

Залишатися в безпеці в Інтернеті

Чому кібербезпека важлива для мене?

Інтернет і соціальні мережі — це дивовижні платформи, які допомагають нам ділитися інформацією та залишатися на зв'язку з друзями та родиною.

Однак злочинці та інші незаконні організації також використовують їх, щоб отримати ваші гроші, інформацію або вас залякати.

Вони можуть діяти з будь-якої точки світу, вільно володіють багатьма мовами та створюють переконливі підроблені веб-сайти. Вони контактують з вами через електронну пошту, соціальні мережі та текстові повідомлення, намагаючись викликати у вас страх або тривогу, щоб ви не могли мислити ясно.

Усе це означає, що ви повинні бути підготовленими та завжди усвідомлювати хитрощі, які вони використовують.

З якими поширеними проблемами я можу зіткнутися в Інтернеті?

Ось деякі з найпоширеніших ситуацій, з якими ми стикаємося.

- Ви отримуєте підозрілий електронний лист або текстове повідомлення, в якому вас просять перейти за посиланням.
 - Ці посилання часто ведуть на підроблені вебсайти, створені для крадіжки ваших логінів або фінансових даних.
- Ви отримуєте підозрілий дзвінок, у якому запитують особисту інформацію.
 - Як і в попередньому випадку, абонент може прикидатися співробітником вашого банку та просити надати інформацію.
- Ви отримуєте повідомлення від когось, хто видає себе за авторитетну особу, намагаючись змусити вас щось зробити.
 - Часто така особа висуває певну загрозу.
- Хтось отримує доступ до одного або кількох ваших онлайн-облікових записів (наприклад, електронної пошти чи соціальних мереж).
 - Якщо хтось отримує доступ до вашого облікового запису, він може викрасти інформацію, перенаправити платежі та навіть видавати себе за вас, щоб потенційно націлитися на ваших друзів чи родину.
- Дані вашої кредитної картки викрадені, або вас ошукують у фіктивному продажу чи інвестиції.

- Шахраї сподіваються, що ви побачите вигідну пропозицію та захочете оплатити її, не замислюючись. Або, можливо, реальний вебсайт став жертвою витоку даних, і ваші дані потрапили в мережу.

Є ще багато таких сценаріїв. Отримайте допомогу зараз –
[Візьміть відповідальність за свою безпеку онлайн.](#)

Як залишатися в безпеці в Інтернеті?

- **Довгі та унікальні паролі.**

- Чим довший пароль, тим він сильніший.
- Створіть запам'ятовуваний пароль довжиною понад 16 символів, об'єднавши чотири випадкові слова (наприклад: TriangleRhinoOperationShoes) і додаючи за потреби цифри, великі літери та символи (наприклад: Triangle&"Rhino"Operation2Shoes).
- Важливо: не повторюйте свої паролі. Якщо злочинець отримає один із ваших паролів, він спробує використати його й для інших облікових записів.
- [Створіть надійні паролі – Візьміть відповідальність за свою безпеку онлайн.](#)

- **Увімкніть двофакторну автентифікацію.**

- Це додаткова інформація – зазвичай це код на вашому телефоні – вам потрібно увійти на веб-сайт.
- Цей метод неймовірно потужний і може зупинити більшість спроб проникнути у ваші облікові записи.
- Ми рекомендуємо використовувати «додаток автентифікатора», якщо він підтримується.
- Для запам'ятовування паролів користуйтеся менеджером паролів та створюйте нові.
- [Налаштуйте двофакторну автентифікацію \(2FA\) – володійте своїм Інтернетом](#)

- **Залишайтеся приватними в Інтернеті.**

- Найкращий спосіб залишатися в безпеці в соціальних мережах – це увімкнути налаштування конфіденційності.
- Це не дозволить випадковим людям, зокрема кіберзлочинцям, переглядати ваші дописи або надсилати вам повідомлення.
- Тим не менш, з обережністю викладайте особисту інформацію про себе, вашу родину або ваших друзів.
- Переконайтеся, що контактні особи є тими, за кого себе видають.
- Остерігайтеся фальшивих запитів на додавання в друзі. Будьте обережні з людьми, які видають себе за журналістів або інших людей, яких ви добре не знаєте.
- [Захистіть свою конфіденційність в Інтернеті - володійте своїм Інтернетом](#)

- **Тримайте все в актуальному стані.**

- Коли ви оновлюєте свій телефон, комп'ютер або програмне забезпечення, це також закриває будь-які дірки в безпеці.
- Зловмисники завжди шукають способи проникнути, а оновлення усувають уразливості.
- Регулярно перезавантажуйте свої пристрої.
- [Будьте в курсі оновлень – володійте своїм Інтернетом](#)
- **Будьте в курсі шахрайств.**
 - Найкраща порада — бути в курсі цих шахрайств і стежити за ними, якщо злочинці спробують зв'язатися з вами на будь-якій онлайн-платформі.
 - Якщо щось здається не так, не спілкуйтеся з особою, яка зв'язалася з вами. Будьте особливо обережні, якщо вони просять гроші, навіть якщо вони виглядають доброзичливо.
 - Передивляйтеся дивні посилання та адреси електронної пошти (наприклад, ваш банк не надіслав вам електронний лист з облікового запису gmail).
 - *Ніколи* не натискайте на посилання у текстових повідомленнях.
 - Застосунки до вашого пристрою завантажуйте лише з офіційних магазинів застосунків.
 - Якщо ви сумніваєтеся, зверніться безпосередньо до організації та не переходьте за жодними посиланнями чи номерами телефонів, які вам надіслали.
 - Намагайтеся бути в курсі ризиків для безпеки в Інтернеті для себе, своєї громади та будь-яких груп, до яких ви належите.
- **Захистіть свою інформацію.**
 - Використовуйте зашифровані месенджери, наприклад, Signal. Це позбавить будь-кого можливості прочитати ваші повідомлення.
 - Надавайте інформацію веб-сайту лише в тому випадку, якщо адреса починається з HTTPS. Літера S означає «безпечно» - тобто будь-яка інформація, що надсилається між вами та веб-сайтом, зашифрована.
 - Розгляньте можливість використання віртуальної приватної мережі (VPN), яка може захистити ваші дані та приховати ваше місцезнаходження.
 - Перевірте, до яких даних і дозволів мають доступ ваші додатки. Наприклад, програмі для фітнесу не потрібен доступ до ваших контактів.

Що робити, якщо мене обдурять або щось гірше?

Є багато місць, куди можна звернутися по допомогу. Усі ці організації не повідомлятимуть ваші дані нікому, якщо ви не дасте на це згоди.

- Ви можете повідомити про кіберінциденти до NCSC через портал CERT NZ, і ми можемо допомогти або зв'язати вас з іншим агентством:
[Повідомити про інцидент | CERT NZ](#)
- Якщо ви втратили гроші, негайно зверніться до свого банку.
- Текстові повідомлення про шахрайство можна безкоштовно пересилати на номер 7726, до служби, яку підтримує Департамент внутрішніх справ.