



د خپل ډیجیټل فوټ پرنټ (Digital Footprint) مدیریت کول

ډیجیټل فوټ پرنټ ټول هغه معلومات دي چې په انټرنېټ کې د آنلاین فعالیت له امله شتون لري. په دې کې ستاسې د خواله رسنیو پوستونه، چټونه، متنونه، براوژینګ تاریخچه، برېښنالیکونه، آنلاین پېرودنې او د موقعیت اطلاعات شاملېږي، خو یوازې په دغو پورې محدود نه دي. ستاسې ډیجیټل فوټ پرنټ کولای شي:

د خلکو ډیجیټل فوټ پرنټ ته لاسرسی پیدا کړي ترڅو هغوی د کرکجنو خبرو او کرکجنو جرمونو تر سره کولو ته وهڅوي.

● ستاسې د کډوالۍ پر کېس باندې منفي واغېز وکړي.

اوس نو باید د خواله رسنیو اکاونټونه، یوزرنومونه/هیندلونه او نور ډیجیټل معلومات د زیاترو عامه کډوالۍ غوښتنلیکونو سره افشا شي او کله چې یو کس متحده ایالاتو ته د دننه کېدو هڅه کوي یا د کورني امنیت وزارت (Department of Homeland Security) له خوا نیول کېږي، نو برېښنايي وسایل یې تلاشي کېږي. د وګړو آنلاین فعالیت کېدای شي د هغوی د توقیف، شړلو، د وضعیت د تنظیم، تابعیت ورکونې، پناه غوښتنې یا نورو مهاجرتي اسانتیاوو په اړه پر پریکړې کولو د اغېز لپاره وکارول شي.

● ستاسې د سګم کېدو خطر زیات کړي. سګمران او

فریبکاران کولای شي ستاسې ډیجیټل فوټ پرنټ وکاروي، ترڅو تاسې هدف وګرځوي، ستاسې هویت نقل کړي یا ستاسې معلومات غلا کړي.

● تاسې د څارنې لپاره پرانیستي پریږدي، له هغې ډلې د

حکومتي ادارو او ظالمانه یا کنټرول کوونکو کسانو لپاره. په دې کې دا هم شامل دي چې خلک پوه شي تاسې چیرته یاست که چېرې ستاسې موقعیت فعال وي یا که تاسې په ټولنیزو رسنیو کې "checking in" کوئ.

● د قرباني کېدو احتمال مو زیاتوي. جرمي کسان د خلکو

ډیجیټل فوټ پرنټ د دې لپاره کاروي تر څو هغوی په نښه کړي او جبري یا تحميلي کارونو ته یې راجلب کړي. بنسټ پالان او نور خطرناک خلک هم کولای شي

د خپل ډیجیټل فوټ پرنټ مدیریت کول ستاسې د خونديتوب، امنیت او شهرت لپاره حیاتي کار دی!

ستاسې د ډیجیټل فوټ پرنټ د مدیریت کولو لپاره 12 مهم ټکي

- 1. خپل وسایل او اکاونټونه مو وساتئ.** ډاډ تر لاسه کړئ چې ستاسې ټول وسایل پیاوړي پسرودونه لري او که ممکن وي دوه فکتوره تصدیق ورکړئ. دوه فکتوره تصدیق داسې دی چې د تصدیق دوه میتودونه وي، لکه یو پسرود او هغه کور چې تاسې یې په خپل تلیفون کې تر لاسه کوئ.
- 2. خپل شخصي معلومات مو مه شریکوئ.** خپل بشپړ نوم، پته، تلیفون شمېره یا نور شخصي معلومات په انټرنېټ او خواله رسنیو کې مه شریکوئ. خپل موقعیت مو په خواله رسنیو کې مه ټگ کوئ. داسې عکسونه مه خپروئ چې ستاسې موقعیت، د استوګنځي ځای، کار ځای یا د بڼوونځي موقعیت څرګند کړي، لکه د کور شمیرې، د سړک نښې، د موټر نمبر پلټونه، د یونیفورم لوګو او نور.
- 3. خپل اکاونټونه مو خصوصي کړئ.** که چېرې تاسې د ټولنیزو ناستو اکاونټونه لرئ، نو ډاډ تر لاسه کړئ چې هغه خصوصي وي. په اصل کې تاسې کولای شئ دا کار خپل اکاونټ ته په تلو سره او بیا هلته Settings یا Privacy ته ورشئ او ډاډ تر لاسه کړئ چې 'private' مو ټاکلی وي.
- 4. زاړه اکاونټونه مو ډیلیټ کړئ.** که چېرې تاسې کوم زوړ اکاونټ نور نه کارو، نو ډیلیټ یې کړئ. دې ته ورته، په نورو زرو وسایلو کې چې لا تر اوسه له تاسې سره شته خو ډېر کم یې کاروئ، نو هلته هم د کلاوډ زیرمه او اکاونټونه غیرفعاله کړئ.
- 5. د خپل موقعیت ټرکر مو خاموشه کړئ.** د دې لپاره چې په یوه وسیله کې د موقعیت ټرکر غیرفعاله کړئ، نو د هغې وسیلې settings ته ولاړ شئ، چې معمولاً تر "Privacy" (محرمیت)، "Security" (امنیت) یا "Location" (موقعیت) لاندې موندل کېږي. له هغه ځایه، د موقعیت خدمات خاموشه کړئ تر څو نور اپلیکیشنونه یا خدماتو ته دا اجازه ور نه کړي چې ستاسې پر موقعیت باندې پوه شي.
- 6. خپل پوستونه مو محدود کړئ.** ډېر کم شمېر اطلاعات په انلاین توګه خپروئ. هغه څه چې خپروئ یې ډېر پام ورسره کوئ ځکه چې کېدای شي هغه څخه ناسم تعبیر واخیستل شي یا تاسې په نښه کېدو لپاره له لوړ خطر سره مخ کړي. د بېلګې په توګه، داسې عکس خپرول چې الکول څښئ، توپک مو په لاس کې وي او داسې نور.
- 7. د هغو خلکو د ملګرتیا غوښتنه مه منئ چې تاسې یې نه پېژنئ.** ډاډ تر لاسه کړئ چې تاسې یوازې د هغو خلکو د ملګرتیا غوښتنه منئ چې تاسې یې پېژنئ. د یوه پروفایل شا ته هر څوک پټیدای شي له هغې ډلې سکمران، قاچاق وړونکي او هغه خلک چې غواړي ستاسې څارنه وکړي. له خپلو اکاونټونو څخه هغه ملګري ډیلیټ کړئ کوم چې تاسې یې په شخصي توګه نه پېژنئ.
- 8. له خپلو تلیفونونو او نوور وسایلو څخه مو حساس مواد او اپلیکیشنونه ډیلیټ کړئ.** که چېرې له هېواده بهر سفر کوئ، نو د کورني امنیت

وزارت (Department of Homeland

Security) اجنټان بنیایي ستاسي برېښنایي وسایل

متحده ایالاتو ته د بېرته راتلو پر مهال په ننوتځي

کې تلاشي کړي. ټول هغه متنونه، عکسونه،

اپلیکیشنونه او نور مواد چې کېدای شي ناسم تعبیر

تري واخیستل شي، هغه ډیلیټ کړئ.

9. په خوندي توګه خبرې اترې وکړئ. د خبرو اترو

داسې اپلیکیشنونه وکاروئ کوم چې سراسري کود

شوی انکریپشن لري لکه WhatsApp، Signal

او Telegram.

یادښت: که څه هم دا ډېر خوندي دي، خو ان د پیغام

رسولو کود شوي پلاټفورمونه کولای شي ستاسې

ډیجیټل فوټ پرنټ سره د زیرمه شوې میټاډاټا له

لارې مرسته وکړي، لکه دا چې له چا سره او څه

مهال خبرې کوئ او همدارنګه ستاسې له خوا

شریک شوي محتوا لکه ویډیوګانې، انځورونه او د

پروفایل معلومات. له دې امله، څه چې شریکوئ په

اړه یې محتاط اوسئ.

10. په وېب کې د ګرځېدو راګرځېدو پر مهال محتاط

اوسئ. د هغو لېږونکو پر لینکونو باندې کلیک مه

کوئ کوم چې تاسې یې نه پېژنئ یا دا چې بې

اعتباره وېب پاڼو ته مه ورځئ، ځکه دا کارونه

کېدای شي ستاسې وسایل پر وېروسونو ککړ او

بالقوه څارنې سره مو مخ کړي.

یوازې اړین معلومات ورکوئ او د له هغو وېب

پاڼو او اپلیکیشنونو سره ډېر احتیاط کوئ کوم چې

تر اړتیا زیات شخصي معلومات در څخه غواړي.

په منظم ډول سره د خپل براؤزر کوکیز او کیش

(cookies and cache) پاکوئ. تاسې کولای

شئ دا کار د خپل براؤزر تنظیماتو (Browser's

Settings) او بیا د محرمیت تنظیماتو (Privacy

Settings) ته په تلو او بیا د براؤزینګ د

اطلاعاتو پاکولو (clear browsing date) یا

ورته غوراویو سره پاک کړئ.

11. یو لنډمهاله یا ژر مصرفه تلیفون وکاروئ. دا ډول

تلیفونونه زیاتره پرې پېد (مخکې اداینې) بڼه سره

وي او په یوه قرارداد پورې تړلي نه وي، چې د

ناڅرګند پاتې کېدو او د ترکینګ د مخنیوي لپاره په

اسانۍ سره کارېدلای شي. خو بیا هم، که چېرې

تاسې یو لنډمهاله تلیفون کاروئ، خو باید ډاډ تر

لاسه کړئ چې ځینې خلک چې غواړي تاسې سره

په اړیکه کې شي (کیز اورکر [caseworker]،

وکیل او داسې نور) نو هغوی باید ستاسې اپډیټ

شوي شمېره ولري. ځینې وختونه خلک دوه

تلیفونونه له ځان سره ساتي- لنډمهاله تلیفون د خپل

انلاین فعالیت لپاره او دایمي تلیفون له مهمو خلکو

سره د مهمو او ثابتو خبرواترو د ساتلو لپاره.

12. د کامري پوښ وکاروئ. په تلیفونونو او لپټاپونو

کې د کامرو پوښ وکاروئ تر څو کله چې استفاده

نه ترې کوئ نو لینزونه یې بلاک وي. دا کار

ستاسې خصوصي حریم ته له ورتلو څخه مخنیوی

کولای شي.