وزارت امنیت داخلی

وزارت امنیت داخلی
دفتر همکاری و ارتباطات (OPE)

منابع برای افراد در مورد تهدید افشای اطلاعات شخصی/داکسینگ (Doxing)

۱۶ جنوری ۲۰۲۴

داکسینگ (Doxing) چیست؟

داکسینگ به جمع آوری اطلاعات شخصی شناسایی‌پذیر یک فرد و انتشار آن به صورت عمومی با اهداف مغرضانه مانند تحقیر عمومی، تعقیب، سرقت هویت یا هدف‌گیری برای آزار و اذیت گفته می‌شود.

مثال های اطلاعات حساس

- اسم مکمل
- معلومات تماس
- آدرس خانه
- اعضای فامیل
- معلومات در مورد محل کار
- معلومات مالی
- شماره سوشل سیکیوریتی

منابع عمومی بدست آوردن اطلاعات حساس

- شریک ساختن مطالب و اطلاعات در شبکه های اجتماعی
- سوابق محکمه و جایداد/دارای
- اعلان محافل عروسی و یا جنازه
- خبرنامه
- کانفرانس ها/جلسات عمومی
- گردهمایی های انترنیتی، بلاگ و میزهای گرد مباحثه
- شبکه های محافظت ناشده
- لیست های ثبت نام رای دهندگان

چگونه میتوانم خودم را از داکسینگ (Doxing) محافظت نمایم؟

- به آنچه که درباره خودتان بصورت آنلاین منتشر می‌کنید، از جمله عکس‌ها و ویدیوها، حتی اگر موقت باشند، **دقت** نموده و **محتاط** باشید.
- اطلاعات شناسایی پذیر (PII) (مانند؛ آدرس، سال تولد، شماره تماس، و غیره) خود را از صفحات اجتماعی خود **حذف** نمایید.
- فالور های خود را **مرور** نموده و درخواست های دوستی افراد ناشناس را **رد** نمایید.
- برای از بین بردن اطلاعات شخصی تان از ویب سایت های سوابق عمومی **درخواست بدهید**. ویب سایت های مشهور شامل ذیل اند؛ BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, and Whitepages.
- برای جلوگیری از ذخیره شدن اطلاعات شخصی تان، برنامه ها/اپلیکیشن ها و افزونه های مرورگر انترنیتی غیر ضروری تان را **حذف نمایید**.
- ردیابی موقعیت (Location) را در برنامه ها/اپلیکیشن ها و صفحات انترنیتی **محدود/خاموش** نمایید. برای هر یک از برنامه ها و ویب سایت ها به صورت جداگانه گزینه ردیابی موقعیت را خاموش نمایید.
- تنظیمات حفظ محرمیت (Privacy) را در هر یک از برنامه ها، شبکه های اجتماعی و دیگر ویب سایت ها **فعال نمایید**.
- تنظیمات تأییدی دو مرحله ای را **فعال نمایید**، از رمز های عبوری مغلق استفاده نمایید، و از استفاده یک رمز برای چندین برنامه و حساب کاربردی اجتناب ورزید.

DHS OPE

چگونه میتوانم خودم را از داکسینگ (Doxing) محافظت نمایم؟

درخواست برای حذف محتوای غیردرست، ناپسند یا تهدیدآمیز
درنظر بگیرید تا با رعایت قوانین و الزامات، درخواست حذف محتوا را به پلتفرم یا وب‌سایت ارسال نمایید.

وقایع را مستند سازی نمایید
اطمینان حاصل نمایید که برای حفظ شواهد اقداماتی انجام دهید. تمام ایمیل‌ها، پیام‌های صوتی و متنی که دریافت می‌کنید را ذخیره نمایید، و از نظرات در رسانه‌های اجتماعی اسکرین‌شات یا عکس بگیرید.

وقایع را گزارش دهید
اگر تهدیدی به امنیت فیزیکی خود دریافت کرده‌اید یا احساس متضرر شدن از جرایم را دارید، واقعه را به نیروهای پولیس محلی و همچنین مدیر رسانه‌های اجتماعی یا وب‌سایت مربوطه گزارش دهید.

منابع و رهنمایی های اضافی

بهترین منابع و روش‌ها برای امنیت سایبری (CISA): cisa.gov/cybersecurity
اساسات و نیاز های سایبری (CISA): cisa.gov/cyber-essentials
نکته (CISA): جلوگیری از حملات انجینیری اجتماعی و فیشینگ (Phishing): cisa.gov/tips/st04-014
بینش (CISA): بهبود امنیت انترنیتی و ایمیل: cisa.gov/publication/enhance-email-and-web-security
رهنمود تهدیدات رسانه های اجتماعی برای کارمندان مکاتب و معلومات مسولین (CISA):
https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

اگر شما قربانی جنایات آنلاین هستید، شما میتوانید در **بخش مرکز شکایات جنایات انترنیتی FBI (IC3)** شکایت خود را از طریق ic3.gov ثبت نمایید.