ОСНОВИ КІБЕРГІГІЄНИ

Електронна пошта містить велику кількість конфіденційної інформації, такої як паролі, фінансові дані, контактна інформація тощо. Несанкціонований доступ до цих даних може призвести до крадіжки даних установи, фінансових втрат або навіть поширення шкідливих програм. Забезпечення безпеки електронної пошти є основною вимогою для збереження конфіденційності інформації.

БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

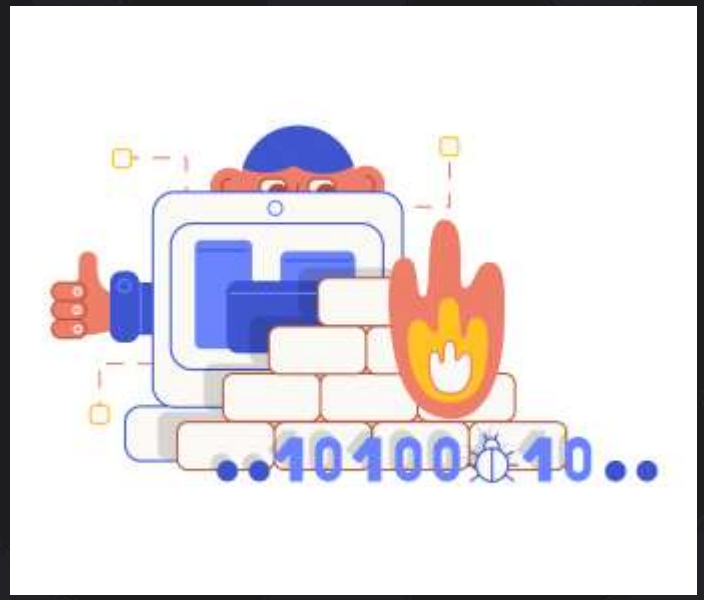
Порада 1. Уникайте підозрілих поштових повідомлень

Будьте обережні при відкритті поштових повідомлень, особливо від незнайомих або недостовірних відправників. Уникайте кліків на посилання або відкривання вкладень, якщо ви не впевнені в їхній надійності. Шахраї часто використовують фішингові техніки, щоб отримати корпоративні дані або встановити шкідливе програмне забезпечення на вашому комп'ютері.

Порада 2. Актуалізація програмного забезпечення

Важливо регулярно оновлювати операційну систему та програмне забезпечення свого комп'ютера або пристрою, що використовується для доступу до електронної пошти.

Виробники програм часто випускають патчі і оновлення, які виправляють виявлені уразливості і забезпечують безпеку користувачів. Встановлення оновлень допоможе запобігти атакам на вашу електронну скриньку.



Порада 3. Захист від фішингу

Фішинг є однією з найпоширеніших загроз електронної пошти. Це метод соціальної інженерії, коли зловмисники намагаються отримати ваші особисті дані, представляючись як довірче джерело. Будьте пильними і уважними до деталей, таких як доменні імена або граматичні помилки в поштових повідомленнях. Ніколи не надавайте особисту інформацію через електронну пошту, якщо ви не впевнені в достовірності отриманого запиту.

Фішинг

Фішинг (англ. phishing, від англ. fishing — ловити рибу) – це спроба оманливим шляхом отримати від вас особисту інформацію в Інтернеті.

Як правило, фішинг здійснюється за допомогою підроблених електронних листів, оголошень або сайтів, подібних до тих, з якими ви вже стикалися раніше.

Якщо ви отримали підозрілий лист:

1. переконайтеся, що електронна адреса й ім’я відправника збігаються;
2. перевірте, чи електронний лист автентифіковано;
3. перш ніж натиснути посилання, наведіть на нього курсор (якщо URL-адреса посилання не відповідає опису, то воно може переспрямовувати на фішинговий сайт);
4. переконайтеся, що в заголовку «Від» указано правильне ім’я.

Порада 4. Захист від вірусів і шкідливих програм

Щоб забезпечити безпеку вашої електронної пошти, встановіть надійне антивірусне програмне забезпечення на своєму пристрої. Регулярно оновлюйте антивірусні бази даних та скануйте свій комп'ютер на наявність шкідливих програм або вірусів. Також уникайте відкриття невідомих вкладень або завантаження файлів з підозрілих джерел.

Топ-7 способів розпізнати фішинговий електронний лист

1. Прохання підтвердити ваші особисті дані

Якщо ви не очікували отримання такого листа, але він раптом прийшов на вашу електронну скриньку, то це сигнал того, що лист може бути фальшивим.

Стежте за повідомленнями електронної пошти з проханням підтвердити особисту інформацію, яку ви ніколи не надали б, наприклад, банківські реквізити чи дані для входу.

Не відповідайте та не натискайте жодних посилань. Якщо ви вважаєте, що існує ймовірність того, що повідомлення електронної пошти є справжнім, краще знайти в інтернеті контактні дані компанії та зв'язатися безпосередньо. Але не використовуйте жодного способу зв'язку, передбаченого в електронній пошті.

2. Адреса відправника не виглядає справжньою

Часто трапляється так, що фішинг-лист надходить з адреси, яка лише видається справжньою. Злочинці прагнуть обманути одержувачів, включивши назву реальної компанії в електронну адресу пошти відправника.

Наприклад: @mail.airbnb.work на відміну від @Airbnb.com

Інший варіант обманути отримувача – зареєструвати домен з назвою реальної компанії, але з помилкою та відправити електронний лист з цього домену. Якщо назва компанії довга, то через неуважність можна не помітити помилки та прийняти фальшивий лист за справжній.

3. Велика кількість помилок в тексті

Прочитайте електронну пошту та перевірте наявність орфографічних та граматичних помилок, а також дивних фраз. Електронні листи від офіційних компаній вичерпно перевіряються на наявність орфографічних, граматичних та інших помилок.

Якщо ви отримали несподіваний електронний лист від компанії з купою помилок, це може бути показником, що насправді це фішинговий лист

4. Наявність підозрілих файлів, прикріплених до листа

Це досить сильна ознака фішингового листа, якщо ви не очікували отримати те чи інше вкладання.

Вкладення може містити зловмисну URL-адресу, що призводить до встановлення вірусу чи зловмисного програмного забезпечення на вашому комп'ютері чи мережі.

Навіть якщо ви вважаєте, що вкладення є справжнім, краще перед завантаженням просканувати його антивірусом або спеціальним онлайн-сервісом для сканування файлів.

5. Текст листа спрямований викликати паніку, поспіх

Фішингові електронні листи зазвичай вселяють паніку у одержувача та спонукають швидко щось зробити (натиснути кнопку, перейти за посиланням та ін.) У листі може стверджуватися, що ваш обліковий запис був зламаний і єдиний спосіб протидіяти цьому – ввести свої дані для входу.

Крім того, в електронному листі може бути вказано, що ваш рахунок буде закрито, якщо ви не діятимете негайно.

Головне, що необхідно зробити у такій ситуації, - це зберігати спокій, не піддаватися на провокацію. Якщо ви маєте сумніви, краще зв'язатися з компанією та уточнити. Але слід уникати використання способів зв'язку, які зазначені у підозрілому листі.

6. Увесь текст посилання міститься у зображенні

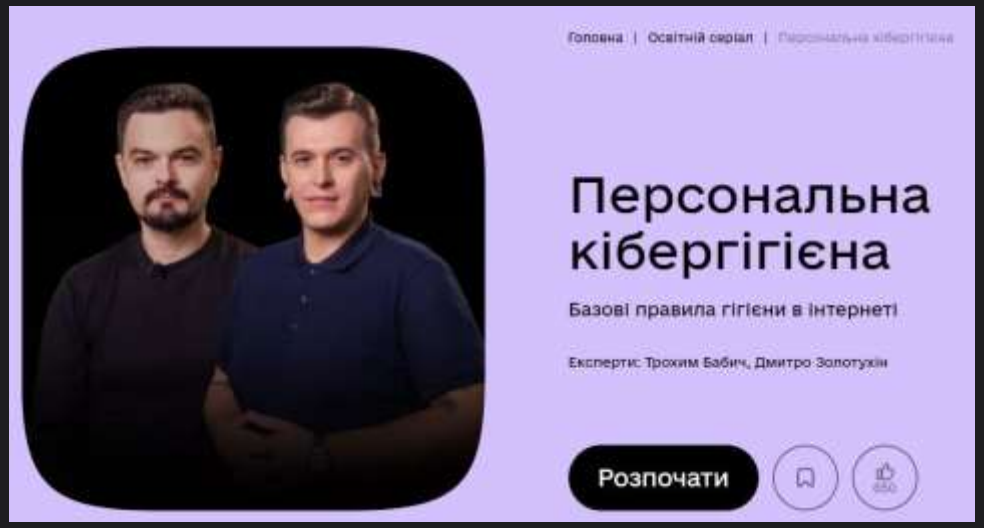
Ще одна ознака фішингового електронного листа – це наявність не звичайного текстового формату, а великого зображення, у якому міститься текст. Часто таке зображення є посиланням на фальшивий веб- сайт чи приховане завантаження вірусу.

7. Неперсоналізоване привітання у листі

Привітання типу "Доброго дня, шановний клієнт" може бути сигналом, що це фішинговий електронний лист. Інтернет-шахраї можуть збирати велику кількість електронних скриньок з відкритих даних, але не мати даних щодо імені отримувача. Тому вони змушені використовувати загальне звернення.

ІПД Держпродспоживслужба
№25.3/4218 від 24.02.2025
арк.1

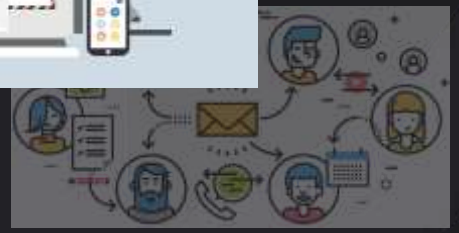
Освітні серіали для підвищення рівня обізнаності кібергігієни



https://osvita.diia.gov.ua/courses/personal-cyberhygiene

https://osvita.diia.gov.ua/courses/cyber-hygiene

Основні правила кібергігієни



1.Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.

2.Користуйтеся антивірусним програмним забезпеченням.

3.Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо).

4.Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу.

5.Не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад, на робочому столі).Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте стійкі паролі, зокрема такі що:

- містять не менше 8 символів;
- містять літери, цифри та спеціальні символи;
- не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо);
- не використовуються в будь-яких інших аккаунтах.

6.Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо)

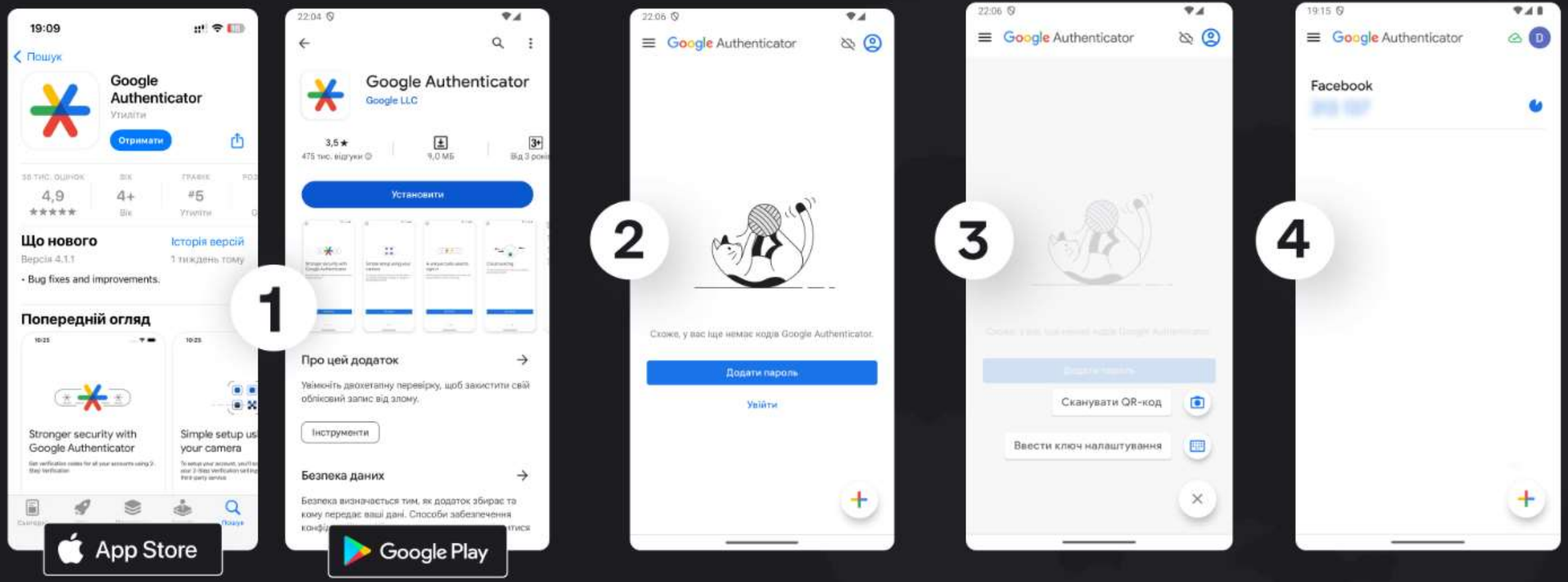
Signal

Viber

WhatsAp
p

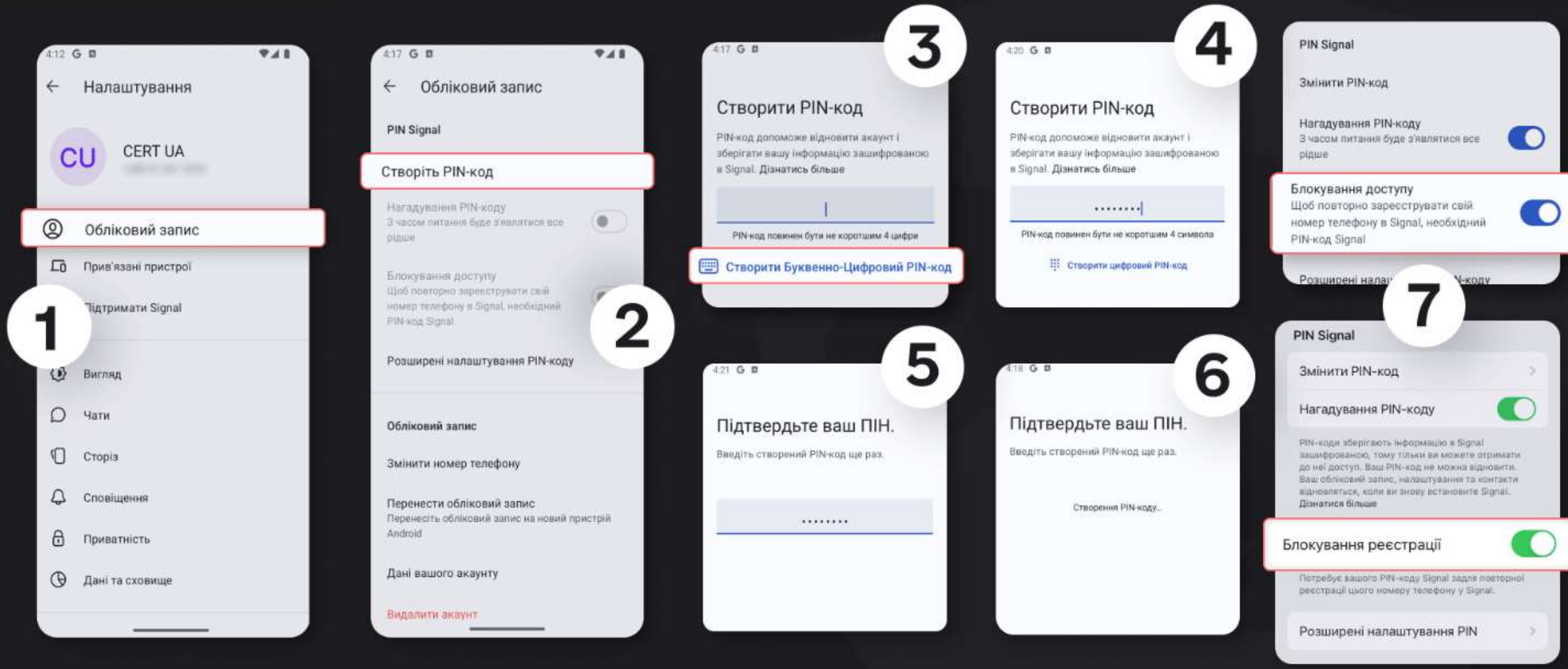
Google
Authenticator

Рекомендації щодо підвищення рівня захищеності облікових записів в месенджерах



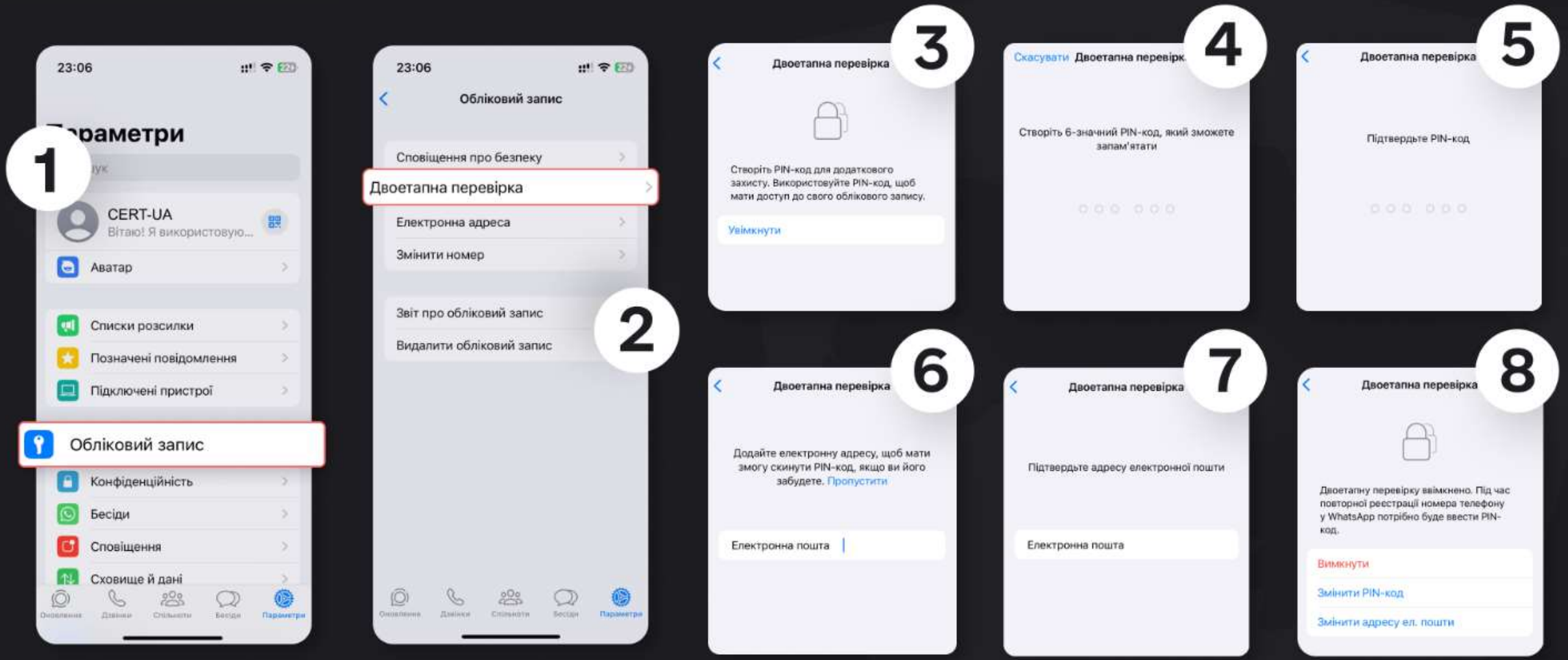
Google Authenticator

Встановлення та використання



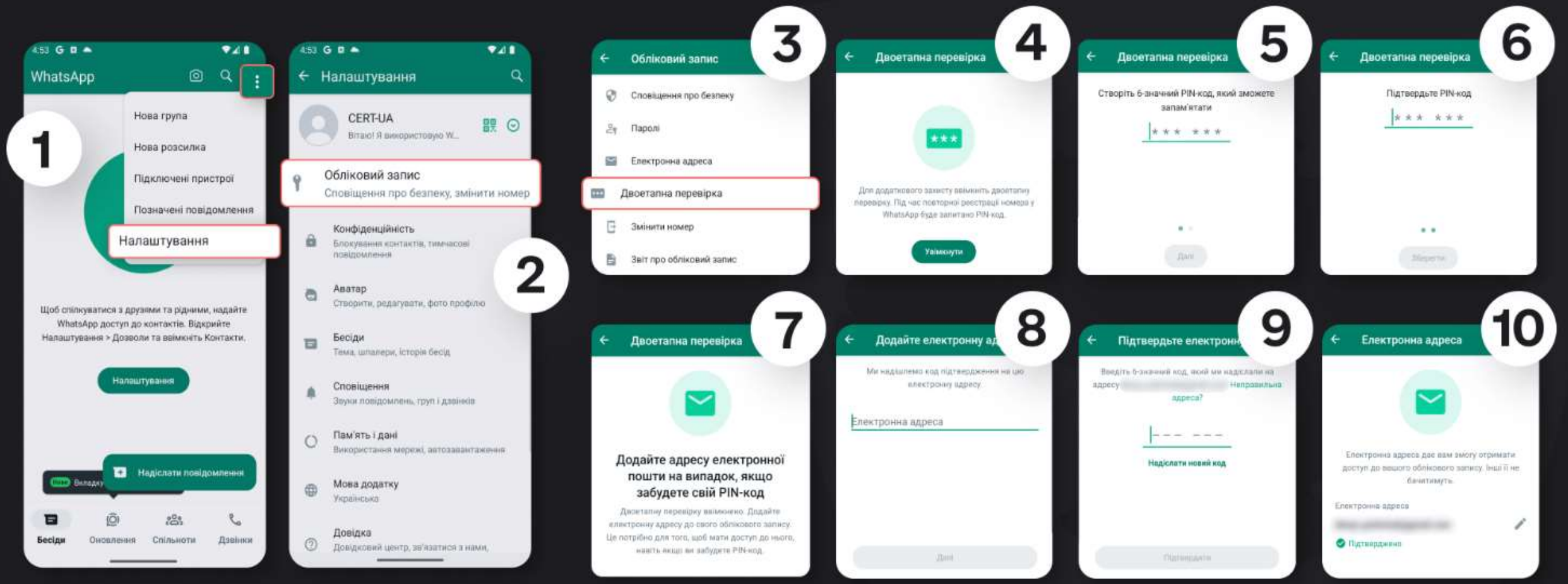
Signal

Налаштування двофакторної автентифікації



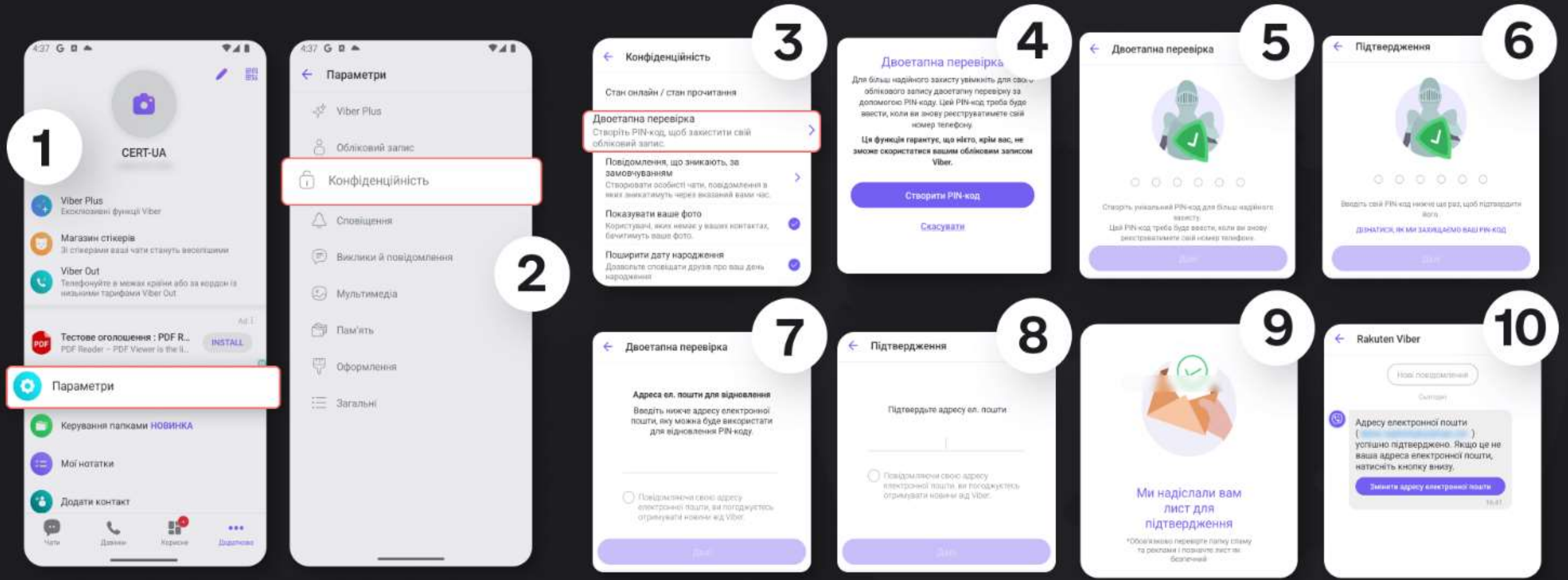
WhatsApp (iOS)

Налаштування двофакторної автентифікації



WhatsApp (Android)

Налаштування двофакторної автентифікації



Viber

Налаштування двофакторної автентифікації