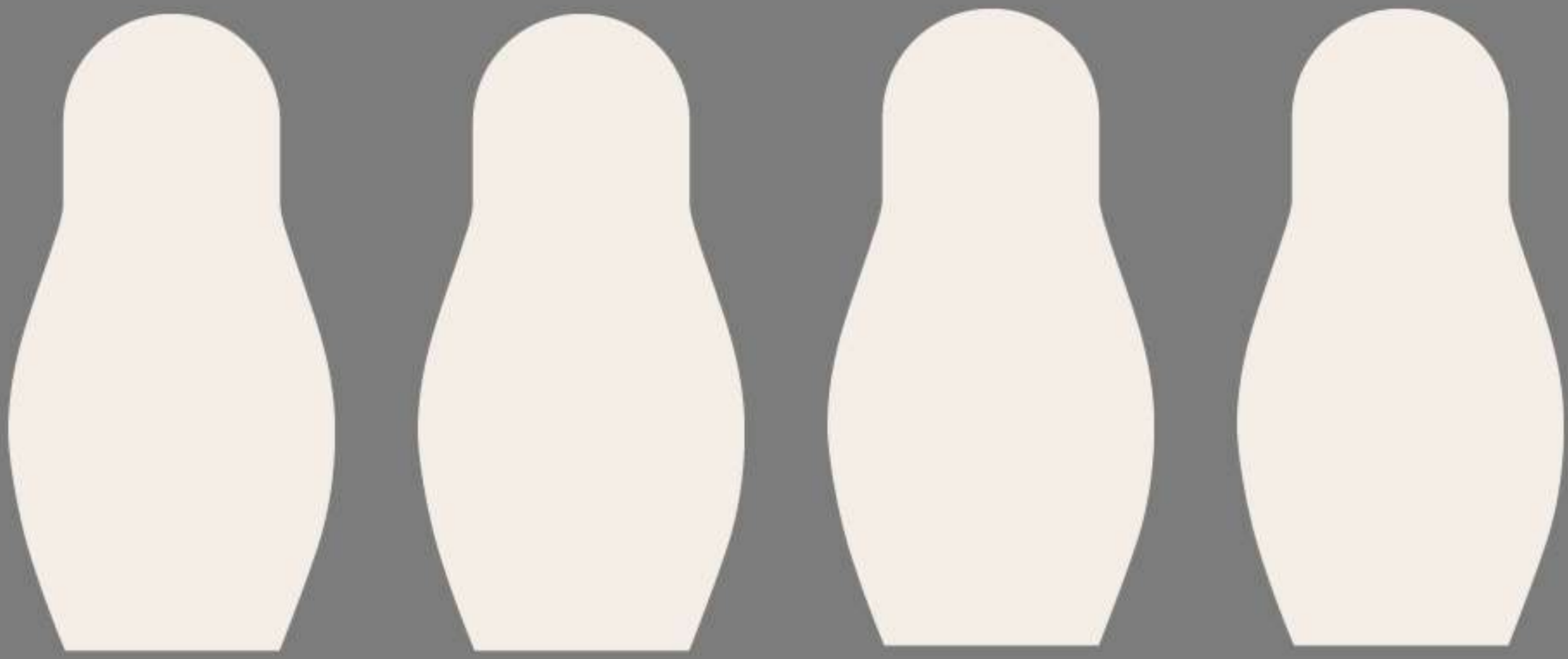
Такі повідомлення базуються на тому, що справді сталося, але **інтерпретація повністю змінює сенс**. Що більше оцінювальних суджень у повідомленні, то нижча імовірність, що це правда. Наприклад, підвищення цін на комунальні послуги путін інтерпретує так: «У людей на Украине нет денег, чтобы оплачивать коммунальные услуги. Им приходится выживать».

Відволікай (distract)

Звинувать своїх опонентів у тому ж, що закидають тобі. Ось що говорить голова МЗС росії про обстріли у Харкові: «Глава МИД России Сергей Лавров заявил, что в Харькове нет российских войск», — натякаючи, що місто обстрілює сама Україна.

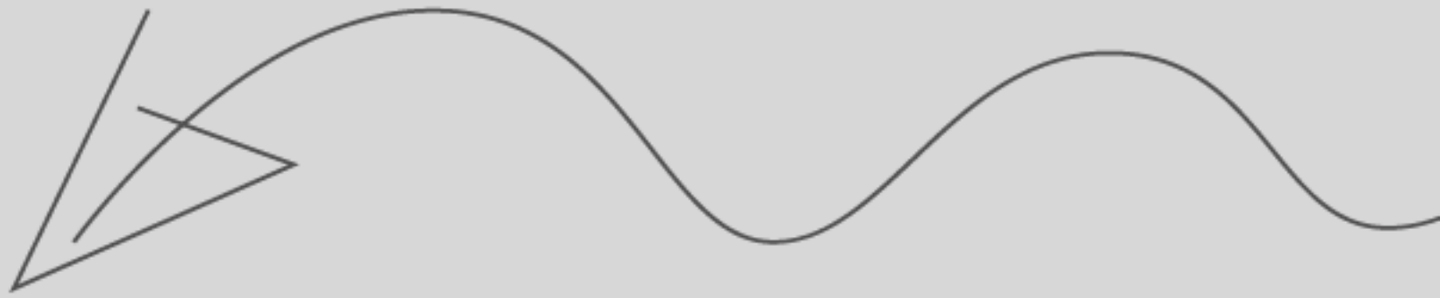
Залякуй
(dismay)

Агресивні повідомлення, щоб залякати опонента та відмовити щось робити, «**повідомлення-лякалки**»

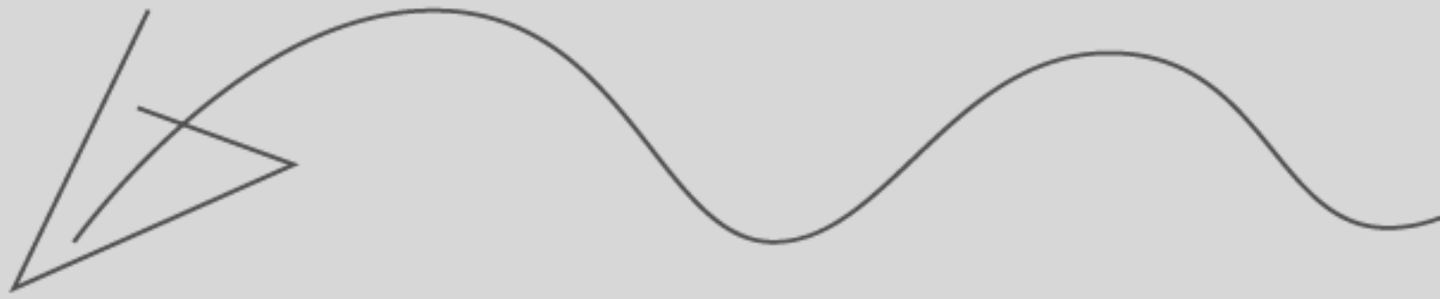


Російська дезінформація може «пролазити» й у наш інформаційний простір.

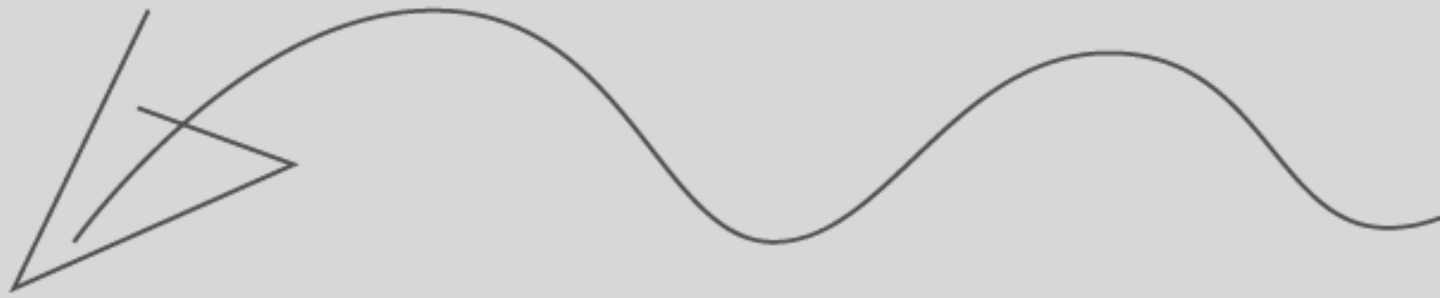
Як реагувати на неї?



Якщо будь-яка новина чи повідомлення викликає у вас сильні та яскраві емоції — **відправте її в карантин** хоча б на 10 хвилин. Лише після того, як розум охолоне, поверніться до цієї новини, щоб критично проаналізувати, **що сталося насправді**.



Якщо ви знайшли дезу в соцмережах, обов'язково **поскаржтеся на цей допис** чи профіль, щоб пост видалили. Наприклад, Facebook дуже не любить дезінформацію та намагається активно її усувати.



Якщо ви побачили дезу, яка активно ширилася соцмережами, — **опублікуйте спростування** та повідомте якомога більшій кількості людей про дезінформацію. Кожен та кожна з нас може долучитися до захисту України на інформаційному полі.

Як працює інформаційна війна?

Далі →

Інформаційна війна — це спосіб впливу на населення через поширення інформації. **Мета** — морально послабити опонента, дезінформувати та залякати.

Під час інформаційної війни:

- публікують та поширюють фейки та маніпуляції про опонента в медіа та соціальних мережах;
- поширюють пропаганду на населення своєї країни та опонента;
- збирають тактичну інформацію про опонента;
- захищають власні інформаційні ресурси від інформаційних атак опонента.

Один з інструментів противника — **ботоферми**. **Бот** — це сторінка несправжньої людини в соцмережі, яка поширює неправдиву інформацію. А **ботоферма** — комп'ютер, який контролює сотні ботів.

Як можна відрізнити бота?

- На сторінці користувача немає особистої інформації.
- Відсутня аватарка / фото, взяте з інтернету.
- Десятки публікацій та репостів за короткий проміжок часу.
- Миттєві відповіді на ваші повідомлення в чатах.

Під час інформаційної війни працюють не лише на опонента, а й на його союзників. Скажімо, під час російсько-української інформаційної війни важливо залучитися підтримкою населення наших країн-союзників. Українцям це вдалося! **У 141 країні світу точно знають, хто агресор у цій війні**.

Що можна **зробити на інформаційному фронті**?

① Перевіряйте будь-яку інформацію, яку ви чуєте або читаєте.

② Довіряйте лише перевіреним джерелам.

③ Поширюйте за кордоном інформацію про російсько-українську війну.

④ Скаржтеся на соцмережі пропагандистів противника та тих, хто поширює неправдиву інформацію про війну.

Яку інформацію про українську армію не можна поширювати?

Далі →

Нині ми як ніколи активно обмінюємося інформацією та новинами у соцмережах. Одні дані рятують життя, інше — можуть нам зашкодити.

Ось список тем, що стосуються нашої армії, які **не можна поширювати за будь-яких умов**.

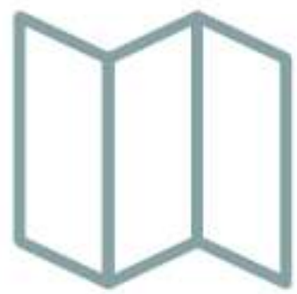
Найменування частин та підрозділів, їхнє розташування

Кількість військових у частинах та підрозділах

Кількість озброєння та техніки, їхні стан і місце зберігання

Дані про зброю, яку надають партнери

Операції, які проводять або планують



Дані про систему охорони та оборони військових частин

Переміщення та розгор-
тання військ (найменуван-
ня, кількість, маршрути)

Порядок залучення сил
(військових) та засобів
(озброєння)

Збір
розвідувальних
даних

Військові частини
та їхню тактику,
методи дій

Унікальні операції
та спосіб
їх виконання

Інформаційна війна — це теж фронт.
Не давайте ворогу зайвої інформації.

Як допомогти Україні, якщо є комп'ютер та інтернет?

Далі →

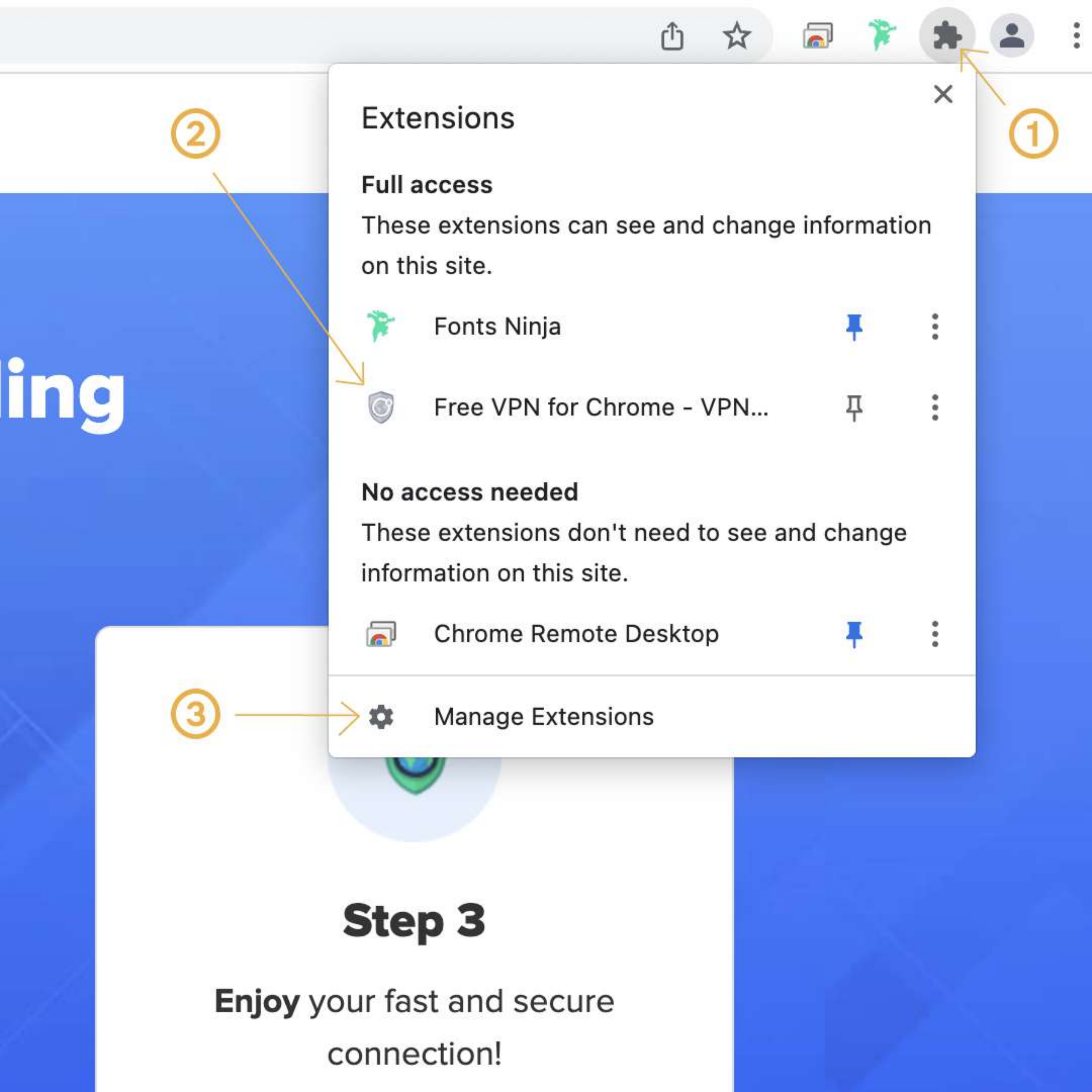
- Вмикаємо ПК чи ноутбук!
- Відкриваємо браузер.
- Якщо у вас не Google Chrome, то встановлюємо веббраузер Google Chrome.

○ Переходимо за покликанням

https://chrome.google.com/webstore/detail/free-vpn-for-chrome-vpn-p/majdfhpaihoncoakbjgbdhglocklcgno?hl

○ Встановлюємо **VeePN**.

○ Натискаємо кнопку ①, потім ② (якщо немає кнопки ② — натискаємо кнопку ③).


Extensions
Full access
These extensions can see and change information on this site.
Fonts Ninja
Free VPN for Chrome - VPN...
No access needed
These extensions don't need to see and change information on this site.
Chrome Remote Desktop
Manage Extensions
1
2
3
ing
Step 3
Enjoy your fast and secure connection!

Developer mode

Free VPN for Chrome - VPN Proxy VeePN

Fast, ultra secure, and easy to use VPN service to protect your privacy online. Enjoy Unlimited Traffic and Bandwidth!

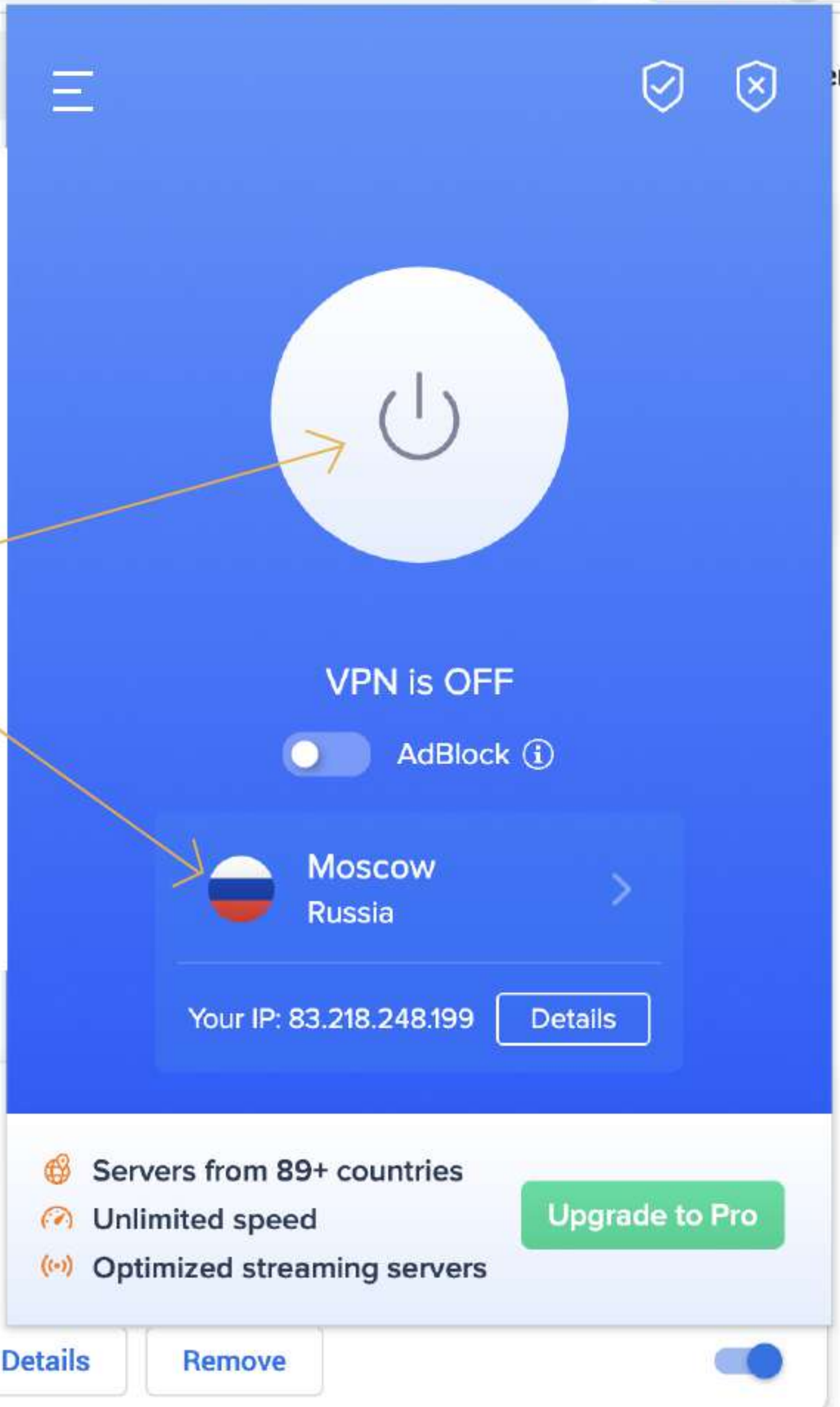
Details

Remove

ymous

Увімкнути

Натискаємо
та обираємо
«россия» та
вмикаємо

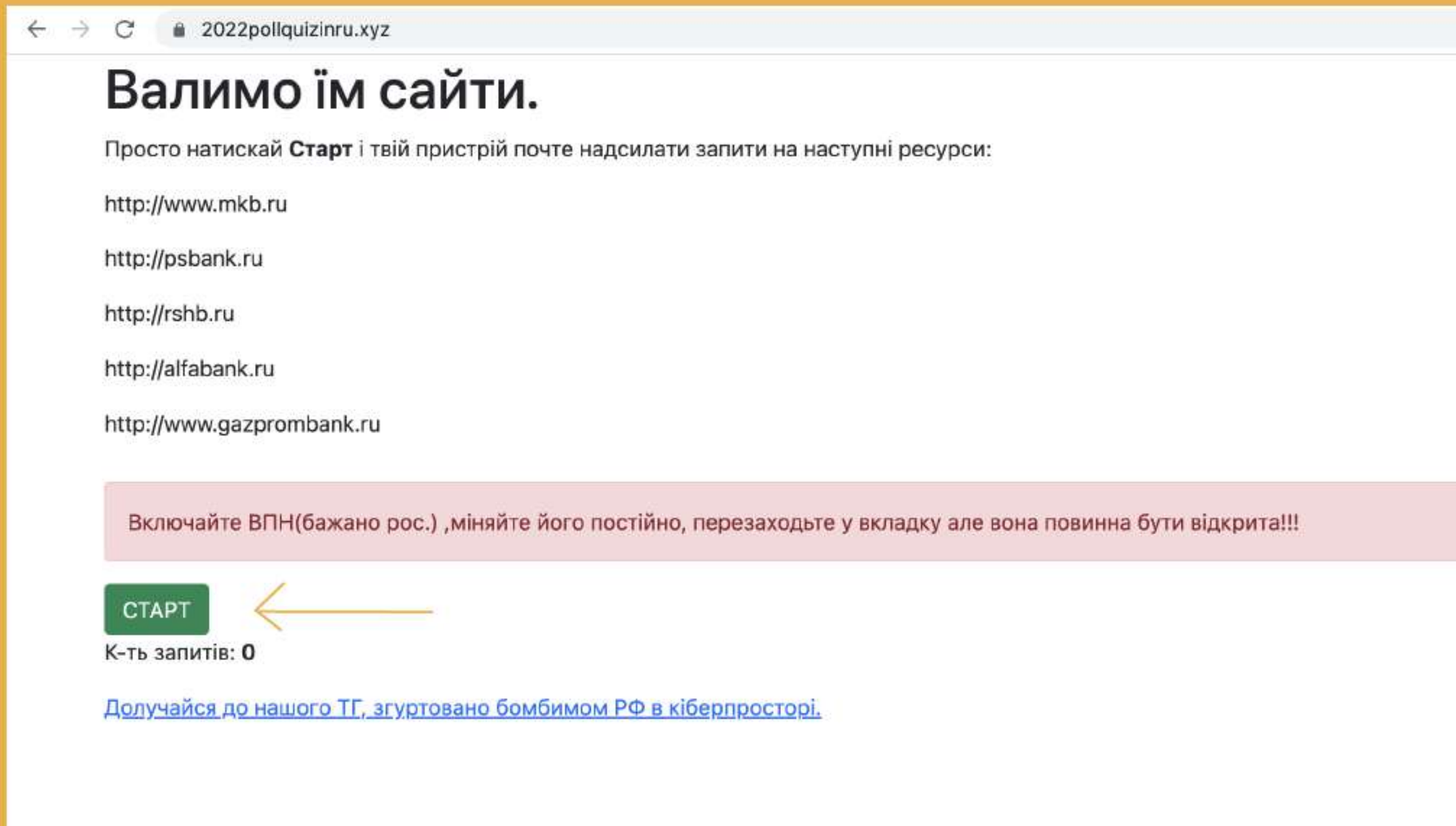


ets
te and edit spreadsheets
emove

Details
Remove

О Переходимо за покли-
канням та натискаємо
«Старт».

https://2022pollquizinru.xyz/

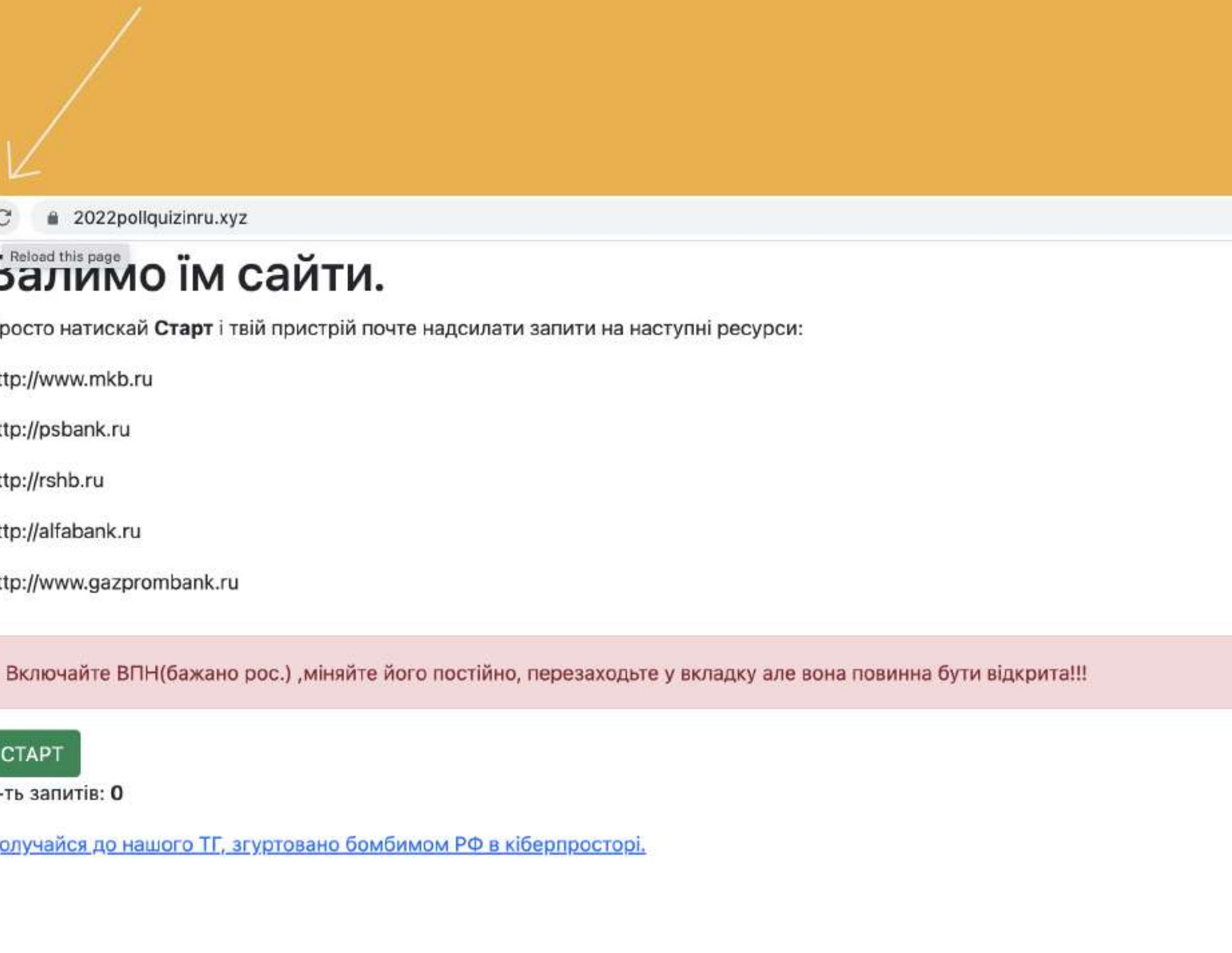


- **Уважно**: закладка повинна бути окремою або верхньою, інакше запити не йдуть.
  Для цього просто перетягніть закладку мишкою вбік. Ютуб або інше дивіться в окремому вікні.

- Вікон може бути декілька (скільки потягне комп).

- Періодично треба змінювати IP, для цього просто заново обирайте регіон «Россия» або інший. Регіон автоматично змінюється на всіх закладках, але їх треба перезавантажити.

- Після зміни IP обов'язково перезавантажте кожну закладку та знову натискайте «Старт».



Готово!
Ви котики,
а рускій
карабль іде
нахуй.

Куди писати, щоб допомогти знайти російських вбивць?

Далі →

- Телеґрам чат-бот **@ruskie_vbyvtsi**. Сюди можна надсилати фото та відео російських військових, які вбивали українців. Якщо у вас є інформація з камер спостереження в Ірпені, Бучі, Гостомелі чи з інших джерел, які зафіксували обличчя рашистів, — надсилайте її в цей бот.

- Телеґрам-бот **t.me/tribunal_ua_bot**. Тут можна повідомити про воєнні злочини проти громадян України.

- dokaz.gov.ua — державний сайт за підтримки Офісу Президента, Міністерства юстиції, Офісу Генерального прокурора та інших організацій для документування воєнних злочинів та злочинів проти людяності.
- Телеґрам-бот t.me/war_crime_bot для документування воєнних злочинів, злочинів проти людяності, порушення прав людини та інших порушень міжнародного та національного права.

- warcrimes.gov.ua — державний сайт за підтримки Офісу Генерального прокурора для фіксації воєнних злочинів проти цивільного населення.

- Телеґрам-бот t.me/oboronaonline_bot, за допомогою якого можна поширити будь-яку важливу інформацію. Пишіть у бот те, що хочете опублікувати. А 200 українських блоґерів розкажуть про це на своїх особистих сторінках.

- culturecrimes.mkip.gov.ua. На сайті можна заповнити анкету та надіслати інформацію про злочини проти культурної спадщини України. Матеріали використають у Міжнародному кримінальному суді в Гаазі та спеціальному трибуналі як докази для кримінального переслідування причетних до злочинів.

- www.facebook.com/Ukraine.5am — фейсбук-спільнота коаліції з документування воєнних злочинів.

- Телеґрам-бот t.me/SaveEcoBot фіксує військові злочини проти довкілля.

Як захистити чат вашого будинку?

Далі →

Нині чати у вайбері й телеґрамі — один із ключових способів комунікації, зокрема між сусідами. Окупанти використовують їх, щоб поширювати паніку, шукати інформацію про певні райони чи житлові комплекси. Ці дані також потрібні для організації мародерства.

Нижче чекліст порад, які допоможуть зробити ваш чат безпечним.

1. Змініть назву чату на нейтральну. Не використовуйте конкретні геодані (назву вулиці, комплексу, району). Наприклад, назву чату «Мешканці вул. Шевченка, 8» замініть на «Наш дім». Завантажте нейтральне зображення. На фото не має бути вашого будинку або двору.

2. Обмежте можливість додавати нових учасників в чат. Ймовірність, що у вас упродовж 4-х днів війни з'явилися нові сусіди — малоймовірна. Випадкові люди можуть використовувати інформацію з чату та особисті дані учасників у ворожих цілях.

❸ Не відповідайте в чатах на запитання, якою дорогою краще поїхати або де розташовано блокпост. Такі теми обговорюйте лише у приватних повідомленнях з людьми, у яких ви впевнені на 100 %.

❹ Якщо в чаті ви не знаєте всіх учасників та не впевнені в них, не поширюйте фото та відео з вікон вашого будинку.

❺ Створіть запасний чат в іншому месенджері, який будете використовувати, якщо основний заблокують.

6. Звертайте увагу на однакові повідомлення. Диверсанти не друкують кожен запит окремо, а копіюють. Часто такі повідомлення містять граматичні помилки.

7. Якщо сумніваєтеся, чи людина дійсно ваш сусід, влаштуйте їй перевірку. Наприклад, запитайте, який у вас тариф на обслуговування прибудинкової території або хто голова ОСББ.

Дбайте про свою безпеку та безпеку сусідів!

Як перевірити людей, що пишуть вам у приватні повідомлення?

Далі →

1

Запитайте звідки (від кого) при-
йшла ця людина, чи хтось із ваших
спільних знайомих може підтвер-
дити її особу.

2

Попросіть представитися, розпові-
сти про себе, дати покликання на
соцмережі (якщо вони порожні чи
новостворені, це поганий знак).

3

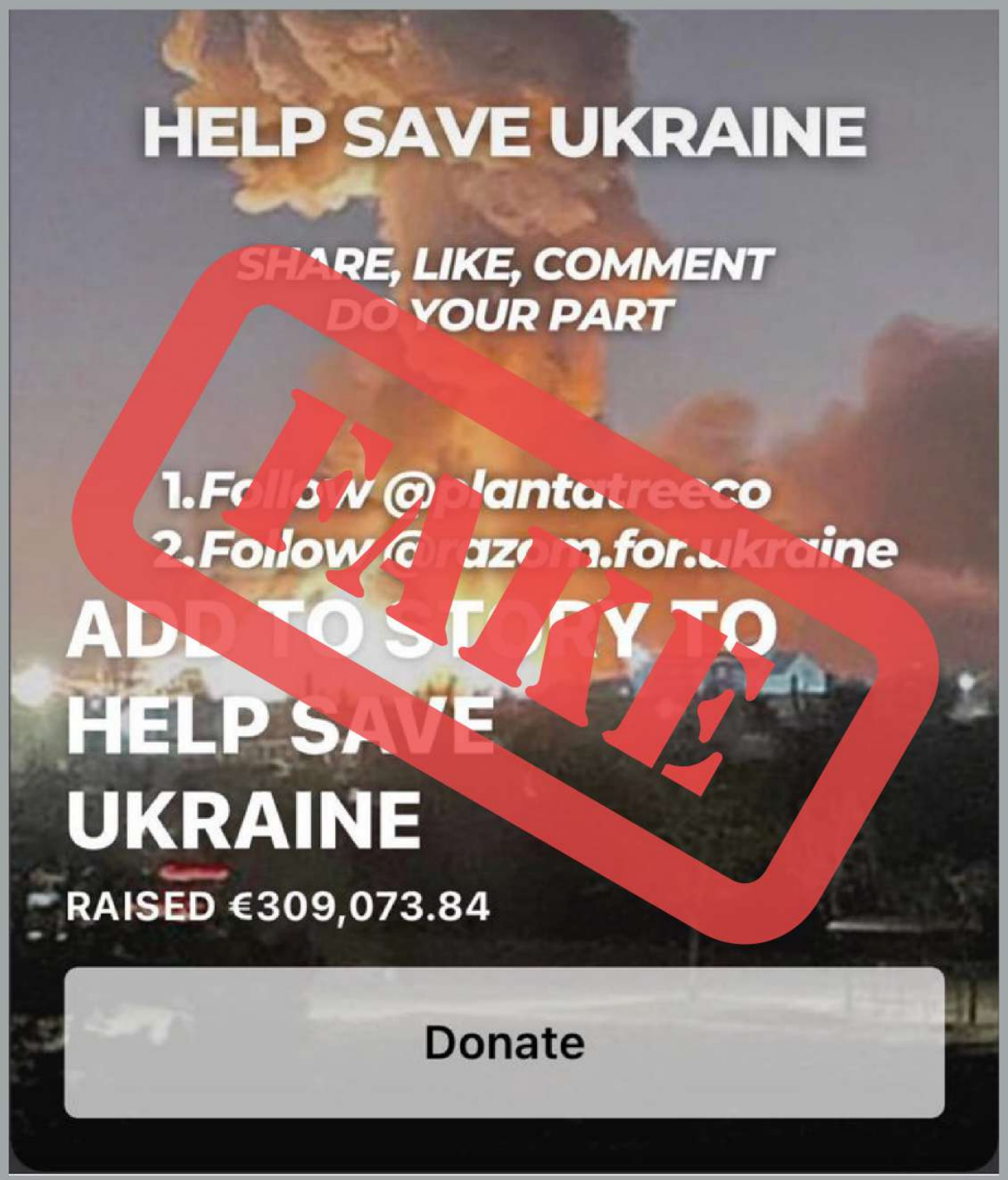
Зверніть увагу, що хоче від вас
людина. Якщо незнайомець запи-
тує вас про місцеперебування, це
вже привід насторожитися.

Довіряйте насамперед родичам та близьким людям, у яких ви точно впевнені.

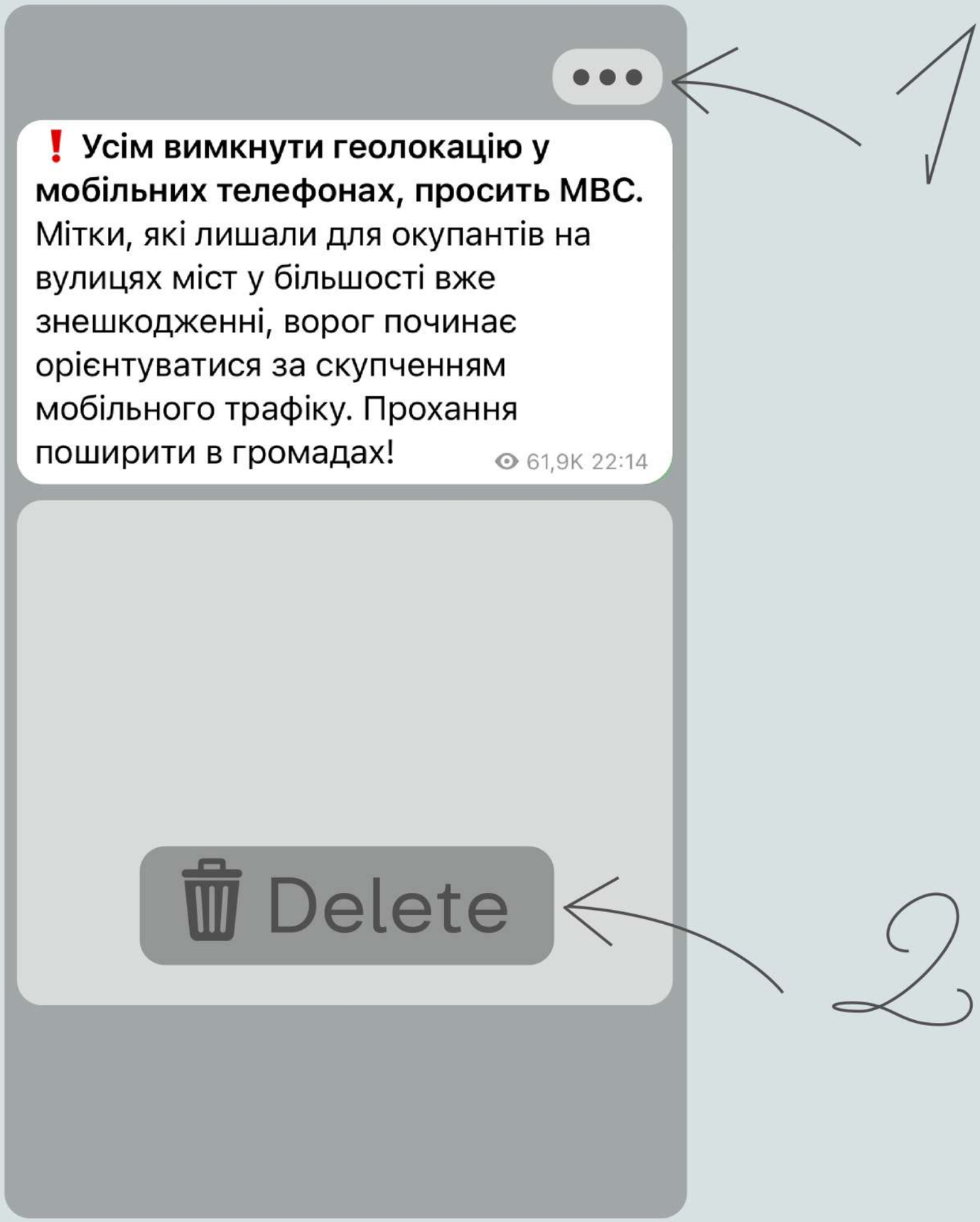
Якщо вам пишуть незнайомці,
які не можуть підтвердити,
що в них немає злих намірів,
краще передавати їхні контакти
в поліцію.

Що робити, якщо ви поширили фейк у фейсбуці чи інстаґрамі?

Далі →

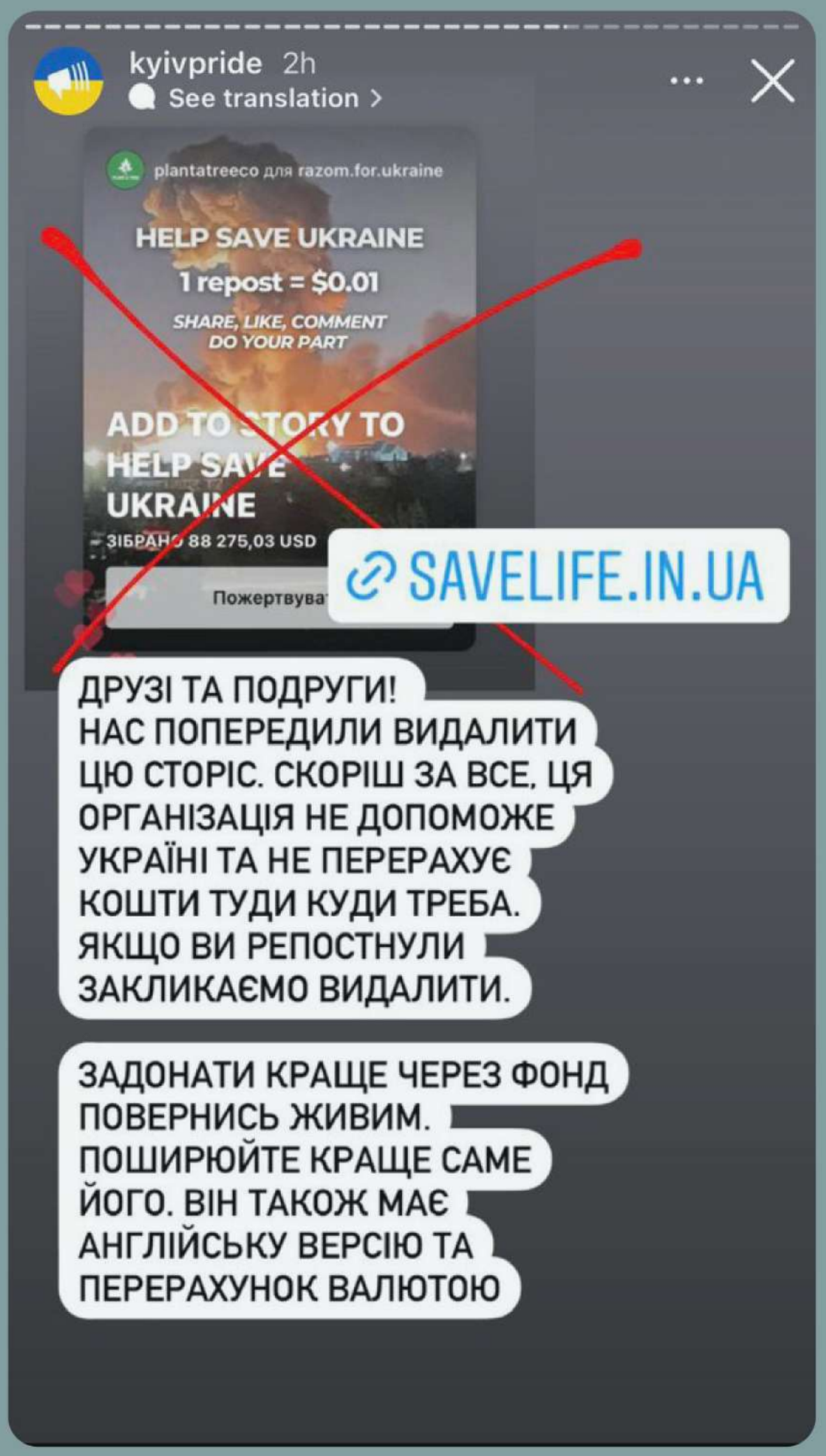


Алгоритм дій в таких ситуаціях залежить від того, скільки людей побачило і поширило фейкову інформацію.



Якщо ви поширили фейк, але майже одразу зрозуміли, що інформація неправдива і ніхто не встиг її побачити чи поширити, можете просто видалити сторіз чи публікацію.

Якщо ваш допис з фейком поширили інші люди, відімкніть можливість ділитися цією публікацією. Далі в описі до допису напишіть, що інформація — фейк. Опублікуйте сторіз, що ваш допис був фейковим і не варто далі поширювати цю інформацію. За кілька годин можете його видалити.



Якщо ви поширили фейкову інформацію у сторіз, обов’язково після неї запишіть сторіз зі спростуванням.

Просто мовчки видаляти фейкову інформацію не варто, адже люди продовжать її поширювати з інших каналів.

Помилятися не страшно, страшно не визнавати помилки.

Чи можуть окупанти підслухати мою телефонну розмову?

Далі →

Технічно будь-який мобільний пристрій з операційною системою можуть прослуховувати. **Чи означає це, що не смартфони підслухати не можна?** Частково так. Адже на звичайний телефон неможливо встановити програмне забезпечення, яке частіше за все дає змогу підслухати розмову. Максимум, що можуть зробити зловмисники, — дізнатися вашу геолокацію.

Як це працює?

Мобільний телефон постійно надсилає запити до мережі, щоби під час дзвінка зв'язуватися з найближчою вежею мобільного оператора (стільником). Ці запити надходять до мережі й фіксують телефон. Його ідентифікаційні дані (номер, IMEI) та положення відносно найближчої вежі з антеною оператора.

Програма «прослуховування» може потрапити в телефон за допомогою:

- завантаження за покликанням або встановлення мобільного застосунку;
- встановлення за допомогою ПК або іншого мобільного пристрою;
- покликання, надісланого через MMS;
- блютуз-каналу;
- вайфай-каналу.

Щоб уникнути прослуховування, варто дотримуватися простих правил безпеки

Вимикайте блютуз та вайфай, коли вони вам не потрібні.

Не зберігайте важливу інформацію в телефоні, або обмежте її до мінімуму. Попри потужні засоби контролю за застосунками, сучасне шкідливе програмне забезпечення стає більш технологічним і складним. Воно може вимагати від користувачів цілком логічних дозволів, за допомогою яких дуже вдало маскується.

Завантажуйте застосунки лише з офіційних магазинів: GooglePlay для Android та AppStore для iPhone. Під час завантаження нової програми краще перевірити надійність розробника та популярність застосунку. Для цього достатньо подивитися на кількість завантажень. У популярних програмах їх зазвичай понад 500 000.

Не під'єднуйтеся до відкритих і потенційно ненадійних вайфай-мереж. Максимально захищайте свій домашній і робочий вайфаї.

Під час спілкування **не поширюйте стратегічно важливу інформацію**, особливо щодо переміщення військ та техніки ЗСУ.