Oregon Department of Justice's
CIVIL RIGHTS UNIT

Руководство по безопасности при распространении личной информации в Интернете (доксинг)

Доксинг: Открытая публикация или совместное использование личной, частной или идентифицирующей информации о другом физическом лице со злым умыслом. Часто такая публикация происходит в Интернете, и цель её состоит в том, чтобы запугать другое лицо или иным образом устрашить его, заставить его замолчать, преследовать, домогаться его или угрожать ему, или побудить другое лицо выполнить подобные действия.

Меры защиты государственных служащих от доксинга

- ☐ Ваши рабочие и связанные с ними электронные письма и текстовые сообщения могут подпадать под действие законов, касающихся требований к обращению с документами публичного характера.
- ☐ Не отправляйте по электронной почте/в виде текстового сообщения то, чем вы не гордились бы, опубликовав это на первой полосе газеты.
- ☐ Не отправляйте никому по электронной почте или в виде текстовых сообщений свой личный номер телефона, домашний или почтовый адрес, а также имена членов семьи, супруги(-а)/партнера или партнёрши или детей на своих рабочих устройствах.
- ☐ Проконсультируйтесь со своим отделом информационных технологий и отделом кадров о мерах защиты, которые могут быть доступны вам, если вы подверглись доксингу, включая управление настройками пересылки, наличие опций шифрования, удаление вашей информации с веб-сайта вашей организации и планирование безопасности в офисе.

Обеспечение безопасности в социальных сетях

- ☐ Сохраняйте учетные записи и дескрипторы закрытыми в своих настройках.
- ☐ Удалите все адреса, информацию о месте работы или учебы, а также о своём местоположении из своей учетной записи (не только скрытые).

- ☐ Не объявляйте, куда вы направляетесь, включая рестораны/парки/мероприятия и населенные пункты/штаты/страны.
- ☐ Принимайте приглашения стать друзьями только от известных вам людей.
- ☐ Разрешайте просматривать свои посты только известным друзьям.
- ☐ Проверьте, кто может распространять ваши посты.
- ☐ Меняйте свои имена пользователя/дескрипторы.
- ☐ Используйте разные и надежные пароли на разных платформах социальных сетей.
- ☐ Не публикуйте фотографии, на которых изображено ваше лицо или лица других людей.
- ☐ Не публикуйте фотографии, по которым кто-то мог бы определить, где вы находитесь/находились.
- ☐ Удаляйте метаданные с фотографий, которые вы публикуете. Помните, что на ваших фотографиях может быть указано ваше местоположение и дата/время, когда была сделана фотография.
- ☐ Определите, куда сообщать о доксинге или разжигании ненависти в социальных сетях.
    - Фейсбук, Снэпчат, Твиттер, Инстаграм, Гугл, Йелп, и др. Все они имеют разные условия использования.

Меры безопасности после того, как вы подверглись доксингу

- ☐ Задокументируйте, что происходит.
- ☐ Делайте скриншоты всего.
- ☐ Попробуйте указать даты/время/имена пользователей.
- ☐ Удалите, если сможете, но сначала быстро задокументируйте.
- ☐ Сообщайте в полицию, если присутствуют угрозы. Обязательно включите:
    - Информацию о защищенном классе, как фактическую, так и воспринимаемую
        - Орегонские и федеральные преступления на почве ненависти не требуют, чтобы преступник правильно идентифицировал ваш защищаемый класс.
    - Соображения безопасности

Commented [CJ1]: Marty, can you please anchor to **Reporting Hate and Bias to the Police** on the toolkit

    - Семья/дети/партнеры
    - Путешествия
    - Публичные выступления
  - Конкретная информация, касающаяся:
    - Неотвратимой опасности: преступник живет поблизости?
    - Какие именно слова были использованы? (Оскорбления, угрозы, оружие)
  - Любые доказательства, включая скриншоты. Помните, что своевременность вашего сообщения в полицию может повлиять на сохранность улик.
  - Обратите внимание на то, что «истинные угрозы», заявленные онлайн, отправленные по почте или сделанные посредством телефонного звонка/оставленные на вашей голосовой почте, могут быть квалифицированы как федеральное преступление. Подайте заявление в ФБР или попросите вашу местную полицию обратиться с перекрестным заявлением в федеральные правоохранительные органы.
- ☐ Измените пароли к своим телефонам, электронной почте и учетным записям в социальных сетях. Убедитесь, что каждый пароль отличается от другого и является сложным.
- ☐ Сообщите об этом на платформу и попросите удалить информацию.
  - Попросите, чтобы ваш дескриптор/имя/информация были добавлены в список «тщательно отслеживаемых», чтобы информацию можно было удалить, как только она появится в другом месте.
- ☐ Обратитесь за поддержкой к кому-нибудь, кому вы доверяете. Вы не одиноки.
- ☐ В законе штата Орегон 2021 HB 3047 предусмотрены гражданско-правовые средства правовой защиты от доксинга. Поговорите с адвокатом, чтобы узнать, есть ли у вас дополнительные гражданско-правовые средства законной защиты.
  - Программа найма юристов по рекомендации коллегии адвокатов штата Орегон
  - Юридическая помощь малоимущим

- Юридический центр штата Орегон для пострадавших от преступлений (OCVLC)

☐ Рассмотрите вопрос об издании приказа о гражданской защите

☐ Рассмотрите информацию, которую вы *можете* контролировать, например, находитесь ли вы вообще на платформе, что вы публикуете, раскрываете своё местоположение и т.д., по сравнению с тем, что вы не контролируете.

☐ Настройте оповещения Google для вашего имени, номера телефона, адреса, чтобы получать оповещения, если информация появится в сети.

☐ Используйте опции отказа от брокера данных – за некоторые услуги вам, возможно, придется заплатить, такие как DeleteMe, Reputation Defender, Privacy Bee, Kanary, OneRep, OptOutPrescreen.com, Do Not Call Registry.

☐ Рассмотрите возможность использования отдельных адресов электронной почты для разных целей.

☐ План обеспечения безопасности:
- На работе – поговорите с сотрудником отдела кадров.
- Дома – составьте четкий план со своей семьей, поговорите с соседями, которым вы доверяете, попросите полицию усилить патрулирование в целях безопасности.
- На публике – путешествуйте с другом, выбирайте альтернативные маршруты, сообщайте доверенному лицу, куда вы направляетесь и когда планируете вернуться.

☐ Поговорите с членами семьи/друзьями об информации, которую они распространяют о вас в Интернете.

Commented [CJ2]: Marty, can you please anchor to **Protective Orders in Oregon** on the toolkit?

Дополнительные ресурсы по онлайн-безопасности (ссылки на английском языке)

Советы по созданию надежных паролей:

Безопасность в Интернете: Создание надежных паролей (gcfglobal.org)

Создайте надежный пароль и более защищенную учетную запись – Справка по аккаунту Гугл

Получите дополнительную информацию о безопасности в Интернете:
Доксинг: Что это такое и как защитить себя? | NortonLifeLock
Пять советов по обеспечению безопасности и конфиденциальности в социальных сетях | Norton.com
Сброс конфиденциальных данных: Руководство по важным настройкам, которые вам следует изменить сейчас | Washington Post
Как удалить информацию о себе из Интернета | comparitech
Вот брокеры данных, которые спокойно покупают и продают вашу личную информацию | журнал Fast Company
Как защитить свои данные и бесплатно удалить личную информацию из Интернета: Бесплатное руководство по самостоятельному отказу от участия | DeleteMe
Как исчезнуть из Интернета | Reader's Digest

Удаление контента из Гугла:
Удаление контента из Гугла – Юридическая помощь
Удалите свою личную информацию из Гугла
Удалите выбранную личную информацию или содержимое доксинга из поисковика Гугл

Законодательство по борьбе с доксингом:
Пресс-релиз, Сенат штата Орегон принял закон по борьбе с доксингом

Сквозное шифрование:
Приложение Signal
Приложение WhatsApp

Оговорка: Ссылки и информация, представленные в этом наборе инструментов, носят исключительно информационный характер, не являются исчерпывающими, не являются юридической консультацией и не отражают одобрения или проверки со стороны Департамента юстиции штата Орегон в отношении коммерчески доступных продуктов. Для получения информации о своих правах и юридических возможностях проконсультируйтесь с адвокатом.