Быстрые и практические советы по цифровой безопасности

УСТАНОВИТЕ МЕССЕНДЖЕР SIGNAL ДЛЯ МАКСИМАЛЬНОЙ КОНФИДЕНЦИАЛЬНОСТИ

Signal позволяет вам использовать сквозное шифрование для защиты ваших звонков и сообщений. Сквозное шифрование – это способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям. Signal поддерживает видеозвонки до 40 участников и также предоставляет вам возможность размывать лица людей на фотографиях.
https://signal.org

ИСПОЛЬЗУЕТЕ WIRE PERSONAL ДЛЯ БОЛЬШЕЙ КОНФИДЕНЦИАЛЬНОСТИ

“Wire Personal” использует сквозное шифрование для защиты ваших звонков, сообщений и видеочатов. Это приложение не отображает номера телефонов ваших друзей, а лишь выбранные ими имена пользователей или псевдонимы.
https://app.wire.com/

ВО ВРЕМЯ ПУТЕШЕСТВИЙ ОТКЛЮЧИТЕ ФУНКЦИЮ РАЗБЛОКИРОВКИ ТЕЛЕФОНА С ПОМОЩЬЮ ОТПЕЧАТКА ПАЛЬЦА ИЛИ РАСПОЗНАВАНИЯ ЛИЦА

Вместо этой функции, используете PIN-код для разблокировки вашего телефона. Самые надежные PIN-коды содержат по крайней мере 10 цифр. Если вы используете PIN-код содержащий всего 4 или 6 цифр, то можете повторять эти цифры снова и снова, пока ваш PIN-код не достигнет нужной длины. Если возможно, добавьте символ в конце вашего PIN-кода, чтобы его было сложнее угадать другим.

ЗАЩИТИТЕ КОНФИДЕНЦИАЛЬНОСТЬ ВАШЕГО МЕСТОПОЛОЖЕНИЯ

Перейдите по ссылке **https://maps.google.com/locationhistory** и удалите историю местоположений за определенное время. Вы также можете удалить историю местоположений за все время, нажав на значок корзины (рядом со значком настроек). Перейдите по ссылке **https://myactivity.google.com**, чтобы удалить отдельные записи о ваших действиях или нажмите “Удалить” и выберите вариант “Все время,” чтобы удалить данные о всех ваших действиях.

ПОМНИТЕ, ЧТО ВАШ ТЕЛЕФОН НАИБОЛЕЕ ЗАЩИЩЕН КОГДА ОН ВЫКЛЮЧЕН

ВКЛЮЧИТЕ СКВОЗНОЕ ШИФРОВАНИЕ ДЛЯ ZOOM КОНФЕРЕНЦИЙ

Нажмите Настройки → Профиль → Посмотреть расширенные функции → Разрешить сквозное шифрование → если настройка отключена, нажмите переключатель, чтобы включить ее. Когда вы планируете новую конференцию, выберите сквозное шифрование, чтобы защитить ваш видеозвонок от слежки, даже со стороны сотрудников Zoom. Учтите, что сессионные залы, личные сообщения и вход в конференцию по телефону будут отключены.
https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

ЗАЩИТИТЕ ВАШУ ЭЛЕКТРОННУЮ ПОЧТУ И АККАУНТЫ В СОЦИАЛЬНЫХ СЕТЯХ

Включите “двухфакторную аутентификацию” (также известна как “двухэтапная аутентификация”) для защиты ваших аккаунтов. Эта функция обеспечивает более надежную защиту аккаунта – злоумышленники не смогут получить к нему доступ, даже если узнают пароль. Узнайте как использовать эту функцию на разных платформах на сайте **https://2fa.directory**

УСТАНОВИТЕ BRIDGEFY

Bridgefy позволяет вам отправлять сообщения, защищенные технологией сквозного шифрования. Это приложение позволяет общаться без мобильного интернета с людьми, физически находящимся рядом с вами, используя Bluetooth для отправки сообщений. Bridgefy позволяет отправлять сообщения на расстоянии до 100 метров. Чем больше пользователей этого приложения, тем дальше смогут доходить ваши сообщения.
https://bridgefy.me/

ЗАЩИТИТЕ ЛИЦА И ТАТУИРОВКИ ОТ ТЕХНОЛОГИЙ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ

Перед тем как делиться фотографиями онлайн, спрячьте лица, татуировки, и отличительную одежду, используя смайлики, стикеры и так далее. Вы также можете использовать встроенные приложения на вашем телефоне, чтобы отредактировать фотографии. Чтобы усилить уровень вашей безопасности, сохраните скриншот отредактированной фотографии. Используете и делитесь этим скриншотом.

CC BY-ND 4.0
Special thanks to @nsamarin & Sage Cheng

TIPS BY CRYPTO HARLEM