

## دليل السلامة ضد الدوكسينغ (استقاء المعلومات الشخصية)

دوكسينغ (استقاء المعلومات الشخصية):

- نشر أو مشاركة معلومات شخصية أو خاصة أو تعريفية علنية عن شخص آخر بقصد ضار. غالبًا ما يحدث مثل هذا النشر على الإنترنت ، والغرض من ذلك هو وضع الشخص الآخر في حالة خوف أو تخويف أو إسكات أو مطاردة أو مضايقة أو تهديد الشخص ، أو تشجيع شخص آخر على القيام بذلك

### الحماية ضد الدوكسينغ لموظفي الدوائر الحكومية

قد تخضع رسائل البريد الإلكتروني والنصوص المتعلقة بالعمل والعمل الخاص بك لقوانين طلب السجلات العامة

لا ترسل بريدًا إلكترونيًا / ترسل رسالة نصية إلى شيء لا تفخر بنشره في الصفحة الأولى من الصحيفة

لا ترسل بريدًا إلكترونيًا أو ترسل رسالة نصية إلى أي شخص برقم هاتفك الشخصي أو عنوان المنزل أو البريد أو أسماء العائلة أو الزوج / الشريك أو الأطفال على أجهزة العمل الخاصة بك

لا ترسل بريدًا إلكترونيًا أو ترسل رسالة نصية إلى أي شخص برقم هاتفك الشخصي أو عنوان المنزل أو البريد أو أسماء العائلة أو الزوج / الشريك أو الأطفال على أجهزة العمل الخاصة بك

تحقق مع أقسام تكنولوجيا المعلومات والموارد البشرية لديك بشأن وسائل الحماية التي قد تكون متاحة لك إذا تم إغفال ذلك ، بما في ذلك إدارة تفضيلات إعادة التوجيه ، إذا كانت هناك خيارات تشفير ، وإزالة معلوماتك من موقع وكالتك على الويب ، وتخطيط السلامة داخل المكتب

### الأمان على وسائل التواصل الاجتماعي

احتفظوا بالإعدادات الخصوصية على حساباتكم

. قوموا بإزالة أي عناوين وأماكن عمل أو تعليم من حسابكم (ليست مخفية فقط).

لا تعلنوا عن وجهاتكم ، بما في ذلك المطاعم / المتنزهات / الأحداث والبلدات / المدن / الولايات / البلدان

لا تقبلوا إلا دعوات الصداقة من الأفراد المعروفين

اسمحوا فقط للأصدقاء المعروفين بمشاهدة مشاركاتكم

مراجعة من يمكنه نشر مشاركاتكم

قوموا بتغيير أسماءكم بأسماء مستعارة.  
استخدموا كلمات سر مختلفة وقوية عبر منصات التواصل الاجتماعي.  
لا تنشروا صورًا تُظهر وجوهكم أو وجوه الآخرين.  
لا تنشروا صورًا حيث يمكن لأي شخص تحديد مكانكم.  
حذف البيانات الوصفية من الصور التي تنشروها. تذكروا أن يمكن لصوركم أن تكشف عن موقعكم، تاريخ / وقت التقاط الصورة.  
حددوا مكان الإبلاغ عن التشهير أو خطاب الكراهية على وسائل التواصل الاجتماعي:

[Facebook](#), [Snapchat](#), [Twitter](#), [Instagram](#), [Google](#), [Yelp](#)

. جميع هذه الشركات لها شروط استخدام مختلفة .

تدابير السلامة بعد تعرضكم للدوكسينج

توثيق ما يحدث

أخذ لقطات من كل شيء

حاولوا تضمين التواريخ / الأوقات / أسماء المستخدمين

احذفوا المضمون، إذا استطعتم، لكن قوموا بالتوثيق أولاً

أبلغوا الشرطة إذا كانت هناك تهديدات. تأكدوا من معلومات الفئة المحمية ، الفعلية او المتصورة

(لا تتطلب جرائم الكراهية في ولاية أوريغون والفيدرالية أن يحدد الجاني طبقتكم المحمية الفعلية

بشكل صحيح)

أبلغوا الشرطة عن مخاوف تتعلق:

بسلامة الأسرة / الأطفال / الشركاء

السفر

المظاهر العامة

:معلومات محددة حول:

وشك الحدث: هل يعيش الجاني بالقرب منكم؟

ما هي الكلمات المستخدمة؟ (إهانات ، تهديدات ، أسلحة)

أي دليل. تذكروا أن توقيت بلاغكم للشرطة يمكن أن يؤثر على حفظ الأدلة

لاحظوا أن "التهديدات الحقيقية" الواردة عبر الإنترنت ، أو المرسله عبر البريد العادي ، أو التي تم

إجرائها من خلال مكالمة هاتفية / تركت على بريدكم الصوتي قد تكون جريمة فيدرالية. قوموا بإبلاغ

مكتب التحقيقات الفيدرالية ، أو شجعوا الشرطة المحلية على إرسال تقريركم إلى سلطات تنفيذ

القانون الفيدرالية

قوموا بتغيير كلمات السر على الهاتف والبريد الإلكتروني وحسابات التواصل الاجتماعي.  
تأكدوا من أن كل كلمة مرور مختلفة ومعقدة.  
قوموا بإبلاغ المنصة اطلبوا إزالة معلوماتكم  
اطلبوا إضافة اسمكم / معلوماتكم إلى قائمة "المراقبة عن كثب" بحيث يمكن إزالة معلوماتكم بمجرد  
ظهورها في مكان آخر  
تحدثوا إلى شخص تثقون بهم للحصول على الدعم.

توفر [قوانين الولاية](#) سبل قانونية مدنية.  
تحدثوا مع محامٍ لمعرفة ما إذا كان لديكم سبل قانونية مدنية إضافية:  
[Legal Aid](#) - برنامج إحالة المحامين بولاية أوريغون  
[\(OCVLC\) مركز قانون ضحايا الجرائم في ولاية أوريغون](#)  
النظر في أحكام الحماية المدنية

قوموا بإعداد [تنبيهات](#) لاسمكم ورقمكم وعنوانكم لتلقي التنبيهات إذا ظهرت عبر الإنترنت  
استخدموا خيارات إلغاء الاشتراك في جمع البيانات - بعض الخدمات غير المجانية:  
[DeleteMe](#), [Reputation Defender](#), [Privacy Bee](#), [Kanary](#), [OneRep](#),  
[OptOutPrescreen.com](#), [Do Not Call Registry](#).  
استخدام عناوين بريد إلكتروني منفصلة لأغراض مختلفة

### خطة الأمان:

في العمل - تحدثوا إلى قسم الموارد البشرية  
في المنزل - ضع خطة واضحة مع عائلتك ، وتحدث إلى الجيران الموثوق بهم ، واطلب من الشرطة زيادة  
دوريات السلامة  
في الأماكن العامة - السفر مع صديق ، وسلك طرقًا بديلة ، وأخبروا شخصًا موثوقًا به أين تذهبون ومتى  
تتوقعون العودة  
قوموا بإجراء محادثات مع أفراد العائلة / الأصدقاء حول المعلومات التي يشاركونها عنكم عبر الإنترنت

موارد إضافية للأمان عبر الإنترنت  
نصائح لإنشاء كلمات مرور قوية

[أمان الإنترنت](#)  
[إنشاء كلمة سر قوية وحساب أكثر أمانًا - مساعدة حساب غوغل](#)



تعرف على المزيد حول أمان الإنترنت

[NortonLifeLock | ما هو الدوكسينغ وكيف تحمي نفسك](#)

[Norton.com | نصائح لتأمين الأمن والخصوصية على وسائل التواصل الاجتماعي](#)

[Washington Post | دليل للإعدادات حول الخصوصية التي يجب عليك تغييرها الآن](#)

[comparitech | كيف تحذف نفسك من الإنترنت](#)

[Fast Company | شركات البيانات التي تقوم بشراء وبيع معلوماتك الشخصية يهدوء](#)

[كيفية حماية بياناتك وإزالة المعلومات الشخصية من الإنترنت](#)

[DeleteMe | دليل سحب المعلومات الشخصية من الانترنت المجاني](#)

[Reader's Digest | كيف تخفي نفسك من الإنترنت](#)

إزالة المحتويات من جوجل

[Legal Help – إزالة المحتوى من جوجل](#)

[Google - إزالة المعلومات الشخصية من جوجل](#)

[Google Search إزالة معلومات التعريف الشخصية من "بحث جوجل"](#)

تشريع

[Anti-Doxing Legislation - بيان صحفي لمجلس الشيوخ في ولاية أوريغون](#)

التشفير من طرف إلى طرف

[Signal app](#)

[Whatsapp](#)

إخلاء المسؤولية: الروابط والمعلومات الواردة في الأدوات هذه هي للعلم فقط ، وليست شاملة ، ولا تشكل نصيحة قانونية ، ولا تعكس تأييدًا من قبل وزارة العدل في ولاية أوريغون فيما يتعلق بالمنتجات المتاحة تجاريًا. للحصول على معلومات حول حقوقك وخياراتك القانونية ،

[استشر محاميا](#)