Короткі корисні поради щодо цифрової безпеки

ВСТАНОВІТЬ КОНФІДЕНЦІЙНИЙ МЕСЕНДЖЕР SIGNAL

Signal дозволяє вам використовувати наскрізне шифрування для захисту ваших повідомлень і дзвінків. Додаток підтримує відеодзвінки до 40 осіб, а також дозволяє розмивати обличчя на фотографіях.
https://signal.org

ВИКОРИСТОВУЙТЕ WIRE PERSONAL, ЯКЩО ВАМ НЕОБХІДНО БІЛЬШЕ КОНФІДЕНЦІЙНОСТІ

Wire Personal використовує наскрізне шифрування для захисту ваших дзвінків, повідомлень та відеочатів. Програма не відображатиме номери телефонів ваших співрозмовників, а лише ім'я користувачів/нікнейми, які вони використовують.
https://app.wire.com/

ЯКЩО ВИ ЗАЛИШАЄТЕ СВІЙ СМАРТФОН, ВИМКНІТЬ РОЗБЛОКУВАННЯ ЕКРАНУ ЛИЦЕМ АБО ПАЛЬЦЕМ

Натомість використовуйте PIN-код. Найнадійніші PIN-коди містять в собі 10 символів або більше. Маєте 4 або 6-значний PIN-код? Подумайте про те, щоб написати свій PIN-код кілька разів, поки не отримаєте новий PIN-код достатньої довжини. При необхідності додайте цифру в кінці, щоби ваш PIN-код було складніше вгадати.

ПІДВИЩУЙТЕ КОНФІДЕНЦІЙНІСТЬ ВАШОГО МІСЦЕЗНАХОДЖЕННЯ

Перейдіть на сторінку **https://maps.google.com/locationhistory** та видаліть ваші подорожі вручну або клацніть на кнопку Кошика (біля Налаштувань), щоб видалити їх усі. Перейдіть на сторінку **https://myactivity.google.com**, щоб стерти ваші особисті дії вручну, або оберіть Видалити, а потім За увесь час, щоб стерти усі існуючі дії.

ПАМ'ЯТАЙТЕ, ЩО ВАШ ТЕЛЕФОН НАЙБЕЗПЕЧНІШИЙ КОЛИ ВІН ВИМКНЕНИЙ

СПРОБУЙТЕ УВІМКНУТИ НАСКІЗНЕ ШИФРУВАННЯ ДЛЯ ZOOM

Натисніть Налаштування → Профіль → Переглянути додаткові функції → Дозволити використання наскрізного шифрування → Увімкнути. Коли ви плануєте нову зустріч, оберіть наскрізне шифрування, щоб захистити ваш дзвінок від перегляду навіть від співробітників Zoom. Примітка: кімнати груп, приватні повідомлення та дзвінки на платні номери Zoom буде вимкнено.
https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

ПІКЛУЙТЕСЬ ПРО БЕЗПЕКУ ВАШОЇ ПОШТИ ТА СОЦМЕРЕЖ

Активуйте «двофакторну аутентифікацію» (2FA) для своїх облікових записів. Це створює додатковий рівень безпеки окрім використання пароля для входу. Дізнайтеся, як його використовувати на кожній платформі за допомогою **https://2fa.directory**

ВСТАНОВІТЬ BRIDGEFY

Bridgefy дозволяє надсилати наскрізні зашифровані повідомлення людям, які знаходяться поблизу вас за допомогою Bluetooth на вашому телефоні. Інтернет або мобільний зв'язок для цього не потрібні. Повідомлення можна надсилати на відстань до 100 метрів. Чим більше людей поблизу використовує додаток, тим далі по відстані можуть поширюватися повідомлення.
https://bridgefy.me/

ЗАХИСТІТЬ ОБЛИЧЧЯ/ТАТУЮВАННЯ ВІД ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ

Закривайте обличчя, татуювання, одяг з принтами за допомогою стікерів та фільтрів. Ви можете використовувати вбудовані програми свого телефону, щоб редагувати фотографії, або накладати необхідні фільтри чи стікери. Щоб підвищити рівень безпеки, зробіть знімок екрану з необхідною відреаговано фотографією та поділіться ним замість функції Поширити самого додатку.

Special thanks to @Knythrou & Sage Cheng

TIPS BY CRYPTO HARLEM