








موارد للأفراد بشأن خطر التشهير من خلال استرجاع واستغلال وثنائق، دوكنج

16 يناير/كانون الثاني 2024









ما هو الدوكسنج؟

يشير **دوكسنج**، **Doxing**، إلى جمع معلومات التعريف الشخصية للفرد ونشرها علناً لأغراض ضارة، مثل الإذلال العلني أو المطاردة أو سرقة الهوية أو الاستهداف للمضايقة.

أمثلة على المعلومات الحساسة

	الاسم الكامل
	معلومات الاتصال
	عنوان المنزل
	أفراد الأسرة
	تفاصيل مكان العمل
	معلومات مالية
	رقم الضمان الاجتماعي

المصادر المشتركة للمعلومات الحساسة

	منشورات مواقع التواصل الاجتماعي
	سجلات الملكية والمحكمة
	إعلانات الزفاف والنعي
	النشرات الإخبارية
	المؤتمرات العامة
	منتديات الويب والمدونات ولوحات المناقشة
	شبكات غير محمية
	قوائم تسجيل الناخبين

كيف يمكنني حماية نفسي من الدوكسنج؟

- كن حذراً بشأن ما تنشره عن نفسك عبر الإنترنت، بما في ذلك الصور ومقاطع الفيديو حتى لو كانت مؤقتة.
- قم بإزالة معلومات تحديد الهوية الشخصية (العنوان وتاريخ الميلاد ورقم الهاتف وما إلى ذلك) من ملفات تعريف الوسائط الاجتماعية الخاصة بك.
- قم بمراجعة متابعيك ورفض الطلبات من أي شخص لا تعرفه.
- اطلب إزالة بياناتك الشخصية من مواقع السجلات العامة. تتضمن مواقع الويب الشهيرة **FastPeopleSearch** و **BeenVerified** و **Whitepages** و **TruthFinder** و **Spokeo** و **PeopleFinders** و **Intelius**.
- قم بإزالة التطبيقات وملفات المتصفح غير الضرورية لمنع جمع بياناتك الشخصية.
- تقييد تتبع الموقع على التطبيقات ومواقع الويب. قم بإيقاف تشغيل خدمات الموقع لكل تطبيق أو منصة تواصل.
- قم بتشغيل إعدادات الخصوصية على وسائل التواصل الاجتماعي والتطبيقات ومواقع الويب الأخرى.
- قم بإعداد التحقق على خطوتين، واستخدم كلمات مرور معقدة، ولا تكرر نفس كلمة المرور لحسابات متعددة.

وزارة الأمن الداخلي | مكتب الشراكة والمشاركة



كيف يمكنني حماية نفسي من الدوكسِنج؟



طلب إزالة المحتوى الكاذب أو المسيء أو التهديدي
فكر في إرسال طلب إزالة إلى النظام الأساسي أو موقع الويب، وفقا للقواعد والمتطلبات.



توثيق ما يحدث
فكر في اتخاذ خطوات للحفاظ على الأدلة. احفظ جميع رسائل البريد الإلكتروني ورسائل البريد الصوتي
والرسائل النصية التي تتلقاها، والنقط لقطات شاشة أو صوراً للتعليقات على وسائل التواصل الاجتماعي.



الإبلاغ عن الحادث
إذا تلقيت تهديدا لسلامتك الجسدية أو شعرت بمضايقة جنائية، فأبلغ عن الحادث إلى جهات إنفاذ
القانون المحلية، بالإضافة إلى منصة التواصل الاجتماعي أو مسؤول موقع الويب.

موارد وإرشادات إضافية

- أفضل ممارسات وموارد الأمن السيبراني لوكالة الأمن السيبراني وأمن البنية التحتية، **CISA**: cisa.gov/cybersecurity
- أساسيات وكالة الأمن السيبراني وأمن البنية التحتية السيبرانية: cisa.gov/cyber-essentials
- نصيحة وكالة الأمن السيبراني وأمن البنية التحتية: تجنب هجمات الهندسة الاجتماعية والتصيد الاحتيالي: cisa.gov/tips/st04
- رؤى وكالة الأمن السيبراني وأمن البنية التحتية: تحسين أمن البريد الإلكتروني والويب: cisa.gov/publication/enhance-email-and-web-security
- إرشادات تصويرية لوكالة الأمن السيبراني وأمن البنية التحتية بشأن تهديدات وسائل التواصل الاجتماعي لموظفي المدارس
والسلطات: <https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic>
- إذا كنت ضحية لجريمة عبر الإنترنت، فقم بتقديم شكوى إلى مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي على
ic3.gov (IC3)