Homeland Security

ڈپارٹمنٹ آف ہوم لینڈ سیکیورٹی
آفس آف پارٹنرشپ اینڈ اینگیجمنٹ (OPE)

ڈاکسنگ کے خطرے سے متعلق افراد کیلئے وسائل

16 جنوری، 2024

ڈاکسنگ کیا ہے؟

ڈاکسنگ سے مراد کسی فرد کی ذاتی طور پر قابل شناخت معلومات (PII) کو اکٹھا کرنا اور اسے بدنیتی پر مبنی مقاصد کے لیے عوامی طور پر جاری کرنا ہے، جیسے کہ عوامی تذلیل، تعاقب، شناخت کی چوری، یا ہراساں کرنے کا ہدف بنانا۔

حساس معلومات کے عام ذرائع

- سوشل میڈیا پوسٹس
- جائیداد اور عدالتی ریکارڈ
- شادی کے اعلانات اور تعزیتی پیغامات
- نیوز لیٹرز
- پبلک کانفرنسیں
- ویب فورمز، بلاگز، اور ڈسکشن بورڈز
- غیر محفوظ نیٹ ورکس
- ووٹر رجسٹریشن لسٹ

حساس معلومات کی مثالیں

- پورا نام
- کانٹیکٹ انفارمیشن
- گھر کا پتہ
- خانان کے افراد
- کام کی جگہ کی تفصیلات
- مالی معلومات
- سوشل سیکیورٹی نمبر

میں اپنے آپ کو ڈاکسنگ سے کیسے بچا سکتا ہوں؟

- اپنے متعلق جو کچھ آپ آن لائن پوسٹ کرتے ہیں اس کے بارے میں **محتاط رہیں**، بشمول تصاویر اور ویڈیوز چاہے عارضی ہوں۔
- اپنے سوشل میڈیا پروفائلز سے PII (پتہ، تاریخ پیدائش، فون نمبر وغیرہ) کو **ہٹا دیں۔**
- اپنے فالوَرز کا **جائزہ لیں** اور کسی ایسے شخص کی درخواستوں کو مسترد کریں جنہیں آپ نہیں جانتے۔
- عوامی ریکارڈ کی ویب سائٹس سے اپنا ذاتی ڈیٹا ہٹانے کی **درخواست کریں۔** معروف ویب سائٹس میں یہ شامل ہیں۔

BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, and Whitepages.

- اپنے ذاتی ڈیٹا کو جمع کرنے سے روکنے کے لیے غیر ضروری ایپس اور براؤزر ایکسٹینشنز کو **ہٹا دیں۔**
- ایپس اور ویب سائٹس پر لوکیشن ٹریکنگ کو **محدود کریں۔** ہر ایپ یا پلیٹ فارم کے لیے لوکیشن سروسز کو بند کر دیں۔
- سوشل میڈیا، ایپس اور دیگر ویب سائٹس پر پرائیویسی کی ترتیبات کو **آن کریں۔**
- دو اسٹیپس کی ویری فکیشن کو **ترتیب دیں،** پیچیدہ پاس ورڈ استعمال کریں، اور متعدد اکاؤنٹس کے لیے ایک ہی پاس ورڈ کو نہ دہرائیں۔

DHS OPE

میں اپنے آپ کو ڈاکسنگ سے کیسے بچا سکتا ہوں؟

غلط، بدسلوکی، یا دھمکی آمیز مواد کو ہٹانے کی درخواست
قواعد اور تقاضوں کے مطابق پلیٹ فارم یا ویب سائٹ پر ہٹانے کی درخواست جمع کرانے پر غور کریں۔

دستاویز کیا ہو رہا ہے
شواہد کو محفوظ رکھنے کے لیے اقدامات کرنے پر غور کریں۔ آپ کو موصول ہونے والے تمام ای میلز، وائس میلز اور ٹیکسٹ پیغامات کو محفوظ کریں، اور سوشل میڈیا پر تبصروں کے اسکرین شاٹس یا تصاویر لیں۔

واقعہ کی اطلاع دیں
اگر آپ کو اپنی جسمانی حفاظت کے لیے خطرہ موصول ہوا ہے یا آپ کو مجرمانہ طور پر ہراساں کیا گیا ہے، تو اس واقعے کی اطلاع مقامی قانون نافذ کرنے والے اداروں کے ساتھ ساتھ سوشل میڈیا پلیٹ فارم یا ویب سائٹ کے منتظم کو دیں۔

اضافی وسائل اور ہدایات

CISA سائبرسیکیوریٹی بہترین طریقہ کار اور وسائل: cisa.gov/cybersecurit

CISA سائبیر اسینشلز: cisa.gov/cyber-essentials

CISA ٹپس: سوشل انجینئرنگ اور فشنگ حملوں سے بچنا: cisa.gov/tips/st04-014 :

CISA انسائیٹس: ای میل اور ویب سیکیورٹی کو بہتر بنائیں: cisa.gov/publication/enhance-email-and-web-security

CISA سوشل میڈیا تھریٹ گائیڈنس برائے سکول سٹاف اور اتھارٹیز انفوگرافک: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

اگر آپ آن لائن جرم کا شکار ہیں تو ایف بی آئی کے انٹرنیٹ کرائم کمپلینٹ سنٹر (IC3) میں شکایت یہاں درج کروائیں۔
ic3.gov