

OUCH!

Ежемесячник по информационной безопасности для всех

Безопасность в социальных сетях: семь советов

Обзор

Сайты социальных сетей, таких, как Snapchat, Facebook, Twitter, Instagram и LinkedIn предоставляют прекрасную возможность для общения, взаимодействия и обмена информацией с людьми по всему миру. Но эти сайты также таят и серьёзную опасность не только для вас, но и для членов вашей семьи, ваших друзей и работодателей. В этом выпуске мы дадим вам семь советов, которые помогут вам общаться в социальных сетях безопасно.

Публикации

Будьте осторожны с тем, что вы размещаете. Абсолютно все, что вы публикуете, может стать достоянием общественности в любой момент, испортив вашу репутацию и будущее; возможно, даже навредит поступлению в университет или помешает получить работу. Совет простой: если вы не хотите, чтобы ваш начальник или близкие о чем-то знали, просто не публикуйте это. Также внимательно относитесь к тому, что публикуют ваши друзья о вас. Вы можете попросить удалить нежелательную информацию о вас.

Настройки конфиденциальности

Почти все сайты социальных сетей предоставляют возможность настраивать конфиденциальность по вашему усмотрению. Подумайте, действительно ли нужно разрешать сайту отслеживать ваше местонахождение и перемещения? Кроме того, настройки приватности могут быть сложными для понимания и они могут часто меняться. Поэтому следует регулярно их проверять, соответствуют ли они вашим пожеланиям.

Заслуживающие доверия приложения

Сделайте вход на сайт безопасным с помощью длинной и уникальной парольной фразы. Парольная фраза – это пароль, состоящий из нескольких слов, который легко запомнить и вводить, но сложно угадать кибер мошенникам.

Дополнительная защита аккаунта

Ещё лучше, подключите двухфакторную аутентификацию для всех ваших аккаунтов. Эта функция будет запрашивать единовременный код вместе с паролем для входа в аккаунт. Это очень простой, но очень надёжный способ защиты аккаунта.

⚠ Обман в социальных сетях

Преступники рассылают мошеннические сообщения, подобные спаму по электронной почте. Например, они пытаются обманным путём получить ваш пароль или номер кредитной карты. Будьте осторожны со ссылками, по которым вы переходите: если от друга пришло подозрительное или странное сообщение, то это, скорее всего, атака злоумышленников, которые выдают себя за вашего друга.

📄 Условия пользовательского соглашения

Внимательно изучите правила сайта, которым вы пользуетесь. Все, что вы публикуете, может стать собственностью сайта.

📊 Работа

Если вы хотите опубликовать рабочую информацию, то это следует предварительно согласовать со своим руководством и получить разрешение на публикацию данных.

Следуя нашим советам, вы сможете использовать интернет ресурсы безопасней. Чтобы получить больше информации о безопасности сайта или сообщить о подозрительной активности своей страницы, обратитесь в Службу Поддержки сайта.

✍ Об авторе

Джессика Баркер – один из признанных экспертов мирового уровня в сфере человеческого фактора компьютерной безопасности. Она является одним из основателей компании [Redacted Firm](#), которая предоставляет консалтинговые услуги для клиентов во многих странах мира. Джессика – известный лектор. Аккаунт в Twitter: [@drjessicabarker](#).



🔗 Ресурсы

- Парольные фразы: <https://www.sans.org/u/B6E>
- Надёжная защита вашего аккаунта: <https://www.sans.org/u/B6J>
- Безопасность детей в сети: <https://www.sans.org/u/B6O>
- Lock Down Your Login: <https://www.lockdownyourlogin.org/>
- Безопасность в социальных сетях: <https://www.kaspersky.ru/resource-center/preemptive-safety/facebook>
- 4 простых совета, которые защитят ваши данные в соцсетях: <https://lifelife.ru/2017/03/28/bezopasnost-v-socsetjah/>

🔍 Лицензия

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется [Creative Commons BY-NC-ND 4.0 license](#). Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: www.sans.org/security-awareness/ouch-newsletter.
Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова