Oregon Department of Justice's
CIVIL RIGHTS UNIT

راهنمای مقابله با داکسینگ

داکسینگ: نشر عمومی یا شریک ساختن معلومات شخصی، خصوصی یا هویتی یک شخص دیگر با قصد سوء نیت. این نوع انتشار معلومات اغلباً در محیط اینترنتی واقع میشود و هدف آن ترساندن، اجبار کردن، ساکت کردن، تعقیب کردن، آزار دادن یا تهدید کردن یک شخص یا تشویق کردن دیگران به انجام دادن این اقدامات است.

محافظت از کارکنان دولتی در مقابل داکسینگ

- ایمیل ها و پیام های کوتاه کاری و مربوط به شغل، ممکن است شامل در قوانین درخواست اسناد عمومی باشد.
- مطالبی را که انتشار آنها در صفحه اول روزنامه باعث سربلندی شما نمیشود، از طریق ایمیل/پیام کوتاه ارسال نکنید.
- نمبر تلیفون شخصی، آدرس خانه یا آدرس پستی، یا تخلص، نام همسر/شریک جنسی، یا نام فرزندان خود را که در دستگاه های کاری ذخیره میکنید، از طریق ایمیل یا پیام کتبی منتقل نکنید.
- اگر قربانی داکسینگ شوید، باید با بخشهای تکنالوجی معلوماتی و منابع بشری به تماس شوید و بپرسید که آنها چه کمکی میتوانند به شما بکنند. تنظیم ترجیحات مربوط به انتقال ایمیل، استفاده از انتخاب های رمزگذاری، حذف معلومات از ویبسایت سازمان و پلانگذاری ایمنی داخل-شعبه ای قسمتی از اقدامات محافظتی مفید است.

ایمنی در شبکه های اجتماعی

- حساب ها و آیدی ها را در قسمت تنظیمات، بر روی حالت خصوصی تنظیم کنید.
- آدرس ها، محل کار یا تحصیل، و مکان های مهم را از حساب خود حذف کنید (پنهان کردن کفایت نمیکند).
- از اعلام کردن مقصد، مثلاً رستورانت/پارک/رویدادها و شهرک ها/شهرها/ایالت ها/کشورها، پرهیز کنید.

- ☐ دعوت دوستی را فقط از اشخاص شناخته شده قبول کنید.
- ☐ قسمی ترتیب کنید که فقط دوستان شناخته شده شما بتوانند پست های شما را ببینند.
- ☐ بررسی کنید که چی کسانی میتوانند پست های شما را ببینند.
- ☐ از نام استفاده کننده/آیدی متفاوت استفاده کنید.
- ☐ در پلتفورم های شبکه های اجتماعی از پسوردهای متفاوت و قوی استفاده کنید.
- ☐ از انتشار عکس های حاوی چهره خودتان یا دیگران پرهیز کنید.
- ☐ از ارسال عکس هایی که تشخیص محل زندگی فعلی/قبلی را امکان پذیر میسازد، پرهیز کنید.
- ☐ اَبَردیتاها را از عکس های ارسالی خود حذف کنید. توجه کنید که عکس میتواند مکان شما و/یا تاریخ/ ساعت گرفته شدن عکس را افشا بسازد.
- ☐ مراجع رسیدگی کننده به راپورهای مربوط به نفرت پراکنی در شبکه های اجتماعی را شناسایی کنید.
  - Facebook، Snapchat، Twitter، Instagram، Google، Yelp و... همگی شرایط استفاده خاصی دارند.

اقدامات ایمنی بعد از وقوع داکسینگ

- ☐ اتفاقات واقع شده را مستند کنید.
- ☐ از صفحه معلومات مهم عکس بگیرید.
- ☐ کوشش کنید تاریخ/ساعت/نام استفاده کننده را در عکس شامل کنید.
- ☐ در صورت امکان، مطلب را حذف کنید ولی در ابتدا و به سرعت آن را مستند کنید.
- ☐ موارد احتمالی تهدید را به پولیس راپور بدهید. موارد زیر را حتماً ضمیمه کنید:
  - معلومات صنف محافظت شده، واقعی و احتمالی
  - طبق قوانین اورگان و فدرال در مورد جرایم نفرت-محور، ضروری نیست که شخص مرتکب جرم حتماً از نوعیت محافظت شده شما خبر داشته باشد.
  - مشکلات ایمنی
  - خانواده/فرزندان/شریک جنسی
  - سفر

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

- حضور در مکان های عمومی
- معلومات خاص درباره:
  - نزدیکی: آیا شخص مرتکب در نزدیکی شما زندگی میکند؟
  - دقیقاً از کدام کلمه ها استفاده شد؟ (توهین، تهدید، سلاح)
- مستندات احتمالی، شامل عکس از صفحه نمایش دستگاه. توجه کنید که ارائه اسناد در زمان راپور به پولیس میتواند به حفظ مستندات کمک کند.
- دقت کنید که "تهدید واقعی" در محیط آنلاین، ارسال شده از طریق پست، یا انجام شده از طریق تماس تلیفونی/وایس میل، ممکن است طبق قانون فدرال جرم فرض شود. با FBI به تماس شوید، یا از پولیس محلی بخواهید که راپور را به مسئولین فدرال ارجاع دهد.

□ پسوردهای تلیفون، ایمیل و اکاونت های شبکه های اجتماعی را تبدیل کنید. دقت کنید که هر پسورد، متفاوت و پیچیده باشد.

□ با مسئولین پلتفورم به تماس شوید و برای حذف معلومات درخواستی بدهید.
- درخواست کنید که آیدی/نام/معلومات شما به لیست "تحت نظارت دقیق" منتقل شود تا امکان پاکسازی معلومات، به محض ظاهر شدن آن در جاهای دیگر، فراهم شود.

□ از اشخاص مورد اعتماد کمک بخواهید. شما تنها نیستید.

□ 2021 HB 3047 اورگان به ارائه خدمات حقوقی مدنی در زمینه داکسینگ میپردازد. با یک وکیل صحبت کنید و ببینید که آیا اقدام حقوقی دیگری میتوان انجام داد یا نخیر.
- پروگرام معرفی وکیل انجمن وکلای اورگان
- مشاوره حقوقی
- مرکز حقوق قربانیان جرم اورگان (OCVLC)

□ برای اخذ دستور محافظت مدنی اقدام کنید

□ معلومات *قابل کنترول*، مانند اعلام حضور در پلتفورم، پست هایی که نشر میکنید، شریک ساختن مکان و... را دقت کنید و ببینید که کدام معلومات قابل کنترول نیست.

□ برای نام، نمبر تلیفون و آدرس خود یک هشدار گوگل (Google Alert) تنظیم کنید تا، در صورت ظاهر شدن این معلومات در جاهای دیگر، هشدار دریافت کنید.

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

- از انتخاب های خارج شدن کارگزاران دیتا استفاده کنید - بعضی از خدمات مانند DeleteMe، Reputation Defender، Privacy Bee، Kanary، OneRep، OptOutPrescreen.com، Do Not Call Registry پولی میباشد.
- برای استفاده های مختلف، از آدرس های ایمیل جداگانه استفاده کنید.
- پلان ایمنی:
  - در محل کار - با بخش منابع بشری به تماس شوید.
  - در خانه - یک پلان شفاف به همراه اعضای خانواده تهیه و ترتیب کنید، با همسایه های مورد اعتماد صحبت کنید، از پولیس بخواهید که تعداد نوبت های گزمه های ایمنی را افزایش بدهد.
  - در مکان های عمومی - با دوستان خود مسافرت کنید، از مسیرهای بدیل استفاده کنید، مقصد و زمان تخمینی برگشت خود را به یک شخص مطمئن خبر بدهید.
- به دوستان/اقارب بگویید که چی نوع معلومات شما را میتوانند در فضای مجازی به اشتراک بگذارند.

منابع دیگر در مورد ایمنی در فضای مجازی (لینک ها به لسان انگلیسی)
نکاتی درباره ساختن پسورد قوی
ایمنی در اینترنت: ایجاد پسورد قوی (gcfglobal.org)
ایجاد پسورد قوی و حساب مصئون تر - راهنمای حساب Google

جهت کسب معلومات بیشتر درباره ایمنی در اینترنت:
داکسینگ: ماهیت ایمنی و روش محافظت از خودتان | NortonLifeLock
5 نکته درباره حفظ امنیت و حریم خصوصی در شبکه های اجتماعی | Norton.com
تنظیم مجدد امنیتی: راهنمای تنظیمات مهمی که همین حالا باید تغییر بدهید | Washington Post
چی قسم خود را از اینترنت حذف کنیم | comparitech
اینجا کارگزاران دیتا به شکل مخفیانه در حال خرید و فروش معلومات شخصی شما هستند | Fast Company
روش محافظت از دیتاها و حذف رایگان معلومات شخصی از اینترنت: راهنمای رایگان و قدم به قدم اعلام انصراف | DeleteMe

روش ناپدید شدن از اینترنت | Reader's Digest

حذف محتوا از Google:
حذف محتوا از Google - راهنمای حقوقی
حذف معلومات شخصی از Google
حذف معلومات هویتی شخصی انتخاب شده یا محتوای شامل در داکسینگ از جستجوی Google

قانون مقابله با داکسینگ:
آگهی رسمی تصویب قانون مقابله با داکسینگ در سنای اورگان

رمزگذاری سر-تا-سر
اپلیکیشن Signal
Whatsapp

اطلاعیه سلب مسئولیت: لینک ها و معلومات ارائه شده در این جعبه ابزار صرفاً برای اطلاع رسانی میباشد، و مکمل نیست، مشاوره حقوقی فرض نمیشود و به معنای تایید شدن محصولات تجاری موجود از طرف وزارت عدلیه اورگان نیست. جهت کسب معلومات بیشتر درباره حقوق خود و انتخاب های حقوقی، بهمراه یک وکیل مشورت کنید.