Безопасность для журналистов на Facebook

facebook Проект "Журналистика на Facebook"

Благодарим наших партнеров за помощь в составлении этого руководства:

CPJ Committee to Protect Journalists

КОМИТЕТ ЗАЩИТЫ ЖУРНАЛИСТОВ

ConnectSafely

CONNECTSAFELY

European Journalism Centre

ЕВРОПЕЙСКИЙ ЦЕНТР ЖУРНАЛИСТИКИ

FRONTLINE FREELANCE REGISTER

INTER AMERICAN PRESS ASSOCIATION (IAPA)

JAMES W. FOLEY LEGACY FOUNDATION

JAMES FOLEY FOUNDATION

MEDIA WATCH

TAIWAN MEDIA WATCH

ДЖОН КЭМФИЛД, МЕГАН ДЕБЛУА, ДИШАД ОТМАН/INTERNEWS

10 ШАГОВ К БЕЗОПАСНОСТИ

Facebook позволяет журналистам по-новому работать, рассказывать истории и общаться с людьми напрямую. Мы хотим помочь защитить их информацию и аккаунты, чтобы они могли чувствовать себя в безопасности и гарантировать безопасность своим источникам и контактам. Мы подготовили 10 советов:

1 ЗАЩИТИТЕ СВОЙ ПАРОЛЬ

Пароль от аккаунта Facebook должен быть уникальным и защищенным. Его нельзя предоставлять другим людям ни при каких обстоятельствах. В пароле не следует использовать личные данные, в том числе имя, номер телефона, дату рождения и почтовый адрес. Рекомендуем пользоваться менеджером паролей, который помогает создавать надежные пароли для всех ваших аккаунтов и хранить их в безопасности.

2 ВКЛЮЧИТЕ УВЕДОМЛЕНИЯ О НЕОПОЗНАННЫХ УСТРОЙСТВАХ

Настройте предупреждения о входе, чтобы получать уведомления в случаях, когда посторонний человек попытается получить доступ к вашему аккаунту с нового или неопознанного устройства.

Чтобы включить уведомления о неопознанных входах, откройте раздел "Безопасность и вход" в настройках. После того как вы включите предупреждения, вы будете получать электронное письмо или уведомление каждый раз, когда кто-то попытается войти в ваш аккаунт из неопознанного устройства или браузера.

3 ВКЛЮЧИТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

Двухфакторная аутентификация — это дополнительное средство безопасности, не позволяющее никому, кроме вас, получить доступ к вашему аккаунту. Включить ее можно в разделе "Безопасность и вход" в настройках. Если вы включите двухфакторную аутентификацию, вам понадобится вводить специальный код безопасности каждый раз, когда вы захотите войти в свой аккаунт на Facebook с нового компьютера, телефона или браузера.

Получить код безопасности можно разными способами.

- Вы можете использовать наш Генератор кодов, если на вашем смартфоне или планшете есть приложение Facebook.
- Если вы используете новейшую версию Chrome или Opera, зарегистрируйте физический ключ безопасности на свой аккаунт и просто подключайте к разъему USB компьютера небольшое устройство. Ключи безопасности можно приобрести у таких компаний, как Yubico. Они поддерживают открытый протокол Universal 2nd Factor (U2F) от FIDO Alliance.
- Кроме того, Facebook может отправлять вам SMS (обратите внимание, что за них может взиматься плата) с кодом для входа каждый раз, когда он вам понадобится.
- Вы также можете получить сразу 10 кодов восстановления и распечатать или записать их на будущее. Храните коды в надежном месте, при желании вручите их копию доверенному другу или коллеге.

4 ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ ПРОВЕРКИ FACEBOOK

Используйте Проверку безопасности для управления настройками безопасности профиля. Вы можете:

- Просмотреть перечень браузеров и приложений, через которые вы входили на Facebook ранее, но не использовали уже более месяца. Вы можете быстро запретить доступ через те из них, которые вам уже не нужны.
- Управлять уведомлениями о входе в ваш аккаунт из неопознанного устройства или браузера.
- Получать советы, как повысить надежность пароля и как часто его менять.

Включите Проверку настроек конфиденциальности, чтобы контролировать, кто может получить доступ к информации о вас и вашим публикациям.

Подробнее о том, как выбрать подходящие настройки конфиденциальности и безопасности, см. в Центре конфиденциальности Facebook: fb.me/myprivacy.

5 УПРАВЛЯЙТЕ СВОИМ ПРИСУТСТВИЕМ НА СТРАНИЦАХ И В ПРОФИЛЯХ

Вы сами определяете степень своей публичности или приватности на Facebook. Вот несколько рекомендаций по управлению публикациями.

ПРОФИЛЬ

- С помощью инструмента выбора аудитории укажите, кто может видеть ваши публикации. Можно делиться контентом со всеми, только с друзьями или даже с пользовательской аудиторией. Пользовательская аудитория позволяет показать тот или иной контент только определенным людям.
- Контролируйте степень публичности ваших публикаций с помощью настроек во вкладке "Хроника и метки". Вы сможете утверждать или отклонять метки, которые друзья добавляют к вашим публикациям. Если вы подтвердите метку, отмеченный пользователь и его друзья смогут видеть вашу публикацию. Подтверждать метки можно в настройках во вкладке "Хроника и метки".
- В "Проверке хроники" укажите, будут ли видны в вашей Хронике публикации, на которых вы отмечены. Если в публикации вас отмечает человек, который не является вашим другом, такие теги автоматически отправляются на проверку хроники. Если вы захотите также просматривать метки от своих друзей, включите функцию "Проверка хроники" для меток от всех пользователей. Функцию "Обзор Хроники" можно найти в настройках во вкладке "Хроника и метки".
- Контролируйте, как выглядит ваш профиль для других людей, с помощью инструмента "Посмотреть как...". Просто откройте свой профиль, нажмите "Посмотреть как..." и посмотрите, как видят ваш профиль все люди или конкретный человек.
- Вы можете разрешить или запретить Facebook распознавать вас на фото и видео. Для этого воспользуйтесь функцией "Распознавание лиц" в разделе "Настройки".

5 ПРОДОЛЖЕНИЕ

СТРАНИЦА

Любой пользователь — редактор соцсетей, журналист, общающийся через свою Страницу с читателями или зрителями, модератор Страницы — может обеспечить безопасность своей Страницы несколькими способами. Выберите нужных людей и назначьте им права администратора, чтобы они управляли вашей Страницей. Ваши коллеги смогут управлять Страницей через свой личный аккаунт. Назначайте им только необходимые роли, ведь не всем нужен полный контроль над Страницей — некоторым будет достаточно прав редактора или рекламодателя.

- Администраторы Страниц должны использовать реальные аккаунты и включить двухфакторную аутентификацию, чтобы не потерять доступ к своим аккаунтам. Facebook по возможности удаляет поддельные аккаунты и аккаунты самозванцев.
- Используйте модерацию Страницы и инструменты фильтрации в настройках Страницы, чтобы контролировать комментарии и публикации гостей. Эти инструменты позволяют блокировать нежелательные слова и включать фильтр ненормативной лексики на Странице. Не забывайте фильтровать различные варианты запрещенных слов. Вы можете добавить между буквами в словах точки или пробелы, а также хэштеги. Например, чтобы запретить слово "оружие", добавьте варианты "о.р.у.ж.и.е.", "#оружие" и "о р у ж и е". Хотя комментарии к публикациям на Странице отключить нельзя, вы можете скрывать или удалять их. Если вы скроете комментарий, его автор не узнает об этом.

5 ПРОДОЛЖЕНИЕ

- Вы можете запретить доступ к своей Странице людям, которые постоянно размещают на ней спам. Снять запрет можно в любое время. Если вы запретите кому-то доступ к своей Странице, этот человек все равно сможет делиться контентом с вашей Страницы в других местах на Facebook, но он больше не сможет размещать на ней публикации, ставить отметки "Нравится" ее публикациям или комментировать их, отправлять сообщения вашей Странице или ставить ей "Нравится".
- Если вы хотите, чтобы кто-то дистанционно запустил трансляцию с вашей Страницы Facebook, предоставьте этому человеку роль представителя Страницы в прямом эфире. Эта роль позволит человеку выйти в прямой эфир, но запретит доступ к другим функциям на Странице.
- Facebook также позволяет вам удалять из своего профиля или Страницы любые комментарии вне зависимости от того, нарушают ли они наши Стандарты сообщества.

6 КОНТРОЛИРУЙТЕ СВОЕ МЕСТОПОЛОЖЕНИЕ В ПУБЛИКАЦИЯХ

Facebook позволяет указывать в публикациях местоположение. Эта функция работает не по умолчанию, но если вы не хотите, чтобы люди узнали, где вы находитесь в данный момент, можете отключить геолокацию. Настройки геолокации можно менять на устройствах под управлением Android и iOS.

7 ОБЕСПЕЧЬТЕ БЕЗОПАСНОСТЬ ПРИ ОБЩЕНИИ

Для частных переписок рекомендуем использовать сервисы для обмена сообщениями, например WhatsApp и Facebook Messenger.

WhatsApp по умолчанию обеспечивает сквозное шифрование для каждого сообщения или звонка. Благодаря сквозному шифрованию ваши сообщения и звонки защищены, поэтому посторонние люди и даже сотрудники WhatsApp не смогут их прочитать или прослушать. Для дополнительной защиты каждое сообщение автоматически получает уникальный замок и ключ. Все это происходит автоматически: чтобы защитить свои сообщения, вам не нужно что-то настраивать или создавать секретные чаты. Ещё вы можете настроить уведомления о смене кода безопасности контакта.

В Messenger для iOS и Android сообщения тоже можно защитить сквозным шифрованием. Доступ к такой секретной переписке будет только у вас и у вашего собеседника. Чтобы начать секретную переписку, на устройстве под управлением Android создайте переписку в Messenger и коснитесь переключателя со значком замка, а в iOS нажмите слово "Секретная". Помните, что эти действия нужно будет выполнить для каждой переписки.

Если вы, например, журналист и хотите скрыть свой IP-адрес, чтобы рекламодатели на Facebook, местные операторы и интернет-провайдеры не узнали, откуда вы выполняете вход, откройте Facebook через браузер Tor. Благодаря этому никто не узнает, откуда и как вы вошли на Facebook. Чтобы открыть Facebook через браузер Tor, перейдите по адресу https://facebookcorewwwi.onion/. Открыть Facebook через Tor на устройствах Android можно через прокси-приложение Orbot, доступное в Google Play.

8 БЛОКИРУЙТЕ ПРЕСЛЕДОВАТЕЛЕЙ

Если вы заблокируете кого-либо, этот человек больше не сможет отмечать вас или видеть публикации в вашей Хронике. Если вы заблокируете друга, этот человек будет удален из друзей. Кроме того, если заблокированный вами пользователь создаст новый аккаунт или попытается связаться с вами из другого аккаунта, мы все равно узнаем его и не позволим ему это сделать.

КАК ЗАБЛОКИРОВАТЬ ПОЛЬЗОВАТЕЛЯ НА ПК

В разделе "Блокировка" вкладки "Настройки" вы можете заблокировать или разблокировать пользователей, сообщения, приложения и Страницы, а также приглашения в приложения и на мероприятия.

КАК РАЗБЛОКИРОВАТЬ КОГО-ЛИБО В MESSENGER

iPhone или iPad:

1. Откройте переписку с человеком, которого хотите заблокировать.
2. Коснитесь его имени в верхней части переписки.
3. Прокрутите вниз и нажмите **Заблокировать**.
4. Коснитесь экрана напротив параметра **Заблокировать сообщения**.

Android:

1. Откройте переписку с человеком, которого хотите заблокировать.
2. Коснитесь, прокрутите вниз, а затем выберите **Заблокировать**.
3. Коснитесь **Заблокировать все сообщения**.

Когда вы блокируете людей, мы не отправляем им об этом уведомления.

Если вам не удается найти человека, которого вы хотите заблокировать, таким способом, перейдите в его профиль и выберите **Заблокировать** из меню на его фото обложки.

9 СООБЩАЙТЕ ОБ ОСКОРБИТЕЛЬНОМ КОНТЕНТЕ И САМОЗВАНСТВЕ

Наилучший способ сообщить об оскорбительном контенте, спаме или самозванстве на Facebook — перейти по ссылке "Пожаловаться" рядом с размещенным контентом. Мы ознакомимся с жалобой и примем меры.

Ниже приведены примеры того, как вы можете пожаловаться нам на контент.

- Чтобы пожаловаться на комментарий на Facebook:
  - Нажмите стрелку вниз в верхнем правом углу.
  - Выберите **Пожаловаться на публикацию**.
- Чтобы пожаловаться на сообщение в Messenger с ПК:
  - Откройте сообщение, на которое вы хотите пожаловаться.
  - Нажмите значок шестеренки в верхнем правом углу.
  - Нажмите **Пожаловаться** или **Заблокировать** и следуйте инструкциям на экране.
- Чтобы пожаловаться на самозванца:
  - Перейдите в профиль человека, выдающего себя за другого.
  - Нажмите многоточие рядом с кнопкой "Сообщение" на фото обложки.
  - Выберите **Пожаловаться**.
- Инструкции для всех типов контента см. здесь: https://www.facebook.com/report

Если вы чувствуете угрозу, обратитесь в правоохранительные органы. Чтобы пожаловаться на преследование правоохранительным органам, сделайте снимки экрана и скопируйте URL страниц с проявлениями нежелательного внимания к вам **до того**, как заблокировать преследователя. Заблокировав пользователя, вы перестанете видеть его предыдущие действия в отношении вас.

10 ЗАПОМНИТЕ ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВЗЛОМА

Если вы считаете, что ваш аккаунт был взломан или используется кем-то ещё, вам нужно как можно быстрее защитить его. Чтобы предотвратить взлом, включите двухфакторную аутентификацию.

Если вы можете войти в аккаунт, рекомендуем сменить пароль. Проверьте корректность контактной информации в своем аккаунте. Если вы не можете войти в свой аккаунт, мы поможем вам его защитить. Для этого мы попросим вас изменить пароль и проверить недавние попытки входа. Либо перейдите по адресу facebook.com/hacked.

Добавьте доверенные контакты

- Выберите 3–5 друзей, которые отправят вам код и URL с Facebook, чтобы помочь вам войти в аккаунт, если у вас будут проблемы с доступом. Каждый из них получит код безопасности с инструкциями. Этот код вам нужно будет ввести на Facebook, чтобы восстановить доступ к своему аккаунту.

Просмотрите недавние электронные письма от Facebook

- В разделе "Безопасность" настроек Facebook вы можете просмотреть список недавних электронных писем от Facebook, связанных с безопасностью.

facebook.com/journalists