Homeland Security

Министерство внутренней безопасности
Управление по партнерству и взаимодействию (OPE)

Ресурсы по защите от доксинга

16 января 2024 г.

ЧТО ТАКОЕ ДОКСИНГ?

Доксинг – это сбор личной информации человека (PII) и ее публичное обнародование в злонамеренных целях, таких как публичное унижение, преследование, кража личности или оскорбление.

ПРИМЕРЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- **Имя и фамилия**
- **Контактные данные**
- **Домашний адрес**
- **Члены семьи**
- **Сведения о месте работы**
- **Финансовая информация**
- **Номер социального страхования (Social Security)**

РАСПРОСТРАНЕННЫЕ ИСТОЧНИКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- **Посты в социальных сетях**
- **Документы о недвижимости и судебные архивы**
- **Свадебные объявления и некрологи**
- **Информационные бюллетени**
- **Открытые конференции**
- **Веб-форумы, блоги и доски обсуждений**
- **Незащищенные сети**
- **Списки избирателей**

КАК ЗАЩИТИТЬ СЕБЯ ОТ ДОКСИНГА?

- **Будьте осторожны**, когда вы размещаете сведения о себе в Интернете, включая фотографии и видео, даже если они временные.
- **Удалите** личные данные (адрес, дату рождения, номер телефона и т. д.) из ваших профилей в социальных сетях.
- **Проверяйте** ваших подписчиков и отклоняйте запросы от тех, кого вы не знаете.
- **Попросите** удалить ваши личные данные с сайтов, содержащих публичные записи. Известные сайты: BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder и Whitepages.
- **Удалите** ненужные приложения и расширения для браузера, чтобы предотвратить сбор ваших личных данных.
- **Ограничивайте** отслеживание местоположения в приложениях и на веб-сайтах. Отключите сервисы определения местоположения для каждого приложения или платформы.
- **Включите** настройки конфиденциальности в социальных сетях, приложениях и на других веб-сайтах.
- **Установите** двухэтапную верификацию, используйте сложные пароли и не повторяйте один и тот же пароль для нескольких аккаунтов.

DHS OPE

КАК ЗАЩИТИТЬ СЕБЯ ОТ ДОКСИНГА?

Требуйте удалить ложный, оскорбительный или угрожающий контент
Подайте запрос на удаление материалов на платформу или веб-сайт в соответствии с правилами и требованиями.

Документируйте происходящее
Примите меры по сохранению улик. Сохраняйте все полученные электронные письма, голосовые сообщения и текстовые сообщения, а также делайте скриншоты или фотографии комментариев в социальных сетях.

Сообщайте о происшествиях
Если вы получили угрозу своей физической безопасности или чувствуете, что вас преследуют, сообщите об этом в местные правоохранительные органы, а также администратору социальной сети или веб-сайта.

ДОПОЛНИТЕЛЬНЫЕ РЕСУРСЫ И РЕКОМЕНДАЦИИ

Лучшие методы и ресурсы CISA по кибербезопасности: cisa.gov/cybersecurity

Основы кибербезопасности CISA: cisa.gov/cyber-essentials

Совет CISA: как избежать атак с использованием социальной инженерии и фишинга: cisa.gov/tips/st04-014

Инсайты CISA: повышение безопасности электронной почты и Интернета: cisa.gov/publication/enhance-email-and-web-security

Руководство CISA по борьбе с угрозами в социальных сетях для персонала школ и органов власти. Инфографика: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

Если вы стали жертвой преступления в Интернете, подайте жалобу в **Центр ФБР по рассмотрению жалоб на преступления в Интернете (IC3)** на сайте ic3.gov