د احتجاج د ازادی لپاره
لا ربنود پاکستان

د احتجاج لپاره مفت ګائیډ یا لارښود (پاکستان)

دا ګائیډ د پاکستان د قوانینو او پالیسیو سره سم د برطانیې د فري پروټیسټ ګائیډ څخه او د ځایي فعالانو او د پرائیویسي انټرنیشنل په همکارۍ جوړ شوے دے.
دا د قانوني مشورې متبادل نه دے او یواځې د احتجاج په حقله د معلوماتو او د محفوظه احتجاج لپاره دے.

پی آیي ګائیډ لپاره لنک:
https://privacyinternational.org/sites/default/files/2021-06/FREE_TO_PROTEST-UK-EDITION.pdf

قانون څه وایي؟

د احتجاج حق په ټوله نړۍ کښې د بنیادي جمهوري ازادۍ په توګه تسلیمیږي.
پاکستان د یو جمهوري ملک په حېث د خپل ولس دغه حق مني.

د پاکستان د اسلامي جمهوریت د 1973 کال د اساسي قانون 16 آرټیکل (ترمیم شوې) هر وګړی ته دا حق ورکوي چې ،د مفاد عامه په ګټه د قانون لخوا وضع شوي هر ډول پابندیو سره سم، په پر امنه توګه او بې وسلې جمع کیدے شي.،،

د پاکستان د اساسي قانون د 16 او 17 آرټیکل ترلاندې د اجتماع (جمع کیدو) او انجمنونو یا اتحادیو په آزادۍ بندیز نشته او ریاست د مفاد عامه لپاره بندیزونه لګولے شي. د دې استثنا ترلاندې، د 1960 مېنټیننس آف پبلک آرډر آرډیننس غوندې قوانین، د عوامي اجتماګانو مخنیوې او د مظاهرچیانو (مظاهره کونکي) ګرفتارولو له استعمال شوي. د 1973 ضابطه فوجدارۍ (سي آر پي سي) دفعه 144 د پنځو نه زیاتو کسانو اجتماګانې ودرولو لپاره

استعمال شوي ده. دا دفعه ،،سرکاري نوکر پېښه خلکو په لار کې د څه قسمه خنډ، زيان، يا د انسان ژوند، صحت يا حفاظت ته د خطر او يا د ولس امن و امان کښې خنډ اچولو، بلوو او جګړې د مخنيوی لپاره ده.،،

پاکستان د انساني حقونو يو شمير نړيوالې معاهدې هم لاس ليک کړې دي او د دغو معاهدو د اصولو او قوانينو پابنده هم دے.

يوه مهمه خبره دا ده چې پاکستان د 1966 انټرنيشنل کوينټ آن سول اينډ پولټيکل رائټس (آئي سي سي پي آر) رياستي فريق دے او 2010 کښي يې تصديق هم کړے دے. د دې معاهدې 21 آرټيکل وائي چې ،،د پرامنې اجتماع کولو حق به تسليمول کيږي، د دې حق په تسليمولو به د قانون مطابق لګول شوې بنديزونو نه علاوه نور بنديزونه نشي لګول کيدے او کوم چې په يوه جمهوري ټولنه کې د قامي سلامتيه يا د ولس تحفظ، مفاد عامه، د ولس صحت يا اخلاقيات، يا د حقونو او آزادئ تحفظ لپاره ضروري وي.،،

دا ګائيډ د انجمنونو يا اتحاديو او د اجتماع د آزادئ د حق د استعمال او په خاصه توګه د چا رازدارئ او د ډېټا معلوماتو ته ورپيښ خطر کمولو له تيار کړے شوے دے. مونږ. امېد لرو چې دا لانديني مواد (چېپټرز) به هاغه خلکو ته د خطر او د دې د مخنيوې په لړ کې مدد ورکړې چې څوک خپل آئيني آزادي استعمالول غواړي.

مونږ. دا دستاويز جوړولو کې خپل وخت او محنت صرف کړے دے چې پکې د حالاتو سرم بدلون کيدے شي او هم دې مقصد لپاره په دې ګائيډ کې د بنه والي، بدلون او د نورو موادو د شاملولو په اړه رائے (فيډ بيک) شريکولے شې. تاسو مونږ. سره خپله رائے په دې ايميل ايډريس شريکولے شي او سبجيکټ کې به "پاکستان پروټيسټ ګائيډ" ليکئ.
info@privacyinternational.org

په احتجاج کې د ګډون نه وړاندې او د احتجاج په وخت ځینې داسې خبرې دي چې فعالان یې خیال ساتي...

۱. د بدن تر یا مرطوب ساتلو لپاره ځان سره اوبه یوسئ. د اوښکو ګاز یا آنسو ګېس په صورت کې خپلې سترګې په اوبو ووینځئ.
۲. بډې سسټم یا ملګرو مرستې نه کار واخلئ. که پولیس احتجاج کونکي د منتشر کولو هڅه کوي نو دا کوشش وکړې چې ستاسو یو تن هم شاته پاتې نشي.
۳. احتجاج کې د ګډون نه مخکې خپل فون مکمل چارج کړئ او احتجاج کې د ګډون سره سم خپل لوکیشن خپلې کورنۍ یا نزدې ملګرو سره شریک کړئ.
۴. په خپل فون پاسورډ یا پاس کوډ ولګوئ او مخ یا فنګر پرنټ پرې مه پریږدئ.
۵. احتجاج ته ځان سره داسې ډیوائس مه راوړې چې هغه حساس معلومات لري.
۶. د دوړې او آلودګۍ نه ځان ساتلو لپاره ماسک واچوئ او څوک چې تصویر (عکس) یا ویډیو جوړوي نو خپل شناخت پټ وساتئ.
۷. که د پولیس لخوا تاسو ته څه قسمه نقصان درځي نو د هغوي ویډیو یا تصویر جوړ کړئ.
۸. په احتجاج کې د ګډون کونکو ملګرو تصویرونه/عکسونه په سوشل میډیا/ټولنیزیو رسنیو مه شیئر کوئ چې د هغوي موجودګي نه ظاهریږي. تاسو د هغوي داسې تصویرونه شریکولے شي چې هغې کې د هغوي شناخت نه ظاهریږي.
۹. ځان او ملګرو لپاره د مشکل حالاتو نه وتو لپاره یو کړن لاره یا ایګزټ سټریټیجي وساتې.

انټرنېټ او د نېټ ورکو د بندېز مخنیوې

د انټرنېټ د بندېز په صورت کې څه کیدے شي؟

له بده مرغه انټرنېټ او د موبائلو د نېټ ورکو بندول په احتجاجونو کې د خنډ اچولو معمول جوړ شوے دے. نه یوازې د انټرنېټ بندول انساني آزادي متاثروي بلکې د ګډوډۍ او مشکله صورتحال کې د مظاهرچیانو (احتجاج کونکو) لپاره د رابطو ذریعې بندولو سره سنګینې نتیجې رامنځته کولے شي. په پاکستان کې په مبینه توګه د انټرنېټ بندیز په لویه پیمانه عوامي اجتماع او احتجاج کنټرولو لپاره استعمالیږي. حکومت اکثره د انټرنېټ بندولو لپاره د پاکستان ټیلي کمیونیکېشنز (ري آرګنائزیشن) ایکټ د 1996 سیکشن 54 (3) لګوي. په دغه ذیلي دفعه کې ویلې شوې دي چې د ولس مشر (صدر) لخوا د ایمرجنسي اعلان پس د پي ټي اے د ایکټ ترلاندې لائسنسي ځنډولې او پکې بدلون کولے شي یا د اپریشن ځنډولو، فعالولو او د خدماتو سبب ګرځېدے شي.

دلته ځینې داسې ایپلي کېشنز شریکوو چې د نېټ ورکو د بندېز اغېز کمولې شي.

فائر چیټ یو ایپلي کېشن دے چې د پیغاماتو د تبادلې لپاره بلوټوټ استعمالوي. دا آئي او ایس او اینډرائیډ دواړو کې کار کوي. او دا 100 او 60 میټرو کې په موثره توګه ښه کار کوي.
برائیر یو میسجنګ ایپ دے چې فعالانو، خبریالانو او هاغه چا لپاره جوړ شوے چې هغوي د خبرو اترو لپاره محفوظه او اسانې رابطې ته ضرورت لري.
بریجیفائي هم یو میسنجنګ ایپ دے چې خلک په دې عارضي نېټ ورکو لکه پیئر ټو پیئر وائي فائي او بلوټوټ د لارې خپل پیغام لیږلې شي چې بل څوک یې ویلې هم نشي. دا هم آئي او ایس او اینډرائیډ دواړو لپاره دے.

یادونه: دا ایپلي کیشنز سخت صورتحال یا سخت وخت کې کارول کیدے شي او د انټرنېټ د بندېز مکمل حل نه دے.

1 Imran Asghar, “No mobile, internet service today,” The Express Tribune, March 23, 2022, https://tribune.com.pk/story/2349211/no-mobile-internet-service-today.
Muneeb Ahmad, “Mobile services to remain suspended in 52 cities on Muharram,” TechJuice, October 10, 2021, https://www.techjuice.pk/mobile-services-to-remain-suspended-in-52-cities-on-muharram/.

1 Berhan Taye, “Pakistan shuts down the internet three times in one week,” Access Now, November 6,
2018, https://www.accessnow.org/pakistan-shutdowns-internet/.

تر اوسه پورې مونږ پاکستان کې د نګرانۍ د صلاحیت په اړه څه معلومات لرو؟

۱. پنجاب سېف سټي اتهارټي سره دا اختیار شته چې احتساب او جرمونو کې کموالي لپاره د ولسي ځایونو څارنه وکړي. راټوله کړې شوې ډېټا 'ډېټا او پروټېکشن پروسیجر' (ډي پي ټهري) ترلاندي کنټرولیږي خو د دې د طریقه کار د نافذ کولو په اړه د شفافیت کموالې دے او د خلکو د ډېټا ریکارډنګ او پروسیس د ولسي آزادئ لپاره د اندیښنې وړ دے.
۲. کال 2019 کې دا خبر مخې ته راغلې وو چې د پاکستان حکومت د ډیپ پیکټ انسپکشن د استعمال د لارې په ملک کې د انټرنېټ د ټریفک څارنې لپاره د کینیډا یوې کمپنۍ سینډ وائن خدمات حاصلول غواړي. دا د پي ټي اے له اړخه د مانیټرنګ اینډ ري کنسلیئشن آف ټیلي فوني ټریفک ریګولیشن 2010 ترلاندې کیدو. دا معلومه نه ده چې آیا د پاکستان حکومت د کینیډا کمپنۍ سره معاهده وکړه.
۳. دي سټیزن لېب په ذریعه شوې د کمپیوټرو د یو فرانزک څېړنې مطابق د کمپیوټرو نظام ته زیان رسونکې مالویئر 'فن فشر' په پاکستان کې فعال دے.

په پاکستان کې د مواصلاتو نګراني یا څارنه د یو شمېر قوانینو د لارې کنټرولیږي

۱. انویسټي ګېشن فار فیئر ټرائل ایکټ (2013) ترلاندې د هائیکورټ د جج نه به وارنټ اخیستي کیږي او د شلم ګرېډ یو سرکاري افسر په ذریعه به د رابطو او ډیوائسز څارنه او ورته د مداخلې اجازه ورکوي.
۲. د الیکټرانک جرمونو مخینوي قانون یا دې پرویوینشن آف الیکټرانک کرائمز ایکټ 2016 کې هغه برخې شاملې دي چې پکې معلومات یا ډېټا ډیر

وخت له ساتل، بدنامي کول یو جرم ګرځول او د پي ټي اے لخوا د آن لائن موادو کنټرول شامل دي.
۳. د مانیټرنګ اینډ ري کنسلیئیشن آف ټیلي فوني ټریفک ریګولیشن 2010 کې د ایس فور په ذریعه د هرې اوږدې فاصلې نړیوال سروس ورکونکې به یو داسې نظام جوړوي چې په خپلو نیټ ورکو د نګرانی او ریکارډنګ اجازت ورکړي.
۴. د پاکستان ټیلي کمیونیکېشن (ري آرګنائزیشن) ایکټ 1996 د قامي سلامتیه په مفاد کې ټیلیفونو او میسجو کې د مداخلت اجازت ورکوي.

1 https://psca.gop.pk/about-us/benefits-and-objectives/
1 https://psca.gop.pk/wp-content/uploads/2021/03/PrivacyPolicyDP3.pdf.
1 https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/
1 https://citizenlab.ca/2015/03/finfisher-lawsuit-to-be-heard-in-pakistans-lahore-high-court/

ستاسو د آلاتو نګرانۍ په اړه یو ګائیډ

په یو احتجاج کې د موبائل فون ایکسټرېکشن څنګه کارول کیدے شي او خپلو معلوماتو (ډېټا) ته خطر څومره کمولې شو؟

د موبائل فون ایکسټریشن ټولز څه کار کوي؟

موبائل فون ایکسټرېکشن داسې ډایوئسز یا آلات وي چې د هغې په ذریعه پولیس د موبائل نه ډېټا اخیستې شي...
۱. ټیلیفون نمبرې یا کانټیکټس
۲. د ټیلي فون کولو معلومات (چاته مو کال کړې دې کله او څومره وخت پورې مو خبرې وکړې)
۳. مېسوجونه، (چاته مو او څه وخت مو کړې)
۴. محفوظه فائلونه: تصویران، ویډیوګانې، آډیو فائل، نور داسې اسناد یا دستاویز
۵. ایپلي کېشن ډیټا (په ایپلي کېشنز کې موجوده ډېټا)
۶. د لوکېشن یا د ځاې معلومات

۷. وائي فائي نېټ ورکو کنېکشن په ذريعه معلومېږي (چې چرته ستاسو موبائل کنيکټ وو. لکه د کار د ځاې يا کيفې په اړه معلومات ورکوي.)
۸. ځينې ايم پي ايز ټولز په کلاؤډ کې محفوظې ډېټا ته هم رسائي حاصلولې شي. که تاسو د خپل ټيلي فون ډيټا پحقله محتاطه يې نو هغې ته بيا هم رسائي کيدې شي خوا که آن لائن محفوظه شوې وي. يا داسي ډېټا چې تاسو ته معلومه نه وي يا که ډيليټ شوي هم وي.

په احتجاجونو کې د موبائل فون ايکسټرېکشن ټولز څنګه استعماليدے شي؟

د برطانيې زياتره پوليس ايم پي اي ټولز اخيستي دي او د احتجاج پشمول نورو حالاتو کې استعمالوي.
د يو موبائل نه ډېټا ويستو يا حاصلولو لپاره پوليس ته به د موبائل فون ضرورت وي. که تاسو نيول شوې يې يا حراست کې يې او يا پوليس ستاسو تلاشي اخلي نو پوليس ستاسو ډېټا حاصلولې شي.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

د خپل موبائل فون سافټ ويئر اپډيټ ساتې که اينډرائيډ وي او که آئي او ايس. اپډيټ کولو سره به نوې سکيورټي فيچرز راځي کوم چې د ايم پي اي نه ډېټا ساتلو لپاره يوه ډېره ښه طريقه ده.
د ټولو ښه خبره دا ده چې د ايم پي اي نه ځان ساتلو لپاره پکار ده چې احتجاج ته خپل ټيلي فون مه وړئ. خو که موبائل فون درسره نه وي نو هم درته مسئلې مخې ته راتلې شي نو داسي هم کيدے شي چې ځان سره هغه موبائل فون کيدئي چې هغې کې ډېر لږ معلومات يا ډېټا وي.
خپل ټيلي فون لاک ساتئ. د رپورټونو ترمخه چې ځينې ايم پي اي ټولز لاک موبائلې هم خلاصولې شي خو دا په فون او د هغې په آپريټنګ سسټم هم ده.
احتجاج ته د تلو نه وړاندې خپل موبائل ډېټا يو کمپيوټر ته واړوې او بيا له خپل موبائل څخه ډېټا ډيليټ کړئ. خو ستاسو پام کې دي وي چې ځينې ايم پي

اي ټولز ډیلیټ شوې ډېټا بیا حاصلولې شي، او که تاسو په کلاوډ کې ډیټا سیو کړې ده نو بیا هم ځینې ایم پي اي ټولز ډېټا حاصلولې شي.

کلاوډ ایکسټرېکشن ټولز په احتجاج کې څنګه استعمالیږي او تاسو خپلې ډېټا ته خطر څنګه کمولې شئ؟

کلاوډ ایکسټرېکشن ټولز څه دي او دا څه کار کوي؟

کلاوډ ایکسټرېکشن ټولز په ذریعه پولیس کولے شي چې ستاسو د موبائل یا نورو ډیوائس د لارې په کلاوډ کې موجوده ډېټا ترلاسه کړي.
د کلاوډ ایکسټرېکشن ټولز استعمالولو مطلب دا دے چې پولیس هغه ډېټا ته رسیدے شي کومه چې تاسو آن لائن سټور کړې وي. هغه ایپلي کېشن دا دے چې په کلاوډ کې ډېټا جمع کوي... سلېک، انسټاګرام، ټیلیګرام، ټوئټر، فیس بک او اوبر.

کلاوډ ایکسټرېکشن ټولز په احتجاج کې څنګه کار کوي؟

۱. د ډېټا ترلاسه کولو لپاره پولیس له به ستاسو موبائل پکار وي. که د احتجاج په وخت تاسو ونیول شې یا مو په حراست کې واخلې نو پولیس ستاسو موبائل په قبضه کې اخیستې شي. دا هم کیدے شي که تاسو یو جرم په خپلو سترګو لیدلې وي یا خپله د یو جرم ښکار شوې یې. (د موبائل فون ایکسټرېکشن پحقله پروټیسټ ګائیډ وګورئي).
۲. دا ټول معلومات د مظاهرچیانو (مظاهره کونکي) او د منتظمینو شناخت او د مظاهره کونکو د ځایې یا مقام او کارروایانو لپاره استعمالیږي.
۳. ستاسو کلاوډ ډېټا یواځې ستاسو په اړه معلومات نه ورکوي بلکې ستاسو ملګرو، کورنۍ یا تاسو چا سره آن لائن رابطه کړې وي لکه (مظاهره کونکي سره) نو د هغوي پحقله هم معلومات ورکوي. لکه مثال په توګه تاسو سره پخوانۍ نمبرې یا کانټېکټس په کلاوډ کې محفوظه وي او د موبائل نه مو ډیلیټ کړې وي.

احتجاج ته د تلو نه مخکې څه سوچ او فکر پکار دے؟

۱. کله چې تاسو کور کې د موبائل د پرېښولو سوچ کوې نو دا يو عملي حل نه دے. تاسو له پکار دي چې موبائل کې د موجوده ايپلي کېشنز کلاؤډ بېک اپ بند کړئ او چې کوم کلاؤډز درسره موجود دي د هغې نه لاګ آؤټ شئ. دې سره به ستاسو ډېټا په کلاؤډ کې نه محفوظيږي او ستاسو موبائل نه به معلوماتو ته رسائي هم نه وي.
۲. يو احتجاج ته د تګ نه وړاندې بايد چې تاسو خبر يې، که تاسو په واټس ايپ اينډ ټو اينډ انکرپټډ پيغامونه استعمال کړې نو دغه ميسجونو پورې هم پوليس ستاسو په موبائل د ايکسټرېکشن ټولز په ذريعه رسائي لرلې شي.
۳. ځينې ايپلي کېشنز لکه اوبر، ټوئټر، واټس ايپ او فيس بک تاسو ته دا اجازه درکوي چې په کلاؤډ کې محفوظ يا سټور ستاسو لوکېشن بند کړي. دې سره دا کيدے شي چې پوليس ستاسو د ځاې معلومات ترلاسه نه کړې شي چې تاسو چرته موجود ويې.

آئي ايم ايس آئي کېچرز په احتجاج کې څنګه استعماليږي او څنګه خپلې ډېټا ته خطر کمولې شئ؟

کال 2015 کې پنجاب انفارمېشن ټيکنالوجي بورډ د ترهګرۍ د مخنيوي محکمو (سي ټي ډي ټيز) لپاره آئي ايم ايس آئي کېچرز د اخيستو لپاره يو ټېنډر نوټس ورکړے وو.

دا آئي ايم ايس آئي کېچرز څه شی دے؟

۱. آئي ايم ايس آئي 'انټرنيشنل موبائل سبسکرائب آئيډينټټي' ته وايي. دا ستاسو سم کارډ لپاره يو ځانګړې شميره ده. آئي ايم ايس آئي کېچرز په سټينګرې هم پيژندلې کيږي.

۲. آئي ایم ایس آئي کېچر یو ډیوائس وي چې خپل شاه خوا موبائلونو سره کنېکټ شي او د آئي ایم ایس آئي ځانګړې شمیرې په ذریعه یو ټیلي فون ټریک کوالې شي یا یې معلومولے شي.
۳. آئي ایم ایس آئي کېچر د ډېرو مضبوطو سګنلو سره د یو موبائل ستنې په شان کار کوي او ورسره شاه خوا موبائلې کنېکټ کوي. دې سره د استعمالونکې د علم بغیر د هغه معلومات ترلاسه کیدے شي.
۴. په دې حالاتو کې ستاسو په اړه د ټولو د رسائي وړ معلومات ستاسو ځاې دے.
د دریو ټاورو په ذریعه د ټیلي فون ستنې (ټاورې) ستاسو لوکېشن معلوموي. داسي دې تاسو ته خپل خدمات وړاندې کوي. ستاسو او د ټیلي فون ستنې ترمینځ یو آئي ایم ایس آئي کېچرز ستاسو ځاې معلومولے شي.
۵. آئي ایم ایس آئي کېچرز په یو فون کې ډېټا نشي ویلې. دا آلات د فون میسجونو او کالونو ترمنځ مداخله کولے شي.
۶. آئي ایم ایس آئي کېچرز په صلاحیتونو او ستاسو موبائل چې کوم نېټ ورک سره کنېکټ وي د هغې استعداد پورې اړه لري چې آیا زیاتې حملې پرې کیدے شي او دې امکان هم لږ وي. ځینې ستینګرې ډیوائسز د کمیونیکېشن پروټوکولز په کمزوریو تکیه کوي او ستاسو فون دې ته ضرورتمند کړي چې خپل استعمال شوې پروټوکول کم (ډاؤنډ ګرېډ) کړي. دې سره ستاسو رابطې ډېرې محفوظې (خوندي) نه وي او په اسانې ورته رسائي کیدې شي. (لکه د مثال په توګه تهري جي او ټو جي کمیونیکېشن کچه ښکته کړي).
۷. آئي ایم ایس آئي کېچرز انکرپټډ میسجونو مواد نشي لوستلې. دا لکه په سګنل، واټس ایپ او وائر میسجونه نشي ویلې.

1 https://eproc.punjab.gov.pk/BiddingDocuments/35144_Tender%20Doc%20-%20Security%20Items%20for%20CTD%20Police%20Stations%20-%20105052015-1.pdf

آئي ایم ایس آئي کېچرز په احتجاج کې څنګه استعمالیدے شي؟

۱. پولیس د آئي ایم ایس آئي کېچرز په ذریعه دا شناخت کولے شي چې څوک په احتجاج کې وو، او دا په یو علاقه کې موجود د ټولو ټیلي فونو آئي ایم ایس آئي نمبرې یا شمېرې معلوموِلو سره کیدے شي.
۲. د آئي ایم ایس آئي کېچرز ځینې قسمونو سره پولیس کولے شي چې د احتجاجونو مخینوې وکړي.
۳. لکه د مثال په توګه دا ستاسو د ټیلي فونو څارنه کولے شي او ستاسو کالونه او میسجونه بلاک کولے هم شي، ستاسو میسجونه ایډیټ کولے شي او داسي هم کولے شي چې ستا لخوا بل چا ته میسجونه ولیږي.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

۱. خپل موبائل فون په ایرپلین موډ اچول او یا بندولو سره آئي ایم ایس آئي کېچرز تاسو نشې معلوموِلے او دا ستاسو رابطي هم نه شي معلوموِلے.
۲. که تاسو غواړئ چې ستاسو ټیکسټ میسجونه په آئي ایم ایس آئي کېچرز معلوم نشي نو تاسو د سګنل او واټس ایپ اینډ ټو اینډ انکرپټډ میسجونه استعمالولې شي. آئي ایم ایس آئي کېچرز یواځي دا معلوموِلے شي چې تاسو دغه ایپلي کېشنز استعمالوې او د میسج مواد نشي ویلې.
۳. آئي ایم ایس آئي کېچرز په ټیلي فون کې موجود مواد نشي لوستلې خو دا خبره یاد ساتئ چې پولیس ډېټا پورې رسائي لپاره نورې ټیکنالوجي لري لکه (موبائل فون ایکسټرېکشن او هیکنګ ټول).

په احتجاج کې د سوشل میډیا مانیټرنګ (ټولنیزیو رسنیو څارنه) څنګه استعمالیدلے شي او خپلې ډېټا ته خطر څنګه کمولې شو؟

د سوشل میډیا مانیټرنګ څارنه څه ده؟

سوشل میډیا پلیټ فارمز لکه فیس بک، ټوئټر، انسټاګرام او په ریډیټ شیئر کړې شوې معلوموِلو څارنه، جمع کول او تجزیه کول دي.
په دې کې د پبلک او پرائیویټ ګروپونو په پاڼړو کې د پوسټ کړي شوې موادو جاسوسي شامله ده. په دې کې د سوشل میډیا پلیټ فارمز نه ډېټا خرابول

(سکرېپنګ) هم شامل دي. ستاسو پوسټ کړې شوې رویو په اړه معلومات هم چې تاسو څه خوښ دي او څه شیئر کوې.
سکریپنګ او د نورو ټولز په ذریعه د سوشل میډیا څارنه په لویه پېمانه د ډېټا د جمع کولو او د تجزیي اجازت ورکوي کوم چې د صارفینو پروفائلز او د هغې په اړه له وړاندې نه د معلوماتو ورکولو لپاره کارول کیدے شي.

سوشل میډیا مانټیرنګ یا د ټولنیزو رسنیو څارنه د احتجاج په لړ کې څنګه استعمالیدے شي؟

۱. د احتجاج منتظمین به اکثر له د سوشل میډیا په ذریعه احتجاج منظم کوي. هم د دې په ذریعه به احتجاج کونکو سره رابطې کوي او د احتجاج عکسونه/تصویران او ویډیوګانې به هم شیئر کوي.
۲. د دې مطلب دا شو چې پولیس کولے شي چې د سوشل میډیا د پاڼړو او ګروپونه چاڼ وکړي یا یې (ډېټا مائن) وکړي او د منتظمینو د شناخت او تړاؤ، د هغوي لوکېشن، د هغوي د هلو ځلو د وخت او نور معلومات ورته وشي.
۳. پولیس کولے شي چې د احتجاج کونکو شناخت معلومولو لپاره د پخواني او راتلونکي احتجاجونو په اړه ستاسو سوشل میډیا وګوري.
۴. ممکنه ده په سوشل میډیا ورکړې شوې د احتجاج تصویرونو او ویډیوګانو نه د احتجاج کونکو شناخت لپاره پولیس فېشل ریکګنیشن ټیکنالوجي یا د مخ پیژندنې ټیکنالوجي یا د ګېټ ریکګنیشن ټیکنالوجي استعمال وکړي.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

۱. که تاسو د سوشل میډیا په اکاؤنټونو خپل عکسونه (تصویرونه) او ویډیوګانې لګوئ نو دې سره د خلکو شناخت او د ځای معلومات کیدے شي.
۲. که ستاسو لوکېشن سیټنګز د سوشل میډیا په پلېټ فارمز یا ستاسو په کیمره یا د تصویرونو په ایپلي کېشن آن یا لګیدلې وي او بیا تاسو د احتجاج مقام یا هغې سره نزدې ځای نه تصویر په سوشل میډیا ورکړئ نو پولیس دغه ځای ته رسائي لرلې شي.

۳. د احتجاج په وخت تاسو کولے شئ چې په سوشل میډیا پلیټ فارمز خپل لوکېشن بند کړې. او که تاسو دا فېصله وکړه چې د احتجاج تصویرونه شیئر کول غواړې نو په هغې کې د اجازت نه بغېر هاغه خلک مه ټېګ کویې کوم چې درسره احتجاج کې شریک دي. دې سره پولیس کولے شي چې په احتجاج کې شریک خلک معلوم کړي.
۴. که تاسو غواړئ چې د خپل احتجاج تصویر په سوشل میډیا ورکړئ نو له دې وړاندې ایګزیف ډېټا لرې کولو ته پام وکړئ. دا یو مېټا ډېټا ده چې تصویرونو سره ټرل شوي وي او دا د ځاې، وخت، تاریخ او تاسو کوم موبائل یا ډیوائس استعمال کړې دې، په اړه معلومات ورکولے شي.
۵. محتاط وسئ، تصویرونو او ویډیوګانو نه هم معلومات کیدے شي لکه تاسو کوم ځاې کې یې هلته څه مشهور یا اهم ودانې (عمارت) خو پکې نه ښکاري. دا په ذهن کي وساتئ چې د تصویر اخیستو یا ویډیو په جوړولو کې داسي څه مه ښایې چې د هغې نه معلوم شي چې تاسو کوم ځاې یې.
۶. که ممکنه وي نو تصویرونه او ویډیوګانې هله سوشل میډیا ته اپلوډ کړې چې هغه مقام یا ځاې نه لاړ شې دا ځکه چې تاسو څوک تعقیب نه کړي یا مو فولو نه کړي او چې کله ریکارډ کړې شوې ویژوئل ډېټا اپلوډ کوئ نو د هغې لپاره وي پي این استعمال کړې.

هیکنګ په احتجاجونو کې څنګه استعمالیدے شي او تاسو څنګه ډېټا ته دا خطر کمولې شې؟

هیکنګ څه شے دے؟

۱. هیکنګ په سسټمونو کې کمزورې ته اشاره کوي یا رپورټ کوي یا یې مرمت کوي او یا ترې ګټه ترلاسه کوي.
۲. هیکنګ ډیوائسز، نېټ ورکو او خدماتو (سروسز) کې د سکیورټي مسئلې په ګوته کوي کوم چې په لکونو خلک استعمالوي او چې کله سسټم ډیزائنرا نو ته رپورټ شي نو سم کړې شي. خو هیکنګ زمونږ ډیوائسز پورې رسائي

لرلې شي او په پټه زمونږ په اړه معلومات ټولولې شي او په ممکنه توګه مونږ او زمونږ ډیوائسز کنټرولوے شي.
۳. وخت سره هیکنګ کې بدلون راځي. دا د لرې فاصلې نه هم کیدے شي خو دا څوک ستاسو ډیوائسز او سسټم ته هم لګولې شي لکه مثال په توګه ستاسو موبائل فون په زوره انلاک کولے هم شي.
۴. داسي هم کیدے شي چې د خلکو په استعمال د هغوي ټېکنالوجي ته رسائي ولري. یو مثال به لکه 'فشنګ' وي چې یو حمله کونکې د یو باوري تن په حېث یا د یو تنظیم په حېث یو داسي لنک او اټیچمنټ ولیږي چې هغه د مالویئر نه متاثره وي.

هیکنګ په احتجاج کې څنګه استعمالیدے شي؟

۱. پولیس د آئي ایم ایس آئي کېچرز په ذریعه رابطې او معلومات هیک کولے شي خو آئي ایم ایس آئي کېچرز یواځې هاغه معلوماتو کې خنډ اچولې شي چې کوم موبائل او د موبائل فون ستنې ترمنځ وي. آئي ایم ایس آئي کېچرز هاغه معلوماتو پورې رسائي نشي لرلې چې ستاسو په ډیوائسز کي موجود وي.
۲. فون، لیپ ټاپ او انټرنېټ سره تړلې نور ډیوائسز چې د احتجاج انتظام یا ګډون په وخت استعمال شوې وي نو پولیس د جدید هیکنګ په ذریعه د هغې نه معلومات ترلاسه کولے شي. دا بیا هم هیک کیدے شي که په دې پاسورډ، فنګر پرنټ یا فیس انلاک لګیدلے وي.
۳. پولیس هاغه ډیوائسز نه هم معلومات اخیستې شي چې د احتجاج کونکو نه ورک شوې یا ضبط کړې شوې وي.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

۱. د هیکنګ نه بچ کیدو لپاره ضروري ده چې خپل فون اپډېټ وساتئ ځکه چې هیکنګ اکثر له هاغه کمزورې ګوري چې ښکاري خو مرمت یې نه وي شوې.

۲. دا خبره یقیني کړئ چې ستاسو فون سستم که اینډرائیډ وي او که آئي او ایس چې نوې ورژن لري او ټول ایپلي کېشنز هم اپډېټ وي چې هغه ستاسو د موبائل فون سکیورټي ښه کوي او د هیکنګ خطره هم کموي.
۳. موبائل فون سره سره نور په بجلی کارکونکي ډیوائسز لاک ساتئ خو ځیني هیکنګ تکنیکونه لاک شوې ډیوائس پوري هم رسائي لري. د سکیورټي لګولو باوجود هغې ته رسائي کول دا په هیکنګ تکنیک او په ډیوائس هم ده چې هدف کوې یې.
۴. احتجاج ته د تلو نه وړاندې د خپل فون ډېټا بل ډیوائس ته واړوئ او هاغه ډیوائس نه ډېټا وباسې کوم چې ځان سره احتجاج ته وړیې خو تاسو ته معلومه دې وي چې ځیني هیکنګ ټولز ستاسو ډیلیټ کړې شوې ډېټا راویستې شي.
۵. داسې په کلاوډ کې محفوظه کړې شوې ډېټا ته هم هیکنګ ټولز رسائي لرلې شي.
۶. د فشنګ بریدونو مخنیوي لپاره تاسو باید د هاغه لنکونو په اړه هم محتاط وسئ چې تاسو یې کلک کوې.

دا په احتجاج کې څنګه استعمالیدے شي؟

۱. ایف آر ټي د احتجاج پشمول عوامي مقاماتو کې د خلکو د مخ شناخت، نګراني یا ټرېک کولو له استعمالیدے شي. د خلکو د اجازت او پوهې بغېر دا په ښکاره هم کیدے شي او په خفیه توګه هم.
۲. ایف آر ټي فعالې کیمرې تصویران اخیستې شي او ویډیو جوړولې شي او د خلکو شناخت هم کولے شي. ایف آر ټي د موجوده تصویرونو او ویډیوګانو تجزیه کولے شي لکه (په سوشل میډیا شیئر کړې شوې د احتجاج تصویرانو او ویډیوګانو.)
۳. څنګه چې د مظاهرینو د مخ ډېټا ټوله کړې شي نو دا ډېټا له وړاندې نه موجود یو یا یو نه زیات د نګرانی فهرست یا واچ لسټ کې واچول شي. چرته چې دا مېچ کولو لپاره د نورو ذرایعو سره کتلې کیږي.

۴. داسي هم کیدے شي چې راتلونکې کې میچ کولو او شناخت لپاره د دغه ډېټا نه د هاغه خلکو یو نوې ډېټا بیس جوړ کړے شي کوم چې احتجاج کې شریک وو.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

۱. که تاسو غواړئ چې ظاهر نه شو نو تاسو کوالې شې چې ماسک واچوې. داسي به ایف آر ټي له مشکل وي چې ستاسو د مخ د نقشونو سم تصویرونه واخلي.
۲. د ایف آر ټي له مشکل پېدا کولو لپاره تاسو په خپل مخ پېنټ یا رنګ وکړې او یا داسې ډیزائن کپړا په مخ واچوې چې د مخ شناخت کې مشکل پیدا کوالې شي. ایف آر ټي کې مسلسل بدلون او بنه والې راځي خو راتلونکي یا مستقبل کې مخ پټول او دغه نورې طریقې غېرموثره ثابته کیدے شي.
۳. د مخ پټولو کپړا د لرې کولو د مطالبې په اړه په هره علاقه کې د پولیسو بېل اختیار دی چې کله دا رپورټ لیکل کیدو نو مونږ د کورونا وائرس وبا په منځ کې وو نو موجوده قواعدوضوابط کې بدلون کیدے شي.
۴. پولیس په سوشل میډیا د تصویرونو او د ویډیوګانو د ریکارډنګز تجزیه په ایف آر ټي کولے شي نو د یو احتجاج نه د یو تصویر پوسټ کولو نه مخکې دې ته پام وکړې چې هغې کې د احتجاج کونکو مخونه ښکاره خو نه دي.
۵. نو داسې آن لائن تصویرونه او ویډیوګانې پوسټ کولو نه مخکې د مخ نه څرګندیدو ټولز (بلرنګ ټولز) وکاروېي.

په احتجاج کې د پولیس ډرون ټېکنالوجي څنګه استعمالیدے شي؟ او تاسو څنګه ځان پټ ساتلې شې؟

اسلام آباد پولیس ستمبر 2022 کې د 'زیان نه رسونکي' ډرونز اخیستو اعلان کړے وو چې امن و امان په ځاې ساتلو لپاره عوامي اجتماع محدوده او منظمه وي.

پولیس ډرونز څه وي؟

۱. د مختلفو سائزونو بې پیلوټه ډرونز د لرې نه کنټرول کیږي.
۲. په دې کې کیمرې لګیدلي دي او د فیشل ریکګنیشن ټیکنالوجي سره فعال کیدے شي.
۳. دې کې سپیکر، نګراني آلات، راډار او په رابطو کي د مداخلت ټولز لکه آئي ایم ایس آئي کېچرز لګیدلي وي.

په احتجاج کې د پولیس ډرون ټېکنالوجي څنګه استعمالیدے شي؟

۱. د کیمرې ډرون په عوامي مقاماتو کې یا احتجاج په ځاې کې د خلکو د مرضې یا د هغوي د معلوماتو بغیر څارنه کولے شي.
۲. داسې ډرونز چې هغه د مداخلت ټیکنالوجې نه لېس وي، د مظاهرې ځاې او شاه خوا علاقه کې مظاهره کونکې ټریک کولے شي او د هغوي ټیلي فونونه او د میسجونو نګراني هم کولے شي.
۳. کوم ډرون کې چې سپیکرې وي نو د مظاهره کونکو سره د خبرو له استعمالیدے شي لکه احکامات، هدایات او خبردارې ورکول.

احتجاج کې د ګډون نه مخکې څه فکر پکار دے؟

۱. د ډرون استعمال او ستاسو شناخت نه ظاهریدل د ډرونز په ټیکنالوجي انحصار کوي.
۲. د فیشل ریکګنیشن ټیکنالوجي او آئي ایم ایس آئي کېچرز په اړه برخې وګورې ولې چې دا داسې ټولز دي چې ډرونز د مظاهره کونکو شناخت لپاره استعمالولې شي.

د پولیسو ډېټا بېس او تجزیاتي ټیکنیکل یا پریډیکټیو پولیسنګ ټولز

پریډیکټیو پولیسنګ څه دی؟

پریډیکټیو پولیسنګ پروګرامز د پولیسو لخوا د دې خبرې اندازه لګولو لپاره استعمالیږي چې چرته او کله یو جرم کیدے شي او څوک دا جرم کولے شي. دا پروګرامونه د کمپیوټر ایلوګرتم په ذریعه د پولیسو ډېټا په ورکولو کار کوي. لکه مثال په توګه یو پروګرام د پخواني جرمونو د شمیرې په اړه د ډېټا اندازه لګولې شي چې راتلونکې کې به جرمونه چرته کیږي او په نقشه کې یې نشاندهي وکړي. خو دا پروګرامونه چې کومه ډېټا استعمالوي دا نامکمله یا په تعصب مبني وي چې د 'فیډ بیک' لوپ لامل ګرځیدے شي او افسران هاغه ځایونو ته لیږي چې چرته له وړاندې نه د پولیسو موجودګي زیاته وي.
نور پریډیکټیو پولیسنګ پروګرامونه دا تجویز ورکولے شي چې خلک څنګه رویه یا چلند کولے شي. دې پروګرامونو کې د خلکو په اړه معلومات ورکوي او بیا دغه پروګرامونه دا فیصله کوي چې آیا د دې خبرې احتمال شته چې دغه تن جرم کولے شي.

د احتجاج په وخت پریډیکټیو پولیسنګ استعمالیدے شي؟

ممکنه ده چې د احتجاج کونکو شناخت لپاره پولیس فیشل ریکګنیشن ټیکنالوجي، آئي ایم ایس آئي کېچرز یا جیو لوکېشن ټیکنالوجي نه کار واخلي او هغه ډېټا بېس او نګرانۍ فهرست یا واچ لسټ ته واچوي.
خلکو ته اکثره معلومه نه وي چې د هغې نوم د پولیس ډېټا بېس یا نګرانې په فهرست کې اچول شوې وي او د دې نه وتل که ناممکنه نه وي نو مشکله ډېر وي.

احتجاج ته د تلو نه وړاندې د کومو خبرو په اړه فکر پکار دے؟

۱. د احتجاج په اړه په آن لائن پلېټ فارم شیئر کړې شوې تصویرانو، ویډیوګانو یا میسجونو نه د احتجاج کونکو شناخت په اړه معلومات اخیستې کیدے شي، او چې کله یې شناخت وشي نو هغوي بیا د څارنې یا نګرانۍ په

لستونو کې واچول شي یا یې پروفائل جوړ کړې شي او پریډیکټیو پولیسنګ ټولز کې شامل کړې شي.
۲. که پولیس تاسو د یو داسې تن په درجه بندۍ کې اچولې وي چې د جرم کولو یې امکان وي نو دا د احتجاج په وخت حراست کې د اخیستو، نیولو، ودرولو او د لټون لپاره استعمالیدے شي.
۳. د حکومت لخوا د شفافیت کموالي او د حکومت د خلاصو پالیسو کموالې د دې ډېټا بېس د ناسم استعمال امکان سېوا کړي.

د قانون نافذ کونکو ډېټا بېسز څنګه په احتجاج کې استعمالیدے شي

پنجاب سېف سټیز اتهارټي (پي ایس سي اې) تر لاندې د پنجاب پولیس انټیګریټډ کنټرول اینډ کمانډ سینټر د ولس سکیورټي (امنیت) ښه کولو په اړه د ډېټا ټولولو واک لري. په دې کې د اعدادوشمار په بنیاد د پولیسو تجزیې په ذریعه د جرم د پېښنو د علاقو نشاندهي، د جرمونو څارنې لپاره د نګرانۍ سسټم جوړول او ولس د تحفظ لپاره د مخنیوي ګامونه اخېستل شامل دي.
دا نظام یا سسټم په اول ځل لاهور کې نافذ کړې شوې وو او په شپږو ښارونو (اسلام آباد، بهاولپور، ملتان، فیصل آباد، ګوجرانواله، راولپنډۍ) کې موجود دی چې د غځولو پلان یې هم شته.
واضح دې وي چې پي ایس سي اې کراچۍ کې هم لس زره کیمرې نصب کړې دي چې اصل مقصد یې سکیورټي ده، که د دې دائره اختیار په نظر کې وساتل شي نو دا ممکنه ده چې تېرو کلونو کې کوم اعدادوشمار جمع کړې شوي نو هغه په ښارونو کې د مظاهرو د نګرانې لپاره استعمالیدے شي.
بل دا، اګست 2022 کې چې د انفارمېشن ټیکنالوجي وزارت لخوا د 'سمارټ پولیسنګ' یو نظام معارفي کړې شوې وو. دې ته 'کرائم اینالېټکس اینډ سمارټ پولیسنګ ان پاکستان' نوم ورکړې شوې وو. د انفارمېشن ټیکنالوجي وزیر اعلان کړې وو چې اسلام آباد ګلګت او مظفر آباد کې 'کرائم اینالېټکس اینډ سمارټ پولیسنګ ان پاکستان' بنیادي سسټمو کار شروع کړې دې.
د برہ معلوماتو نه علاوه د جرمونو د کمولو کوششونو کې د آئي ټي وزارت ډیجیټائزیشن لپاره ځینې ګامونه اخیستي دي لکه په لویو پېمانه د پولیس تانو

ډیجیټائزیشن سره سره هوټېل آئي او ټریول آئي، ایف آئي آر درج کول او شکایت درج کولو طریقه کار پکې شامل دي.
د اندیښنې وړ خبره دا ده چې د پاکستان غوندې ملک کې په لویه پیمانه ذاتي ډېټا جمع کړې کیږي چرته چې د دې په اړه څه قوانین هم نشته او نه يې د ساتنې په اړه.

د څارنې په وخت د خپلو ډیوائس د تحفظ په اړه ګائیډ

ډېټا لوکېشن پورې رسائي څنګه په بنه ډول کنټرول کیدے شي؟

زما د فون لوکېشن چرته سټور یا محفوظه دې؟

ستاسو د فون لوکېشن په دوه طریقو خپل لوکېشن لټولې شي یو د جي پي ایس او بل د موبائل نیټ ورک د لوکېشن استعمال

جي پي ایس

جي پي ایس (ګلوبل پوزیشننګ سسټم) د سېټلائټ د لارې ستاسو فون په سم ډول لټولے شي (د یو مېټرو دننه). دا ستاسو په موبائل فون کې د جي پي ایس په چپ تکیه کوي.
ستاسو په استعمال کې کوم فون دے؟ کېدے شي د هغې جي پي ایس لوکېشن په فون کې محفوظه یا سټور وي یا په یو کلاؤډ سروس لکه ګوګل کلاؤډ یا آئي کلاؤډ کې. دا ستاسو په استعمال کې د یو داسې ایپ نه هم اخیستې کیدے شي چې جي پي ایس ته رسائي لري.

د موبائل نیټ ورک ځائے یا مقام

ستاسو د انټرنیټ سروس په ذریعه پولیس ستاسو ځاې ته رسائي لرلې شي

د دي مطلب دا شو چې پولیسو ته ستاسو د موبائل فون ضرورت نشته چې تاسو کوم ځای کې د احتجاج لپاره موجود وپې.
هم دغه معلوماتو حاصلولو لپاره آئي ایم ایس آئي کېچر ز چې سټینګرې په نوم هم پیژندلې کیږي یو ډیوائس دی چې په یو علاقه کې د موبائل نېټ ورک سره کنېکټ کړې شوې موبائل ټریک کولے شي او هغې کې مداخله کولے شي.

خپل لوکېشن ډېټا څنګه په ښه ډول کنټرول کیدے شي

جي پي ایس

خپل لوکېشن پوري رسائي محدوده کړې

جي پي ایس په معامله کې دا دومره اسان دې چې تاسو خپل لوکېشن آف کړې (چې لوکېشن سروسز ورته وایې). خو دا خبره ذهن کې وساتئ چې په تېرو ځایونو کې چرته ستاسو لوکېشن آن وو نو هغې ته رسائي کیدے شي.
تاسو ته په خپل فون د جي پي ایس د استعمالیدو ضرورت کیدے شي لکه تاسو که په یو احتجاج کې یې او د خپل حفاظت په خاطر خپل ملګري یا کورنۍ سره معلومات شریکول غواړې. په دغه صورت کې د لوکېشن په اړه کم نه کم معلومات خپرولو لپاره د ایپلي کېشنز د لوکېشن اجازت چیک کړئ.
ټولو ایپلي کېشنز کې د مقام یا ځاې پورې د رسائي اجازت لرلې کولو سره په آن لائن اکاؤنټ کې ډېټا نشي محفوظه کیدے.
که تاسو ته ښخي د یو ایپلي کېشن استعمال ضرورت وي چې هاغه جي پي ایس ډېټا ته رسائي لري نو د ایپلیکېشن د سیټنګز جاج واخلې چې آیا ستاسو لوکېشن سټور شوې او که د فون په ایپ کې دې. لکه د مثال په توګه چې کله تاسو ګوګل اکاؤنټ کې لاګ ان یې او تاسو ګوګل مېپس استعمالوې او تاسو غواړې چې لوکېشن هسټري غېرفعاله شي نو ستاسو لوکېشن هسټري به په ګوګل اکاؤنټ کې محفوظه نه وي.
که ستاسو لوکېشن سروسز آن وي او تاسو تصویر ویستې وي نو چې چرته تصویر اخیستې شوې د هغې لوکیشن به مېټا ډېټا چې ورته ایکزیف ویلي

کیږي، پکې شاملیدے شي. که تاسو غواړې چې لوکېشن سروسز غېر فعاله کړې نو تاسو د سافټ ویئر یا ایپلي کېشن په ذریعه ایګزف ډېټا ختمولې شې. لکه د مثال په توګه چې کله تاسو تصویر لیږ يې نو د میسجونو ایپ سګنل ایګزف ډېټا ختمه کړي.
دا رنګ وائي فائي او بلوټوټ بندولو سره ستاسو فون د رسائې ځایونو او د لوکېشن معلومات ورکولو نه ودروي.

موبائل نېټ ورک لوکېشن

چې کله د موبائل نېټ ورک خبره راځي نو د کنټرول کولو یواځنې لار يې دا ده چې دغه نېټ ورک سره کنېکنش مه کاروئ.
که ستاسو فون بند وي یا په ایرپلېن موډ یا فیراڈې کیج کې ساتلو سره ستاسو به موبائل نېټ ورک سره رابطه ختمه شي او داسې به د جي ایس ایم جیو لوکېشن ناممکنه شي.
فیراډې کیج یا ټیلي فون بندول موبائل نېټ ورکو سره رابطې ودروي او یواځې په ایرپلین موډ د استعمال مطلب دا دے چې په ځینې طریقو بیا هم رابطې کیدے شي لکه (بلوټوټ یا جي پي ایس).

دا ټول چرته جمع کیږي؟ یا چرته سټور کیږي؟

کله چې هم تاسو موبائل استعمالوې نو تاسو ډېټا جوړوې لکه د مثال په توګه تاسو تصویر اخلې او ویډیوګانې جوړوې، چې کله تاسو نوټس او اسناد جوړوې یا پکې ترمیم کوې او چې کله تاسو نوې نامې یا نمبرې په موبائل کې اچوې نو تاسو ډېټا تیاروې.
دا ټوله ډېټا د ایپلي کېشنز په ذریعه جوړیږي... ستاسو کیمره، فوټو ایپس، سوشل میډیا ایپس، نوټس ایپس او ستاسو کانټیکټس ایپس یو څو مثالونه دي.
دا خبره کول مهمه ده چې کله تاسو په فون یو فائل جوړوې نو زیاتره وخت تاسو 'مېټا ډېټا' جوړوې لکه د مثال په توګه د یو تصویر به مېټا ډېټا وي چې په کوم وخت او ځاې کې اخیستې شوې دي.

دا ټوله ډېټا به ستاسو د فون انټرنل میموري، (که ستاسو فون سره د ایکسټرنل ډېټا کارډ وي) یا په کلاوډ دواړو کې محفوظیږي که تاسو کوم یو هم کلاوډ سروس بېک اپ لپاره استعمالوې.

پولیس ستاسو تصویرونو/عکسونو، کانټیکټس او اسنادو پورې څنګه رسائي حاصلولې شي؟

پولیس په یو څو طریقو ډېټا پورې رسائي لرلې شي. دا په دې هم ده چې دا څنګه سټور کیږي

که تاسو خپله ډېټا فون کې محفوظه کوې بیا دې ته 'موبائل فون ایکسټریکشن' ډیوائس په ذریعه رسائي کیدے شي. کوم چې ستاسو فون سره کنېکټ کیدے شي او ټوله ترې ډاؤن لوډ کیدے شي. دا طریقه کار د فاصلې نه نشې استعمالیدے پولیس ته به خپله د فون پورې د رسائې ضرورت وي.
ډیوائس هیک کول یو جدید تکنیک دې چې ستاسو فون کې یو خاص مقدار ډېټا ته رسائي کولے شي خو دا ضروري نه ده چې ټولې ډېټا ته رسائي ولري.
موبائل فون ایکسټریکشن د لارې پولیس کولے شي چې ستاسو ډېټا ته رسائي ولري خو هیکنګ کې خپله یا فزیکل رسائي نشې کیدے. د دې مطلب دا شو چې د احتجاج نه وړاندې یا ورستیو هر وخت دا طریقه کارول کیدے شي.
که تاسو خپل تصویرونه اسناد یا کانټیکټس سینک کوې (لکه آئي کلاوډ، ډراپ باکس یا ګوګل ډرائیو په ذریعه). پولیس د فاصلې نه 'کلاوډ ایکسټریکشن' ټولز په ذریعه ستاسو د علم او اجازت بغېر معلوماتو ته رسائي لرلې شي او یا کلاوډ ورکونکې سروس ته قانوني درخواست کولے شي.

خپلو تصویرونو، کانټېکټس او اسنادو پورې د رسائې خطر څنګه کمولې شو؟

کلاوډ ایکسټریکشن تیکنیکونو هدف د جوړیدو مخنیوي لپاره تاسو له به په مکمل توګه د کلاوډ سروس نه ډډه کول وي.

که تاسو په مکمل توګه د کلاوډ سروس نه ډډه کوئ نو دا تاسو لپاره مشکل ودرولی شي. تاسو کولے شئ چې د حساس نوعیت مواد مه اپلوډ کوئ. د ایپلي کېشنز سېټنګز او فیچرز جاج اخیستو سره هم تاسو معلومولے شئ چې ستاسو د فون ډېټا چرته آن لائن بیک اپ کیږي (لکه د مثال په توګه چې د واټس ایپ بیک اپ په ګوګل ډرائیو محفوظه وي) نو که څه هم ستاسو واټس ایپ میسجز اینډ ټو اینډ انکرپټډ وي. د کلاوډ ایکسټرېکشن ټولز په ذریعه دې مسیجونو پورې ګوګل ډرائیو ته رسائي کیدے شي.
خو د ټیلي فون د یو استعمالونکي په توګه تاسو په هاغه ډېټا کنټرول لرلې شي چې تاسو یې خپله جوړه وې او دا چرته سیو یا محفوظه ده. ستاسو په اړه ستاسو فون کې کوم معلومات موجود دي نو که داسې ټولز ستاسو په فون استعمال شي نو تاسو ته به ښه معلومه وي چې ستاسو کومې ډېټا ته رسائي کیدے شي.
دا خبره باوري کړئ چې ستاسو د فون مواد انکرپټډ دې او دا چې ستاسو آپرېټنګ سسټم او ایپلي کېشنز اپ ډېټ دي. دې سره به دا وشي چې موبائل فون ایکسټرېکشن او هیک کولو ځینې طریقو له وجې به خطر کم شي.

ډیجیټل کمیونیکېشنز

زما کمیونکېشنز یا رابطې چرته محفوظه دي؟

ټېکسټ میسجونه/فون کالز: روایتي موبائل رابطې د موبائل نېټ ورکو د لارې کیږي. په عام توګه دغه رابطې ټیکسټ میسجز او فون کال ایپلي کېشنز د لارې کیږي کوم چې ستاسو په فون کې موجود دي. د ټیلي فون کالونه چرته هم سټور نه وي. ټیکسټ میسجز ستاسو په فون او د وصول کونکې په فون کې موجود وي دا هم په عارضي توګه فراهم کړې شوې نېټ ورک سره سټور کیدے شي.
میسجنګ ایپلي کېشنز: په انټرنېټ د میسجونو په پلېټ فارمونو تر ډېره حده محفوظه رابطې کیږي دا په دې هم ده چې تاسو کوم میسجنګ ایپلي کېشن استعمالوئ. ستاسو میسجونه او د وصول کونکي سره دغه میسجونه سټور

کیدے شي او ممکنه ده چې آن لائن هم سټور شوې وي. ځیني د میسجونو ایپلي کېشنز د بیک اپ حل هم شته. یا به هغه آن لائن موجود وي یا په فون کې. ځینې میسجنګ ایپلي کېشنز په مختلفو قواعدوضوابطو یا په پروټوکولز تکیه کوي چې مطلب یې دا دې چې ځیني د مسیجونو ایپلي کېشنز ته د نورو په مقابله د مداخلت زیاته خطره ده.
سوشل نېټ ورکس: د سیلف هوسټډ سسټمز نه علاوه په سوشل میډیا ستاسو رابطې د خدمات ورکونکو (سروس پرووائډر) سره محفوظه وي.

زما رابطو پورې رسائي څنګه کیدے شي؟

ځینې داسي طریقې دي چې پولیس ډېټا پورې رسائي لرلې شي او دا په دې هم ده چې چرته تاسو سټور کړې ده.
ستاسو په فون کې محفوظ کړې شوې رابطو پورې رسائي (لکه چې ټیکسټ میسجنګ اېپ کې ستاسو خبرو ته) د موبائل فون ایکسټرېکشن په ذریعه کیدے شي او دا ستاسو فون سره کنېکنټ کیدو نه پس سټور کړې شوې ډېټا ډاؤن لوډ کولے شي.
د ډیوائس په هیک کولو هم رسائي کیدے شي... دا یو داسي تیکنیک دې چې ورته د فیزیکل رسائې ضرورت نشي کیدے.
که ستاسو رابطې په یو سروس پرووائیډر یا سوشل نېټ ورک کیږي (مسینجر، ټیلي ګرام، انسټاګرام، ټک ټاک) نو پولیس ستاسو د اجازت او علم بغیر دې ته د کلاؤډ ایکسټرېکشن ټیکنالوجي په ذریعه رسائي حاصلولې شي.
هم دغه تیکنیک ستاسو د رابطو بیک اپس پورې د رسائي لپاره کارول کیدے شي (لکه د مثال په توګه ګوګل درائیو/ آئي کلاؤډ نه د واټس ایپ ډېټا).
په سوشل نېټ ورکو ستاسو رابطې هر څوک کتلې شي یا پبلک وي (لکه یو فیس بک ګروپ کې ستاسو خبرې) نو ورته پولیس سوشل میډیا انټیلي جنس ټولز (ایس او سي ایم آئي این ټي) په ذریعه رسائي کولے شي.
آئي ایم ایس آئي کېچرز په ذریعه پولیس ستاسو ټیکسټ میسجونه او ټیلي فون کالونه په منځ کې ودرولو، ریکارډ یا ثبتولو یا په هغې کې (ممکنه غیرقانوني)

مداخلت کولے شي. آئي ایم ایس آئي کېچرز یو داسې ډیوائس ته ویلې شي چې د څه په مدد هغه ټول موبائل فونې یو مخصوصه علاقه کې ټریک کیدے شي. ستاسو میسجونو او پیغامونو تا د رسائې لپاره قانوني لار هم اختیار کیدے شي. ستاسو ډېټا یا رابطې مواد چې کومو کمپنیو سره دې نو د قانون د لارې ورته درخواست کیدے شي. (لکه د مثال په توګه فیس بک ته).

د رابطو پورې د رسائې خطر څنګه محدوده کیدے شي؟

خطر کمول دې عمل سره شروع کیږي چې تاسو کومه ډېټا شیئر کوې هغه تاسو کنټرول کولے هم شې او دا تاسو چا سره او په کومه ذریعه شیئر کوې. چې کله تاسو ډېر حساس معلومات شیئر کوې نو خپل ذاتي حېثیت کې ورسره ملاقات وکړې یا په شخصي توګه ناسته وکړې.
که په ذاتي حېثیت کې ملاقات نه کول یو آپشن دې نو د موبائل فونو ټېټه یا کمه سکیورټې هم پام کې وساتې او اینډ ټو اینډ انکرپټډ میسجونو ایپلي کېشنز په استعمالولو غور وکړې.
خو دا ذهن کې وساتې که تاسو د میسجونو ایپلي کېشن لپاره کلاؤډ بیک اپ استعمالوې نو دغه مواد ته د کلاؤډ ایکسټرېکشن ټولز په ذریعه رسائي کیدے شي. د رابطو د یو بلې ذریعې یا چېنل د لارې د مظاهره کونکو د شناخت تصدیق وکړې. (لکه د مثال په توګه په یو بل پلیټ فارم ورته میسج وکړې، یا په انکرپټډ ایمیل یا په وائس او یا په ویډیو).

یونیک آئیډېنټفائرز (منفرد شناخت لرونکې): څه شې دے او دا چرته ستور وي؟

ستاسو فون او سم کارډ کې یونیک آئیډېنټفائرز دي چې ستاسو شناخت لپاره پولیس ورته رسائي لرلې شي.
آئي ایم ایس آئې (انټرنیشنل موبائل سبسکرائبر آئیډنټټي) منفرده یا ځانګړې شمیره ده چې ستاسو سم کارډ سره تړلې وي. دا نشې بدلیدے که تاسو په یو بل فون کې سم کارډ هم واچوې.

که ستاسو د موبائل فون سبسکرپشن وي نو آئي ایم ایس آئې به ذاتي معلوماتو سره تړل شوې وي لکه (ستاسو نامه او پته).
آئي ایم اي آئې (انټرنیشل موبائل ایکوپمنټ آئېډنټټي) هم یو منفرد نمبر دې چې ورسره ستاسو د فون پیژندګلو کیدلے شي او که تاسو فون بدلوې نو تاسو سره به یو نوې آئي ایم اي آئې وي.
آئي ایم ایس آئې او آئي ایم اي آئې د مخصوص ټولز نه علاوه په اسانه نشې بدلیدلے ځکه چې دا ستاسو او ستاسو موبائل معلوماتو سره تړل شوې وي لکه (ستاسو نامه او پته او د موبائل برانډ یا ماډل).
د اشتهار آئي ډي یا اېډ آئي ډي: اېډ آئېډنټفائرز آئي ایم ایس آئې او آئي ایم اي آئې نه مختلف وي ځکه چې دا وخت سره بدلیږي. اېډ آئي ډیز د اېډورټائزرز لخوا په ایپلي کېشنز او په ویب سائټ یا ویب پاڼه کي استعمالیږي چې ستاسو شناخت وکړي او هدف کړې شوې اشتهارات وړاندې کړي. دا ستاسو ذاتي معلوماتو سره هم نه وي تړل شوي (لکه ستاسو نامې سره) خو دا نورې داسې ډېټا نه ظاهریدے شي لکه (جیو لوکېشن، استعمال کړې شوې ایپلي کېشن، کتل شوې ویب سائټس یا ویب پاڼو). اېډ آئي ډیز ستاسو د فون سسټم نه تیاریږي او ستاسو د فون په سیټنګز کې هم ښکاري او دا مینولي بیا د سره بحالیدے شي.
نور آئېډنټفائرز: ستاسو په فون کې ځینې داسې نور عناصر شته چې په نړیوال کچ یونیک آئېډنټفائرز لري لکه (ستاسو وائي فائې لپاره میک ایډریس یا د بلوټوټ لپاره بي ډي اې ډي ډي).

یونیک آئېډنټفائرز ته رسائي څنګه کیدے شي؟

۱. ستاسو آئي اېم ایس آئې او آئي ایم اي آئي پولیس د آئي ایم ایس آئي کېچر په ذریعه حاصلولې شي. دا یو داسې ډیوائس دے چې نېټ ورک سره کنېکټ شوې ټول آن موبائل ټریک کولے شي. یو ځل چې دې آئېډنټفائرز کې مداخله وکړي نو دا ستاسو ذاتي معلومات ترلاسه کولے شي.
۲. دا ستاسو په فون کې د ایپلي کېشنز او کتل شوې ویب سائټ په ذریعه ستاسو اېډ آئي ډي ته رسائي کولے شي. دا نبغ په نبغ ستاسو ذاتي معلوماتو (نامه او پتې) سره نه وي تړل شوې دا ستاسو لوکېشن ډېټا پشان نورې ډېټا

سره تړل کيدے شي. ځيني ډېټا بروکرز يا کمپنۍ ستاسو فون نه معلومات حاصلولې شي او په پوليس يې خرڅولې شي.
۳. ستاسو مېک ايډرس غوندې نور يونيک آئيډېفائرز وائي فائي هاټ سپاټ نه هم معلوميدے شي خو دا ذاتي معلوماتو سره تړل ډېر مشکل دې کوم چې ستاسو د شناخت لپاره استعماليدے شي. او په دې ورستيو کې راغلې د آئي او ايس او اينډرائيډ ورژنز نوې او نامعلومه نېټ ورکو سره رابطه کوي نو هغه ستاسو مېک ايډريس دوکه کولے شي.

د يونيک آئيډنټېفائرز لخوا د شناخت کيدو خطر څنګه محدود کولے شو

که تاسو په يو احتجاج کې يې او هلته تاسو د فون ټريک کولو آئي ايم ايس آئې کېچرز د خطر نه ځان بچ کول غواړې نو د ټولو زيات موثره به دا وي چې فون د نېټ ورک سره مه کنېکټ کوې. فون په ايرپلين موډ يا په فيراډې کيج کې ساتلو سره به ستاسو فون د موبائل ستنو نه پټ وي او دې سره به آئي ايم ايس آئې کېچرز نه هم.
که دا ضروري وي چې تاسو موبائل نېټ ورک سره کنېکټ کول غواړې نو يو بيل پري پيډ سم واخلې (کله چې تاسو يو نوې سم واخلې نو هغه ډېر لږ معلومات ورکوې). که تاسو داسې کوې نو ياد ساتئ چې که ستاسو فون په تېرو مختلفو وختونو کې په مختلفو سم کارډونو سره د پوليس آئي ايم ايس آئي کېچرز سره کنېکټ وو نو ستاسو اصل سم کارډ سره به پري پيډ سم تړل ممکنه وي. د دې وجه ستاسو فون کې يونيک آئيډنټفائر آئي ايم اي آئي دې.
په باقاعده توګه خپله ايډ آئي ډي بيا نوې کول د هم هاغه يو آئي ډي د لاندې ستاسو د فون هلې ځلې جمع کيدو نه بچ کيدو لپاره يو ښه طريقه ده. که ستاسو موبائل کې دا آپشن وي نو تاسو ذاتي اشتهارونه غېرفعال کولے شې. دا به اپيلي کېشنز او ويب پاڼو د يونيک آئيډنټفائر پورې رسائي ودروي.
تاسو آن لائن ټريک کولو او ستاسو معلومات ټولولو نه کمپنۍ ودرولو لپاره 'ايډ بلاکر' يو ښه طريقه ده.

په احتجاجونو کې د پوليس څارنې په اړه د ډېټا د حقونو په اړه فيکټ شيټ

پریوینشن آف الیکټرونکس کرائمز ایکټ 2016 یا الیکټرونک د جرمونو مخنیوې قانون
د دې قانون سیکشن 35 (2) ترلاندې افسران ډیوائس او ډېټا معامله ګوري

د قانون مطابق عملدرآمد

د معلوماتو د نظام د رازدارۍ تحفظ لپاره ګامونه

شک 36 افسرانو ته د ضبط کړې شوې د ډېټا سسټمونو سره د معاملې هدایت ورکوي. په دې کې دا هم شامل دي چې افسران د هغه شیانو فهرست جوړ کړي چې کوم ضبط کړې شوې دي او هغه فهرست د انفارمېشن سسټم او د ډېټا مالک ته یې ورکړې.
شک 41 د معلوماتو د رازدارۍ په اړې دې. د دې ترلاندې هغه تن، خدمت ورکونکې یا تفتیشي افسر ته د دریو کالو د قید سزا او یا پرې لس لاکه جرمانه لګول کیدے شي څوک چې بې له رضامندې معلومات افشا کوي او چاته زیان رسولو یا ورته ګټه ورکولو بغېر ډېټا ورکړې او یا د معاهدې خلاف ورزي وکړي.

معلوماتو ته د لاسرسي حق قانون (آر ټي آئي)

د پاکستان آئین آرټیکل 19 اې مطابق د پاکستان څلوررو واړو صوبو او په وفاقي کچ سرکاري ادارو کې موجود معلوماتو او ریکارډ ته د رسائې اجازت ورکوي.

،،ولسي وګړې د قوانینو ترلاندې د ولسي اهمیت په ټولو چارو کې د سرکاري محکمو نه معلومات حاصلولې شي.،،

Federal: Right of Access to Information Act 2017

Punjab: The Punjab Transparency and Right to Information Act 2013

Khyber Pakhtunkhwa: KP Right to Information Act 2013

Sindh: Sindh Transparency and Right To Information Act 2016

Balochistan: Balochistan Right to Information Act 2021

خلک او ادارې انفارمېشن کمشنر سره رابطه کولے شي او د هغې په دائره اختيار کې د معلوماتو د حصول لپاره درخواست ورکولے شي. په داسې قانوني سهولتونو کې استثنا او خبرداري په ذريعه معلومات محدوده کيدے شي. که د دې معلوماتو نه څه جرم کيدے شي د يو کېس په تفتيش کې خنډ يا قامي سلامتيه متاثريدې شي.

په احتجاجي مظاهرو کې د پوليس افسرانو عکسونه/تصويرونه اخيستل

کال 2018 کې د پنجاب پوليس مشر په ټولو تانو کې موبائل فون، ليپ ټاپ او په کيمرو د بنديز په اړه هدايات جاري کړې وو. زموږ د معلوماتو ترمخه څه واضحه پاليسي يا قاعده نشته چې هغه په احتجاجونو کې د پوليس افسرانو تصوير جوړول جرم ګرځوي. احتجاجونه عوامي اجتماع ده نو په فوټوګرافي پابندي لګول د رائې د آزادئ يا د بيان د آزادئ خلاف کيدے شي.
د پوليسو افسرانو لخوا غير آئيني او د ضرورت نه زيات د طاقت استعمال په اړه تصويري او ويډيوګرافک شواهد مثالونه ثبت شوې چې هغې د غېر ضروري يا بې تناسب د طاقت استعمال ته د خلکو توجو اړولې څوک چې د احتساب غوښته کوي.