

مجازي فضا کې د تعقيب د مهارولو او د سايبري ځورونو سره مقابله

• زماني موده: ۱ ساعت

• د زده کړو هدف: په مجازي فضا کې د خپل ځان په اړه د لاس رسې وړ معلوماتو پيژندل، د شخصي معلوماتو د حذفولو زده کړه، د څارنې رامنځ ته کيدل، د شخصي او کاري معلوماتو د جداوالي په برخه کې ستراتيژي ...

معلوماتي نښه چې له تاسو کيدای شي په لاس يې راوړي

خبريالان او فعالان کيدای شي د خپلو ځينو کارونو له امله د ګواښ لاندې راشي او غچ اخيستنې سره مخ شي. يو ددغو کړنلارو د هغوی چپولو (سکوت) ته اړ ايستل او ډاکسينګ **doxing** دی: بریدکوونکي کوم معلومات چې په ټولنيزو شبکو او مسلکي يا حرفوي ويب سايټونو کې خپرېږي د خپل هدف پر وړاندې د هک، ناوړې استفادې يا افترا او سپګاوي لپاره ورڅخه کار اخلي.

ډانکسينګ چې د انگليسي **Doxing** [ډاکس څخه اخيستل شوی: په انگليسي کې **dox**: مخفف **documents**) اسنادو په معنی دی (د پلټنې عمل او د شخصي اطلاعاتو عمومي خپرول يا د معلوماتو پيژندګلوي کونکی په ځانګړي ډول هغه معلومات چې د افرادو د پيژندګلوئ سبب کېږي) د يو فرد يا يو سازمان په اړه دي چې په اينټرنیټ کې خپرېږي.

د همدې له امله اهمیت لري چې پوه شو چې زموږ په اړه په مجازي فضا کې کوم معلومات د لاس رسې وړ دي. هغه څه دا معلومات کولی شي زموږ په تړاو يو څه افشا کړي په باب يې فکر وکړو او که چيرې امکان لري د حذفولو په هکله يې لاس په کار شو.

اينټرنیټ نه هيروي. په بشپړ ډول زموږ د انلاين ډاټا (**Datas**) حذفول ممکن ستونزمن کار اوسي. ممکن دا ډاټا د **archive.org** په څير سايت کې ذخيره شوي وي، يا د (**Capture**) په بڼه عکس زموږ د نندارې لاندې پانې څخه ذخيره شوی او نورو سره شريک شوی وي. همدارنگه کيدای شي دا ډاټا د ځينو کسانو له خوا په ويب سايټونو او يا د کاروونکو حسابونو له لارې خپره شوې وي چې تاسو پرې کنټرول نلرئ.

بنآ ډاټا (Datas) :

- د خپل ځان او د خپلې کورنۍ د نږدې غړو په اړه ولټوئ.
- د لټون لپاره د گوگل پرته له نورو ماشینونو څخه لکه یا هو، بینګ او... څخه کارواخلئ.
- په گوگل کې د لټون د پرمختللي فن څخه په کار اخیستنې سره کولی شئ چې دا وارزوئ چې ستاسو په اړه کوم شخصي معلومات په مجازي فضا کې او په انلاین بڼه د لاس رسي وړ دي:
- د پوهاوي لپاره ایا ستاسو ادرس او د تیلیفون شمیره په مجازي فضا کې خپره شوې ده او د لاس رسي وړ ده، په گوگل کې په دا ډول ولټوئ:
- *نوم د کورنۍ نوم " آدرس \\\07

لینک ورکړل شي

مجازي او انلاین فضا کې د شخصي معلوماتو پاکول

- ټولنیزو شبکو کې ستاسو کاروونکي حسابونه خپلو ټولنیزو شبکو کې کاروونکي حسابونه، عکسونه او ویدیوګانې او همدارنګه ستاسو د خپرو شویو موضوعاتو په اړه خپاره شوي نظریات او تبصرې وارزوئ.
- هغه څه چې حذف یې غواړي یاداشت یې کړئ.
 - دا کار په منظم ډول ترسره کړئ او هڅه وکړئ په خپله زمانې کلیده کې لازمه موده (هر و ۶ میاشتو کې) د یادونې لپاره وټاکئ.

ستاسو په خپلو ویب سایټونو کې

د خپل ویب سایټ پرمخ او د بل هر ویب سایټ چې اداره کوئ یې، د حساسو معلوماتو د پیژندلو لپاره ارزونه ترسره کړئ او د امکان په حد کې د حذفولو لپاره یې لارې ومومئ. د مثال په توګه، د فیزیکی ادرس یا ستاسو د ایمیل بنودلو پر ځای د یو انلاین فورمې څخه ګټه واخلئ.

د نورو په سایټونو کې

کولی شئ د ویب ستایت څخه چې تاسو په تړاو یې معلومات خپاره کړي، وغواړئ چې دا معلومات حذف کړي. خو ترسره کول یې حتمي نه دي او وخت ته اړتیا لري او د ویب سایټونو د مدیرانو ښه نیت پورې هم تړاو لري. په ورته وخت کې په اروپا کې د ۲۰۱۴ کال راهیسې کیدای شي د خپل "هیرولو له حق" د قانون څخه ګټه پورته شي او د [Google Search](#) څخه وغواړئ چې ستاسو په اړه لینکونه د خپل نوملړ څخه حذف کړي.

خپله کورنۍ او خپلوان وپوهوئ

د خپلې کورنۍ او دوستانو سره د هغو معلوماتو په اړه خبرې وکړئ چې ستاسو او د نورو په هکله یې خپوروي. هغوی ته دا وضاحت ورکړئ چې تاسو کوم معلومات غواړئ چې شریک یې کړئ او کوم معلومات غواړئ چې محرم پاتې شي. همداشان هغوی ته د خپلو خپرونکو موادو د محدودولو په اړه چې تاسو په کې ټګ (Tag) کوي هم یادونه وکړي

د پېښې علاج د پېښیدو دمخه وکړئ

خبرداري په لاره واچوئ

د [ګوګل خبرداري](#) د نوم، ادرس او نور معلومات لکه زیږیدو نیټه یا د ایمیل ادرس، فعال کړئ. د خبرداري په پروګرام کې خپلې عامې املایي تیروتنې د خپل نوم په برخه کې هم په پام کې ونیسئ.

د فعالیتونو جداوالی

د کاراو د خپل شخصي ژوند د مختلفو حسابونو څخه کار واخلي: د ایمیل یو ادرس د کار لپاره، یو بل د شخصي کارونو لپاره، دا اقدام په ټولنیزو شبکو کې د کاروونکو حسابونو لپاره ممکن ګټور اوسې. ددې کار لپاره د مختلفو سټراتیژیو څخه کار واخلي:

- واقعي هویت
- ناپېژاند
- مستعار نوم

هڻه	اعلان	خطر	
-	+	+	واقعی هویت
+	-	-	ناپیژاند
+	+	-	مستعار نوم
+	+	-	دلہ بیز هویت

د خپلو ټولنیزو شبکو د پروفایلونو تنظیمات (Settings) و ارزوئ

ددې لپاره چې چې پوه شئ چې تاسو په ټویټر، فیسبوک، اینستاگرام او ټیک ټاک او... کې کوم معلومات خپاره شوي، باید خپلو ټولنیزو شبکو کې په حسابونو کې دخصوصي حریم تنظیمات (settings) و ارزوئ.

د لا زیاتې خبرتیا لپاره : تاسو کولی شئ په اینټرنیټ کې د خپل حضور د ټرنګوالی لپاره د [namechecker](#) په څیر سایټونه و ارزوئ. یا ددې لپاره چې په دې پوه شئ چې یو پخوانی حساب په یو پلټفورم (Flat form) او یا په یو انلاین سرویس کې (چې کیدای شي ستاسو ځینې معلومات په کې ساتل شوي وي) له یاد څخه مو وتلي نه وي کولی شئ د [whatsmyname](#) څخه کار واخلئ.

ایا ستاسو ایمیل هک شوی؟

دا وڅیړئ چې ایا ستاسو کوم یو حساب د درز (Leakage) ستونزې سره نه دی مخ شوی. د ایمیل خپل ادرس په [Firefox Monitor](#) او یا هم [haveibeenpwned](#) کې داخل (Enter) کړئ. د خپل ایمیل ادرس داخل کړئ او [pwned](#) باندې کلیک وکړئ.

ځورونه- جوړجاری یا حتی بشپړ حذف

کله چې د سایبري ځورونې قرباني کیږئ کوم کارونه باید ترسره کړئ؟

ک. له چا څخه مرسته وغواړئ

په دې اړه له خپلو نږدې خپلوانو سره خبرې وکړئ. د سایبري ځورونې پرمهال ترټولو مهم اقدامات: چپ مه پاتې کېږئ او انزوا مه غوره کوئ. که چیرې اړتیا پېښه شي تاسو کولی شئ د توپاني وضعیت پر مهال د خپلو کاروونکو حسابونو مدیریت اعتمادي کسانو ته د مدیریت لپاره وسپارئ.

م. مستند یې کړئ

د خپل ځان اړوند د سایبري ځورونې ټول حقایق (facts) مستند کړئ. تر نندارې لاندې اینټرنیټي پاڼې څخه تصویرونه واخلي، د سایبري ځورونې اړوند ټول پیغامونه او معلومات (پخپله او یا هغه چاته مو چې د خپلو کاروونکو حسابونو مدیریت سپارلی) ثبت کړئ. دغه معلومات تاسو ته د خبرداري په ورکولو او ددغه وضعیت په روښانه کولو کې مرسته کوي. همداشان د عریضې د ثبتولو له لارې شکایت کول به گټور اوسي.

ق. قفل یې کړئ

په ټولنیزو شبکو کې خپل حسابونه قفل کړئ. د خپل خصوصي حریم اړوند تنظیمات (settings) بدل کړئ ترڅو ورته د هغوی لاس رسی بند شي. یا خپل حسابونه په بشپړ ډول خصوصي کړئ. یا د خصوصي حریم د پرمختللي انتخاب (option) څخه لکه " ما مه پیداکوه" یا " زما د دوستانو لیست خپور / شریک نه کړئ. همداشان حتمي د سایبري ځورونکي او بریدکوونکي بند کړئ.

ح. حذف یې کړئ

کوم محتویات چې د ځورونکوله خوا خپاره شوي، حذف یې کړئ، اینټرنیټ کې ډیر د لټون ماشینونه د حذفولو غوښتنو ته د انلاین پښتنو له لارې د حذف غوښتنې ورکوي. د لټون د هر ماشین لکه Bing, Qwant, Google, Yahoo و... کولی غوښتنه وکړئ.

گ. رپوټ یې ورکړئ

پلټ فامونو ته د محتویاتو راپور ورکړئ:

شکایت وکړئ

- [Facebook](#)
- [Twitter](#)
- [LinkedIn](#)
- [Instagram](#)
- [Snapchat](#)
- [TikTok](#)
- [WhatsApp](#)
- [YouTube](#)

د پولیسو مرکز یا په لیکلي بڼه د خپل ولایت عدلي چارواکو ته په لاس کې د لرلو ټولو اسنادو په وړاندې کولو سره خپل شکایت ثبت کړئ.

یو ساتونکی وگماری

[BodyGuard](#) یو پروگرام دی چې د آیفون او اندروید ورته لاس رسی لري او په ژوندۍ بڼه مخالف لورې محتویات، نژاد پالنې، هوموفوبیک یا د جنسي او اخلاقي اړوند څوړونې له لارې مدیریت کړئ.



Secure Your Digital World With BodyGuard Mobile Security

Compare BodyGuard Security		BodyGuard Mobile Security	VS	Other Mobile Security
SECURITY	Real Time Web Security	✓		X
	Wi-Fi Security	✓		X
	VPN Security	✓		X
	Scan Type	Automatic		Manual
	App Security	✓		✓
	Virus Security	✓		✓
PRIVACY	Unblock Blocked Website	✓		X
	Private Browsing	✓		X
	Lock Your Apps	✓		X
UTILITIES	Compatibility	Android & iOS		Android
	Find Country Of Your Apps	✓		X
	Discover Your Exposed Data	✓		X
	Recover Your Lost Device	✓		X



Identity & Fraud Protection



Private & Safe Browsing



Global VPN Servers



Locate Your Lost Device

د لا زيات پوهاوي لپاره

[د توتم فارسي لوستونه](#)