په افغانستان کې د خبریالانو لپاره د ډیجیټل امنیت لارښود

وری ۱۴۰۵ هـ ل

لیکوال: احمد قریشي

AFJC
Afghanistan Journalists Center
مرکـــز خبـــرنگاران افغانســـتان
د افغانســـتان د خبـــریالانو مرکـــز

د مطالبو لړليک

پاڼه

سرلیک

په ننۍ نړۍ کې خبریالان په ډیجیټل فضا کې له بېلابېلو ګواښونو سره مخ دي، چې کولای شي د هغوی شخصي او مسلکي خوندیتوب وګواښي. سایبري بریدونه، هک، غیرقانوني څار، سانسور او جاسوسي له یادو ګواښونو څخه دي، چې د ډېټا، سرچینو او اړیکو د خوندیتوب ارزښت جوتوي. د یادو ګواښونو په اړه د خبریالانو د پوهاوي لوړول او سمه روزنه د هغوی د خپلواکۍ، امنیت او مسلکي کار په ساتنه کې کلیدي ونډه لوبوي.

دا لارښود د ډیجیټلي ګواښونو پر وړاندې مبارزه کې د عملي ټکو، کړنلارو او اغیزناکو وسایلو د وړاندې کولو په موخه جوړ شوی، څو له خبریالانو سره مرسته وکړي، چې په انلاین چاپېریال کې د خپل امنیت کچه لوړه کړي او له خپلو حساسو اطلاعاتو او سرچینو څخه ساتنه وکړي.

په یاد ولرئ، چې په انټرنټ او مجازي فضا کې د محافظتي ګامونو لپاره تو ټولو شپه وخت، د یوې پېښې له رامنځته کېدو وړاندې دی، هر څومره چې ژر اقدام وکړئ، هغومره د خطر د پېښېدو کچه کمېږي.

لومړی څپرکی

په انلاین فضا کې د امنیت ټینګښت لپاره اساسي مفاهیم او ټولیزې کړنلارې

۱,۱. په انلاین فضا کې له خپلې ډېټا ساتنه وکړئ

خبریالان په زیاتېدونکي ډول د سایبري بریدونو او انټرنټي ځورونو موخه ګرځي. په دې بریدونو کې ځینې کسان د انټرنټي لټون له لارې د خبریالانو شخصي معلومات لټوي، څو هغوی وګواښي او ووېروي. خبریالانو ته سپارښتنه کېږي چې خپل انلاین پروفایل په منظم ډول وڅاري او د امکان په صورت کې خپل اطلاعات لرې کړي.

د خپلې انلاین ډېټا د لا ښې ساتنې لپاره:

۱,۲. خپل مشخصات په انټرنټ کې ولټوئ

- خپل نوم او نور شخصي اطلاعات لکه پته، د ټلفن شمېره او د زېږېدلو نېټه د لټون په ټولو موټورونو لکه (Google, Bing, Yahoo) په انلاین توګه ولټوئ.

- تاسې کولای شئ په براوزر یا د لټون موتور کې، د ناپېژاند حالت یا خصوصي حالت څخه ګټه واخلئ. دا حالتونه تاسې ته اجازه درکوي چې د انټرنټ د کارولو پر مهال، تاریخچه، کوکیانې او د وېب‌پاڼو معلومات ستاسې په وسیله کې ذخیره نه شي. په Google Chrome براوزر کې، د ناپېژاند حالت د فعالولو لپاره د شي اړخ په پاسنۍ برخه کې پر درېیو ټکو کلیک وکړئ او د (New Incognito Window) برخه وټاکئ. په Microsoft Edge براوزر کې هم کولای شئ پر درېیو ټکو کلیک وکړئ او د (New InPrivate Window) برخه وټاکئ. دا لارې ساده او اغېزمنې دي او د انټرنټ د کارولو پر مهال ستاسې شخصي حریم خوندي ساتي او مرسته کوي چې ستاسې د فعالیتونو اړوند معلومات په وسیله کې ذخیره نه شي، په دې توګه ستاسې خصوصي حریم خوندي پاتې کېږي.
- د انځور معکوس لټون وکړئ: خپل د خوښې وړ انځور پورته (Upload) کړئ ترڅو ووینئ چې په انټرنټ کې په کومو ځایونو کې خپور شوی دی.
- د خپلو خپلوانو یا د کورنۍ د غړو په اړه هم لومړنۍ ډېټا او اطلاعات وپلټئ، ترڅو وګورئ چې د هغوی په اړه کوم اطلاعات د لاسرسي وړ دي.
- هر هغه اطلاعات نوټ کړئ، چې غواړئ محدود یا پاک شي.

۱،۳. په مجازي فضا کې خپله ډېټا پاکه یا محدوده کړئ

- په ټولنیزو شبکو کې خپل معلومات یا انځورونه پاک کړئ یا یې لاسرسی محدود کړئ.
- په منظم ډول د خپلو ټولنیزو پاڼو د حسابونو د خصوصي حریم تنظیمات وڅارئ، څو ډاډه شئ چې د خپلو معلوماتو له هغې برخې سره چې عام خلک ورته لاسرسی لري، موافق یاست.
- د خپلې کورنۍ له غړو او یا ملګرو څخه وغواړئ چې ستاسو شخصي ډېټا د خپلو ټولنیزو شبکو له حسابونو څخه پاکه کړي.
- وقایوي ګامونه واخلئ څو د کورنۍ له غړو سره مرسته وکړئ چې د خپلو ټولنیزو شبکو حسابونه خوندي کړي، د بېلګې په توګه، هغوی ته وښایئ چې څنګه په دې شبکو کې خصوصي حریم تنظیم کړي. د بېلګې په توګه، د فیسبوک حساب د مدیریت او د خصوصي حریم ساتنې لپاره، خپل حساب ته ننوځئ او د شي لاس پورته اړخ کې د خپل پروفایل انځور کېکاړئ، بیا د تنظیماتو او خصوصي حریم (Settings & Privacy) برخې ته لاړ شئ او وروسته (Privacy Checkup) وټاکئ او هغه ډول یې تنظیم کړئ چې تاسو یې غواړئ. میتا (Meta) شرکت چې د فیسبوک مالک دی، په دې ټولنیزه شبکه کې یې د خبریالانو د امنیت ساتنې لپاره ځانګړی لارښود خپور کړی دی. د لا ډېرو معلوماتو لپاره دې پتې ته (Journalist Safety) سر ورښکاره کړئ.
- انټرنټي ارشیف سایټونه لکه (Wayback Machine) وڅارئ او په یادو سایټونو کې خپله ډېټا پاکه کړئ. دا سایټونه د وېب‌پاڼو زړې نسخې ساتي او د هغوی ډېټا ذخیره کوي.
- په اروپا کې د «هېرېدو حق» (Right to be Forgotten) قانون خلکو ته اجازه ورکوي، چې په ځانګړو شرایطو کې غوښتنه وکړي څو د دوی شخصي ډېټا د لټون له موتورونو او انټرنټي پلټفارمونو څخه پاکه شي. په امریکا کې هم په ګډوني خدمتونو (subscription services) کې د نوم لیکنې له لارې د ډېټا د پاکولو امکان برابرېږي.

۱،۴. هغه وقایوي اقدامات چې ستاسو د امنیت په شه والي کې مرسته کولای شي

- د انټرنټ د منظمې څارنې لپاره یوه د یادونې برنامه جوړه کړئ، څو وګورئ چې ستاسو په اړه کوم اطلاعات د لاسرسي وړ دي. دا کار تاسو سره مرسته کوي چې د خپلو شخصي معلوماتو په اړه خبر واوسئ او که چرته ناسم یا نا غوښتل شوي اطلاعات ووینئ، ژر تر ژره لازم ګامونه واخلئ تر څو ستاسو امنیت او خصوصي حریم خوندي پاتې شي.

- د خپل نوم او همدارنګه نورو شخصي اطلاعاتو لپاره د ګوګل خبرتيا تنظيم کړئ. د دې کار لپاره، لومړی د خپل ګوګل حساب ته ننوځئ او د (Google Alerts) وېب‌پاڼې ته لاړ شئ، بيا د (Create an alert) په برخه کې يوه خبرتيا تنظيم کړئ. د ښلګې په توګه، خپل نوم حتی د املايي تېروتنو سره وليکئ او شخصي اطلاعات لکه د زېږېدو نېټه او نور مشخصات د لټون په برخه کې دننه کړئ او وروسته د خبرتيا د جوړولو تېی کېکاږئ. په دې ډول، هر کله چې ستاسو اطلاعات په انټرنټ کې ښکاره شي، تاسو ته به د خبرداري يو برېښنالیک درواستول شي. په دې توګه کولای شئ په انلاين فضا کې د خپل خصوصي حريم د ښه مديريت لپاره لازم اقدامات ترسره کړئ.
- د خپلو حسابونو امنيت د دوه پړاويز تاييد (Two-factor authentication) او د اوږد او ځانګړي کوډ په کارولو سره لوړ کړئ.

۱,۵. په انټرنټ کې خپل امنيت لوړ کړئ

خبريالان د اطلاعاتو او څېړنو د لټون لپاره انټرنټ پورې تړلي دي، چې د امنيتي تدابيرو په پام کې نه نيولو سره خپل ځان او سرچينې له ګواښ سره مخ کوي. د انټرنټي خدمتونو وړاندې کوونکي، دولتونه، شرکتونه او مجرمين د انټرنټ د کارووونکو په اړه ډېټا راټولوي، چې کولای شي له هغوی څخه د خبريالانو پر وړاندې ګټه واخلي.

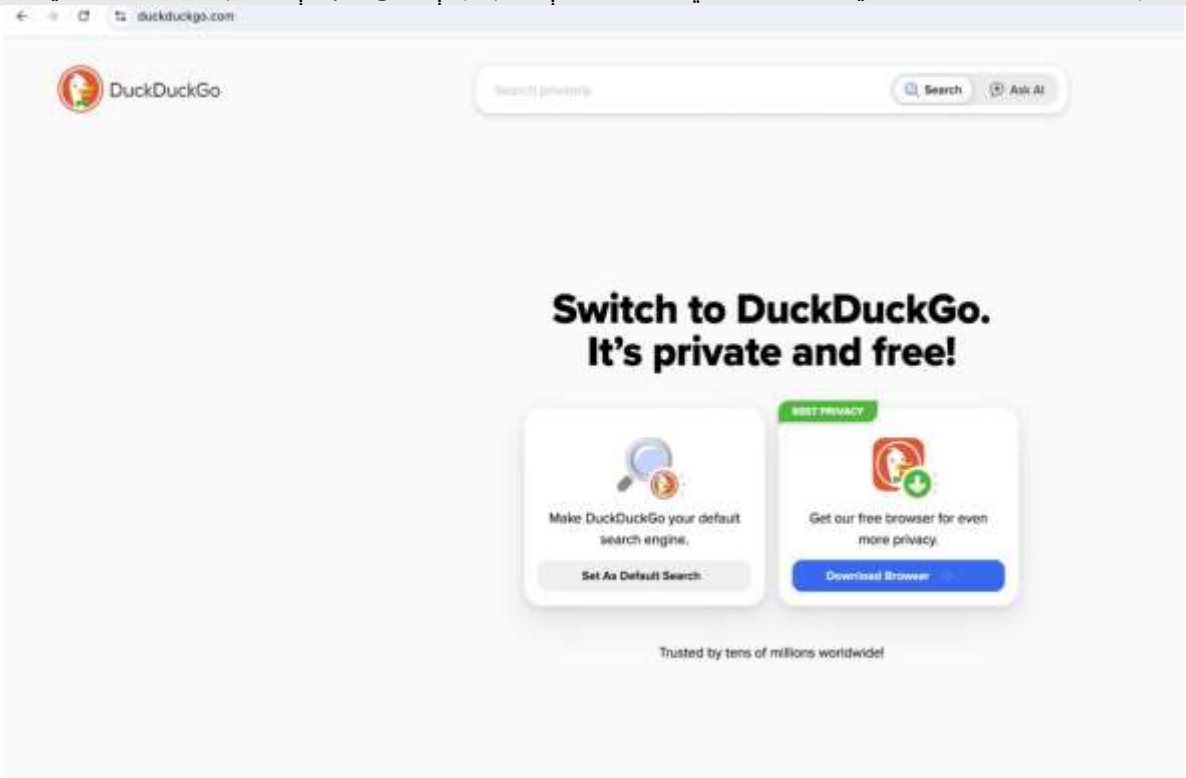
۱,٦. کوم شيان په انټرنټ کې زموږ رازونه افشا کوي

- هغه وېب‌پاڼې چې ګورو يې
- هغه وېډيو ګانې چې ګورو يې
- هغه لټونونه چې ترسره کوو يې
- آنلاين خدمتونه
- مصرف شوی وخت
- د براوزر تاريخچه
- کوکيانې
- ډانلوډونه
- اوتومات بشپړښت
- د ګوګل په ګډون د براوزرونو له خدمتونو څخه ګټه اخيستنه

که تاسو د ګوګل د لټون موتور ته داخل شوي ياست، دا سيستم ستاسو ټول فعاليتونه تعقيبوي. د دې لپاره چې پوه شئ ستاسو له کارونو څخه په دې براوزر کې څه ثبت شوي دي، دې پتې ته سر ورښکاره کړئ (myactivity.google.com) او د خپل حساب له لارې اقدام وکړئ.

۱,۷. له انټرنټ څخه د خوندي ګټې اخیستنې لارې چارې

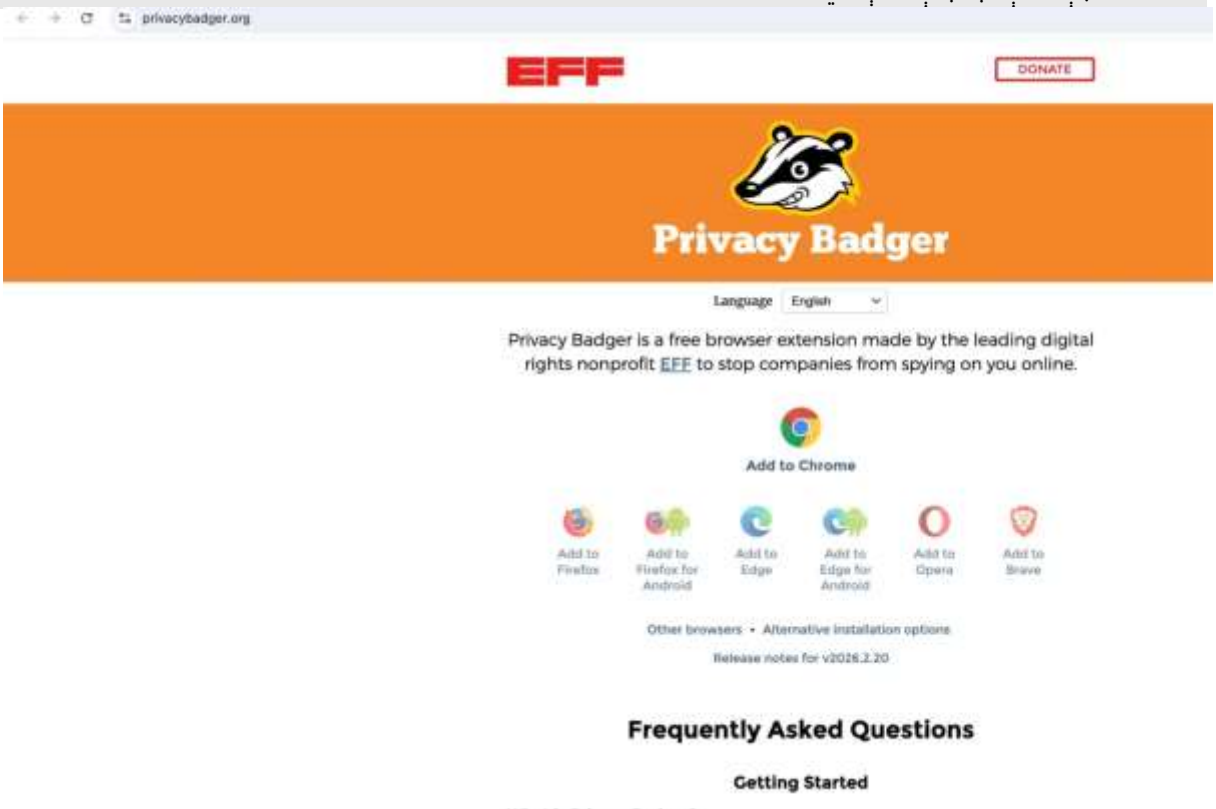
- د انټرنټي خدمتونو وړاندې کوونکي شرکت د مالکیت په تړاو پلټنه وکړئ او پوه شئ چې د یاد شرکت د انټرنټ (ISP) حکومتونو ته د ستاسو د ډېټا د لېږد پر وړاندې څه قانوني ژمنې لري. وخېړئ چې ستاسو په تړاو کومه ډېټا ساتل کېږي او دا ساتنه تر کوم مهال ده. د دې کار لپاره د انټرنټي خدمتونو وړاندې کوونکي شرکت ویب‌پاڼې ته لاړ شئ او د زمونږ په اړه یاهم د خصوصي حریم ساتنې برخه وګورئ.
- د یوې خصوصي مجازي شبکې یا (Virtual Private Network – VPN) په کارولو سره، د خپل انټرنټ د لټون سابقه د انټرنټي شرکت له څارنې وساتئ. پام مو وي چې که د وي پي ان (VPN) له لارې له انټرنټ سره وصل شوی، یاد شرکتونه دا چاره ثبتوي. د دې اندېښنې له منځه وړلو لپاره داسې وي پي ان (VPN) وټاکئ چې ستاسې د لټون سابقه نه تعقیبوي او نه یې ثبتوي، ځکه دغه معلومات کېدای شي له حکومتونو او نورو سره شریک شي. دا ډول وي پي ان (VPN) ستاسې انټرنټي اړیکه د خوندي منځګړو سرورونو له لارې خوندي کوي او معمولاً د معلوماتو د کوډولو (Encryption) وړتیا هم لري. په دې برخه کې غوره ده داسې وي پي ان (VPN) وکاروئ، چې په بل هېواد کې جوړ او ځای پر ځای وي، ځکه دا کار هغه حکومت ته چې تاسې پکې ژوند کوئ، ستاسې معلوماتو ته لاسرسی ستونزمن کوي.
- اوس مهال ډېرې وېب‌پاڼې کوډ شوي دي، یعنې که څه هم خلک پوهېدلی شي، چې تاسې کومه وېب‌پاڼه ګورئ یا کوم انلاین خدمت ته ننوتلې یاست، خو د هغې پاڼې منځپانګه نه شي لیدلای. ډاډ تراوسه کړئ، چې د هرې ویب‌پټې یا URL په پیل د (https) نښه موجوده وي، ځکه دا د امنیتي قفل او ستاسې او وېب‌پاڼې ترمنځ د اړیکې د کوډېدلو څرګندونه کوي.



- د (DuckDuckGo.com) لټون موتور په ځیرک ډول کوډ شوی او په انلاین فضا کې د کاروونکو پر خصوصي حریم او امنیت تمرکز لري. که تاسو له دې موتور څخه ګته واخلئ، سیستم یې هڅه کوي څو له وېب‌پاڼو سره ستاسو اړیکې تر ډېره بریده

کوډ (Encryption) کړي. په دې معنا چې د لټون او وېب‌پاڼو د کتنې پر مهال ستاسو اطلاعات نښه خوندي پاتې کېږي او د نورو له‌خوا يې د لیدل کېدو احتمال کمېږي.

- کله چې تاسې يوه وېب‌پاڼه ګورئ، يادە ويب‌پاڼه ستاسې په اړه ځينې معلومات راټولوي يا ستاسې انټرنټي پته (IP) چې ستاسې نږدې موقعيت ښکاره کوي. همداراز د هغې وسيلې په اړه معلومات هم ثبتوي چې تاسې يې له لارې وېب‌پاڼې ته وصل شوي ياست او دا هم ثبتوي چې تاسې څه وخت دغه وېب‌پاڼه ليدلې ده.
- د اعلانونو بندوونکی (Ad-blocker) نصب کړئ، څو له هغو زيان‌رسوونکو پټو پروګرامونو (Pop-up) څخه مو وساتي چې ډېرى وخت په اعلانونو کې وي. دا اعلانونه چې د انټرنټ د کارولو پر مهال د وړو او نا غوښتل شويو پنجرو په بڼه ښکاره کېږي، کېداى شي ويروسونه يا نور زيانمن پروګرامونه ولري. دا وسيله تاسې ته اجازه درکوي چې ځينې ځانګړې وېب‌پاڼې، لکه باورې يا ستاسې د خوښې خبرې وېب‌پاڼې، له بندولو څخه جلا کړئ، څو اعلانونه يې په عادي ډول ښکاره شي. د بېلګې په توګه، خپل براوزر لکه (Chrome)،(Mozilla Firefox) پرانيزئ، د لټون په برخه کې (Ad-blocker) وليکئ، بيا له معتبرو انتخابونو څخه لکه (Adblock Plus يا uBlock Origin) يو انتخاب او نصب کړئ. له نصب وروسته، د تنظيماتو په برخه کې وټاکئ چې کومې وېب‌پاڼې بندې شي.



- د (Privacy Badger) پروګرام نصب کړئ، څو وېب‌پاڼې او اعلان خپروونکي ونه شي کولای هغه پاڼې تعقيب کړي چې تاسې يې انلاين ګورئ.
- په ناپېژانده توګه له انټرنټ څخه د ګټې اخيستنې لپاره کولی شئ د (Tor Browser) وړيا سافټوير پر خپله وسيله نصب کړئ. دا سافټوير مرسته کوي چې ستاسې انټرنټي ترافيک له ځانګړو لارو تېر شي او ستاسې هويت پټ پاتې شي.

- همداراز، کولی شئ له (Tails) پروګرام څخه هم، چې یو وړیا عامل سیسټم دی او ستاسې ټول انټرنټي فعالیتونه د (Tor) شبکې له لارې لېږدوي، هم ګټه واخلئ. دا سافټویر د خبریالانو او هغو کسانو لپاره ډېر ګټور دی چې د پرمختللې ټکنالوژۍ لرونکي هېوادونو کې د حساسو موضوعاتو، لکه دولتي فساد، په اړه څېړنې کوي. د دې سافټویر له کارولو مخکې، هرو مرو په خپل هېواد کې د دې د کارونې اړوند قوانین وڅېړئ.
- حکومتونه، مجرمین او نور کسان کولی شي جعلي وېب‌پاڼې جوړې کړي چې ستاسې د شخصي معلوماتو، لکه کوډونو، د بانکي کارت معلوماتو او نورو جزئیاتو د راټولولو لپاره وکارول شي. له دې امله، مخکې له دې چې کومه وېب‌پاڼه وکاروئ یا ور ننوځئ، وګورئ چې د هغې ویب‌پته (URL) سمه لیکل شوې وي او په (https) سره پیل شوې وي.
- د امکان په صورت کې، د عامه کمپیوټرونو له کارولو څخه، په ځانګړې ډول په کافي‌نټونو یا د خبریالی په خونو کې، ډډه وکړئ. عامه کمپیوټرونه کېدای شي په زیان‌رسوونکو سافټویرونو یا جاسوسي پروګرامونو ککړ وي. که اړ یاست چې له عامه کمپیوټر څخه ګټه واخلئ، خپلو شخصي حسابونو ته مه ننوځئ او حتماً له هغو ټولو پروګرامونو څخه چې کارولي مو دي، ووځئ یا (Logout) شئ او د براوزر تاریخچه هم پاکه کړئ.

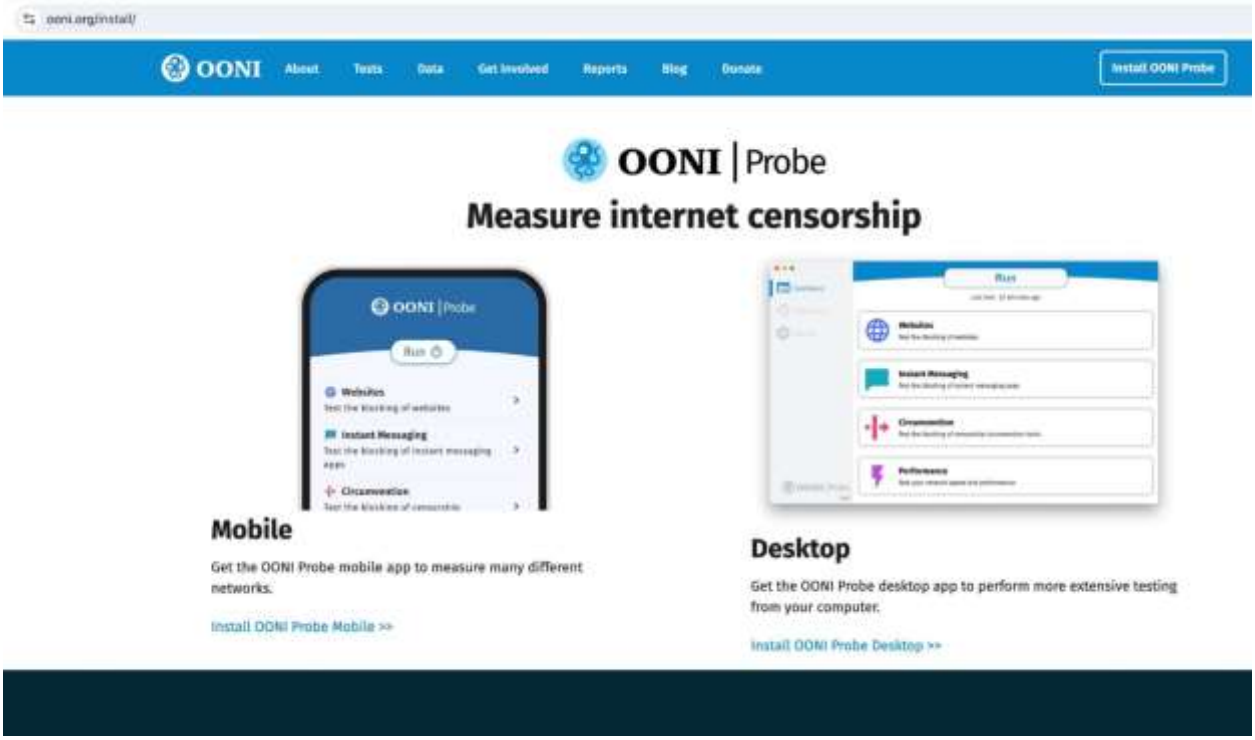
۱،۸. په انټرنټ کې سانسور او محدودیتونه وپېژنئ

دولتونه، شرکتونه او د انټرنټي خدمت وړاندې کوونکي کله ناکله له داسې سافټویرونو څخه کار اخلي چې خپل کارووونکي په ازاد ویب کې د لاسرسي وړ ځانګړو وېب‌پاڼو او خدمتونو ته له لاسرسي منع کړي. دې کار ته د انټرنټ فلټر کول یا بندیز لګول ویل کېږي، چې د سانسور یوه بڼه ده. فلټر کول په ښلاښلو لارو ترسره کېږي. سانسور کوونکي کولای شي حتی په کوډولو (Encryption) ټولې وېب‌پاڼې،

د کوربه‌توب خدمتونه یا انټرنټي ټکنالوژۍ بندې کړي. کله ناکله محتوا د هغو کلیدي کلمو له مخې بندېږي چې پکې موجودې وي. کله چې وېب‌پاڼې کوډ (Encryption) شوې نه وي، سانسور کوونکي کولای شي جلا جلا وېب‌پاڼې هم بندې کړي.
د انټرنټ له سانسور یا فلټر څخه د تېرېدو لپاره بېلابېلې لارې شتون لري. ځینې یې تاسې له ځانې ساتي، خو ډېرې یې دا کار نه کوي. کله هغه څوک چې ستاسې انټرنټي اړیکه کنټرولوي، کومه وېب‌پاڼه فلټر یا بنده کړي، نو تاسې تقریباً تل کولای شئ د اړتیا وړ معلوماتو ته د لاسرسي لپاره له سانسور څخه د تېرېدو له یوې وسیلې ګټه واخلئ.
په پام کې ولرئ، چې د فلټر ماتولو یا له سانسور څخه د تېرېدو هغه وسیلې چې د خصوصي حریم یا امنیت ساتنې ژمنه کوي، تل خوندي او خصوصي نه وي. همداراز هغه وسیلې چې د «ناپېژانده کوونکي» (Anonymizer) اصطلاح کاروي، تل ستاسې هویت په بشپړه توګه نه شي پټولای.

۱,۹. په انټرنټ کې له سانسور څخه د تېرېدلو یا مخنیوي لارې چارې

ستاسې جغرافیایي موقعیت او د سانسور ډول په ځېر عوامل، چې تاسې ورسره مخ یاست، د دې په ټاکلو کې مرسته کوي چې له سانسور څخه د تېرېدلو لپاره کومه لاره ښه کار کوي. که ډاډه نه یاست چې له کوم ډول بندیز سره مخ یاست، نو (OONI Probe) پروګرام مرسته کولای شي چې د بندیزونو ډولونه وپیژنئ، خو دا امکان هم شته، چې ستاسې د انټرنټي شبکې اداره کوونکی انټرنټي شرکت، پوه شي چې تاسې له دې سافټویر څخه کار اخلئ او ځینې هېوادونه کېدای شي وتوانېږي چې دا سافټویر په بشپړه توګه بند هم کړي.



په کمپیوټر کې د دې اپلکیشن د نصبولو لپاره دې (OONI Probe mobile app) او په ګرځنده ټلفن کې د دې اپلکیشن د نصبولو لپاره دې (OONI Probe for MacOS) پټې ته سر ورښکاره کړئ.
سره له دې، هرځومره چې ستاسې د انټرنټي فعالیتونو په اړه معلومات کم وي، هومره به د انټرنټي خدمتونو وړاندې کوونکي (ISP) لپاره دا ستونزمنه وي چې د فعالیتونو څانګړي ډولونه په انتخابي ډول بند کړي. له همدې امله، د انټرنټ په کچه له کوډ شویو

(Encryption) معیارونو څخه کار اخیستل، لکه (HTTPS) او کوډ (Encryption) شوی (DNS)، په ځینو حالاتو کې ګټور تمامېدای شي.

۱,۱۰. د خپل ډومېن خدمت وړاندې کوونکی بدل کړئ او له کوډ شوي ډومېن څخه ګټه واخلئ

که انټرنټي شرکتونه د «ډومېن نوم سیستم» یا (Domain Name System - DNS) له لارې د وېب‌پاڼو په بندولو سره ستاسې د لاسرسي مخنیوي کوي، کولی شئ د ډومېن خدمت د وړاندې کوونکي په بدلولو یا د کوډ (Encryption) شوي ډومېن په کارولو سره ېرته وېب‌پاڼو ته لاسرسی ومومئ.

د ډومېن د کوډولو لپاره دې پټې ته سر ورښکاره کړئ (د ډومېن کوډول)

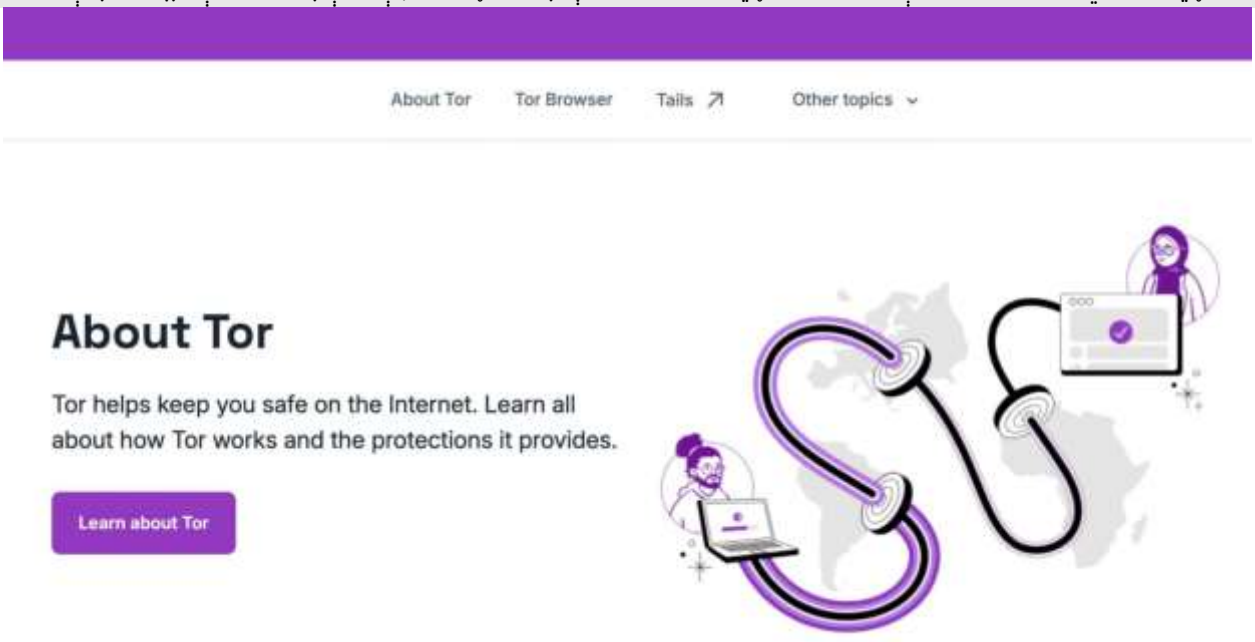
د ډومېن سیسټم د انټرنټ د بنسټ یوه مهمه برخه ده چې د ټلفن د دفترچې په څېر کار کوي. یعنې دا سیستم مرسته کوي چې د انټرنټ کاروونکي وکولای شي هغه وېب‌پاڼې چې غواړي ورته لاسرسی پیدا کړي، په اسانه پیدا او له سرورونو سره یې اړیکه ټینګه کړي. د ډومېن (سایټونو) خاوندان د خپلې پاڼې د اړیکو معلومات او نور جزئیات په دې سیستم کې ثبتوي او کاروونکي کولی شي پوښتنې وکړي او دغه معلومات ترلاسه کړي.

۱,۱۱. د کمپیوټر او (ایفون، انډرایډ) ټلفنونو لپاره د وي پي ان او « تور» براوزر څخه ګټه اخیستنه

که تاسې د انټرنټي پټو (IP) یا انټرنټي پروتوکولونو د ځانګړي ډول سیمه‌ییز بندیز سره مخ یاست، نو د یوه باوري وي پي ان (VPN) کارول ښایي له دې وضعیت څخه په ټېرېدلو او د سانسور په ماتولو کې له تاسو سره مرسته وکړي، که څه هم ممکن له محدودیتونو سره مل وي او یا هېڅ کار ونه کړي.

وي پي ان (VPN) هغه وسیله ده چې ستاسې ټوله انټرنټي ډېټا کوډ (Encryption) کوي او د بل سرور له لارې یې لېږدوي، ترڅو تاسې سره مرسته وکړي، چې هغو وېب‌پاڼو ته لاسرسی وموميء چې ستاسې په سیمه کې بندې شوې وي. دا وسیله ستاسې د انټرنټي معلوماتو لېږد د نورو له سترګو پټوي، خو پام مو وي چې د دې خدمت وړاندې کوونکی کېدای شي بیا هم د هغو وېب‌پاڼو سابقه وساتي چې تاسې یې ګورئ، یا حتی درېیم شخص او یا حکومت ته اجازه ورکړي چې ستاسې انټرنټي فعالیتونو ته مستقیم لاسرسی ولري.

که ستاسې د ډومېن سیستم بند شو یا انټرنټي پروتوکولونه غیرفعال شي او وي پي ان (VPN) هم له سانسور څخه په ټېرېدو کې مرسته ونه کړي، نو ښایي Tor براوزر له تاسې سره مرسته وکړي. دا سافټویر د دې لپاره جوړ شوی چې تاسې په انټرنټ کې ناپېژانده پاتې شئ.



تور براوزر له سانسور څخه د ټېرېدو لپاره مختلف انتخابونه لري، خو پام مو وي چې هر څوک چې ستاسې د شبکې فعالیتونه لیدلی شي، پوهېدای شي چې تاسې له دې ځانګړې وسیلې څخه ګټه اخلئ. په بېلابېلو سیسټمونو کې له (Tor) څخه د ګټې اخیستنې د څرنګوالي په اړه د پوهاوي لپاره لاندې پټو ته سر ورښکاره کړئ: (لینوکس)، (مک)، (وینډوز)، (انډرایډ)، (آیفون).

۱,۱۲. بند شویو پیغام رسوونکو اپلکیشنونو ته د لاسرسي لپاره له منځګړي سرور څخه ګټه واخلئ

که داسې حالت رامنځته شي چې «خوندي» پیغام‌رسوونکي اپلېکېشنونه لکه واتساپ یا سیګنال بند شو او تاسې یې په پرانیستلو برلاسي نه شوئ، نو ښایي د منځګړي سرور (Proxy Server) په کارولو سره وکولای شئ دا محدودیت مات کړئ. دا کار تاسې ته اجازه درکوي چې له نورو سره اړیکه وساتئ، په داسې حال کې چې اپلیکېشن بند شوی وي. منځګړي سرورونه چې د داوطلبانو له‌خوا چلول کېږي، ډاډ ورکوي چې ستاسې اړیکې له پیل څخه تر پایه پورې کوډ شوې پاتې کېږي، یعنې هېڅوک، حتی هغه څوک هم چې سرور یې فعال کړی، نه شي کولای ستاسې د پیغامونو منځپانګه وویني. خو منځګړی سرور بیا هم ستاسې د انټرنټ پته یا (IP) لیدلی شي.

د منځګړي سرور د کارولو د څرنګوالي په اړه د معلوماتو لپاره، د واتساپ لپاره دې (WhatsApp) او د سیګنال لپاره دې (Signal) پټې ته سر ورښکاره کړئ.

دوهم څپرکی
د حسابونو امنیت

۲,۱. د خپلو حسابونو خصوصي حریم او مدیریت تنظیم کړئ

خبریالان د انلاین حسابونو بېلابېل ډولونه کاروي چې پکې د دوی، د دوی د همکارانو، کورنیو او سرچینو اړوند شخصي او کاري اطلاعات موجود وي. د دغو حسابونو خوندي کول، منظم بیک‌اپ (Backup) اخیستل او د اضافي معلوماتو پاکول، د دوی د ډېټا په ساتنه کې مرسته کوي.

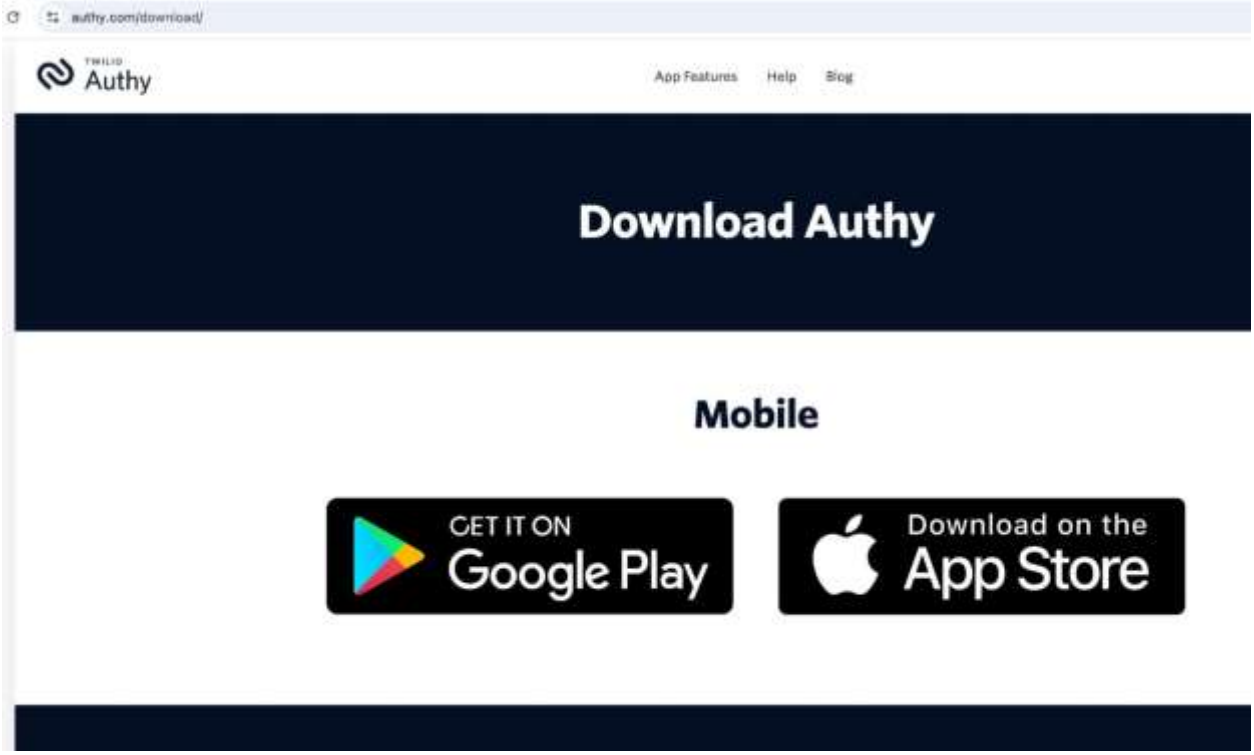
- مخکې له دې چې په انلاین پلټفارمونو کې نوم‌لیکنه وکړئ او له انلاین خدمتونو لکه ټولنیزو شبکو، پیغام‌رسوونکو اپلېکېشنونو او برېښنالیکي خدمتونو څخه ګټه اخیستل پیل کړئ، د هغوی شرایط او اصول په دقت ولولئ، څو پوه شئ چې د دغو خدمتونو مالک کوم شرکت دی او په کوم هېواد کې فعالیت کوي. همداراز وګورئ چې دغه شرکتونه ستاسې له اطلاعاتو او ډېټا سره څه کوي. پام مو وي چې که په دې معلوماتو کې د نفوذ یا د قانوني غوښتنې په صورت کې، کوم خطرونه ښایي تاسې او ستاسې سرچینې وګواښي. دا موضوع په ځانګړي ډول هغه وخت مهمه ده چې تاسې له انلاین خدمتونو څخه د سرچینو سره د اړیکو یا د هغوی د معلوماتو د ساتلو لپاره ګټه اخلئ، لکه ټولنیزې شبکې، پیغام‌رسوونکي اپلېکېشنونه او هغه خدمتونه چې غږیزې مرکې په متن بدلوي. د ټکنالوژۍ د هغو شرکتونو د شفافیت راپورونه هم ولولئ چې تاسې یې خدمتونه کاروئ، څو پوه شئ چې دوی کله او څنګه د حکومتونو هغو غوښتنو ته ځواب ورکړی چې د کاروونکو د معلوماتو د پاکولو یا سپارلو غوښتنه یې کړې ده.
- د هغو انلاین خدمتونو او اپلېکېشنونو په اړه چې تاسې یې کاروئ، تل له وروستیو معلوماتو ځان خبر وساتئ. که کومه امنیتي ستونزه یا د مالکیت بدلون پکې رامنځته شي، نو پام ورته وکړئ، ځکه دا ښایي د دې نښه وي چې د پخوا په پرتله یې امنیت کمزوری شوی دی.

۲,۲. د هویت د تایید دوه پړاویز سیستم په فعالولو سره د خپلو حسابونو امنیت لوړ کړئ

د هک پر وړاندې ستاسو له حسابونو څخه د ساتنې له تر ټولو اغېزمنو لارو څخه یوه هم د دوه پړاویز تایید (Two-factor authentication) فعالول دي. دوه پړاویز تایید یو اضافي امنیتي پوښښ دی چې اوس مهال یې ډېرې انلاین خدمتونه وړاندې کوي. د امکان په صورت کې، دا سیسټم د خپلو ټولو حسابونو لپاره فعال کړئ.

ستاسو انلاین حسابونه لکه ټولنیزې رسنۍ یا برېښنالیک، د هغو قفلونو په شان دي چې باید خوندي وساتل شي. اوس که یوازې یو ساده قفل ولرئ، ښایي څوک یې خلاص کړي، خو که څو قفلونه وي، نو د غله لپاره کار سختېږي. دوه پړاویز تایید (FA۲) دقیق همداسې کار کوي. کله چې دا سیستم فعال وي، حساب ته د ننوتلو لپاره د ساده کوډ سربېره باید یو ځانګړی کوډ هم داخل کړئ چې عموماً ستاسو ټلفون یا برېښنالیک ته لېږل کېږي. دا په دې معنا چې که څوک ستاسو کوډ هم غلا کړي، د دوهم کوډ پرته به حساب ته ډنډه نه شي.

د دوه پړاویز تایید بېلابېل ډولونه شته او تاسو کولای شئ د پیغام (SMS) پر ځای له اپلېکېشنونو لکه (Authy) څخه کار واخلئ، د دې اپلېکېشن په نصبولو سره، د تایید کوډ د دې پر ځای چې د پیغام له لارې موبایل ته راولېږل شي، همماغه اپلېکېشن ته استول کېږي چې ستاسو په ټلفن کې نصب وي. دا طریقه لا ډېره خوندي ده او د هک کېدو احتمال کموي.



د هویت د دوه پړاویز تایید دې اپلیکیشن او د نصب څرنګوالي په ټړاو د لا ډېرو معلوماتو لپاره دې پټې (Authy) ته سر ورښکاره کړئ.

ټول هغه انلاین خدمتونه چې دوه پړاویز تایید وړاندې کوي، باید تاسو ته د بیک‌اپ کوډونه (Backup codes) هم درکړي، څو که مو له دې لارې حساب ته لاسرسی ونه موند، وکولای شئ له دغو کوډونو ګټه واخلئ. دا کوډونه یو ځل کارېدونکي وي او تاسو یې د ټلفن یا اپلېکېشن له لارې د کوډ ترلاسه کولو پر ځای کارولی شئ. پام مو وي چې د دغو بیک‌اپ (Backup) کوډونو یوه نسخه وساتئ، کولای شئ چاپ یې کړئ، یا یې په خوندي ځای کې کېږدئ او یا یې د کوډونو د مدیریت په پروګرام کې ذخیره کړئ.

د دوه پړاویز تایید ترځنګ، داسې کوډونه جوړ کړئ چې له ١٦ تورو څخه اوږده وي. دا کوډونه باید د شمېرو، نښو او تورو ګډ ترکیب ولري. د پخوانیو کوډونو له بیا کارولو ډډه وکړئ او شخصي معلومات لکه د زېږېدو نېټه مه کاروئ، ځکه دا ډول معلومات په اسانی سره په انټرنټ کې موندل کېدای شي.

٢,٣. د خپلې وسیلې لپاره د کوډونو مدیریت رامنځته کړئ

د کوډونو مدیر (Password Manager) چې د کوډونو د اتومات دننه کولو (Auto-fill) ځانګړتیا لري، کوډونه په وېب‌پاڼو کې ساتي او په اوتومات ډول یې ستاسو حساب ته د ننوتلو پر مهال دننه کوي. که څه هم کاروونکي کله ناکله د ننوتلو په جعلي پاڼو دوکه کېدای شي، خو د کوډونو مدیر دا ټېروتنه نه کوي، ځکه جعلي پاڼې پېژني او خبرداری ورکوي یا د کوډ له دننه کولو څخه مخنیوی کوي. غوره ده، چې د خپل حساب د امنیت لوړولو لپاره، له ناڅاپي، تصادفي او اوږدو کوډونو څخه کار واخلئ، هغه کوډونه چې د تورو، شمېرو او نښو په تصادفي او بې‌نظمه ترکیب جوړ شوي وي. که د کوډونو د مدیریت اپلېکېشن د کوډ له ډکولو څخه ډډه وکړه، باید احتیاط وکړئ

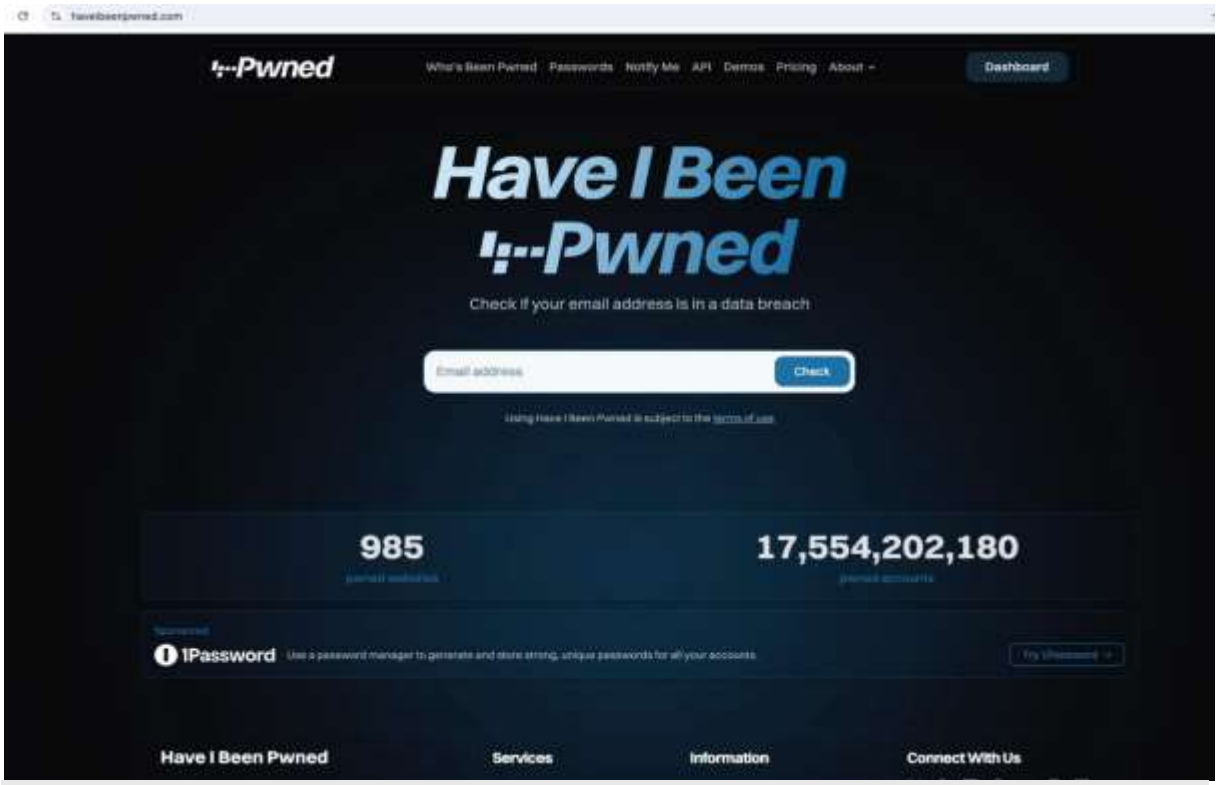
او د ویب‌پاڼې رښتینولۍ د هغې د ویب‌پتې (URL) له لارې وڅېړئ، یا هم د براوزر د پته لیکې (Address Bar) له لارې نېغ په نېغه خپل حساب ته ننوځئ یا (Login) شئ.

د کوډونو مدیر د ټاکلو او نصبولو لپاره، لومړی باید یو مناسب اپلېکېشن په خپل کمپیوټر یا موبایل کې نصب کړئ.

(LastPass)، (Dashlane)،(1Password)، او (Bitwarden)د هغو مشهور اپلېکېشنونه له ډلې دي چې د کوډونو مدیریت لپاره کارول کېږي. تاسو کولای شئ تر ارزونې وروسته، د خپلې خوښې مطابق له یادو اپلکېشنونو څخه یو نصب کړئ.

۲,۴. د خپلو حسابونو منځپانګه مدیریت کړئ

- په پام کې ونیسئ چې ستاسو په هر حساب کې کوم اطلاعات ساتل شوي دي او که ستاسو حساب ته نفوذ وشي، نو تاسو، ستاسو کورنۍ او ستاسو سرچینو ته به څه پایلې ولري.
- په انټرنټ کې خپل کاري او شخصي ژوند جلا وساتئ او په یوه حساب کې د مسلکي او شخصي اطلاعاتو له ګډولو څخه ډډه وکړئ. دا کار د دې سبب کېږي چې که ستاسو له حسابونو څخه یو ته نفوذ وشي، نو نورو معلوماتو ته د لاسرسي خطر محدود پاتې کېږي.
- د خپل خصوصي حریم (Privacy) پر تنظیماتو بیا کتنه وکړئ او وټاکئ چې کوم اطلاعات، په ځانګړي ډول په ټولنیزو شبکو کې، عام شکاره شي. هر هغه معلومات چې نه غواړئ نور خلک یې ووینې، پاک یا پټ کړئ. د بېلګې په توګه، په فېسبوک کې د نښې لوري پورته برخه کې پر خپل نوم کلیک وکړئ، بیا (Settings & Privacy) ته لاړ شئ او وروسته (Privacy Checkup) وټاکئ. په دې برخه کې د فېسبوک د خصوصي حریم د تنظیم او مدیریت لپاره بېلابېل انتخابونه ځای پر ځای شوي دي.
- د هر ډول حساسو معلوماتو یا هغو مواردو بیک‌اپ (Backup) واخلئ چې نه غواړئ عام شي، لکه شخصي پیغامونه او برېښنالیکونه او په بل خوندي ځای کې یې وساتئ. له بیک‌اپ (Backup) اخیستلو وروسته، دا معلومات له خپل حساب یا وسیلې څخه پاک کړئ، څو د غیرمجاز لاسرسي مخه ونیول شي. که غواړئ خپل معلومات په انلاین فضا لکه Google Drive، Dropbox یا OneDrive او یا هم په لېږد وړ بهرنیو حافظو (External Drives) کې وساتئ، ډاډ ترلاسه کړئ چې فایلونه په سمه توګه کوډ (Encryption) شوي وي، څو د غیرمجاز لاسرسي پر وړاندې په سمه توګه خوندي پاتې شي.
- هغه حسابونه چې نور یې نه کاروئ، لکه برېښنالیکونه، د ټولنیزو شبکو حسابونه او یا په انلاین پلورنځیو کې خپل حسابونه، پاک کړئ. په یاد ولرئ چې له پاکولو مخکې د هغو اطلاعاتو یوه کاپي وساتئ چې اړتیا ورته لرئ. د هر حساب له دایمي ترلو وړاندې، ټول معلومات تري پاک کړئ.



- د دې لپاره چې ډاډ ترلاسه کړئ ستاسو حسابونه هک شوي یا له امنیتي تیري سره مخ شوي دي که نه، د (haveibeenpwned.com) وېبپاڼې ته لاړ شئ او د خپل بریښنالیک په داخلولو سره د پلټنې پایله وګورئ. که پوه شوئ چې ستاسو حساب ته نفوذ شوی، نو هماغه حساب ته ننوځئ او خپل کوډ بدل کړئ. که نور نه غواړئ له هغه حسابه څخه ګټه واخلئ، نو د حساب له پاکولو مخکې ټوله منځپانګه پاکه کړئ.
- که د نیول کېدو له خطر سره مخ یاست، یا اندېښنه لرئ چې څوک مو وسایلو ته غیرمجاز لاسرسی پیدا نه کړي، نو د برېښنالیکونو او ټولنیزو شبکو په ګډون، له خپلو حسابونو څخه د ګټې اخیستنې وروسته حتماً له سیستم څخه ووځئ او د خپل براوزر تاریخچه پاکه کړئ. د بېلګې په توګه، په (Google Chrome) یا (Microsoft Edge) کې د ښي لوري پورتني اړخ کې پر درې ټکو کلیک وکړئ، بیا (History) انتخاب کړئ او د لټون سابقه پاکه کړئ. د براوزر د لا ښه مدیریت او نورو انتخابونو لپاره د (Settings) برخې ته لاړ شئ. بله بېلګه: که غواړئ دا کار په فېسبوک کې ترسره کړئ، خپل حساب ته ننوځئ، پر درې ټکو کلیک وکړئ او د (Activity Log) له لارې د خپلو فعالیتونو او لټونونو سابقه پاکه کړئ.
- په منظم ډول د خپلو حسابونو د فعالیت برخه یا (Account Activity) وڅارئ، څو وګورئ چې آیا ستاسو حساب ته له ناپېژانده وسایلو څخه څوک دننه شوي چې تاسو یې نه پېژنئ که نه. که کومه ناپېژانده وسیله مو حساب ته ننوتې وي، نو سمدستي خپل حساب له هغې وسیلې څخه (Log out) کړئ.
- د عامه کمپیوټرونو لکه کافينټونو او یا د نورو کسانو د ځیرکو موبایلونو له لارې خپلو حسابونو ته له ننوتلو ډډه وکړئ. که بله لار نه وي، نو له ګټې اخیستنې سمدستي وروسته له خپل حساب څخه (Log out) ووځئ او د براوزر تاریخچه پاکه کړئ.

درېيم څپرکی
د سايبري بريدونو پر وړاندې ساتنه

۳,۱. سايبري دوکه کوونکي بريدونه وپېژنئ او پر وړاندې يې چمتووالی ونيسئ

د خپلو دښمنانو يا بدغوښتونکو تخنيکي وړتياوې وارزوئ، څو احتمالي ګواښونه او دا چې تاسو يا ستاسو نږدې کسان څنګه هدف ګرځېدلی شي، درک کړئ. دا ارزونه له تاسو سره مرسته کوي چې د سايبري دوکه کوونکو بريدونو (Phishing) پر وړاندې خپل امنيت لا پياوړی کړئ. خبريالان ډېری وخت يو عمومي پروفايل لري او د اړيکو معلومات يې د دې لپاره شريک وي چې خبرونه، معلومات او سرچينې ترلاسه کړي. هغه بدغوښتونکي او هکران چې غواړي د خبريالانو معلوماتو او وسايلو ته لاسرسی پيدا کړي، کولای شي خپله خبريال، د هغه همکاران يا د کورنۍ غړي د دوکه کوونکو بريدونو موخه وګرځوي.

دا ډول بريدونه معمولاً د برېښنالیکونو، لنډو پيغامونو (SMS)، د ټولنيزو شبکو د پيغام‌رسوونکو اپليکېشنونو يا شخصي چټونو له لارې ترسره کېږي، چې په ظاهره باوري او قانوني ښکاري. دغه پيغامونه داسې جوړ شوي وي چې ترلاسه کوونکی وغولوي او اړ يې کړي چې حساس معلومات ورکړي، پر زيانمنو ټرونو (لينکونو) کليک وکړي، يا ککړ فايلونه ډانلوډ کړي، څو زيانمنوونکي پروګرامونه نصب شي.

د زيانمنوونکو پروګرامونو (Malware) او جاسوسي وسايلو بېلابېل ډولونه شته چې د پېچلتيا له پلوه توپير لري. خو تر ټولو پرمختللي ډولونه يې کولای شي بريدګر ته دا زمينه برابره کړي چې له لرې واټنه د خبريال وسيلې او ټولو معلوماتو ته لاسرسی پيدا کړي، پرته له دې چې کارووونکی پرې خبر شي.

۳,۲. تلفني دوکه کوونکي بريدونه جدي وګڼئ او د مخنيوي لارې يې زده کړئ

ټلفوني دوکه کوونکي بريدونه (Vishing) د ډيجيټلي درغلۍ يو ډول دی، چې موخه يې د ټلفني اړيکو له لارې د قربانيانو د حساسو او شخصي معلوماتو غلا کول دي. په دې طريقه کې مجرمان د ټولنيزې انجنيرۍ له لارو ګټه اخلي، ټلفني اړيکې نيسي او ځانونه د بانکونو، ټکنالوژۍ شرکتونو، دولتي يا نړيوالو ادارو استازي معرفي کوي.

د دغو بريدونو اصلي موخه دا وي چې قربانيان وهڅوي څو مهم معلومات لکه د بانکي کارت شمېره، کوډ، ملي شمېره او يا د بانکي حسابونو معلومات افشا کړي. دا ډول بريدونه له انلاين دوکه کوونکو بريدونو (Phishing) سره ډېر ورته والی لري، خو پکې د برېښنالیک يا ټروني (لينک) د لېږلو پر ځای مستقيمه ټلفوني اړيکه کارول کېږي.

د دې ډول بريدونو څخه د خوندي پاتې کېدو لپاره، له ناپېژاندو او مشکوکو اړيکو سره ډېر احتياط وکړئ. حساس معلومات يوازې هغه وخت شريک کړئ چې د اړيکه نيوونکي هويت مو په بشپړه توګه تاييد کړی وي. په ټلفني اړيکو کې هېڅکله بانکي رمزونه، د کارت شمېره يا شخصي معلومات له بشپړ ډاډ پرته مه ورکوئ. غوره ده چې له هر اقدام مخکې د رسمي وېب‌پاڼو له لارې يا له رسمي شمېرو سره د مستقيمې اړيکې په وسيله د اړيکې ريښتينوالی وڅېړئ. همدارنګه په بانکي حسابونو او برېښنالیکونو کې د امنيتي سيستمونو لکه څو پراويز تاييد (دوه پراويز) کارول مرسته کوي څو مجرمين ستاسې حياتي معلوماتو ته لاسرسی پيدا نه کړي.

۳,۳. سافټویرونه تازه (Update) کړئ

د سافټویرونو د اتومات تازه کېدلو (Software Updates) ځانګړنه فعاله کړئ. دا کار هغه پېژندل شوې امنیتي نیمګړتیاوې له منځه وړي چې زیانمنوونکي پروګرامونه یې ستاسو سیسټم ته د نفوذ لپاره کارولی شي. ډېرى دوکه کوونکي سایبري بریدونه (Phishing Attacks) چې له زیانمنوونکو پروګرامونو (malware) څخه ګټه اخلي، د سافټویرونو پر امنیتي کمزوریو تکیه لري. د زیانمنوونکو پروګرامو او جاسوسي پروګرامونو بېلابېل ډولونه شته، چې تر ټولو پرمختللي بېلګې یې بریدګر ته دا توان ورکوي چې له لرې واټنه د قرباني وسایلو لکه کمپیوټر او موبایل او همداراز د هغوی ټولو معلوماتو ته بشپړ لاسرسی پیدا کړي. کله چې کومه امنیتي نیمګړتیا یا زیانمنوونکې خلا ومومدل شي، د سافټویر جوړوونکي تازه (Update) نسخې خپروي، څو دغه ستونزه حل شي. د سافټویرونو له زړو نسخو څخه ګټه اخیستنه د سایبري بریدونو او نفوذ خطر زیاتوي، ځکه زاړه سافټویرونه ښایي داسې امنیتي کمزورۍ ولري چې بریدګر تري ناوړه ګټه واخلي او ستاسو پر سیستم زیانمنوونکي پروګرامونه نصب کړي.

۳,۴. شکمن پیغامونه او برېښنالیکونه له رالېږونکي سره وڅېړئ

د دې لپاره چې ډاډ ترلاسه کړئ ترلاسه شوی برېښنالیک یا پیغام جعلي او دوکه کوونکی نه دی، له بلې لارې له هغه کس سره اړیکه ونیسئ چې ادعا کوي پیغام یې درلېږلی دی او ترې وغواړئ چې د برېښنالیک متن درته کاپي کړي یا د فایل د پرانیستل شوي حالت انځورونه درولېږي، څو ډاډ ترلاسه کړئ چې فایل ککړ او زیانمن نه دی. د بېلګې په توګه، که ستاسو بانک داسې برېښنالیک درلېږلی وي چې مشکوک لینکونه پکې وي، نو مستقیم د بانک رسمي وېب‌پاڼې ته لاړ شئ یا د بانک رسمي شمېرې ته زنګ ووهئ. یا که ستاسو کوم ملګري یا اشنا کس د برېښنالیک له لارې په غیرعادي ډول انځورونه درلېږلي وي، هغه ته یو پیغام واستوئ او د برېښنالیک او ضمیمه شوي فایل جزئیات ورسره وڅېړئ. دا کار تاسو له دې څخه ساتي چې د جعلي برېښنالیکونو په دام کې ولوېږئ. همداراز له هغو برېښنالیکونو سره ډېر احتیاط وکړئ، چې مشکوکې غوښتنې پکې شوې وي: دوکه کوونکي برېښنالیکونه ښایي ادعا وکړي چې د ټکنالوژۍ شرکتونو یا د انټرنټ د تخنیکي ملاتړ له خوا دي او له تاسو وغواړي چې خپل رمز، حساس معلومات یا د سیسټم د جوړولو او یا د ستونزې د حل لپاره د لرې واټن لاسرسی ورکړئ، څو یو تخنیکي کس مو سیسټم ته داخل شي او ستونزه حل کړي. هېڅکله پر داسې غوښتنو باور مه کوئ او تر هر اقدام مخکې د سرچینې رښتینولي او اعتبار وڅېړئ. معتبر او رسمي شرکتونه معمولاً د تخنیکي ملاتړ په اړیکو کې له کارووونکو څخه دا ډول غوښتنې نه کوي.

۳,۵. شکمن فایلونه په خوندي پلتفارمونو کې پرانیزئ

ځینې خبریالان تمه لري چې د برېښنالیک یا د هغه ضمیمه شوي فایلونه له ناپېژانده کسانو ترلاسه کړي. د بېلګې په توګه، خبریالان ډېرى وخت له بېلابېلو سرچینو اسناد تر لاسه کوي. خو دا معلومول چې د (Word،(Excel یا (PDF) فایلونه زیانمن پروګرامونه نه لري، ستونزمن کار کېدای شي. په داسې حالتونو کې هېڅکله پر ډاونلوډ شوي فایل دوه ځله کلیک مه کوئ. پر ځای یې، فایل نورر پروګرامونو لکه (Google Drive) ته پورته (Upload) کړئ او هلته یې وګورئ. دا کار فایل په انټرنېټ یا وېب‌پاڼه (HTML) بدلوي او په دې توګه ستاسو پر وسیله د زیانمنوونکو پروګرامونو د نصبېدو احتمال ډېر کمېږي.

که تاسو د نویو سافټویرونو له زده‌کړې سره راحت یاست او دومره ډېر شکمن برېښنالیکونه ترلاسه کوئ چې د اضافي وخت د مصرفولو ارزښت لري، نو سپارښتنه کېږي چې له ځانګړو عملیاتي سیستمونو څخه کار واخلئ چې د زیانمنوونکو پروګرامونو اغېز محدودوي.

د (Tails) او (QubesOS) په څېر عملياتي سيسټمونه کولای شي ستاسو امنيت د سايبري بريدونو پر وړاندې زيات کړي، ځکه دا سيستمونه داسې جوړ شوي چې د زيانمنوونکو پروګرامونو اغېز محدودوي. دواړه سيستمونه د لپټاپونو او ډيکسټاپ کمپيوټرونو لپاره طرحه شوي دي.

تاسو همداراز کولای شئ شکمن او نامطمئن ټرونې (لینکونه) او فایلونه (VirusTotal) ته پورته (Upload) کړئ. دا په اصل کې یو انلاین خدمت دی چې فایلونه او ټرونې (لینکونه) د زیانمنوونکو پروګرامونو او ویروسونو د پېژندلو لپاره آنالایز (Analysis) او سکن کوي او

ګوري چې آيا په زيانمنوونکو پروګرامونو ککړ دي که نه. دا خدمت فايلونه او ټرونې د بېلابېلو انټي‌ويروس موتورونـو لـه لارې ارزوي او پايلې يې وړاندې کوي. که څه هم دا حل لاره بشپړه نه ده او شايي نوي ويروسونه يا هدفي بريدونه ونه پېژني، خو بيا هم تر هېڅ شه ده. په ياد ولرئ چې هر فايل يا ټرونی چې تاسو يې عامو وېب‌سـايټونو لکـه (VirusTotal) يـا (Google Drive) تـه پورتـه کـوئ، شـايي د هماغه شرکت کارکوونکي يا هغه کسان يې ووينې چې دغو سايټونو ته لاسرسی لري. نو که په فايل کې حساس يا محـرم معلومـات وي، غوره ده له نورو خوندي لارو ګټه واخلئ.

۳,٦. خپلو حسابونو ته د ننوتلو لپاره له امنيتي کيلي څخه ګټه واخلئ

ځينې وېب‌پاڼې تاسو ته دا امکان درکوي چې د دوکه کوونکو بريدونو د مخنيوي او لا زيات امنيت لپاره له ځانګړو هارډوير کيلي ګانو (Hardware Token) څخه ګټه واخلئ. دا وسايل ستاسو له براوزر (Browser) سره اړيکه نيسي، څو وېب‌پاڼې ته د ننوتلو لپاره د هويت د تصديق بهير ترسره کړي. دې طريقې ته «نړيوال دوهم عامل» يا (U۲F) ويل کېږي. دا يو معياري امنيتي ميتود دی چې د کوډ ترځنګ د هويت د تاييد دوهم پړاو هم زياتوي. د دې طريقې د کارولو لپاره، تاسو لومړی وېب‌پاڼې ته ننوځئ، بيا کله چې له تاسو وغوښتل شول، امنيتي کيلي له خپل کمپيوټر يا موبايل سره ونښلوئ او د ننوتلو تڼۍ يې کېکاړئ. که هغه وېب‌پاڼه جعلي وي، براوزر يې تشخيصوي او اجازه نه ورکوي چې تاسو وردننه شئ. نو حتی که کوم خرابکار ستاسو کوډ هم غلا کړي، بيا هم نشي کولای ستاسو حساب له خطر سره مخ کړي. دا امنيتي حل لارې ستاسو حساب د هکرانو پر وړاندې خوندي ساتي.

YubiKey شرکت (د دغو امنيتي کيلي ګانو له مشهورو جوړونکو څخه)، د U۲F ټکنالوژی په اړه نور معلومات وړاندې کوي. دا طريقه له عادي «دوه پړاويز تاييد» (Two-Factor Authentication) څخه توپير لري، ځکه امنيت يې لا قوي دی. هغه کسان چې د هک کېدو له لوړ خطر سره مخ وي، کولای شي د ياد شرکت امنيتي کيلي وکاروي. دا يو کوچنی او د لېږد وړ وسيله ده چې د کمپيوټر يا نورو وسايلو سره په نښلېدو، د فزيکي امنيتي کيلي په توګه کار کوي.

۳,۷. د شکمنو غوښتنو درلودونکو برېښنالیکونو پر وړاندې له دقت څخه کار واخلئ

- د هغه څه منځپانګه چې ترلاسه کوئ يې، په دقت وڅېړئ: له هغو برېښنالیکونو او پیغامونو سره په احتیاط چلند وکړئ چې له تاسو غواړي یو کار په بېړه ترسره کړئ، یا ډېرې جذابې او غیرواقعي ژمنې کوي. دوکه کوونکي برېښنالیکونه ښایي ادعا وکړي چې د ټکنالوژۍ شرکتونو یا د انټرنټ د تخنیکي ملاتړ له خوا دي او له تاسو وغواړي چې خپل کوډ یا حساس معلومات ورولېږئ، یا کوم داسې کس ته چې ځان د سیسټم د ترمیم متخصص درپېژني، اجازه ورکړئ څو ستاسو سیسټم ته له لرې واټنه داخل شي. هېڅکله پر دغسې غوښتنو باور مه کوئ او تر هر اقدام مخکې د سرچینې رښتینولي او اعتبار وڅېړئ. معتبر او رسمي شرکتونه معمولاً د تخنیکي ملاتړ پر مهال دا ډول غوښتنې نه کوي.
- د ضمیمه یا هم د بریښنالیک ضمیمه شوي فایلونه له ښکته کولو یا ډاونلوډ مخکې وګورئ. یعنې پر فایل کلیک وکړئ او د فایل انځور یا د منځپانګې لنډیز وګورئ. که شک لرئ، له لېږونکي سره اړیکه ونیسئ او تري وغواړئ چې منځپانګه د متن یا انځورونو په بڼه دروښيي.
- په خپل برېښنالیک کې د بهرنیو انځورونو د ښودلو تنظیمات جوړ کړئ. په برېښنالیکونو کې انځورونه د دې لپاره کارېدلی شي چې معلومه کړي کوم کس او په کوم وخت کې برېښنالیک پرانیستی دی. ښایي تاسو له ډېرو ورته تبلیغاتي برېښنالیکونو سره مخ شوي یاست، خو همدا طریقه په دوکه کوونکو بریدونو کې هم کارول کېږي. نو د خپل محرمیت د خوندي ساتلو لپاره غوره ده داسې تنظیمات وکړئ چې ستاسو بریښنالیک — که Outlook وي او که Gmail — د بهرنیو انځورونو له ښودلو مخکې له تاسو اجازه وغواړي. د دې لپاره د برېښنالیک (ngs برخې ته لاړ شئ، بیا د (Privacy) یا (Images / External Images) برخه پرانیزئ او د (Ask before displaying external images) برخه فعاله کړئ. دا کار ستاسو د فعالیت د څار مخه نیسي او د برېښنالیکونو امنیت مو لوړوي.
- مخکې له دې چې پر ټرونو (لینکونو) کلیک وکړئ، ماوز (Cursor / Mouse Pointer) پرې ودروئ، څو وګورئ چې د هغه (URL) یا ویب پته څنګه ښکاري او معتبره برېښي که نه. د لېږونکي د حساب جزئیات او د پیغام منځپانګه په دقت وڅېړئ، څو ډاډ ترلاسه کړئ چې معتبر دی. په املا، ګرامر، بڼه یا د خبرو په طرز کې کوچني توپیرونه ښایي د جعل، دوکې یا د حساب د هک کولو نښه وي. ټروني (لینکونه) کېدای شي د ورته تورو یا هغو ډومېنو نومونو (Domain) په کارولو سره، چې له اصلي او قانوني ډومېنونو سره توپیر لري، تاسو داسې وېبپاڼې ته هدایت کړي چې ظاهراً د هغو خدمتونو په څېر ښکاري چې تاسو يې کاروئ، لکه (Gmail) یا (Dropbox) .
- په ډلهییزو چټونو او ګروپي پیغامونو کې، په ځانګړي ډول په واتساپ کې، له مشکوکو لینکونو او فایلونو سره ډېر احتیاط وکړئ. واکمن چارواکي یا مجرمان ښایي د ډېرو غړو لرونکو ګروپونو چټونو ته نفوذ وکړي او د ککړو لینکونو او فایلونو له لارې کارووونکي موخه وګرځوي.
- د امکان په صورت کې، د پیغامونو او ټرونو (لینکونو) د ارزونې لپاره د اپلېکېشنونو د کمپیوټري نسخې (Desktop) څخه کار واخلئ. لویه صفحه مرسته کوي چې ترلاسه شوې منځپانګه ښه وارزوئ او په یو وخت کې د څو کارونو د ترسره کولو احتمال کم شي.

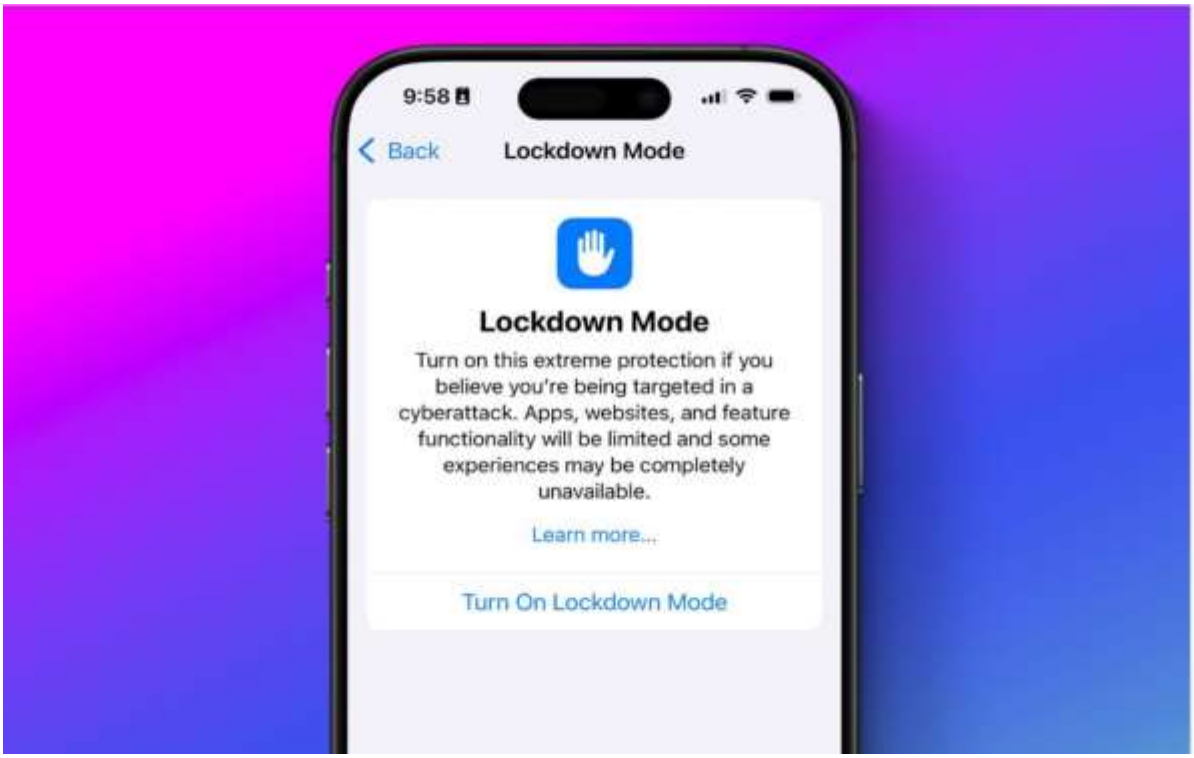
څلورم څپرکی
د وسایلو او تجهیزاتو امنیت

۴,۱. د کمپیوټر او ګرځنده ټلفن بشپړ کوډول

خبریالان د منځپانګې د تولید، ساتنې او له سرچینو سره د اړیکو لپاره له ګڼو وسایلو څخه کار اخلي. ډېرى خبریالان هماغه وسایل هم په کور او هم د کار په ځای کې کاروي، چې که ورک، غلا یا ضبط او مصادره شي، ښایي د هغوی ډېر معلومات افشا شي. له همدې امله خبریالان باید خپل کمپیوټرونه، موبایلونه، ټابلیټونه او بهرني حافظې لکه (flash drive یا USB) کوډ (Encryption) کړي، څو نور کسان ونشي کولای له کوډ پرته معلوماتو ته لاسرسی ولري.

دا امنیتي ټکي له تاسو سره مرسته کوي، چې د خپلو وسایلو او معلوماتو د ساتنې لپاره غوره لارې چارې زده کړئ:

- خپل کمپیوټر، موبایل، براوزرونه او اپلیکېشنونه پر اتومات تازه کېدلو (Update Automatically) تنظیم کړئ.
- خپل کمپیوټر کوډ (Encryption) کړئ. د معلوماتو د خوندي ساتلو لپاره، که د (mac) سیستم کاروئ، د (FireVault) پروګرام نصب کړئ. که د وینډوز سیستم کاروئ، (Bitlocker) فعال کړئ. د لینوکس سیستمونو لپاره له LUKS څخه ګټه واخلئ.
- خپل موبایل کوډ (Encryption) کړئ. په انډرایډ موبایلونو کې د کوډولو (Encryption) د فعالولو لپاره Settings > Security > Encrypt Your iPhone ته لاړ شئ. ایفونونه له ۲۰۱۴ کال راهیسې وار له مخې کوډ شوي دي.
- که iCloud لرئ، خپل حساب د (Advanced Data Protection) په فعالولو سره نور هم خوندي کړئ. ای‌کلاوډ د اپل شرکت د کلوډ یا مجازي حافظې (Cloud) یوه برخه ده، چې (انځورونه، اړیکې، پیغامونه او نور فایلونه) پکې ساتل او بیک‌اپ (Backup) کېدای شي.
- یوه منظمه برنامه جوړه کړئ چې په وسایلو کې ساتل شوي معلومات وڅېړئ، بیک‌اپ (Backup) ترې واخلئ او هغه معلومات پاک کړئ چې نه غواړئ نور ورته لاسرسی ولري.
- حساس اطلاعات او بیک‌اپونه (Backup) بهرنیو حافظو (External Hard Drive) ته انتقال او کوډ (Encryption) کړئ.
- خپل وسایل د کوډ یا (PIN Code) په وسیله قفل کړئ. که د تلاشي پوستو یا سرحدونو له لارې تېرېږئ او د وسایلو د پلټنې، ضبط یا مصادرې اندېښنه لرئ، نو د بایومتریک امنیتي سیستمونو لکه (د ګوتې نښه یا د څېرې پېژندنه) مه کاروئ. د کوډ او PIN کارول وسایلو ته لاسرسی سختوي او ستاسو د محرمیت په ساتنه کې اغېزناک دي.
- په خپلو وسایلو لکه کمپیوټر او موبایل کې د اپلیکېشنونو تنظیمات وڅېړئ او هغه اختیارونه محدود کړئ چې ستاسو د معلوماتو راټولولو ته اجازه ورکوي. د دې لپاره د وسیلې یا اپلیکېشن Settings ته لاړ شئ، بیا د (Security & Privacy) برخه په دقت وګورئ او اړین اقدامات ترسره کړئ.
- له خپلو وسایلو څخه غیر ضروري یا اضافي اپلکېشنونه پاک کړئ.



سرچينه: EFF

- که د Apple وسایل کاروئ او اندښنه لرئ چې د جاسوسي سافټویرونو هدف وګرځئ، نو د خپل آی‌کلوډ (icloud) حساب په ټولو اړوندو برخو کې د «Lockdown Mode» یا امنیتي قفل حالت فعال کړئ.
- که د اندرایډ موبایل کاروئ، هغه بند کړئ او لږ تر لږه په ورځ کې یې یو ځل ګل او روښانه کړئ، څو زیانمن سافټویرونه، په ځانګړي ډول د جاسوسي پروګرامونه، له منځه ولاړ شي.
- مخکې له دې چې خپل کمپیوټر کوډ (Encrypt) کړئ، یو اوږد او قوي کوډ جوړ کړئ چې په هېڅ بل حساب یا وسیله کې نه وي کارول شوی. دغه کوډ باید لږ تر لږه ۱۵ کرکټرونه ولري او د شمېرو، نښو او تورو ګډ ترکیب پکې وي یا له داسې بې‌اړیکو کلمو جوړ وي چې له یو بل سره تړاو ونه لري.
- پام مو وي چې هر څوک ستاسې کوډ ته لاسرسی ولري، یا تاسې دې ته اړ کړي چې د خپلې وسیلې کوډ خلاص کړئ، هغه به ستاسې معلوماتو ته هم لاسرسی پیدا کړي.
- د شپې له خوا یا هغه وخت چې له خپلو وسایلو کټه نه اخلئ، بند یې کړئ، په ځانګړي ډول که اندښنه لرئ چې د چارواکو له لوري به ضبط یا تلاشي شي. د وسیلې بندول د کوډ ځانګړنه فعاله ساتي او له بیا روښانه کېدو وروسته د خلاصولو لپاره کوډ ته اړتیا وي.
- هر وخت چې غوښتنه وشوه، د خپل عملیاتي سیستم، پروګرامونه او براوزرونه تازه (Update) کړئ. زاړه سافټویرونه امنیتي کمزورۍ لري او کېدای شي ستاسې په وسیلو کې د زیانمنوونکو پروګرامونو د نصب زمینه برابره کړي. دا موضوع په ځانګړي ډول هغه وخت ډېره مهمه ده چې احساس کوئ ښایي د پرمختللو جاسوسي سافټویرونو هدف وګرځئ.
- په خپلو وسایلو کې خوندي شوي معلومات وڅېړئ او فکر وکړئ چې دا معلومات څنګه تاسې یا نور خلک له خطر سره مخ کولای شي.
- په منظم ډول حساس اطلاعات، په ځانګړي ډول هغه پیغامونه چې ترلاسه کړي یا استولي مو دي، پاک کړئ. د دې لپاره چې دښمن ونه شي کولای پاک شوي فایلونه بېرته ترلاسه کړي، که ممکن وي د پاکولو خوندي (Secure Delete) سافټویر وکاروئ

څو وسیله بشپړه پاکه کړي، که دا امکان نه وي، نو وسیله بیا ریسیټ (Reset) کړئ. له هغو اطلاعاتو څخه چې ساتل یې غواړئ، بیک‌اپ (Backup) واخلئ، که نه ټول اطلاعات به مو له منځه ولاړ شي. پام مو وي چې حکومتونه یا هغه کسان چې تخنیکي مهارتونه لري، شایي پاک شوي اطلاعات بېرته ترلاسه کړای شي.

- په منظم ډول د خپلو وسیلو له فایلونو بیک‌اپ (Backup) واخلئ، څو که وسیله خرابه، ورکه یا غلا شوه، اطلاعات مو خوندي پاتې شي. دغه بیک‌اپونه کوډ (Encrypt) کړئ او له کور یا دفتره بهر یې وساتئ، په ځانګړي ډول په بهرني هارډ ډرایفونو (External Drive) کې یې وساتئ.
- په ګرځنده ټلفنونو کې هغه فایلونه، انځورونه او ویډیوګانې چې تاسو یې پاکوئ، په لنډ مهاله ډول بل ځای ته لېږدول کېږي او ترڅو چې له هغه ځایه هم پاکې نه‌شي، په اسانۍ سره بېرته ترلاسه کېدلای شي. په سامسونګ موبایلونو کې، د فایل تر پاکولو وروسته باید د «ګالري» یا « د فایلونو مدیریت» برخې ته ننوځئ او د «Trash» برخه پیدا کړئ، که هلته فایلونه موجود وي، هغه هم پاک کړئ ترڅو بشپړ له منځه ولاړ شي او د بېرته راګرځولو امکان یې کم شي. خو په ایفون کې، پاک شوي فایلونه نېغ په نېغه د (Recently Deleted) یا «وروستي پاک شوي» برخې ته ځي. د بشپړ پاکولو لپاره باید دې برخې ته داخل شئ او بیا د (Delete All) یا «ټول پاک کړه» تڼۍ کېکاږئ. دا بهیر ډاډ ورکوي چې فایلونه په بشپړ ډول له وسیلې څخه پاک شوي او بېرته ترلاسه کول یې ډېر ستونزمن یا ناممکن ګرځي.
- پام مو وي چې ستاسې وسیله شایي خپل معلومات د موبایل له اړوند کلاوډ حساب (Cloud Account) سره ذخیره کړي. په مجازي فضا کې خوندي شوي معلومات شایي کوډ (Encryption) شوي نه وي. د دې کار د مخنیوي لپاره، د تنظیماتو په برخه کې د اتومات بیک‌اپ (Automatic Backups) ځانګړنه غیرفعاله کړئ.
- خپل وسایل په عامه ځایونو کې، په ځانګړي ډول د چارج پر مهال، بې پامه مه پرېږدئ، ځکه غلا کېدای شي یا زیانمنوونکي پروګرامونه پکې نصب کېدای شي.
- له هغو جانبي حافظو (USB Drive) څخه ګټه مه اخلئ چې په ځینو مراسمو کې وړیا ورکول کېږي. امکان لري دغه حافظې ویروسونه یا نور زیانمن پروګرامونه ولري چې ستاسې کمپیوټر ککړ کړي.

۴,۲. د خپلو وسایلو منځپانګه له لرې واټن پاکه کړئ

په خپلو وسایلو کې داسې تنظیمات فعال کړئ چې وکولای شئ د اړتیا پر وخت یې اطلاعات له لرې واټنه پاک کړئ:

- په انډرایډ وسایلو کې د دې ځانګړنې د فعالولو لپاره، د Settings برخې ته لاړ شئ او د (Find My Device) او (Location) برخې فعاله کړئ. وروسته، د هغه ګوګل حساب له لارې چې ستاسې وسیله ورسره تړلې ده، د (Erase Device) یا د وسیلې د پاکولو برخه انتخاب کړئ. په ایفون کې، د Settings برخې ته لاړ شئ او د (Find My iPhone) او (Send Last Location) برخې فعالې کړئ، بیا د Apple ID له لارې خپل حساب ته ننوځئ او د وسیلې د پاکولو برخه پیدا کړئ.
- د دې لپاره چې وکولای شئ د خپلو وسایلو ډېټا له لرې واټنه پاکه کړئ، اړین تنظیمات باید مخکې له هرې ستونزې فعال شوي وي. دا ځانګړنه باید له مخکې فعاله وي، یعنې تر هر ډول پېښې وړاندې له لرې واټن د پاکولو تنظیمات بشپړ کړئ. پام مو وي چې وسیله یوازې هغه وخت له لرې واټن پاکېدلای شي چې د (Wi-Fi) یا د موبایل شبکې له لارې انټرنټ سره نښلول شوې وي. که وسیله غلا یا ضبط شي او د الوتکې حالت (Airplane Mode) فعال شي، نو له لرې واټن د معلوماتو پاکولو امکان له منځه ځي.
- همدارنګه په پام کې ولرئ چې په ځینو مواردو کې له لرې واټن د ډېټا پاکول شایي قانوني محدودیتونه ولري. نو د دې کار له ترسره کولو مخکې، اړوند قوانین او مقررات په پام کې ونیسئ.
- د خپلو وسایلو د ترمیم لپاره، یوازې معتبرو او رسمي خدماتي مرکزونو ته مراجعه وکړئ.
-

پنځم څپرکی
امن او کوډ شوې اړیکې

۵,۱. له امن او کوډ شوي پیغام رسوونکو اپلکېشنونو څخه ګټه اخیستنه

خبریالان کولای شي د کوډ (Encryption) شویو پیغام‌رسوونکو اپلېکېشنونو یا هغو سافټویرونو په کارولو سره چې برېښنالیکونه (Encrypt) کوي، څو یوازې ټاکل شوی ترلاسه کوونکی یې ولوستلای شي، له خپلو سرچینو سره لا خوندي اړیکې ټینګې کړي. کوډول د پیغامونو منځپانګه ساتي، خو هغه شرکتونه یا اداره چې په دې بهیر کې دخیلې وي، ښایي د پیغامونو میټا ډېټا (Metadata)، لکه د پیغام د لېږلو وخت، ترلاسه کوونکی او نور جزئیات، وګوري. شرکتونه د معلوماتو د راټولولو، ساتلو او د چارواکو غوښتنو ته د ځواب ورکولو په اړه بېلابېل سیاستونه او تګلارې لري.
پیغام‌رسوونکې اپلېکېشنونه په بنسټیز ډول له بشپړ کوډېدلو (End-to-End Encryption) ملاتړ کوي، یعنې کارووونکي ته اړتیا نه وي چې کوډ په جلا ډول فعاله کړي او اطلاعات د لېږونکي له وسیلې څخه د ترلاسه کوونکي پورې په کوډ (Encryption) شوې بڼه انتقالېږي. دا ډول کوډول (Encryption)دا معنا هم لري چې معلومات د اړوند شرکت یا اداره پر سرورونو هم کوډ شوي پاتې کېږي، نو د قانوني غوښتنې له لارې د منځپانګې ترلاسه کول ناشوني کېږي. خو پام مو وي چې که هر څوک د پیغام لېږونکي یا ترلاسه کوونکي وسیلې ته لاسرسی ولري، یا د اپلېکېشن اړوند حساب کوډ ترلاسه کړي، بیا هم د پیغام منځپانګه لوستلای شي. (Signal) او (WhatsApp) هغه پیغام‌رسوونکي اپلېکېشنونه دي چې په بنسټیز ډول له بشپړ کوډېدلو ملاتړ کوي. هغه کارووونکي چې داسې اپلېکېشنونه کاروي چې په بنسټیز ډول کوډول نه لري، ښایي اړتیا ولري چې بشپړ کوډېدل پخپله فعاله کړي.

۵,۲. ډېټا او میټا ډېټا څه ته وایي

په ډیجیټلي علم او ټکنالوژۍ کې، (Data) د معلوماتو او ارقامو په معنا ده. دا معلومات کېدای شي شمېرې، متن، انځورونه، غږونه او هر ډول نور اطلاعات وي چې په ډیجیټلي بهیرونو کې تولید، ذخیره او لېږدول کېږي. په ساده ډول، هر هغه څه چې مور یې په کمپیوټرونو او ډیجیټلي سیستمونو کې لولو او لیکو، لکه د برېښنالیکونو متنونه، انځورونه، پیغامونه او نور، ډېټا بلل کېږي.
له بلې خوا، د ډېټا په اړه معلوماتو ته میټا ډېټا (Metadata) ویل کېږي. میټا ډېټا مرسته کوي چې ډېټا ښه وپېژندل شي، مدیریت او ګټه ترې واخیستل شي. د بېلګې په توګه، د یوه انځور میټا ډېټا کې کېدای شي د انځور اخیستلو نېټه، ځای، د کامرې ډول، د انځور اندازه او نور تخنیکي معلومات شامل وي. د ډیجیټلي امنیت په برخه کې، میټا ډېټا د ډېټا د لېږد څرنګوالي، د لېږلو وخت، د کارونکي یا مسؤل سیسټم او نورو تخنیکي جزئیاتو په اړه مهم معلومات ورکولای شي، چې د ډېټا په پېژندنه او ساتنه کې مرسته کوي.
ډېرى وخت میټا ډېټا کوډ (Encrypt) شوې نه وي او ښایي د هغه هېواد چارواکي یا د قانون پلي کوونکي اداره یې غوښتنه وکړي چې تاسې پکې ژوند کوئ. که د خپل خصوصي حریم او میټا ډېټا په اړه اندېښنه لرئ، نو له هغو کوډ (Encryption) شویو پیغام‌رسوونکو اپلېکېشنونو څخه ګټه واخلئ چې تر ټولو لږ ډېټا راټولوي.

۵,۳. پیغام رسوونکو اپلکیشنونو کې د امنیت لوړولو لارې چارې

- د هغه پیغام‌رسوونکي اپلېکېشن په اړه چې کاروئ یې، څېړنه وکړئ چې مالک یې څوک دی، د کارووونکو کوم ډول معلومات ساتي، کومې میټا ډېټا (Metadata) ته لاسرسی لري او ایا دغه معلومات د دولتونو له لوري غوښتل شوي دي که نه.

همدارنګه وګورئ چې د کارووونکو د معلوماتو د شریکولو د غوښتنو په وړاندې د دوی تګلاره څه ده. ټکنالوژیک شرکتونه باید هر کال د دولتونو له لوري د ډېټا د پاکولو یا شریکولو د غوښتنو په اړه رونې او شفاف راپور خپور کړي.

- په منظم ډول له خپلو پیغامونو بیک‌اپ (Backup) واخلئ او وروسته یې پاک کړئ، څو ستاسې په وسیله یا حساب کې د معلوماتو کچه کمه پاتې شي. د خپلو اسنادو، پیغامونو او څورسنیزو فایلونو د ارزونې لپاره یو منظم پلان جوړ کړئ او ډاونلوډ شوي فایلونه یا د سکرین شاټ (Screenshot) انځورونه له وسیلې او اپلېکېشن څخه بهر، په یوه کوډ (Encryption) شوې بهرنۍ حافظه کې وساتئ. پام مو وي چې دا پیغامونه ښایي د هغه چا په حساب کې لا هم موجود وي چې تاسې ور استولي دي.
- پوه شئ چې ستاسې له پیغام‌رسوونکي اپلېکېشن څخه لېږل شوي انځورونه او اسناد په موبایل کې په کوم ځای کې ذخیره کېږي. هر هغه څه چې تاسې یې ډانلوډ کوئ، لکه انځورونه، په وسیله کې خوندي کېږي او ښایي نورو وسیلو یا اپلېکېشنونو ته هم کاپي شي، په ځانګړي ډول هغه وخت چې له خپلې ډېټا بیک‌اپ (Backup) اخلئ.
- هغه مخاطبان چې ستاسې په موبایل کې ذخیره دي، له پیغام‌رسوونکو اپلېکېشنونو او کلاوډ حسابونو سره همغږي کېږي. له همدې امله، هغه شمېرې چې تاسې یې له یوه ځایه پاکوئ، ښایي په بل ځای کې لا هم پاتې وي. د بشپړ پاکولو لپاره، اړینه ده چې د همغږۍ تنظیمات وګورئ او ډاډ ترلاسه کړئ چې بدلونونه په ټولو پلاتفورمونو او حسابونو کې پلي شوي دي. د دې لپاره د موبایل Settings ته لاړ شئ، بیا د (Accounts & Sync) برخې ته ننوځئ او اړوند کلاوډ حساب لکه (Google Contacts یا iCloud) وټاکئ. د اړتیا په صورت کې اړیکې همغږې یا پاکې کړئ.
- د امکان په صورت کې، خپل پیغام‌رسوونکی اپلېکېشن په کوډ قفل کړئ، څو که بل څوک ستاسې موبایل ته لاسرسی وموميِ، د اپلېکېشن منځپانګه ونه شي لیدلای.
- که اپلېکېشن د نوم‌لیکنې قفل (Registration Lock) ځانګړنه لري، هغه داسې فعاله کړئ چې هر څوک ستاسې د موبایل شمېرې په کارولو سره اپلېکېشن نصبوي، اړ شي ستاسې ټاکلی کوډ هم داخل کړي.
- په Signal پیغام‌رسوونکي اپلېکېشن کې د یو یوزرنیم (Username) په جوړولو سره د خپل ټلفن شمېره خوندي کړئ. د دې پر ځای چې د ټلفن شمېره مو له نورو سره شریکه کړئ، خپل یوزرنیم (Username) شریک کړئ. د دې لپاره د خپل حساب (Account) تنظیماتو ته لاړ شئ او د خصوصي حریم (Privacy) په برخه کې د خپلې خوښې یوزرنیم (Username) جوړ کړئ.
- ځینې اپلېکېشنونه لکه(WhatsApp) ستاسو د پیغامونو له منځپانګې څخه د ټلفن شمېرې اړوند په کلاوډ یا مجازي حساب کې بیک آپ (Backup) اخلي. د پروګرام په تنظیماتو کې کولای شئ د بیک‌اپ کوډول (Encryption) فعاله کړئ او ورته اوږد او ځانګړی کوډ (Password) وټاکئ. که نه غواړئ بیک‌اپ واخیستل شي، دا برخه په تنظیماتو کې غیرفعالولای شئ. پام مو وي، که اپلېکېشن پاک او بیا نصب کړئ، په اپلېکېشن کې د پیغامونو په ګډون، ټوله زېرمه شوې منځپانګه، له منځه ځي.
- د(Apple) د وسایلو او د (iOS) سیسټم کارووونکي دې پام وکړي چې په (Signal) کې ستاسو د اړیکو تاریخچه له(iCloud) سره همغږي کېږي. د اپلېکېشن په تنظیماتو کې کولای شئ دا همغږي غیرفعاله کړئ.
- په(Signal) او(WhatsApp) کې د ورکېدونکو پیغامونو ځانګړنه دا اسانتیا برابروي چې پیغامونه له ټاکلې مودې وروسته په اتومات ډول پاک شي. که تاسو اندېښنه لرئ چې ټلفن به مو ورک، ضبط یا توقیف شي او پیغامونه به مو د لاسرسي وړ وګرځي، نو دا ځانګړنه فعاله کړئ. د دې لپاره په سیګنال کې پر اړوند کس یا ډلې کلیک وکړئ، بیا د خبرو اترو تنظیماتو (Chat Settings) ته ولاړ شئ او هلته د ورکېدونکو پیغامونو (Disappearing Messages) برخه وټاکئ او د پیغامونو د پاکېدو وخت فعال کړئ. په(WhatsApp) کې هم دا برخه د اړوند کس یا ډلې د خبرو اترو په تنظیماتو کې شته. د دې بهیر له بشپړېدو وروسته به، پیغامونه په ټاکلي وخت کې په خپله پاک شي.
- هم(Signal) او هم(WhatsApp) دا اسانتیا برابروي چې انځورونه او ویډیوګانې د ترلاسه کوونکي له لوري تر یو ځل لیدلو وروسته پاکې شي. د حساسو انځورونو د لېږلو پر مهال د دې ځانګړنې فعالول ګټور تمامېدای شي. د دې لپاره هغه انځور یا

ویډیو وټاکئ چې مقابل لوري ته یې لېږئ، خو د لېږلو تېې تر کېکاږلو مخکې په انډرایډ او ایفون کې پر هغه ګرد نښان کلیک وکړئ چې په منځ کې یې د (۱) نښه وي. په Signal کې، د انځور یا ویډیو تر ټاکلو وروسته او د لېږلو تېې تر کېکاږلو مخکې، پر هغه کوچني ګرد نښان کلیک وکړئ چې د دوو سترګو په شان نښه لري، څو د «یو ځل لیدلو» (Photo/Video set to view once) ځانګړنه فعاله شي. د دې ځانګړنې له فعالېدو وروسته، ترلاسه کوونکی یوازې یو ځل انځور یا ویډیو پرانیستلای شي او وروسته به په خپله پاکه شي. (WhatsApp) همداراز د سکرین‌شاټ (ScreenShot) اخیستل بندوي، خو پام مو وي چې ترلاسه کوونکی بیا هم کولای شي د بلې وسیلې په واسطه ستاسو له پیغام یا فایل څخه انځور واخلي

- همداراز، Signal او WhatsApp د ویډیویي اړیکو لپاره د بشپړ کوډېدلو (End-to-end encryption) اسانتیا برابروي.
- Signal د خصوصي حریم او امنیت له پلوه پیاوړې ځانګړنې لري، له همدې امله د کاري ګټې اخیستنې لپاره تر ډېره مناسب ګڼل کېږي. له واتساپ څخه د ګټې اخیستنې د څرنګوالي لارښود د لوستلو لپاره دې (WhatsApp) او د زیګنال لپاره دې (Signal) پټې ته سر ورښکاره کړئ.
- که پر خپل واتساپ د جاسوسي بریدونو (Spyware) اندېښنه لرئ، د حساب د دقیقو امنیتي تنظیماتو (Strict Account Settings) ځانګړنه فعاله کړئ. د دې لپاره لاندې پراوونه تعقیب کړئ: (Settings ⟶ Account ⟶ Privacy ⟶ Strict Account Settings) په ځینو نسخو کې ښایي دا ځانګړنه موجوده نه وي، خو که په تنظیماتو کې وي، فعالول یې ستاسو د حساب امنیت لوړوي. له دې وروسته د خپل پیغام‌رسوونکي د لا زیات امنیت لپاره د دوه پړاویز تاییدیې (Two-step verification) ځانګړنه هم فعاله کړئ.

شپږم څپرکی
د کمپیوټرونو او ځیرکو موبایلونو کوډول

د حافظې د بشپړ کوډولو (Full Disk Encryption) معنی دا ده چې ستاسو د کمپیوټر یا ټلفن ټوله ډېټا قفل او کوډ کېږي، ترڅو د غلا یا غیرمجاز لاسرسي په صورت کې ډېټا خوندي پاتې شي. کله چې دا سیستم فعال وي، د وسیلې د بندېدو پر مهال ډېټا کوډ (Encryption) کېږي او له بېرته روښانولو او د کوډ له دننه کولو وروسته بیا پرانیستل کېږي.

٦,١. څه ډول د خپل کمپیوټر ډېټا په خوندي توګه پاکه کړو

په نویو کمپیوټرونو کې د جامد حالت حافظو (Solid-State Drives - SSDs)، د USB نښلونکو وړ حافظو او د کوچنیو حافظوي کارتونو (SD Cards) لپاره د فایلونو خوندي پاکېدل (Secure Deletion) دا معنا لري چې هغه فایلونه چې تاسو یې پاکوئ، په حقیقت کې په بشپړه توګه نه پاکېږي، بلکې یوازې پټ کېږي او د هغوی ځای د نویو معلوماتو د لیکلو لپاره خالي کېږي. تر هغه وخته چې پر دغه ځای بیا لیکنه ونه شي، پاک شوی فایل لا هم په حافظه (Disk) کې پاتې وي او بېرته راګرځېدلی شي، که څه هم ظاهراً نه ښکاري. له همدې امله عادي پاکول بسنه نه کوي او یو څوک کولای شي د ځانګړو وسایلو په کارولو سره پاک شوي فایلونه بېرته ترلاسه کړي. خوندي پاکول (Secure Deletion) یوازې پر ګرځنده حافظو (Spinning Disk Drives) په باوري ډول کار کوي. که تاسو خپل کمپیوټر له ۲۰۱۵ کال وروسته اخیستی وي، ډېر احتمال شته چې هغه د جامد حالت حافظه ولري. په جامد حالت حافظو، وړو حافظو او حافظوي کارتونو کې د معلوماتو خوندي پاکول ډېر ستونزمن کار دی. که تاسو SSD یا USB Flash Drive کاروئ، ستاسو د معلوماتو د ساتنې

غوره لاره کوډول ده. په دې ډول، که فایل لا هم په حافظه کې پاتې وي، هر هغه چاته ته چې ورته لاسرسی پیدا کړي، د ګډوډو او بې‌معنا معلوماتو په څېر ښکاري او نه شي کولای تاسو د کوډ خلاصولو ته مجبور کړي.

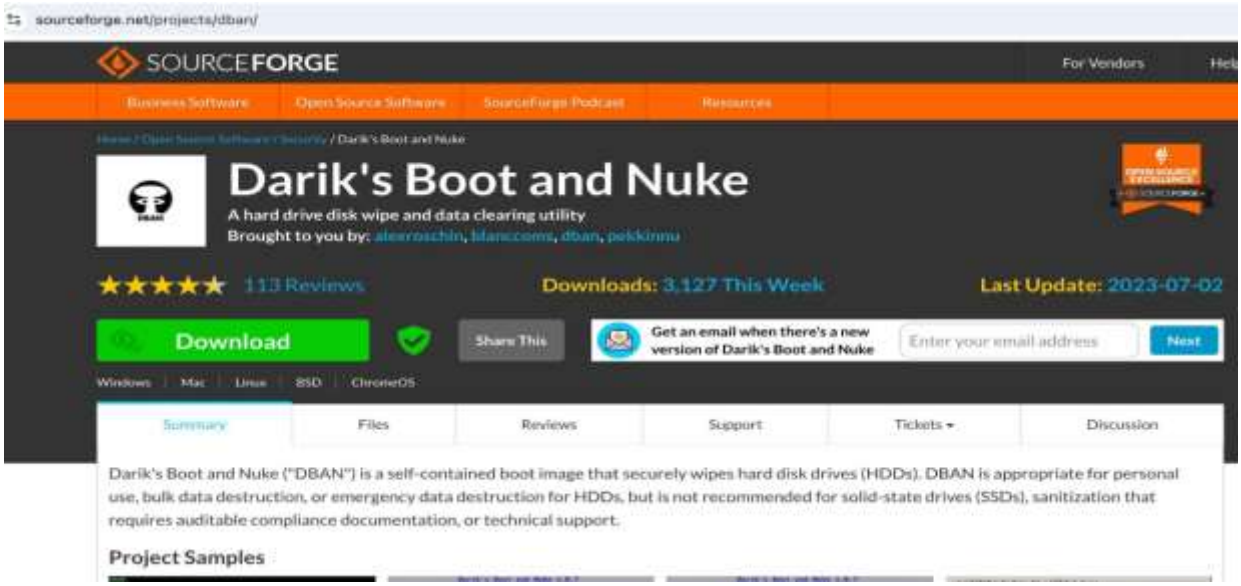
د ویندوز، مک، لینوکس کمپیوټرونو او ایفون ټلفون د کوډولو په ټراو د معلوماتو لپاره لاندې پتو ته سر ورښکاره وکړئ:

(Windows) ، (Mac)، (Linux)، (iPhone)

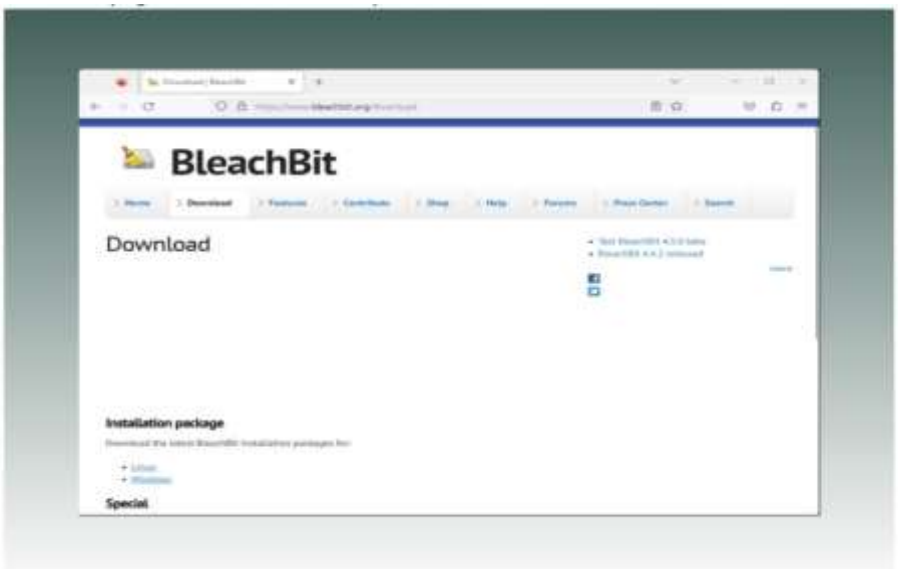
د جامد حالت حافظو او د دې موضوع په اړه چې ولې یې خوندي پاکول ستونزمن دي، د لا زیاتو معلوماتو لپاره دې (Deletion on SSDs) پتې ته سر ورښکاره کړئ.

که له زړو کمپیوټرونو څخه چې حرکت لرونکي حافظې (Spinning Disk Drives) لري کار اخلئ، لاندې ټکي په پام کې ونیسئ:

که غواړئ خپل زوړ کمپیوټر وغورځوئ، وپلورئ یا بل چا ته یې ډالۍ کړئ، باید ډاډ ترلاسه کړئ چې هېڅ څوک نه شي کولای ستاسو شخصي اطلاعات بېرته ترلاسه کړي. د پلور یا بیاکارونې څخه مخکې، باید د کمپیوټر حافظه په بشپړه توګه پاکه کړئ، څو ستاسو حساس معلومات خوندي پاتې شي.



د (Darik's Boot and Nuke) وسیله د همدې کار لپاره طراحي شوې ده. د دې بهیر د څرنګوالي په اړه د پوهاوي لپاره دې (پتې) ته سر ورښکاره کړئ



سرچينه: EFF

د غير ضروي فايلونو د پاکولو له ځانګړي سافټويرونو څخه ګټه اخيستنه

په(Microsoft Windows) او (Linux) کمپيوټرونو کې چې حرکت لرونکې حافظې لري، سپارښتنه کېږي، چې د غير ضروري فايلونو د خوندي پاکولو لپاره له (BleachBit) څخه چې د پرانيستي سرچينو (Open- source) د پاکولو يوه وسيله ده، ګټه واخلئ. دا پروګرام کولای شي په چټکۍ او اسانه ډول هغه فايلونه غوره کړي، چې د خوندي پاکولو لپاره وي. همداراز، د فايلونو د پاکولو لپاره ځانګړي او شخصي شوي لارښوونې هم په کې ليکل کېدلای شي.

٦,٢. په کمپيوټر کې د فايلونو د خوندي پاکولو وسايل کوم محدوديتونه لري

په پام کې ولرئ چې پورته ياد شوي د خوندي پاکولو وسايل يوازې هغه فايلونه پاکوي کوي چې ستاسو د کمپيوټر په حافظه يا هارډ ډيسک (Disk Hard) کې موجود وي. يعنې که ستاسو فايلونه په نورو ځايونو کې بيک‌اپ (Backups) شوي وي، لکه بهرنۍ حافظې (External Drives, USB)، د برېښنالیک سرورونه، کلاوډ يا مجازي حافظه (Cloud Storage)، يا په موبايل کې وي، دا وسايل يې نه شي پاکولای. د يو فايل د خوندي پاکولو لپاره بايد د هغه ټولې نسخې په ټولو ځايونو کې پاکې شي. همداراز، کله چې فايل په کلاوډ (لکه Dropbox يا نورو د فايل شريکولو خدمتونو کې) ذخيره شوی وي، عموماً دا تضمين نشته چې هغه فايل به د تل لپاره په بشپړه توګه پاک شي.

له بده مرغه، د خوندي پاکولو وسايلو بل محدوديت دا دی چې حتی که د يو فايل ټولې نسخې هم پاکې شي، بيا هم کېدای شي د هغه فايل ځينې نښې ستاسو په سيستم کې پاتې شي. دا نښې د دې لپاره نه دي چې فايل سم نه دی پاک شوی، بلکې ځکه پاتې کېږي چې د عملياتي سيستم (Operating System) يا د نورو پروګرامونو ځينې برخې د هغه فايل په اړه معلومات ساتي.

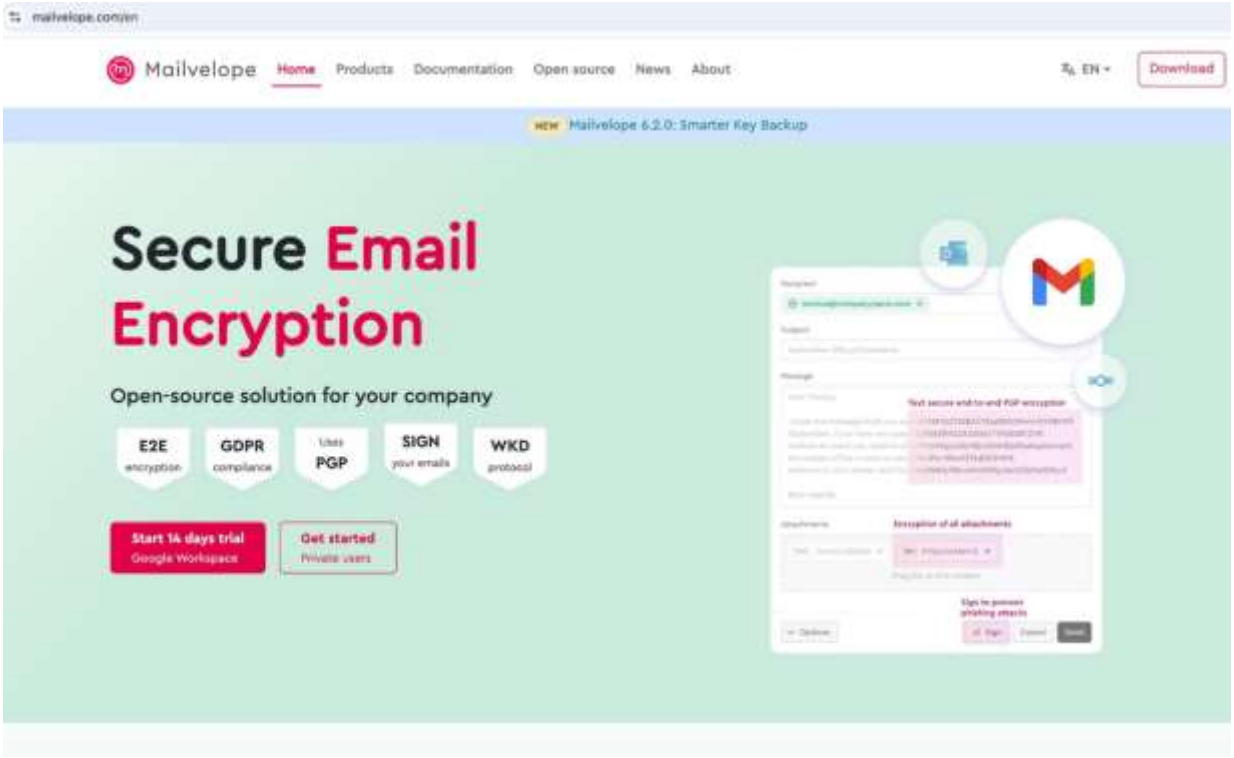
اووم څپرکی
د برېښنالیک له لارې د اړیکې ټینګښت

۷,۱. د برېښنالیک له لارې اړیکې څومره خوندي دي

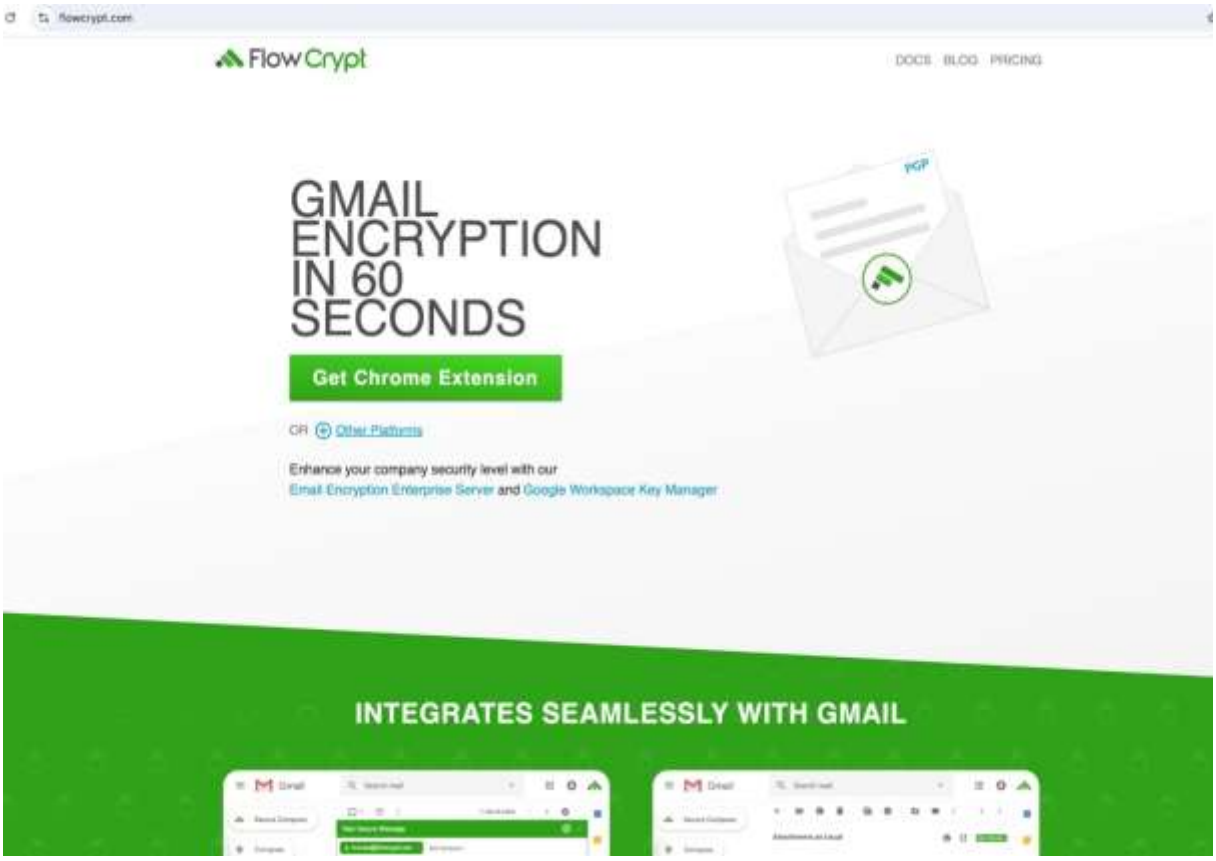
په یاد ولرئ چې د برېښنالیک اړیکې د اوربدو وړ دي او بریښنالیکونه د څو سرورونو له لارې لېږل کېږي، هر سرور کولای شي پیغام وڅېړي.
په ساده ژبه، د د برېښنالیک د لېږلو په بهیر کې برېښنالیکي پیغامونه د لېږونکي له وسیلې څخه بېلابېلو سرورونو ته انتقالېږي او دا لاره معمولاً له څو سرورونو څخه تېرېږي. هر یو سرور چې د لېږد په دې مسیر کې وي، د پیغام د منځپانګې او جزئیاتو د کتلو توان لري، ځکه چې ډېری برېښنالیکي اړیکې د متن په بڼه او پرته له بشپړ کوډ (Encryption) ترسره کېږي. سربېره پر دې، ځکه چې بریښنالیکونه د لېږد پر مهال له بېلابېلو لارو تېرېږي، هر سرور کولای شي د څارنې د یوې برخې په توګه عمل وکړي او د پیغام منځپانګه وګوري یا یې ثبت کړي. دا موضوع د برېښنالیکونو د امنیت او خصوصي حریم د ارزښت څرګندونه کوي.

۷,۲. د برېښنالیک له لارې د اړیکو امنیت لوړ کړئ

د کوډ (Encryption) شوي برېښنالیک کارول، تاسو سره مرسته کوي چې د برېښنالیک له لارې د اړیکو امنیت زیات کړئ. کوډول (Encryption) هغه بهیر دی چې پکې یو عادي متني پیغام په داسې بڼه بدلېږي چې نه لوستل کېدونکی ښکاري او یوازې پاکل شوی ترلاسه کوونکی یې لوستلای شي.
یو شمېر داسې د کوډ (Encryption) شوي برېښنالیکونو وړاندې کوونکي شتون لري او خبریالان کولی شي ترې ګټه واخلي. ځینې دغه وړاندې کوونکي نورې کوډ (Encryption) شوې اسانتیاوې هم لري، لکه د کلاوډ یا مجازي حافظه، تقویم او مخاطبین. یعنې کوډېدل (Encryption) پکې له وړاندې شتون لري.(Proton Mail) او (Tuta Mail) د کوډ شویو بریښنالیکي خدمتونو بېلګې دي.
که تاسو یو کوډ (Encryption) شوی برېښنالیکي خدمت کاروئ او هغه چا ته برېښنالیک لېږئ چې هماغه خدمت کاروي، د پیغام منځپانګه په اوتومات ډول کوډ (Encryption) کېږي. خو که اړتیا وي داسې چا ته برېښنالیک ولېږئ چې د بل برېښنالیک خدمت کاروي، نو باید دا برخه فعاله کړئ او له مقابل لوري وغواړئ چې د برېښنالیک د پرانیستلو لپاره یو کوډ وکاروي.
د برېښنالیکي خدمتونو ځینې وړاندې کوونکي لکه Gmail په بنسټیز ډول د کوډولو (Encryption) ځانګړنه نه لري. که تاسو له Gmail څخه کار اخلئ او کوډولو (Encryption) ته اړتیا لرئ، نو ځینې وسیلې شته چې دا کار درته اسانه کوي.



د هغو مسلکي کاروونکو لپاره چې په څو برېښنالیکي خدمتونو کې لکه Yahoo،Gmail او Outlook کې کوډول غواړي، د (Mailvelope) وسیله مناسبه ده.



او هغه کسان چې یوازې له Gmail څخه ګټه اخلي او غواړي په اسانه او چټک ډول کوډ ایښودنهڕېښنالی (Encryption) کړي، FlowCrypt غوره انتخاب دی.

د بېلګې په توګه، د FlowCrypt د کارولو لپاره،(flowcrypt.com) ویب‌پاڼې ته لاړ شئ او لاندې مرحلې تعقیب کړئ: (Get Chrome Extension, Add to Chrome, Add Extension, Continue with Gmail, your email address, Allow, Create A New Key, passphrase, create)

د دې مرحلو له بشپړېدو وروسته، لېږل شوي او ترلاسه شوي برېښنالیکونه په اوتومات ډول کوډ (Encryption) او بېرته پرانیستل کېږي او ستاسو د اړیکو امنیت زیاتېږي. خو په پام کې ولرئ، چې که څه هم ستاسو برېښنالیکونه کوډ شوي وي، بیا هم د بریښنالیک خدمت وړاندې کوونکی ښایي ځینې میټا ډېټا (Metadata) لکه د برېښنالیک موضوع او د ترلاسه کوونکي پته وساتي. د برېښنالیک خدمت شرایط او پالیسی په دقت ولولئ، څو پوه شئ چې کومه ډېټا کوډ (Encryption) شوي او کومه نه ده.

پای

سرچینې:

د خبریالانو د ملاتړ نړیواله کمیټه(Committee to Protect Journalists-CPJ)

د الکترونیک مرز بنسټ(Electronic Frontier Foundation)

بې پولې خبریالانو (Reporters Without Boarders-RSF)

د آنلاین تاوتریخوالي پر ضد ائتلاف (Coalition Against Online Violence)