د افرادو لپاره د شخصي اطلاعاتو افشاء کولو (Doxing) ګواښونو په اړه سرچينې

۱۶ جنوری ۲۰۲۴

ډاکسينګ (Doxing) څه شی دی؟

ډاکسينګ د يو فرد په اړه د شخصي پېژندلو معلوماتو (PII) راټولول او د مغرضانه موخو لپاره لکه عامه سپکاوی، تعقيب، د هويت غلا، يا د ځورونې په موخه په عامه توګه د هغې نشرول دي.

د حساسو اطلاعاتو مثالونه

- بشپړ نوم
- د اړيکې معلومات
- د کور آدرس
- د کورنۍ غړي
- د کار/وظيفې په اړه معلومات
- مالي معلومات
- د سوشل سيکيوريټي شمېره

د حساسو اطلاعاتو ترلاسه کولو عمومي سرچينې

- په ټولنيز رسنيو کې د اطلاعاتو او مطالبو شريکول
- په محکمه کې او د جايداد/شتمنيو سوابق
- د ودونو و يا د جنازې په اړه عمومي اعلانات
- خبرنامه
- کانفرانسونه او يا عمومي جلسات
- د انټرنيټ غونډې، بلاګونه او ګردي ميزونه
- ناخوندي شوي شبکې
- د رايې ورکوونکو د نوم ليکنې ليست

زه څنګه کولی شم د ډاکسينګ (Doxing) څخه ځان خوندي وساتم؟

- د هغه څه په اړه **محتاط اوسئ** چې تاسو د خپل ځان په اړه آنلاين پوسټ کوئ، د عکسونو او ويډيوګانو په شمول حتی که لنډمهاله وي.
- خپل شخصي پېژندلو معلومات (PII) (د بېلګې په توګه پته، د زيږون نېټه، د اړيکو شمېره، او نور) له خپلو ټولنيزو پاڼو څخه **لرې کړئ**.
- د خپلو فالورانو **بياکتنه وکړئ** او د نامعلومو خلکو څخه د دوستۍ درخواست **رد کړئ**.
- د عامه ريکارډونو ويب پاڼو څخه د خپل شخصي معلوماتو **حذف کولو غوښتنه وکړئ**. مشهور ويب پاڼې لاندې دي؛

  BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, and Whitepages.
- د دې لپاره چې ستاسو شخصي معلومات خوندي پاتې شي، خپل د کمپيوټر او ګرځنده ټيليفونونو څخه غير ضروري پروګرامونه/اپليکيشنونه او د انټرنيټ براوزر ايکسټينشنونه **حذف کړئ**.
- په برنامو/اپليکيشنونو او انټرنيټ پاڼو کې د موقعيت تعقيب آپشن **محدود/بند کړئ**. د هر برنامې او ويب پاڼې لپاره په جلا توګه د موقعيت تعقيب اختيار بند کړئ.
- په هر پروګرام، ټولنيزو شبکو او نورو ويب پاڼو کې د محرميت تنظيمات **فعال کړئ**.
- د دوه مرحلې تاييد تنظيمات **فعال کړئ**، مغلق پاسورډونه وکاروئ، او د مختلفو اپليکيشنونو او حسابونو لپاره د ورته پاسورډ کارولو څخه ډډه وکړئ.

زه څنګه کولی شم د ډاکسینګ (Doxing) څخه ځان خوندي وساتم؟

د غلط، ناوړه، یا ګواښونکي مطالبو لرې کولو غوښتنه وکړئ
په پام کې ونیسئ چې د مقرراتو او قوانینو سره سم پلیټ فارم یا ویب پاڼې ته د مطالبو لرې کولو/حذف کولو غوښتنه وسپارلئ.

پیښې مستند کړئ
ډاډ ترلاسه کړئ چې تاسو د شواهدو ساتلو لپاره ګامونه پورته کوئ. ټول بریښنالیکونه، غږیز پیغامونه او متنونه چې تاسو یې ترلاسه کوئ خوندي کړئ، او په ټولنیزو رسنیو کې د ځان په اړه د نظریاتو سکرین شاټونه یا عکسونه واخلئ.

د پیښو راپور ورکړئ
که تاسو خپل فزیکي خوندیتوب ته ګواښ ترلاسه کړی یا احساس کوئ چې تاسو د جرم قرباني شوي یاست، د پیښې په اړه خپل محلي پولیس ځواک او همدارنګه د مربوطه ټولنیزو رسنیو یا ویب پاڼو مدیرانو ته راپور ورکړئ.

اضافي سرچینې او لارښوونې

د سایبر امنیت غوره کړنې او سرچینې (CISA): cisa.gov/cybersecurity

د سایبر اساسات او اړتیاوې (CISA): cisa.gov/cyber-essentials

یادونه (CISA): د ټولنیز انجینرۍ او فشینګ (Phishing) بریدونو مخنیوی: cisa.gov/tips/st04-014

د CISA انسایټ: د بریښنالیک او ویب امنیت ته وده ورکړئ cisa.gov/publication/enhance-email-and-web-security

د ښوونځي کارمندانو لپاره د ټولنیزو رسنیو ګواښونو او د مدیرانو لپاره د معلوماتو لارښود (CISA) https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

که تاسو د آنلاین جرم قرباني یاست، تاسو کولی شئ **د FBIدا د انټرنیټي جرمونو شکایت مرکز (IC3) ته د** ic3.gov له لارې شکایت درج کړئ.