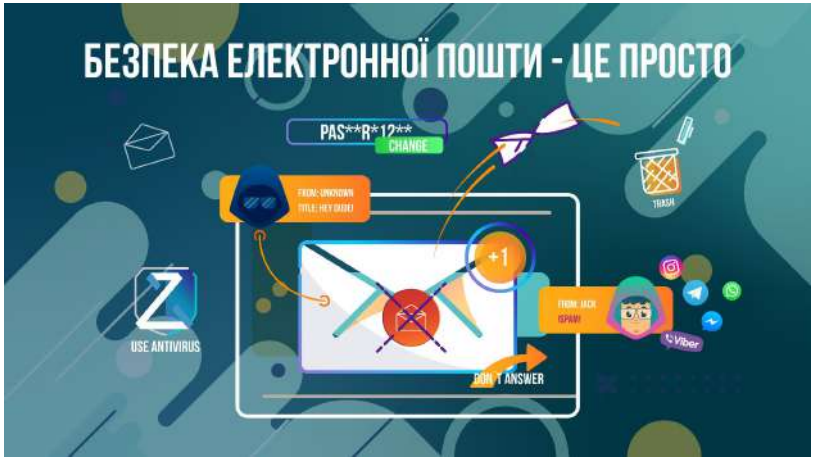
Основи кібергігієни



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

БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Департамент інформації та цифрових рішень Одеської міської ради

Порада 1. Уникання 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 ваші особисті 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.

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.**

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. *Наприклад, зловмисник може надіслати вам електронний лист, який виглядатиме так, ніби його відправлено зі структури ОМР, щоб ви надали певну інформацію.*

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.**

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 граматичних помилок в тексті листа

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.

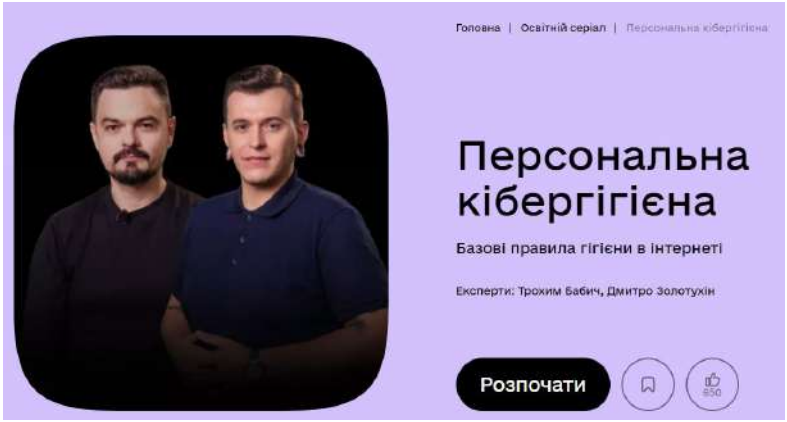
Головне, що необхідно зробити у такій ситуації, - це зберігати спокій, не піддаватися на провокацію. Якщо ви маєте сумніви, краще зв'язатися з компанією та уточнити. Але слід уникати використання способів зв'язку, які зазначені у підозрілому листі.

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.

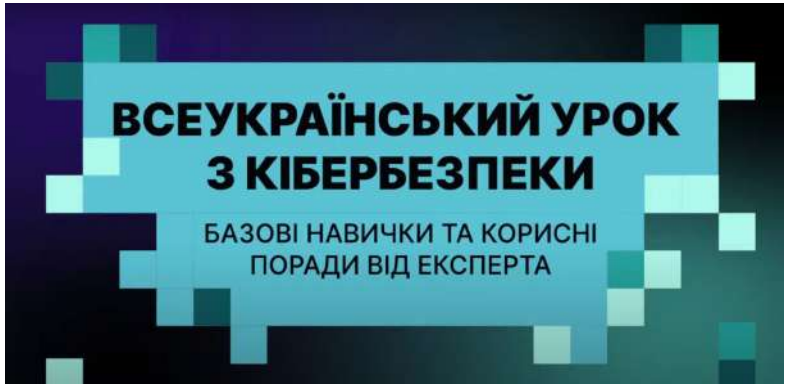


https://osvita.diia.gov.ua/courses/personal-cyberhygiene

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

КІБЕРГІГІЄНА.

Онлайн-серіали на плафтормі ДІЯ.ОСВІТА



https://www.youtube.com/watch?v=eVYrBbDpTz0

КІБЕРГІГІЄНА.

Всеукраїнський урок з кібергігієни: базові правила та корисні поради від експерта щодо безпеки онлайн

Основні правила кібергігієни

CERT-UA
https://cert.gov.ua/

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

2. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

3. Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.

4. Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».

5. Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо ви знайшли пристрій всередині офісу або на вулиці, чи отримали його поштою або з доставкою, чи незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити та перевірити його вміст – є велика ймовірність, що пристрій є небезпечним.

Довіряйте лише власним пристроям та будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях.

При підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення.

Відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

6. 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.

7. Уникайте використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).

8. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Сьогодні найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не відкривати файли навіть з безпечними розширеннями. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, усе одно потрібно перевірити (у телефонному режимі або в будь-який інший спосіб), чи дійсно ця особа надсилала вам повідомлення з вкладенням.

9. Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом **VirusTotal** для перевірки підозрілих файлів (VirusTotal дозволяє одночасно сканувати більш ніж 50-ма антивірусами). Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що, завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

VirusTotal — служба, що перевіряє підозрілі файли та полегшує швидке виявлення вірусів, хробаків, троянів і всіх видів шкідливих програм, що визначаються антивірусами.

Тричі подумайте перед відкриттям вкладень.

1. Під час користування інтернет-ресурсами (інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на вебсайти, які ви зазвичай не відвідуєте.

* Будьте уважним до проявів інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі “Інтернет” є фішинг. Особливу увагу варто звертати на доменне ім'я інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (**facelook.com**, **goooogle.com** тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній та самостійно «віддати» власні автентифікаційні дані.
* У разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з’єднання HTTPS, перевіряйте SSL-сертифікат вебсайту, щоб переконатися, що він не клонований або не підроблений.
* Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами на кшталт **tinyurl.com**, **bit.ly**, **ow.ly** тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.
* Використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.

2. Будьте обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не "схвалюйте" і не "приймайте" нічого похапцем.

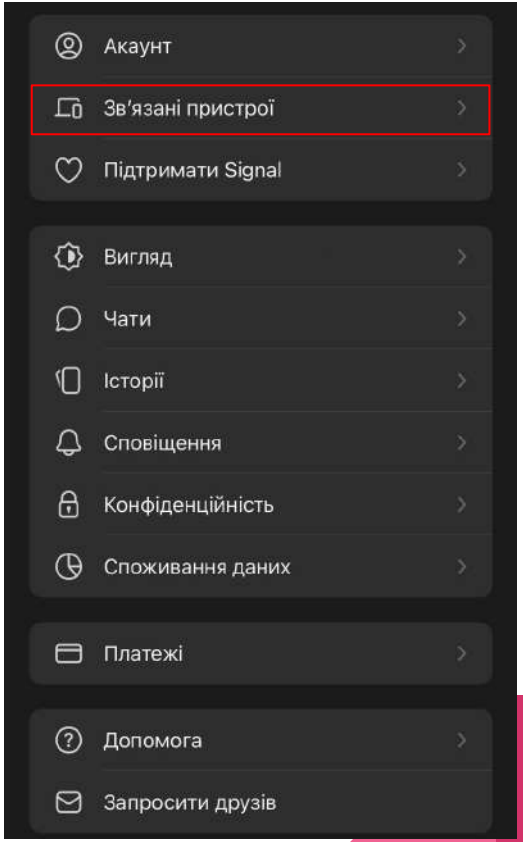
3. Під час використання віддаленого доступу необхідно обмежити доступ за допомогою "білого списку" (IP whitelisting) .

4. Установіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій.

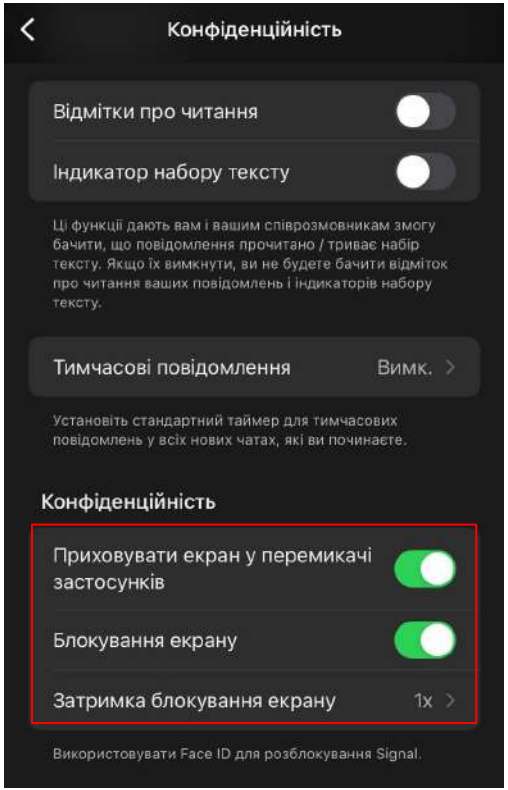
РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБЛІКОВИХ ЗАПИСІВ В МЕСЕНДЖЕРАХ ТА СОЦІАЛЬНИХ МЕРЕЖАХ

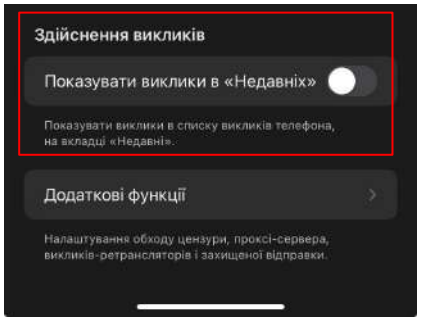
1.Месенджер Signal

Рекомендуємо періодично перевіряти інші активні сесії Вашого Signal-акаунта та закривати підозрілі чи невідомі. Перевірити Ви можете натиснувши на піктограму акаунта та перейшовши в пункт “Прив'язані пристрої”.

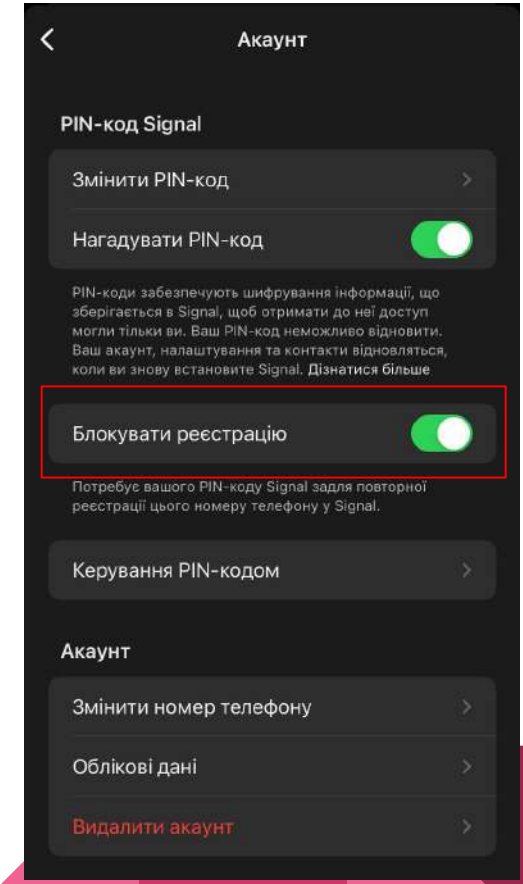


Також в меню ‘Конфіденційність” увімкніть пункти “Приховувати екран в перемикачі застосунків”, “Блокування екрану” та встановіть затримку на блокування екрану на 1 хв. Крім того, для користувачів iOS рекомендується вимкнути пункт “Показувати виклики у розділі “Недавні”.





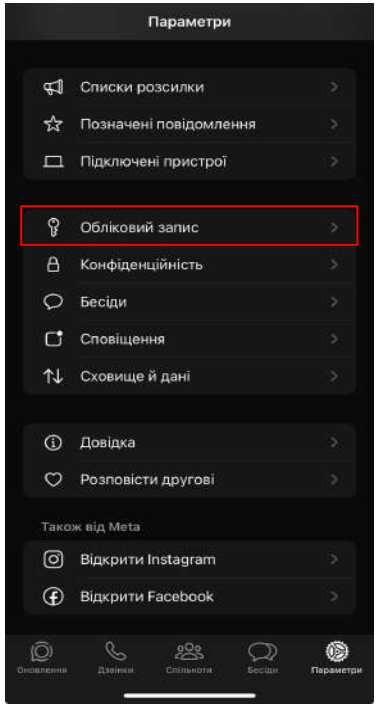
У пункті меню “Обліковий запис” увімкніть пункт “Блокування реєстрації” для унеможливлення використання Вашого номера для повторної реєстрації акаунта в Signal та доступу до Ваших повідомлень.

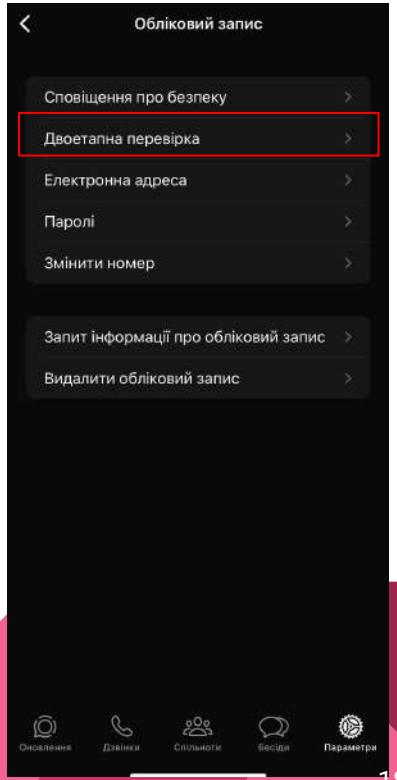


При отриманні повідомлення від невідомого номера з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

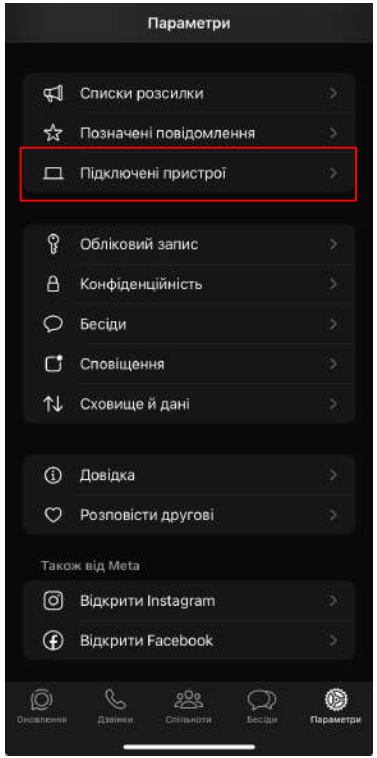
2.Месенджер WhatsApp

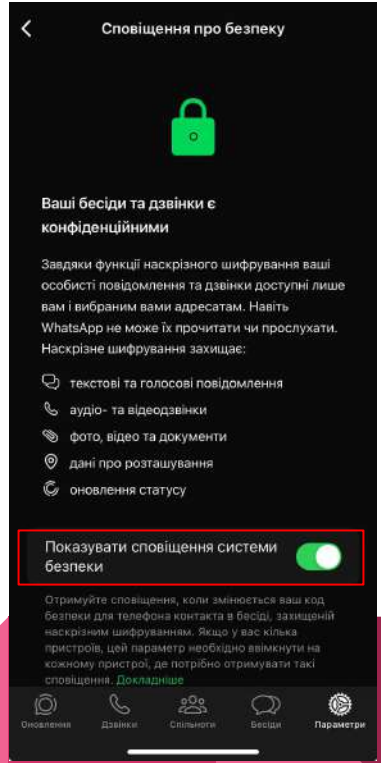
Для безпечного користування WhatsApp налаштуйте двохфакторну автентифікацію. Для цього перейдіть в “Параметри” та меню “Обліковий запис”. Там при переході в меню “Двоетапна перевірка”, керуючись підказками застосунку, налаштуйте двофакторну автентифікацію (необхідно буде вказати шестизначний пароль та електронну пошту).





Крім того, періодично перевіряйте пристрої, на яких авторизовано Ваш акаунт WhatsApp в меню “Підключені пристрої”, а також в меню “Обліковий запис”, перейшовши в пункт “Безпека”, увімкніть функцію “Показувати сповіщення системи безпеки”.

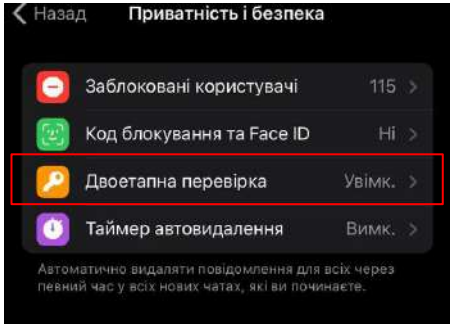




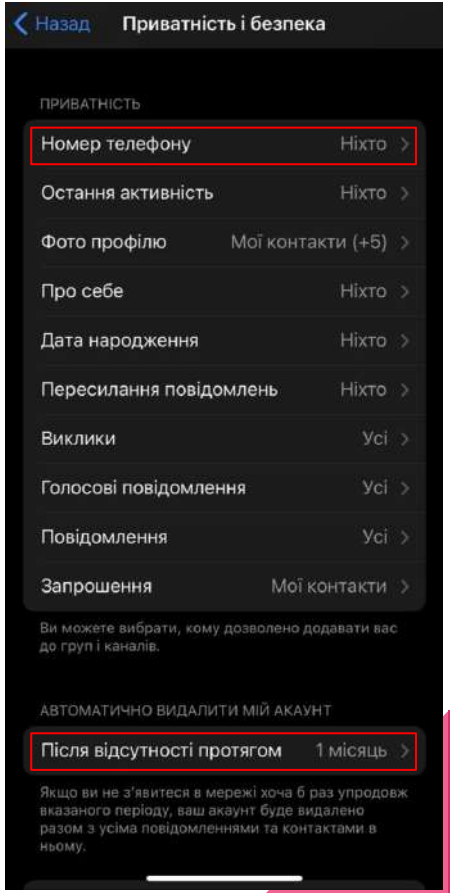
При отриманні повідомлення від невідомого номера з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

3.Месенджер Telegram

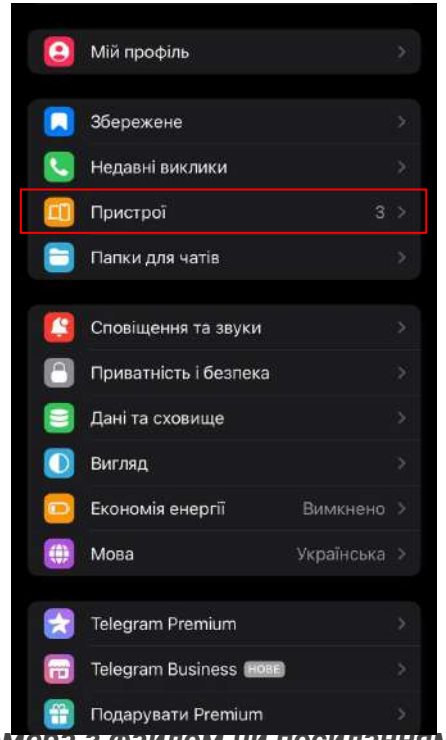
У цьому месенджері також варто налаштувати двохфакторну автентифікацію. Для цього перейдіть до “Параметри” та в меню “Приватність і безпека” оберіть “Двоетапна перевірка”. Буде запропоновано встановити пароль та електронну пошту для його відновлення. Встановлюйте складний пароль (більше 8 символів, великі та малі літери, символи, цифри) та не використовуйте пароль, який Ви вже використовуєте в іншому месенджері, соц. мережі чи електронній пошті.

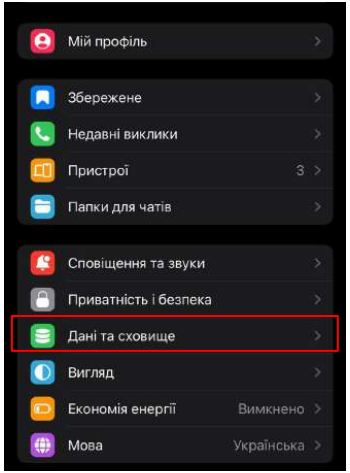


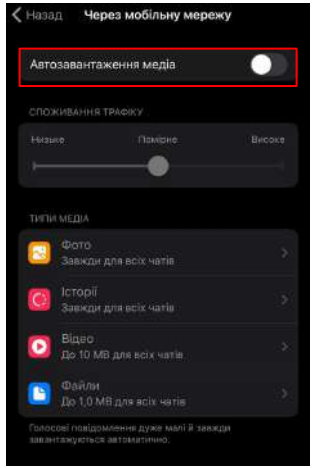
У цьому ж меню встановіть, щоб Ваш номер телефону не відображався нікому, а також автоматичне видалення акаунту після 1 місяця відсутності.

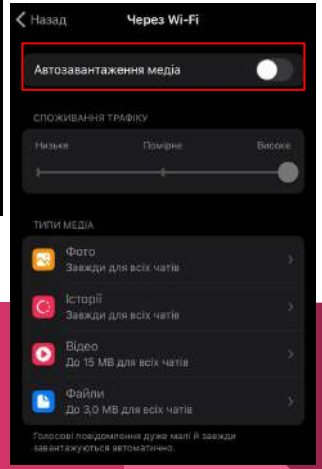


Періодично перевіряйте меню “Пристрої” на наявність невідомих Вам пристроїв, з яких авторизований Ваш акаунт. Також рекомендується в меню “Дані та сховища” вимкнути автозавантаження медіа як через мобільну мережу, так і через Wi-Fi.









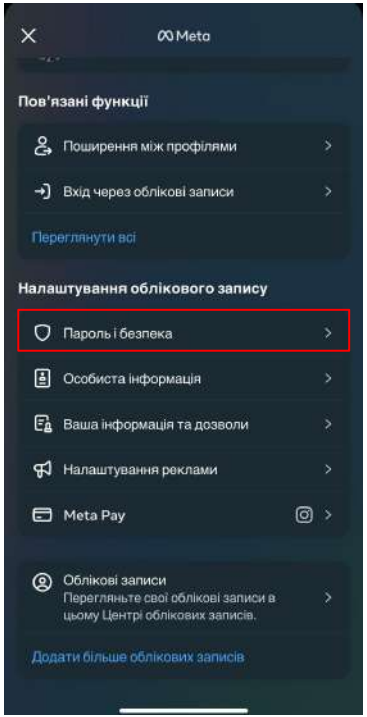
При отриманні повідомлення від невідомого номера з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

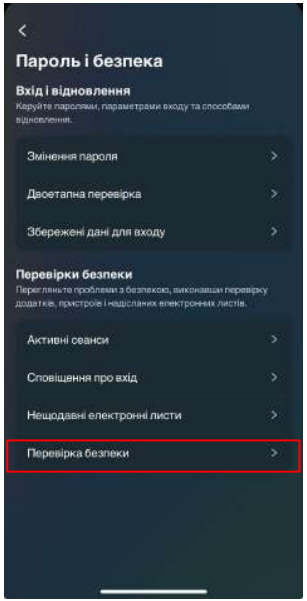
4.Соціальна мережа Instagram

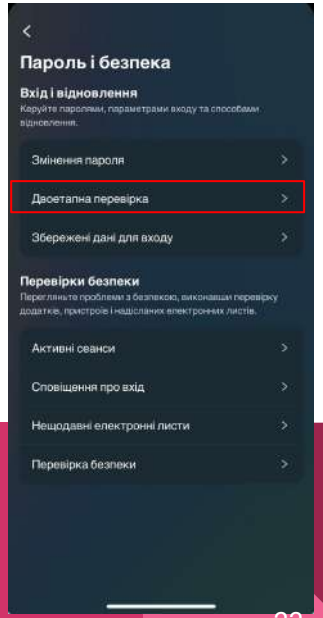
Для кожного облікового запису рекомендується налаштувати двохфакторну автентифікацію. Для цього відкрийте застосунок, перейдіть у “Налаштування” та відкрийте пункт “Безпека”.

Натиснувши на пункт “Перевірка безпеки”, Ви отримаєте рекомендації від Instagram щодо підвищення рівня захищеності вашого акаунта, зокрема можуть бути рекомендації щодо зміни і пароля на більш надійний, підтвердження електронної пошти, мобільного телефону та встановлення двофакторної автентифікації.

Встановити “Двоетапну перевірку” можна шляхом окремого додатку для автентифікації, текстового повідомлення на номер телефону чи за допомогою WhatsApp (попередньо увімкнувши отримання повідомлення за номером).







Також в меню “Безпека” перейдіть до пункту “Входи в обліковий запис” та перевірте чи не було авторизації до Вашого акаунта з невідомого Вам пристрою. У разі виявлення подібного, одразу закрийте інший сеанс.

Рекомендується періодично змінювати пароль до облікового запису, встановлюючи складний пароль, що не використовується в інших соц. мережах, месенджерах чи електронних поштах, а також не відкривати можливі посилання, що можуть надійти в особистих повідомленнях або написані в коментарі до посту.

5.Соціальна мережа Facebook

Захист Вашого акаунта Facebook також залежить від правильних налаштувань. Для цього відкрийте застосунок, перейдіть до “Меню”, прогортайте до низу і оберіть пункт “Налаштування”, після чого відкрийте “Пароль і безпека”. В цьому меню Ви можете перевірити важливі налаштування безпеки за рекомендаціями Facebook, а також змінити пароль, що варто робити періодично і встановлювати унікальні та складні паролі. Також варто налаштувати двоетапну перевірку, для цього натисніть “Використання двоетапної перевірки” та, керуючись рекомендаціями Facebook, оберіть зручний для Вас метод двофакторної автентифікації.

Після налаштування поверніться до попереднього меню “Пароль і безпека”, перевірте, з яких пристроїв Ви авторизовані до акаунта в пункті “Авторизовані входи”, а також, відкривши меню “Отримувати сповіщення про підозрілі входи”, увімкніть сповіщення на пошті та у додатку.

Не відкривайте та не зберігайте вкладені файли у підозрілі повідомлення, отримані у Messenger Facebook, а також не переходьте за посиланнями, отриманими в повідомленнях чи написаних в коментарі до посту. Періодично перевіряйте активні пристрої як описано вище.

6.Соціальна мережа Twitter

Для підвищення безпеки Вашого облікового запису(-ів) у соціальній мережі Twitter відкрийте застосунок, натиснувши на піктограму профілю, відкрийте меню “Налаштування та конфіденційність” та оберіть “Безпека та доступ до профілю”. В цьому меню, натиснувши на пункт “Безпека”, налаштуйте двофакторну автентифікацію за допомогою текстового повідомлення на мобільний телефон, додатку для автентифікації або ключа безпеки. Також рекомендується увімкнути функцію “Захист від скидання пароля” в меню “Безпека” для унеможливлення зміни пароля без Вашого підтвердження.

Перейдіть до меню “Безпека й доступ до профілю” та в пункті “Додатки та сеанси” перевірте наявні інші несанкціоновані сеанси, підключені застосунки, а також авторизовані пристрої.

Періодично змінюйте пароль, для цього перейдіть в меню “Налаштування та конфіденційність” та оберіть “Ваш профіль” та пункт “Змініть свій пароль”. Не переходьте за посиланнями, які можете отримати в особистих повідомленнях або в коментарях до твіту.