Oregon Department of Justice's
CIVIL RIGHTS UNIT

Посібник із боротьби з розповсюдженням особистих даних

Розповсюдження особистих даних або доксинг: Публічна публікація або розповсюдження особистої, приватної чи ідентифікаційної інформації про іншу людину зі злим наміром. Часто така публікація відбувається в Інтернеті, і її мета полягає в тому, щоб налякати іншу людину або залякати її іншим чином, змусити замовкнути, щоб переслідувати людину, турбувати її чи загрожувати їй або навіть надихнути когось іншого зробити це.

Захист державних службовців від поширення особистих даних

- ☐ Ваша робота та пов'язані з нею електронні листи і текстові повідомлення можуть підпадати під дію законів про запити публічних записів.
- ☐ Перед тим, як надсилати щось електронною поштою або в текстовому повідомленні, подумайте, чи прийнятно те, що ви пишете, якщо воно опиниться на першій сторінці газети.
- ☐ Не рекомендується використовувати робочі пристрої для надсилання електронною поштою або текстовими повідомленнями особистих даних, таких як номер телефону, домашня або поштова адреса, а також імена членів сім'ї, чоловіка/партнера або дітей.
- ☐ Зверніться до відділу інформаційних технологій (IT) та відділу кадрів для отримання інформації про доступні засоби захисту, якщо ви стали жертвою доксингу і ваші особисті дані були опубліковані. Вони зможуть надати вам інформацію про такі заходи, як управління налаштуваннями переадресації, наявність варіантів шифрування, видалення вашої інформації з веб-сайту вашої організації та планування безпеки в офісі.

Безпека у соціальних мережах

- ☐ Установіть приватні налаштування для своїх облікових записів та ідентифікаторів.
- ☐ Видаліть всі адреси, місця роботи або навчання та розташування зі свого облікового запису (не лише приховані).

- ☐ Не оголошуйте, куди ви йдете, включаючи ресторани/парки/заходи та міста/штати/країни.
- ☐ Приймайте запрошення у друзі лише від відомих вам людей.
- ☐ Дозволяйте переглядати ваші повідомлення лише знайомим.
- ☐ Перевірте, хто може ділитися вашими повідомленнями.
- ☐ Урізноманітнюйте свої імена користувача та ідентифікатори.
- ☐ Використовуйте на платформах соціальних мереж різні та надійні паролі.
- ☐ Не розміщуйте фотографії, на яких зображені ваше чи чуже обличчя.
- ☐ Не публікуйте фотографії, на яких можна визначити, де ви перебуваєте/були.
- ☐ Зітріть метадані з фотографій, які ви публікуєте. Пам'ятайте, що ваші фотографії можуть показати ваше місцезнаходження та дату/час, коли було зроблено фотографію.
- ☐ Визначте, куди повідомляти про поширення особистих даних чи розпалювання ненависті у соціальних мережах.
    - Facebook, Snapchat, Twitter, Instagram, Google, Yelp тощо мають різні умови використання.

Заходи безпеки після розповсюдження особистих даних

- ☐ Документуйте те, що відбувається.
- ☐ Робіть скріншоти всього.
- ☐ Намагайтеся включати дати/час/імена користувачів.
- ☐ Видаліть, якщо це можливо, але спочатку швидко задокументуйте.
- ☐ Повідомте поліцію, якщо є погрози. Обов'язково вкажіть таке:
    - Інформація про захищену категорію, як фактичну, так і ймовірну
        - Федеральні закони і закони штату Орегон про злочини на ґрунті ненависті не вимагають, щоб правопорушник обов'язково коректно ідентифікував категорію, яка є об'єктом захисту.
    - Міркування безпеки
        - Сім'я/діти/партнери
        - Подорожі
        - Публічні виступи
    - Конкретна інформація щодо:
        - Пряма небезпека: чи злочинець живе поблизу?

        - Які саме слова були використані? (Образи, погрози, зброя)
    - Будь-які докази, включаючи скріншоти. Пам'ятайте, що своєчасність вашої заяви в поліцію може вплинути на збереження доказів.
    - Зверніть увагу, що «справжні погрози», викладені в Інтернеті, надіслані поштою або зроблені телефоном/залишені у вашій голосовій пошті, можуть бути федеральним злочином. Напишіть заяву до ФБР або попросіть місцеву поліцію направити звіт до федеральних правоохоронних органів.
- ☐ Змініть паролі до свого телефону, електронної пошти та облікових записів у соціальних мережах. Переконайтеся, що кожен пароль є унікальним і складним.
- ☐ Повідомте платформу і попросіть видалити інформацію.
    - Попросіть, щоб ваш ідентифікатор/ім'я/інформація були додані в «список, що ретельно відстежується», щоб інформація могла бути видалена, щойно вона з'явиться в іншому місці.
- ☐ Поговоріть про підтримку з кимось, кому ви довіряєте. Ви не самотні.
- ☐ У Законі штату Орегон 2021 HB 3047 передбачені цивільно-правові засоби правового захисту від поширення особистих даних. Проконсультуйтеся з адвокатом, щоб дізнатися, чи є у вас додаткові цивільні засоби правового захисту.
    - Програма рекомендацій Колегії адвокатів штату Орегон
    - Юридична допомога
    - Юридичний центр штату Орегон для жертв злочинів (OCVLC)
- ☐ Розгляньте варіант цивільного охоронного ордеру
- ☐ Приділіть увагу інформації, яку ви *можете* контролювати, наприклад, перебування на платформі взагалі, ваші публікації, спільне використання розташування тощо, а не тому, що ви не можете контролювати.
- ☐ Створіть сповіщення Google для імені, номера телефону та адреси, щоб отримувати повідомлення, якщо відповідна інформація з'явиться в Інтернеті.
- ☐ Використовуйте опції відмови від передачі даних брокерами, за деякі послуги вам, можливо, доведеться платити, як, наприклад DeleteMe, Reputation Defender, Privacy Bee, Kanary, OneRep, OptOutPrescreen.com, Do Not Call Registry.

- ☐ Розгляньте можливість використання окремих адрес електронної пошти для різних цілей.
- ☐ План безпеки:
  - На роботі – поговоріть із відділом кадрів.
  - Вдома – складіть чіткий план із сім'єю, поговоріть із перевіреними сусідами, попросіть поліцію посилити патрулювання.
  - На публіці – подорожуйте з другом, вибирайте альтернативні маршрути, повідомляйте довіреній особі, куди ви прямуєте і коли збираєтесь повернутися.
- ☐ Поговоріть із членами сім'ї/друзями про інформацію, яку вони передають про вас в Інтернеті.

Додаткові ресурси безпеки в Інтернеті (посилання англійською мовою)
Поради щодо створення надійних паролів:
Безпека в Інтернеті: Створення надійних паролів (gcfglobal.org)
Створіть надійний пароль та безпечніший обліковий запис – Довідка – обліковий запис Google

Дізнайтесь більше про безпеку в Інтернеті:
Розповсюдження особистих даних або доксинг: Що це таке і як захистити себе | NortonLifeLock
5 порад про безпеку та конфіденційність у соціальних мережах | Norton.com
Скидання конфіденційності: Посібник із важливих налаштувань, які слід змінити зараз | Washington Post
Як видалити себе з інтернету | comparitech
Ось брокери даних, що тихо купують і продають вашу особисту інформацію | Fast Company
Як захистити свої дані та безкоштовно видалити особисту інформацію з Інтернету: Безкоштовний посібник із самостійної відмови від реєстрації | DeleteMe
Як зникнути з Інтернету | Reader’s Digest

Видалення контенту з Google:
Видалення контенту з Google – юридична допомога
Видалити особисту інформацію з Google
Видалити вибрану особисту інформацію або особисті дані з пошуку Google.

Законодавство щодо боротьби з поширенням особистих даних:
Прес-реліз. Сенат штату Орегон ухвалив закон щодо боротьби з поширенням особистих даних

Міжабонентське шифрування:
Signal app
Whatsapp

Обмеження відповідальності: Посилання та інформація, надані в цьому наборі інструментів, призначені виключно для інформаційних цілей, не є повними або вичерпними, не є юридичною консультацією та не відображають схвалення чи перевірку Міністерством юстиції штату Орегон щодо комерційно доступних продуктів. Для отримання інформації про ваші права та юридичні можливості проконсультуйтеся з адвокатом.