مقابله با ازارگری سایبری و مهار ردیابی خود در فضای مجازی

- مدت زمان: ۱ ساعت
- هدف درس نامه : یادگیری شناسایی اطلاعات قابل دستیابی درباره خود در فضای مجازی، حذف اطلاعات شخصی، ایجاد نظارت، استراتژی‌های جداسازی داده‌های شخصی و کاری و....

داکسینگDoxing

خبرنگاران و کنشگران می‌توانند برای برخی از کارهایشان مورد تهدید و انتقام‌گیری قرار بگیرند. یکی از روش‌های به سکوت وادار کردن آن‌ها استفاده از داکسینگ **doxing** است: مهاجمان از اطلاعاتی که در شبکه‌های اجتماعی و وب‌سایت‌های حرفه‌ای منتشر شده است برای هک، سوءاستفاده یا افترا علیه هدف خود استفاده می‌کنند.

داکسینگ Doxing

داکسینگ به انگلیسی Doxing برگرفته از داکس (به انگلیسی: dox مخفف documents به معنی اسناد) ، عمل تحقیق و نشر دادن در عرصه‌ی عمومی اطلاعات شخصی یا اطلاعات شناسایی کننده (به ویژه اطلاعاتی که منجر به شناسایی افراد می شود) دربارهٔ یک فرد یا نهاد در اینترنت

شناسایی اطلاعاتی که از شما می‌توان بدست آورد

- بنابراین، **اهمیت دارد بدانیم چه اطلاعاتی درباره ما در فضای مجازی قابل دسترسی هستند.**
- به آنچه که این اطلاعات می‌توانند درباره ما فاش کنند، فکر کنیم
- اگر امکان دارد برای حذف آن‌ها اقداماتی بدست گیریم .

اینترنت فراموش نمی‌کند!

حذف کامل داده‌های نشر شده‌ی از ما در فضای مجازی ممکن است دشوار باشد. این داده‌ها ممکن است در سایتی چون archive.org ذخیره شده باشند، یا به شکل تصویر (کاپتور) از صفحه نمایش ما ذخیره شده و با دیگران به اشتراک گذاشته شوند. همچنین ممکن است این داده‌ها توسط افرادی در وب‌سایت‌ها یا حساب‌های کاربری منتشر شده باشند، که شما بر آن‌ها کنترل ندارید.

شناسایی اطلاعات قابل دستیابی

شناسایی اطلاعات قابل دستیابی: چگونه؟

داده‌ها را :

- درباره‌ی خود و اعضای خانواده و نزدیکان خود جستجو کنید.
- از موتورهای جستجوگر دیگری به جز گوگل مانند یاهو، بینگ و .... نیز استفاده کنید.
- با استفاده از فن جستجوی پیشرفته در گوگل، می‌توانید بررسی کنید که چه اطلاعات شخصی درباره شما در فضای مجازی و به شکل آنلاین قابل دسترسی است:

- برای دانستن آیا آدرس شما و یا شماره تلفنم شما در فضای مجازی نشر شده است و قابل دسترسی است، در گوگل اینگونه جستجو کنید :

*"نام نام خانوادگی" "آدرس *"* - برای شماره تلفن: *"نام نام خانوادگی" "07*"*

پاک کردن اطلاعات شخصی در فضای مجازی و آنلاین

در شبکه‌های اجتماعی

- در حساب‌های کاربری شبکه‌های اجتماعی خود، عکس‌ها و ویدئوها و همچنین نظرات و کامنت‌ها را درباره‌ی مطالب منتشر شده خود بررسی کنید.
- آن‌چه را که می‌خواهید حذف شود، یادداشت کنید.

- این کار را به شکل منظم انجام دهید و سعی کنید در تقویم خود زمانی لازم (هر ۶

در وب‌سایت‌های‌تان

بر روی وب‌سایت خود و هر سایت دیگری که اداره می‌کنید، بررسی کنید تا اطلاعات حساس را شناسایی کرده و در حد امکان راه‌هایی برای حذف آنها پیدا کنید.
به عنوان مثال، به جای نمایش آدرس فیزیکی یا ایمیل‌تان از یک فرم تماس آنلاین استفاده کنید

در سایت‌های دیگر

می‌توانید از وب‌سایتی که اطلاعاتی درباره شما نشر کرده است، بخواهید که این اطلاعات را حذف کنند. اما انجام آن اقدامی حتمی نیست و زمان‌بر است و به حُسن نیت مدیران وب‌سایت نیز بستگی دارد.
با این حال، در اروپا، از سال ۲۰۱۴ می‌توان از قانون «حق فراموشی» خود استفاده کرد و از Google Search

خانواده و نزدیکان خود را آگاه کنید

- با خانواده و دوستان خود در مورد اطلاعاتی که درباره شما و دیگران منتشر می‌کنند، صحبت کنید
- به آن‌ها توضیح دهید کدام اطلاعات را شما می‌خواهید به اشتراک بگذارید و کدام اطلاعات را محرمانه می‌دانید
- به آن‌ها در باره‌ی محدود کردن نشرهایشان که در آنها شما را تگ کرده‌اند، تذکر کنید.
- .

هشدارها را راه‌اندازی کنید

راه‌اندازی هشدارها

- هشدارهای گوگلرا برای نام، آدرس و دیگر اطلاعاتی مانند تاریخ تولد یا آدرس ایمیل، فعال کنید.
- در تنظیمات هشدار اشتباه‌های املایی متداول در نام خود را هم پیش‌بینی کنید .

جداسازی فعالیت‌ها

جداسازی فعالیت‌ها: چگونه

از حساب‌های متفاوت برای کار و زندگی شخصی خود استفاده کنید: یک آدرس ایمیل برای کار، یکی دیگر برای کارهای شخصی، این اقدام برای حساب‌های کاربری در شبکه‌های اجتماعی نیز ممکن است مفید باشد.

استراتژی‌های متفاوت بکار گیرید

چگونه؟

	خطر	معروفیت	تلاش
هویت واقعی	+	+	-
ناشناس	-	-	+
نام مستعار	-	+	+
هویت جمعی	-	+	+

تنظیمات صفحه‌های شبکه‌های اجتماعی خود را بررسی کنید

برای آنکه بدانید چه اطلاعاتی از شما در توییتر- Twitter، فیسبوک - Facebook، اینستاگرام - Instagram و تیک‌تاک - Tiktok و .... منتشر شده است، باید تنظیمات حریم خصوصی حساب‌های شبکه‌های اجتماعی خود را **بررسی** کنید.

برای آگاهی بیشتر

می‌توانید چگونگی حضور خود را در اینترنت با سایت‌هایی مانند namechecker بررسی کنید.
یا برای آنکه بدانید که یک حساب قدیمی را در یک پلتفرم یا سرویس آنلاین (که برخی اطلاعات شما ممکن است در آن حفظ شده باشد) فراموش نکرده‌اید می‌توانید از سایت whatsmyname استفاده کنید.

آیا ای‌میل شما هک شده است؟

بررسی کنید که آیا کدام یک از حساب‌های شما دچار نشت اطلاعات نشده است. آدرس ایمیل خود را در Firefox Monitor یا در haveibeenpwned وارد کنید. آدرس میل خود را وارد کنید و ***pwned*** *را کلیک کنید.*

چه کاری باید انجام دهید وقتی که قربانی آزارگری سایبری می‌شوید؟

کمک بخواهید

- در هنگام آزارگری سایبری، مهمترین اقدام‌ها : سکوت نکنید و منزوی نشوید. با یکی از نزدیکان‌تان در این مورد مشوره کنید.
- اگر لازم شد، می‌توانید در مدت وضعیت طوفانی، مدیریت حساب‌های کاربری‌تان را به فردی مورد اعتمادی بسپارید تا او مدیریت کند.
-

مستند سازی کنید

- همه مدارک آزارگری سایبری علیه خود را مستند کنید. از صفحه نمایش- مانیتور- تصویر بگیرید.
- همه‌ی پیام‌ها و اطلاعات مرتبط با آزارگران سایبری را (خود یا فردی که حساب‌تان را در اختیارش گذاشته‌اید) ثبت کنید.
- داشتن این اطلاعات به شما برای اخطار دادن و روشن کردن این وضعیت کمک

قفل کنید

- حساب‌های شبکه‌های اجتماعی خود را قفل کنید. تنظیمات حریم خصوصی را تغییر دهید تا دسترسی به آنها را محدود و مسدود کنید.
- حساب‌های شبکه‌های اجتماعی خود را قفل کنید.
- یا از گزینه‌های حافظ حریم خصوصی پیشرفته‌تر مانند "من را پیدا نکن" یا "لیست دوستان من را نشر/اشتراک‌گذاری نکن" استفاده کنید. و حتما آزارگران و متجاوزان سایبری را مسدود کنید.

محتواهای آزارگرانه را به پلتفرم‌ها گزارش دهید

- Facebook
- Twitter
- LinkedIn
- Instagram
- Snapchat
- TikTok
- WhatsApp
- YouTube

شکایت کنید

به پوسته پلیس یا به صورت کتبی به مقام‌های عدلی ولایت خود با ارائه تمام مدرک‌های در دسترس اعلام شکایت کنید.

برای دانستن بیشتر

Totem را به زبان دری فارسی دنبال کنید

Know your troll