



Home » Технології » Українців заманюють доступом до чужого WhatsApp: чим закінчується така спокуса

Українців заманюють доступом до чужого WhatsApp: чим закінчується така спокуса

DMITRUK ANDRIY — 04 Червня 2026, 01:53 2 Mins Read — ТЕХНОЛОГІЇ



WhatsApp / © unsplash.com

Важливі новини щодня — додайте «Експерт» в улюблені джерела Google

Шахраї почали активно поширювати схему, яка обіцяє доступ до чужих повідомлень у WhatsApp. Насправді ж користувачі ризикують втратити гроші та повний контроль над своїм смартфоном.

Про це повідомляють фахівці з кібербезпеки.

Зловмисники використовують цікавість, ревнощі та бажання прочитати чуже листування. Потенційним жертвам пропонують спеціальні сервіси або програми, які нібито дозволяють переглядати повідомлення інших користувачів WhatsApp.

Для доступу до такої послуги зазвичай просять невелику суму — від 200 до 500 гривень. Саме невисока ціна часто знижує пильність людей.

Після оплати користувачу надсилають посилання на додаток, який необхідно встановити на смартфон. Під час інсталяції програма запитує доступ до контактів, SMS-повідомлень та інших персональних даних.

Саме на цьому етапі шахраї отримують можливість контролювати пристрій.

Після встановлення шкідливого програмного забезпечення зловмисники можуть перехоплювати SMS із кодами підтвердження від банків, отримувати доступ до збережених паролів та навіть керувати мобільним банкінгом.

За інформацією експертів, особливу небезпеку становить те, що жертви часто не помічають ознак злому. Кошти можуть списуватися поступово невеликими сумами, а важливі повідомлення від банку блокуються або приховуються.

У результаті людина дізнається про проблему лише тоді, коли втрачає значну частину грошей або повністю виявляє порожні рахунки.

Фахівці наголошують, що отримати доступ до чужого WhatsApp за допомогою подібних програм неможливо. Месенджер використовує наскрізне шифрування, тому всі сервіси, які обіцяють «зламати» переписку, є шахрайськими.

Якщо користувач уже встановив підозрілий додаток або передав доступ до своїх даних, рекомендується негайно заблокувати банківські картки, змінити паролі та звернутися до кіберполіції.

Експерти також радять завантажувати програми лише з офіційних джерел, не переходити за сумнівними посиланнями та нікому не повідомляти коди підтвердження з SMS.

Читайте ЕКСПЕРТ у Google News

ПІДПИСАТИСЯ

Помітили помилку у матеріалі? Повідомте редакцію: corrections@expert.in.ua



ОСТАННІ НОВИНИ

СЬОГОДНІ

02:06 Жінка замкнулася у квартирі на три десятиліття: наслідки шокували навіть лікарів

01:53 Українців заманюють доступом до чужого WhatsApp: чим закінчується така спокуса

01:13 Вчені виявили небезпечний ефект вейпів: які смаки завдають найбільшої шкоди

00:55 Вчені розшифрували геном акули, яка живе 400 років: у чому секрет її довголіття

00:53 Чернівці вирвалися в лідери за цінами на оренду: наскільки подорожчали квартири

00:45 Вчені знайшли сліди зниклої планети: куди могла подітися п'ята планета-гігант

00:33 Розкрито таємницю кольорів паспортів: чому одні країни обирають червоний, а інші зелений

00:23 Українців попередили про борги у Німеччині: що потрібно зробити перед поверненням додому

00:14 Лікарі пояснили, як швидко прибрати свербіж після укусу комахи: прості способи допоможуть одразу

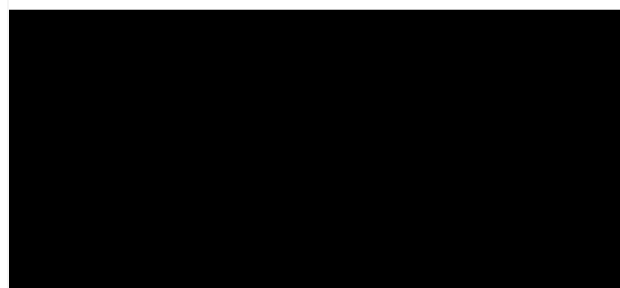
00:04 Вчені знайшли під кладовищем колонію з 5,5 мільйона бджіл: вона існує вже понад століття

LOAD MORE

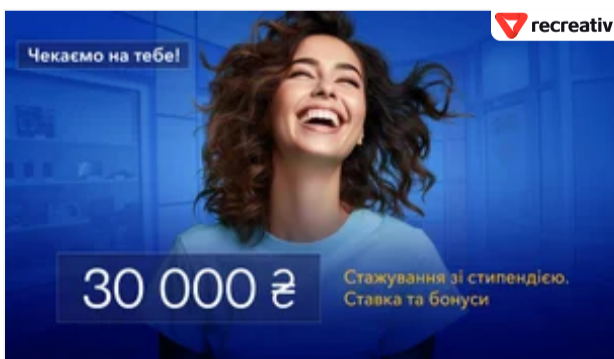
WhatsApp кібербезпека шахраї



Літня колекція суконь SALE



Якщо з'явилися варикозні вени або синюшні вузли, застосуйте це



Мрійте, прагніть, досягайте! Відкриті вакансії з конкурентною зп

КАТЕГОРІЇ НОВИН

Всі новини

Україна

Політика

Економіка

Світ

Стиль життя

Авто

Технології

Суспільство

Здоров'я

ІНФОРМАЦІЯ

Про проект

Автори

Редакційна політика і стандарти

Політика використання ШІ

Політика конфіденційності

Правила коментування

Контакти

ТОВ «НОВА МІДІА ГРУПА» © 2014—2026

Реєстрація R40-06871 у Реєстрі суб'єктів у сфері медіа

Адреса: 01014, м. Київ, вул. Звіринецька, 63

editor@expert.in.ua
corrections@expert.in.ua
reklama@expert.in.ua