Afghan Witness

د ښځو او نجونو لپاره ډیجیټل خوندیتوب

افغان ویټنس

دغه لارښود د دې لپاره جوړ شوی چې تاسو پر هغې اړینې پوهې سمبال او د وسایلو پر کارونې پوه کړي چې تاسو په ډیجیټل چاپیریال کې د خپل ځان د خوندیتوب لپاره ورته اړتیا لرئ. په داسې حال کې چې د دې لارښود اصلي مخاطبین افغانې نښځې او نجونې دي، خو هر څوک کولای شي د دغه لارښود له محتویاتو (منځپانګې) څخه ګټه پورته کړئ.

په داسې یو چاپیریال کې چې آزادي محدوده ده، ټولنیزې رسنۍ او د ډیجیټلي اړیکو نور ډولونه د ګډون (مشارکت) د مهمې وسیلې په توګه کارول کیږي. خو له بله پلوه بیا ډیجیټل خوندیتوب او محرمیت ډیری وخت له خطر سره مخ وي او افراد د دوی له آنلاین فعالیتونو، اړیکو یا نورو ډیجیټلی معلوماتو له مخې پیژندل کیدای شي.

که چیرې تاسو د زده کړې یا له نورو سره د اړیکې نیولو په لټه کې یاست او یا هم یوازې په انټرنیټ کې د لټون په حال کې یاست، دا مهمه ده چې په شئ چې څنګه کولای شئ خپل آنلاین فعالیتونه خوندي کړئ. د هغو میتودونو په تعقیبولو سره چې په دې لارښود کې راغلي، تاسو کولای شئ خپل شخصی محرمیت پیاوړی کړئ او د هغو ستونزمنو حالاتو سره سره چې ورسره مخ یاست، په ډیجیټلی نړۍ کې په ډاډه توګه برخه واخلئ.

ستاسو پیاوړتیا ستاسو په کمزوریو کې پرته ده.

د مطالبو نومړۍ

۱. د امنیتي خطرونو پېژندنه

د ګواښ سرچینه

د خپل ځان خوندیتوب لپاره، تاسو باید هغه **خطرونه** وپیژنئ چې ورسره مخ یاست.

دا چې کیدای شي دغه ګواښونه د چا لخوا پیښ شي په لاندې مثالونو کې یې وګورئ:

- د کورنۍ هغه غړي چې ستاسو د ټولنیزو رسنیو پروفایل تعقیبوي.
- ناغوښتی او نا بللی خواستګار چې په ډېره مینه مو تعقیبوي.
- هغه چارواکي چې تاسې دروي او ستاسو ټیلفون پلټي.
- یو با نفوذه کس چې ستاسو مینه وال دی.
- ناپېژانده اشخاص چې ستاسو د آنلاین پوسټونو له کبله تاسو په نښه کوي.

هر یو پورتنی حالت **بیلابیل امنیتي** خطرونه له ځان سره لري. د ټیلفون له ناڅاپي او تصادفي پلټنې څخه د ځان ساتلو لپاره اقدامات له هغو اقداماتو نه توپیر لري چې تاسو یې باید د انټرنېټ قهرجنو کارووونکو یا هغو ځواکمنو چارواکو څخه د خپل ځان پټولو لپاره ترسره کړی چې ستاسو د پېژندنې په لټه کې دي.

خطر په دې پورې اړه لري چې 'د ګواښ عامل' (هغه څوک چې تاسې ګواښي) ستاسو په اړه څومره پوهیږي او د دغه کس سرچینې، نفوذ او تخنیکي وړتیاوې څومره پیاوړې دي. دې خبرې ته له پام پرته چې ګواښ له کومه ځایه راځي، **نښه دا ده چې تل ډېر احتیاطي اقدامات ترسره کړو.**

چاپېریال

امنیتي خطرونه چې تاسو ورسره مخامخ کېږئ، هغه ځای پورې اړه لري **چیرې چې تاسو ژوند کوئ**.

په متحده ایالاتو یا اروپا کې قوانین ستاسو د شخصي معلوماتو ساتنه کوي. په عمومی ډول، ستاسو په دستګاوو کې موجود معلومات یا ستاسو د آنلاین فعالیت نېټه په آسانۍ سره ترلاسه کیدای نه شي مګر دا چې محکمې تاسو خطرناک مجرم یا جدي امنیتي ګواښ وګڼي.

په دې ځایونو کې، ستاسو اصلي خطرونه دا دي: هغه معلومات چې تاسو یې په آنلاین پلټفارمونو کې شریکوی، ستاسې دستګاوې له لیرې هیک کېږي، یا ستاسو په نږدې چاپېریال کې یو کس ستاسو دستګاه ته لاسرسۍ مومي.

د **افغانستان** په څېر یو هیواد کې حالات ډېر توپیر لري. بې له قانونی ملاتړه، نه یوازې ستاسو د ټولنیزو رسنیو پوسټونه بلکه د انټرنیټ ټرافیک او ستاسو په دستګاوو کې موجود **هر ډول** معلومات کیدای شي ستاسو لپاره امنیتي خطرونه وي.

د **افغانستان چارواکي** د هغو کسانو په اړه چې پخواني دولت او د امریکا دولت سره یې کار کړی، ډېره **بایومټریک دیټا** (معلومات) او همداراز په عامه توګه د هېواد د وګړو په اړه لا ډېره دیټا (معلومات) لري چې دوی دغه دیټا د سیمه ییزو فعالانو، خبریالانو او نورو کسانو د پېژندنې لپاره کاروي.

په داسې یو حالت کې ګواښونه کیدای شي د یو حسود کس لخوا چې محدود تخنیکي مهارتونه لري یا د پراخو معلوماتو او تخصص درلودونکې امنیتي اداري لخوا وي. **د هغه کس ټکنالوژیکي وړتیاوې کمې مه ګڼئ چې تاسو ته د زیان رسولو یا په آنلاین ټوګه ستاسو د تعقیبولو په لټه کې دي.**

مختلفې تګلارې

د ګوابښ مختلفې سناریوګانې ښایي مختلفو تګلارو او د ساتنې کچې ته اړتیا ولري.

په لاندې برخه کې هغه دوه مثالونه دي چې دغه موضوع تشریح کوي:

لوړ مهارتونه - بې له فزیکي لاسرسۍ نه

که چیرې ستاسو 'د ګوابښ عامل' له لوړو تخنیکي مهارتونو نه برخمن وي خو ستاسو دستګاه ته مستقیم فزیکي لاسرسی نلري، نو دا خورا مهمه ده چې تاسو:

- د اړیکې نیولو لپاره پر **شخصي حریم متمرکز اپلیکیشنونه** وکاروئ
- د خپل **انټرنیټ ټرافیک پټولو لپاره** اختصاصي مجازي شبکه (VPN) یا Tor براوزر (شبکې) په څېر وسیلې وکاروئ
- خپل وسایل د هیک کېدو څخه خوندي کړئ
- په **ټولنیزو رسنیو** کې خپل د شخصي حریم تنظیمات **لوړې کچې ته ورسوئ**

ټیټ مهارتونه - فزیکي لاسرسی

که چیرې ستاسو د ګوابښ عامل د ټیټو تخنیکي مهارتونو څخه برخمن وي خو ښایي ستاسو دستګاه ته مستقیم فزیکي لاسرسی ولري، تاسو باید حساس معلومات د داسې طریقو له لارې پټ کړئ چې په آسانۍ سره د موندلو وړ نه وي. دغه کار د لاندنیو طریقو له لارې ترسره کیدای شي:

- د غیر معمولي اپلیکیشنونو کارول، **کوډ لرونکي یا شفري ژبه**، خپله دستګاه په **بې زیانه معلوماتو ډکول**، لکه د ګټو چټ ګروپونو یا د پیشوګانو عکسونه.
- همداراز تاسو کولای شئ چې **په بهرني هارد ډرایو یا د معلوماتو د ساتلو په اپلیکیشن کلاوډ کې خپل حساس معلومات پټ کړئ** ترڅو د دوی لپاره د هغو معلوماتو موندل ستونزمن کړئ چې تاسو ته د زیان رسولو په موخه کارول کیدای شي.

دا خورا مهمه ده چې خپل محرمیت او امنیت لوړې کچې ته ورسوئ، په ځانګړې توګه که تاسو ډاډه نه یاست چې ګوابښ له کوم ځایه راځي.

خو که څوک ستاسو دستګاه ته لاسرسی وموميِ، دا هم مهمه ده چې په دستګاه کې د ګڼ شمېر **پر محرمیت متمرکزو اپلیکیشنونو** په شتون یا په بشپړه توګه له معلوماتو د خالي دستګاه په کارولو سره د پلټونکي شک را ونه پاروئ.

په داسې یو حالت کې په دې اړه **شخصي قضاوت** چې ستاسو په قضیه کې **سم توازن** څنګه ښکاري، مهم دی.

ټولنيز انجنيرى برید

د ټولنيزې انجينري برید څه شی دی؟

د ټولنيزې انجينري برید داسې يو تاکتيک دی چې د هيکرانو لخوا ستاسو د غولولو لپاره کارول کيږي ترڅو ستاسو شخصي معلومات غلا کړي. کيدای شي دا هيکران تاسو ته ځان يو با اعتباره کس معرفی کړي، لکه يو ملګری، د کورنۍ غړی، يا حتی يو شرکت چې تاسو يې پېژنئ.

د ټولنيزې انجينري برید عام تاکتيکونه

د هويت غلا: کيدای شي يو شخص د داسې يو ملګري يا خپلوان په توګه تاسو ته ځان دروپيژني چې مرستې ته اړتيا لري. دوی ښايی له تاسو د پيسو ليږلو يا شخصي معلوماتو شريکولو غوښتنه وکړي. دې ته پام ولرئ چې يو کس چې تاسو يې پېژنئ د هر وخت په څير تاسو سره اړيکه نه نيسي او نا آشنا حالت لري.

بيړنی حالت ښودل: هيکران ښايي بيړنی حالت رامنځته کړي او ادعا وکړي چې که تاسو په چټکۍ سره عمل و نه کړئ، يو بد څه به پېښ شي . د بيلګې په توګه، دوی ښايي ووايي "که تاسو سمدلاسه خپل پټنوم ونه وايئ نو ستاسو اکاونټ به بند شي!"

فيشينګ څه شی دی؟

فيشينګ د ټولنيزې انجينري د برید يوه بڼه ده چې له دې لارې هيکران تاسو ته جعلي پيغامونه ليږي او په دې کار سره ستاسو د حساسو معلوماتو د ترلاسه کولو لپاره تاسو غولوي.

دا ډول پيغامونه د برېښنالیک، اس ام اس، ټولنيزو رسنيو يا ټيلفون له لارې ليږل کيدای شي.

د فيشينګ عامې نښې

شکمن لينکونه: په هغو پيغامونو کې لينکونه په پام کې ونيسئ چې تاسو ته د ننوتلو بلنه درکوي او يا تاسو نه د شخصي معلوماتو غوښتنه کوي. دا لينکونه کيدای شي جعلي ويب پاڼو تللو ته لاره هواره کړي چې اصلي ښکاري، خو ستاسو د معلوماتو غلا کولو لپاره جوړې شوې دي.

غير عادي غوښتنې: هغو پيغامونو ته پام وکړئ چې د شخصي معلوماتو، پټنومونو يا مالي معلوماتو غوښتنه کوي. شرکتونه او قانوني سازمانونه په عام ډول له دې لارې د حساسو معلوماتو غوښتنه نه کوي.

له غلطيو ډکه ژبه: ډيری فيشينګ پيغامونه املايي او ګرامري غلطۍ لري يا داسې ژبه کاروي چې عجيبه ښکاري.

څنګه ځان خوندي کړو

د سرچينې کره والی تأييد کړئ: که چيرې تاسو شکمن پيغام ترلاسه کوئ، د پيژندل شوي او د اعتبار وړ ميتود په کارولو سره (لکه د ټيلفون شمېره يا برېښنالیک پته چې تاسو مخکې له دې درلودل) شخص يا سازمان سره اړيکه ونيسئ.

مشکوکو لينکونو باندې کليک مه کوئ: په لينکونو باندې ماوس وساتئ او وګورئ چې په لينکونو کې څه ښکاری. که لينک عجيب ښکاره شو يا د استوونکي کس ويب پاڼې سره سمون نه درلود، وربانديې کليک مه کوئ.

د خوندي کولو سافټوير کارول: په خپلو دستګاوو کې د خوندي کولو سافټوير نصب او آپډيټ کړئ. دا کار کولای شي د ضرر رسوونکو پيغامونو او ويب پاڼو په پيژندلو او بندولو کې مرسته وکړي.

که فکر کوئ چې د فيشينګ برید سره مخ شوي ياست، څه بايد وکړئ؟

ځواب مه ورکوئ: که چيرې تاسو شکمن پيغام ترلاسه کړ، ځواب مه ورکوئ او په هيڅ لينک باندې کليک مه کوئ.

راپور يې کړئ: پيغام هغه پلټفارم ته راپور کړئ چې تاسو پکې پيغام ترلاسه کړی. د بېلګې په توګه، که پيغام د برېښنالیک له لارې راغلی وي، تاسو کولای شئ پيغام د 'سپم' يا 'فيشينګ' په توګه په نښه کړئ.

خپل پټنوم بدل کړئ: که تاسو فکر کوئ چې ښايي د فيشينګ برید سره مخ شوي ياست، سمدلاسه خپل پټنومونه (پاسوردونه) بدل کړئ ترڅو ستاسو اکاونټونو ته د لاسرسۍ مخه ونيول شي.

۲. د اپلیکیشنونو او دستګاوو خوندي کول

کیدای شي ستاسو دستګاوې خوندي نه وي

ستاسو دستګاوې، لکه ستاسو ټیلفون یا لپ ټاپ، ستاسو معلومات، موقعیت او چلند په ډیفالټ توګه **تعقیبوي**. هغه کسان چې ستاسو دستګاه یې **هیک** کړې یا **چارواکي** دي، که هغوی له اړینو مهارتونو نه برخمن وي، کولای شي ستاسو دستګاه ته لاسرسی وموميِ. که چېرې څوک ستاسو دستګاه ته لاسرسی ولري، کولای شي په آسانۍ سره **ستاسو ټول معلومات او اړیکې د واټساپ په څیر اپلیکیشن له لارې وپلټي**.

د ګرځنده ټیلفون کوډ کول

د خپل ګرځنده ټیلفون د **کوډ کولو** په اړه ډاډ ترلاسه کړئ ځکه چې که ستاسو ګرځنده ټیلفون ورک او یا غلا شي، دا کار ستاسو د معلوماتو د خوندي کولو لپاره خورا اړین دی. کوډ کول ستاسو ډیټا (معلومات) په داسې بڼه بدلوي چې یوازې د سم 'کوډ یا شفر ماتونکې کیلی' پواسطه لوستل کیدای شي چې ستاسو د ګرځنده ټیلفون **پټنوم یا PIN** سره تړاو لري. د خپلې دستګاه د خوندیتوب لوړې کچې ته رسولو لپاره **د پیاوړي پټنوم (پاسورډ) د درلودو په اړه ډاډ ترلاسه کړئ**. **د آیفون ګرځنده ټیلفونونه په ډیفالټ توګه کوډ** شوي دي. د **انډرویډ ۱۰** او د هغه نه په پورته موډلونو کې هم وسیله **په ډیفالټ توګه** کوډ شوې ده. په زړو ماډلونو کې، کوډ کول باید په لاسي ډول فعاله شي.

د اندرویډ په زړو موډلونو کې، تاسو **'Settings > Security > Encryption'**ته د تللو له لارې کولای شئ وګورئ چې ستاسو ټیلفون کوډ شوی که نه.

که ستاسو دستګاه کوډ شوې نه وي، کولای شئ د (تنظیمات> امنیت> کوډ کول) برخې ته د تللو له لارې دکوډ کولو سیسټم فعال کړئ.

خو په یاد ولرئ چې د دغه کار ترسره کول له یو نه تر دوه ساعتونو پورې وخت نیسي او دستګاه د بیټرۍ بشپړ چارجولو ته اړتیا لري - که ستاسو دستګاه په ناڅاپي ډول د دغې پروسې بشپړیدو نه مخکې بنده شي، ستاسو تلیفون به نور کار ونکړي: تاسو باید خپله وسیله له سره تنظیم یا ریسیټ (reset) کړئ که نه نو تاسې به د معلوماتو له لاسه ورکولو خطر سره مخ شئ.

د پیغام لېږلو خوندي اپلیکیشنونه وکاروئ

د **عادي تلیفوني شبکې** له لارې اړیکه نیول او یا د **لنډو پیغامونو** (SMS) لېږل خورا ناخوندي اړیکې دي ځکه چې ستاسو اړیکې په آسانۍ سره ثبت کیدای شي. د خوندي پیغام رسولو سیستمونو، لکه واټساپ یا سیګنال کارول خوندي دي.

سیګنال د پیغام لیږلو یو خورا خوندي پروګرام دی. د سیګنال پروګرام له پای تر پای د کوډ یا رمز ورکونې آسانتیا برابروی او دا پدې معنی ده چې یوازې تاسو او هغه کس چې تاسو ورسره اړیکه کې یاست پیغامونه لوستلای شي. د سیګنال پروګرام هم یوه خلاصه سرچینه ده او دا پدې معنی ده چې کارپوهان د دې پروګرام کوډ ته لاسرسی لري ترڅو د دغه پروګرام د فعالیت څرنګوالی وڅېړي او د رونوالي او اعتبار په اړه یې ډاډمن شي.

واټساپ هم د پیغامونو، ټیلفوني زنګونو، عکسونو او ویډیوګانو لپاره له پای تر پای د کوډ یا رمز ورکونې آسانتیا برابروی. واټساپ د کارووونکو د خوښې وړ اپلیکیشن ده او په پراخه کچه کارول کیږي او د خوندي اړیکې نیولو لپاره غوره انتخاب دی.

د خپلو دستګاوو د لا خوندي کولو لپاره نور اختیارونه، لکه د **دوه مرحلو تاییدِ**، د **پیغامونو د پاکولو او د اپلیکیشنونو د ټړلو** اختیارونه فعال کړئ - چې په لاندې پاڼو کې تاسو ته ښودل کېږي. په عام ډول د خپلې شمېرې د شریکولو په اړه محتاط اوسئ او **د خپل شخصي حریم تنظیمات په منظم ډول وڅارئ** ترڅو تاسو ته معلومه شي چې څوک ستاسو معلومات لیدلای شي.

د کمپیوټر خوندي کول

ستاسو د کمپیوټر خوندي کول، په ځانګړي ډول په حساسو شرایطو کې، ستاسو د شخصي معلوماتو او خصوصي حریم ساتلو لپاره اړین دي. د اعتبار وړ انټي وایرس (سافټویر) نصب کړئ او خپل فایر وال فعال کړئ ترڅو د پوستغالو او بدو وایرسونو او غیر مجاز لاسرسي پر وړاندې ستاسو له کمپیوټر نه ساتنه وشي. د امنیتي زیانمنتوب د حل لپاره خپل د کمپیوټر عملیاتي سیستم او پروګرامونه په منظم ډول تازه (اپډیټ) کړئ.

د پوستغالو او بدو وایرسونو (MALWARE) څخه د کمپیوټر ساتنه

انټي وایرس (Antivirus)

که چیرې تاسو د ډېرو کارونو د ترسره کولو لپاره د ویندوز کمپیوټر کاروئ، دWindows Defender پوستکالی (سافټویر) په کافي توګه خوندي دی - په دې شرط چې تاسو دغه سافټویر تازه او فعاله وساتئ. که تاسو د ځینې اضافي اختیارونو په لټه کې یاست، نو یو نبه اختیار د Bitdefender سافټویردی چې هم په وړیا توګه او هم په پیسو ترلاسه کیدای شی.

د مک (Mac) کمپیوټر لپاره، ډیفالټ انټي وایرس په عمومي ډول ډیر خوندي دی. خو که تاسې د ډیر امنیت په لټه کې یاست، د Malwarebytes سافټویر د وایرس وړیا سکنر او انټي وایرس پروګرام ځان سره لري.

له یو نه زیات انټي وایرس مه کاروئ – امکان لري دغه انټي وایرسونه په سمه توګه د یو بل د کار کولو مخه ونیسي.

فایروال (Firewall)

فایروالونه ستاسو د کمپیوټر د امنیت اړینه برخه ده او ستاسو د دستګاه او د انټرنیټ احتمالي ګواښونو ترمنځ د **خنډ** په توګه عمل کوي. فایروال د مخکې ټاکل شوي امنیتي قوانینو پراساس د شبکې راتلونکي او تلونکي ټرافیک څیړي او **کنټرولوي**. فایروال د فلټر په توګه کار کوي او خوندي ټرافیک ته د تیریدو اجازه ورکوي او همداراز د **زیان رسوونکي یا شکمن ټرافیک مخه نیسی**.

ویندوز او مک (Mac) کمپیوټرونه **په خپل ځان کې دننه** فایر والونه لري چې د انټرنټ ټرافیک د څیړلو او فلټر کولو له لارې په اساسي کچه خوندیتوب برابروي. د دې تنظیمول د ویندوز **امنیتي تنظیماتو** یا د مک کمپیوټرونو د **امنیت او خصوصی حریم تنظیماتو** له لارې آسانه دی.

په ویندوز 10 یا ویندوز 11 کې د 'Start' تنې کیکاړئ، او لاندې مراحل تعقیب کړئ:

’Settings > Update & Security > Windows Security > ‘Firewall & Network protection

په دې کار سره دلته تاسو به د خپل ویندوز فایروال حالت وګورئ. باید ډاډه شئ چې **د 'ON' تنې رونبانه ده**. که تاسو د لا ډیر امنیت او خوندیتوب په لټه کې یاست او د فایر وال څخه بهر کنټرول غواړئ، کولای شئ د ویندوز کمپیوټر لپاره د Tinywal سافټویر (په وړیا توګه) او د مک کمپیوټر لپاره Little Snitch سافټویر(په پیسو) تر لاسه کړئ.

اپډیټونه

د سافټویر تازه کول یا اپدیټ کول د ډیجیټلی چاپیریال د خوندي ساتلو لپاره یو له خورا مهمو ګامونو څخه ګڼل کیږی. منظم اپډیټ د نویو ګواښونو پر وړاندې ستاسو د دستګاوو په خوندې کولو کې مرسته کوي او ډاډ درکوی چې ستاسې پروګرامونه په سمه توګه کار کوي.

نوې زیانمنې تل په سافټویر کې موندل کیږي او هیکران په چټکۍ سره د دغو زیانمنو نه د ګټې اخیستنې لارې چارې پیدا کوي. د سافټویر په اپډیټونو کې ډیری وخت د نویو موندل شویو زیانونو حل لارې شاملې دي. خپل د سافټویر منظم اپډیټ کولو له لارې تاسو هغه امنیتي تشې ډکوئ چې یو هیکر له هغوی نه د ګټې اخیستلو په لټه کې دی.

عمومي لارښوونې

- بلوتوت غیر فعال کړئ
- د لټون نیټې پاکې کړئ یا د خصوصي لټون حالت وکاروئ.
- په خپل ټیلفون کې حساس معلومات مه ساتئ.
- په پیغامونو کې د حساسو معلوماتو لیږلو څخه ډډه وکړئ.
- حساس پیغامونه/عکسونه/ویډیوګانې پاک کړئ.
- خپل ټیلفون یوازې مه پریږدئ.
- د بل چا له ټیلفون څخه خپلو اکاونټونو ته مه ننوځئ.

که فکر کوئ چې تالاشۍ سره به مخ شئ

لاندني وسایل ځان سره مه لیږدوئ

دغه وسایل کولای شي امنیتي خطر رامنځته کړي ځکه چې د شخصي معلوماتو ترلاسه کولو یا ثبتولو لپاره کارول کیدای شي.

- ګرځنده ټیلفونونه
- ځیرک ساعتونه
- لپ ټاپ کمپیوټر یا ټابلیټ
- GPS (نړیوال موقعیت ټاکونکي سیسټمونه)

د خوندي کولو لپاره نور ګټور اقدامات

په شفر یا کوډ خبرې وکړئ

د دې لپاره چې ځان ته د چا پام وا نه ړوئ، د مهمو پیغامونو لیږلو لپاره ساده جملې یا نښې وکاروئ.

د مثال په توګه د 'هوا څنګه ده؟' جمله د 'آیا تاسو خوندي یاستئ؟' جملې د شفر یا کوډ په توګه کارول کیدای شي. خپل د اعتبار وړ ملګرو سره د دغو کوډونو د کارولو په اړه مخکې له مخکې موافقه وکړئ.

حساس چټونه (لیکنې) پاک کړئ

د ضرورت پر وخت د خپل خصوصی حریم د خوندي کولو لپاره، ناخوندي او له خطرنه ډکې مکالمې په منظم ډول پاکې کړئ.

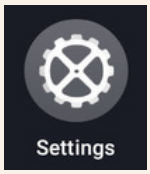
دغه لارښوونې نښایي یو څه نا آشنا ښکاره شي، خو کیدای شي په سختو شرایطو کې ژښتینې ژغورونکي وي. یو ګام وړاندې واخلئ او خوندي پاتې شئ!

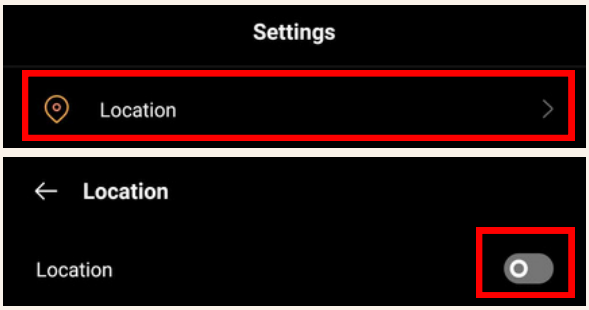
د ګرځنده دستګاه (وسیلې) د امنیت د تنظیمولو لپاره ګامونه

د اندروید ټیلفون خوندي کول

د خپل ګرځنده ټیلفون وای فای، GPS (نړیوال موقعیت ټاکونکی سیستم) او انټرنیټ غیر فعال کړئ.

‘Settings’ → ‘Location.’



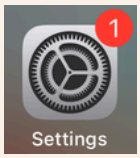


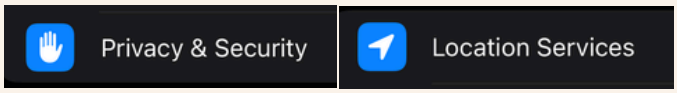
کیږ اړخ ته د تنې په کشولو سره، لوکیشن (موقعیت) بند کړئ.

د آیفون ټیلفون خوندي کول

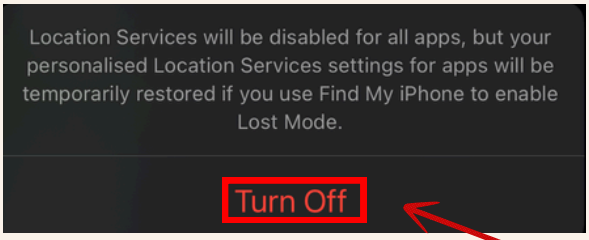
وای فای او GPS (نړیوال موقعیت ټاکوونکی سیستم) غیر فعال کړئ.

‘Settings’ → ‘Privacy & Security’ → ‘Location Services’





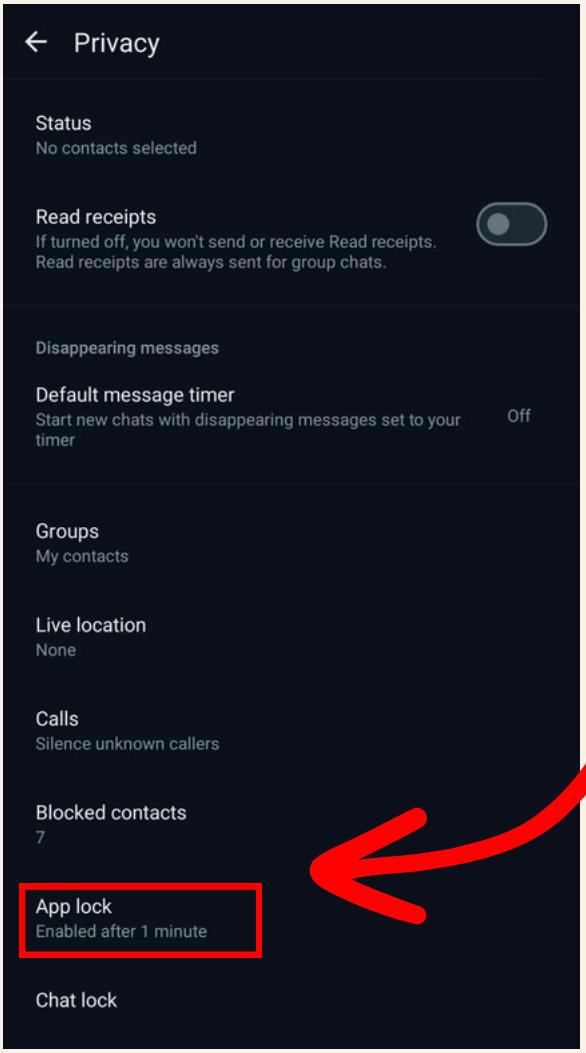
د هر اپلیکیشن لپاره د اصلي سلایډر یا انفرادی سلایډرونو په کارولو سره ټول ‘Location Services’بند کړئ.



د لوکیشن بندولو لپاره په سلایډر باندې کلیک وکړئ.

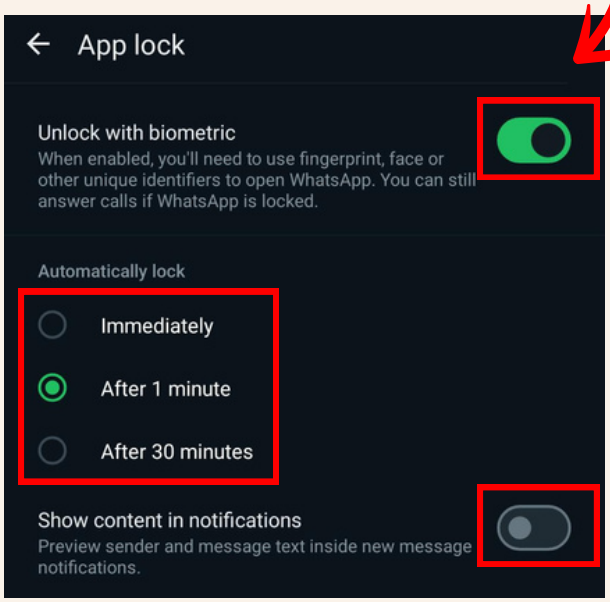
په واټساپ کې د خصوصي حریم د تنظیمولو په اړه ګامونه

د واټساپ ټرل



د واټساپ تنظیمات راخلاص کړئ:
‘Settings’ → ‘Privacy’ → ‘App lock.’

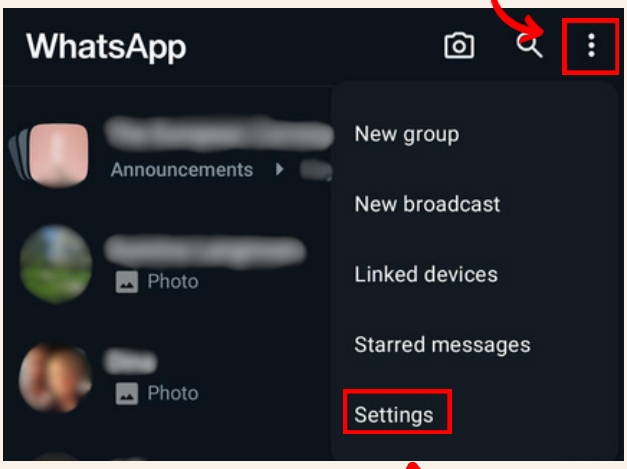
د ‘Unlock with biometric’ ټنۍ فعاله کړئ ← د تایید لپاره د ګوتو نښې سنسر لمس کړئ یا خپل مخ سکن کړئ.

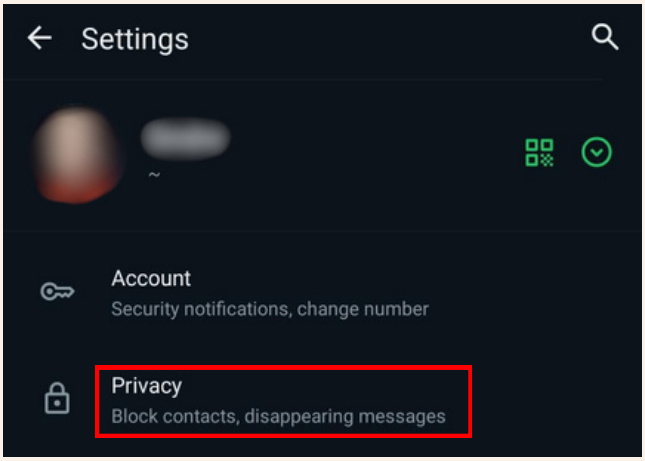


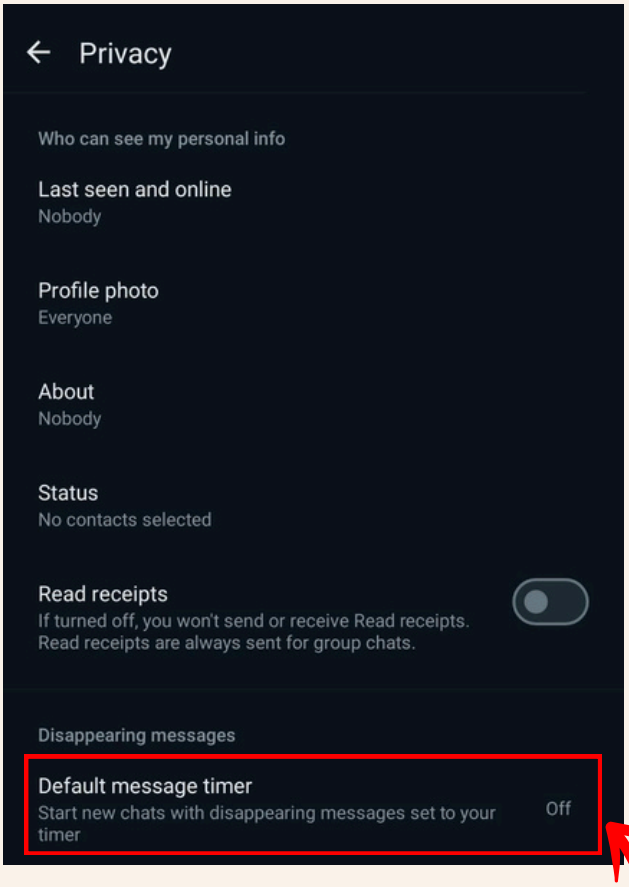
د اپلیکیشن د بندولو موده وټاکئ او د 'show content in notifications' ټنۍ غیر فعاله کړئ.

د پیغامونو د ورکېدو (غاییبیدو) د ځانګړنې فعالول او بندول

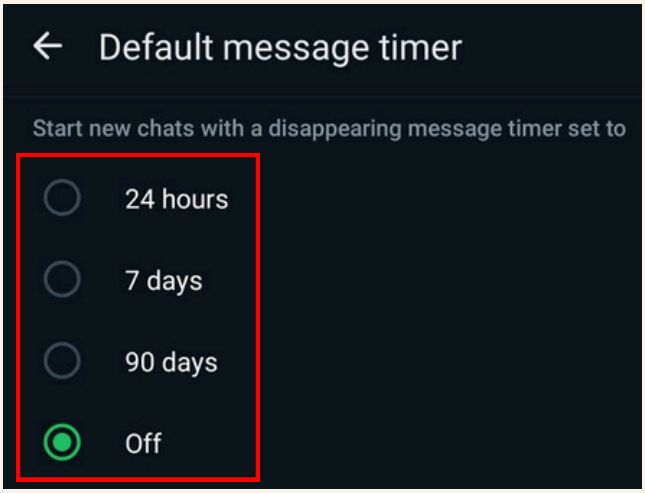
د درې ټکو تنۍ کیکاږئ او بیا ← 'تنظیمات' ← 'خصوصي حریم ته لاړشئ







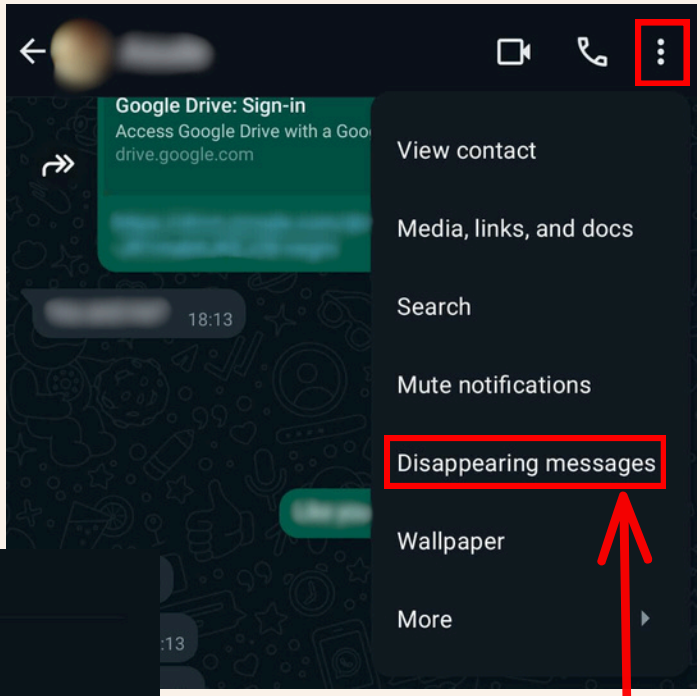
'Default message timer' په باندې کلیک وکړئ.



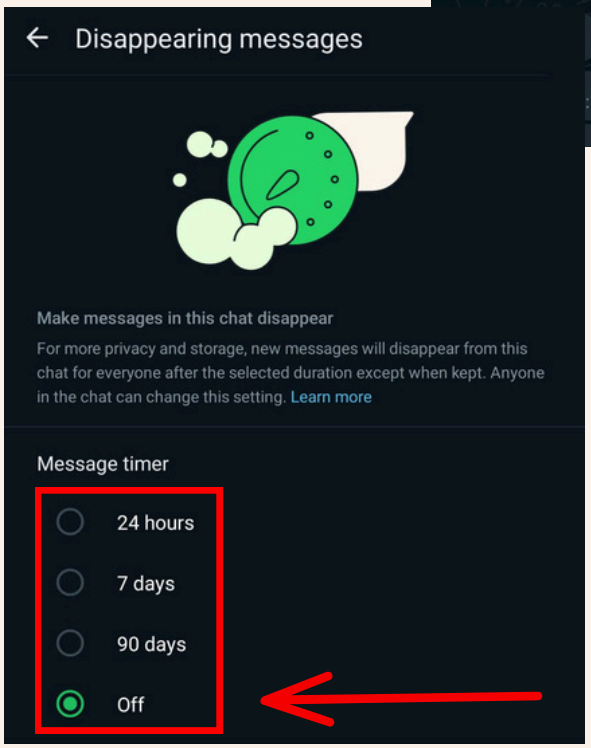
۲۴ ساعته، ۷ ورځې، ۹۰ ورځې یا 'Off' انتخاب کړئ.

په خصوصي مکالمو کې د پیغامونو د ورکېدو د ځانګړنې فعالول

یوه مکالمه (چټ) خلاصه کړئ او د اړیکه نیوونکي کس په نوم باندې کلیک وکړئ (یا دري ټکي انتخاب کړئ).

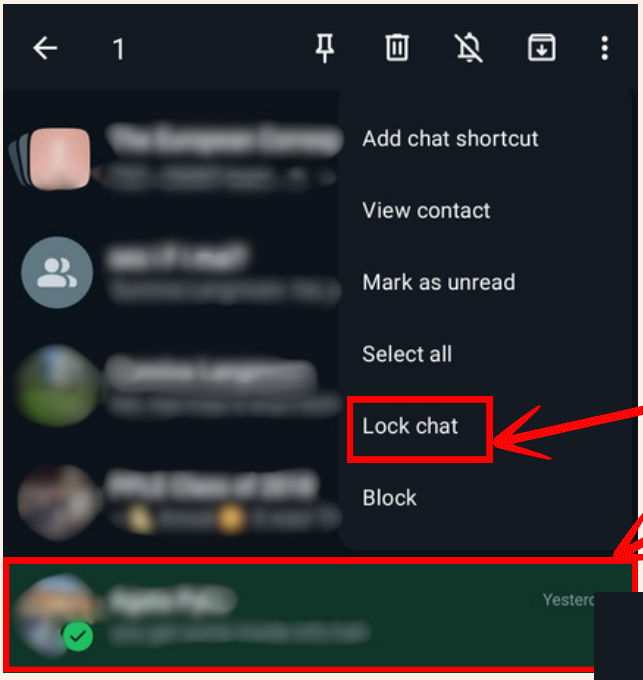


ورکیدونکو پیغامونو (Disappearing messages) باندې کلیک وکړئ.



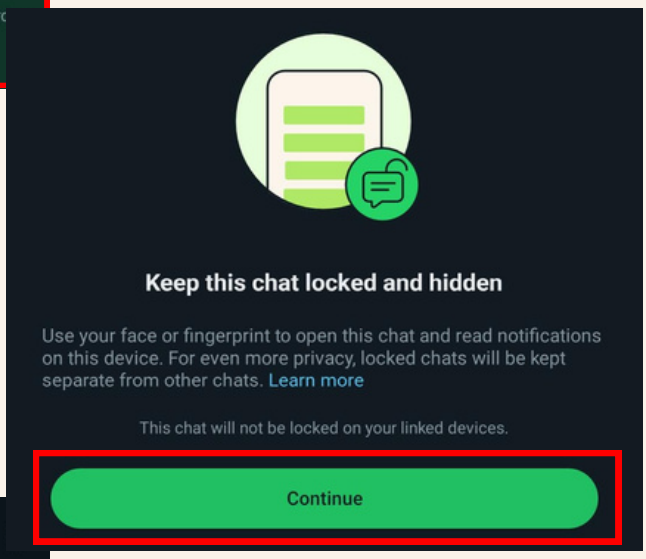
۲۴ ساعته، ۷ ورځې، ۹۰ ورځې یا 'Off' انتخاب کړئ.

د مکالمې (چټ) د بندولو طریقه

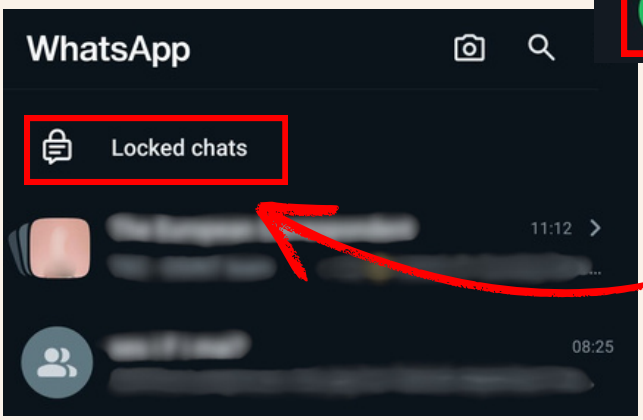


پر هغې مکالمې باندې چې تاسو یې بندول غواړئ، ګوته کیکاړئ او د څو ثانیو لپاره یې ورباندې ټینګه ونیسئ

← 'Lock Chat' انتخاب کړئ.



← د 'Continue' تڼۍ (اختیار) کیکاړئ.
← د بندولو لپاره خپل مخ یا د ګوتو نښه تایید کړئ.

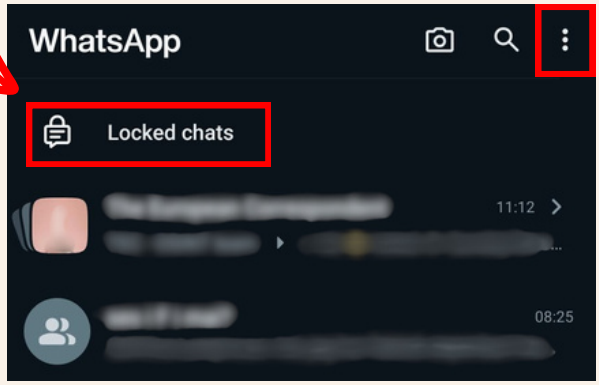


ستاسو مکالمې (چټ) اوس 'قفل شوي مکالمې' فولډر ته ولیږدول شوې!

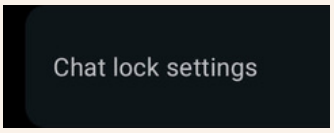
خپلې مکالمې د (پټ کوډ) په کارولو سره خوندي (قفل) کړئ.

وروسته له دې چې تاسو د مکالمې قفل فعال کړ، کولای شئ خپلې مکالمې د یو پټ کوډ له لارې چې ستاسو د ټیلفون پټنوم څخه توپیر ولري، خوندي کړئ.

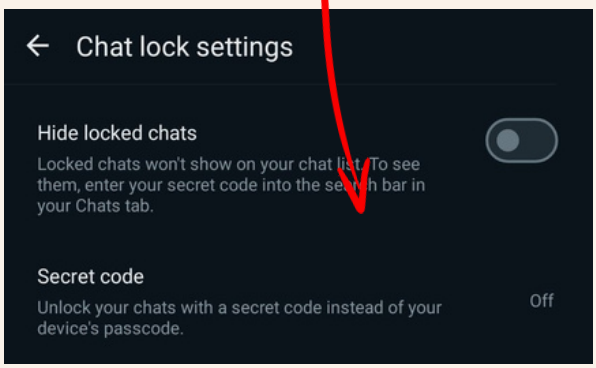
د قفل شویو مکالمو فولډر خلاص کړئ ← د صفحې په پورتنۍ ښۍ خوا کې په دریو ټکو باندې کلیک وکړئ.



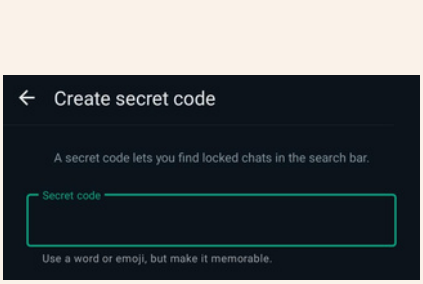
← 'د مکالمې د بندولو تنظیمات' یا (Chat lock settings) انتخاب کړئ.



← 'پټ کوډ' یا (Secret Code) باندې کلیک وکړئ .



← پټ کوډ جوړ او تایید یې کړئ.

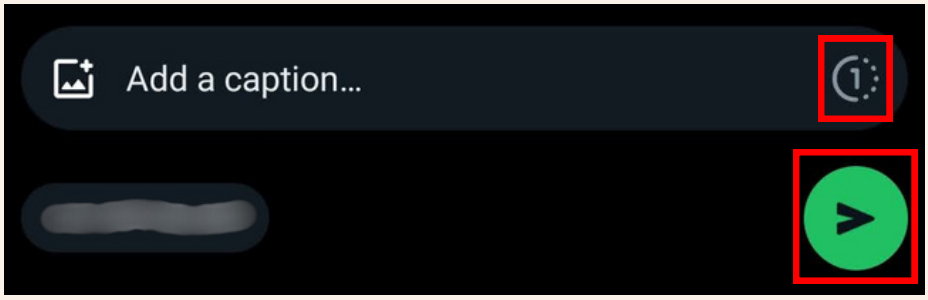


د یو ځل لپاره د لیدلو وړ عکسونه/ویډیوګانې واټساپ کې ولیږئ

یوه انفرادي یا ګروپي مکالمه (چټ) خلاصه کړئ.

د لیږلو لپاره عکس یا ویډیو انتخاب کړئ یا په کامرې عکس یا ویډیو واخلئ.

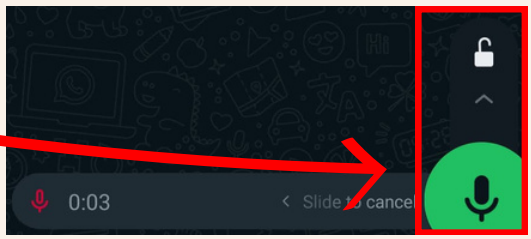
د صفحې په ښکته ښي کونج کې د ① پر تڼۍ کلیک وکړئ او وروسته له هغه د ➤ تڼۍ کیکاږئ.



د یو ځل لپاره خپریدونکي غږیز پیغامونه واټساپ کې ولیږئ

یو انفرادی یا ګروپی مکالمه (چیټ) خلاص کړئ.

مایکروفون د ګوتې په واسطه لاندې ښیې کونج ته ښکته کړئ او بیا یې پورته کش کاږئ.

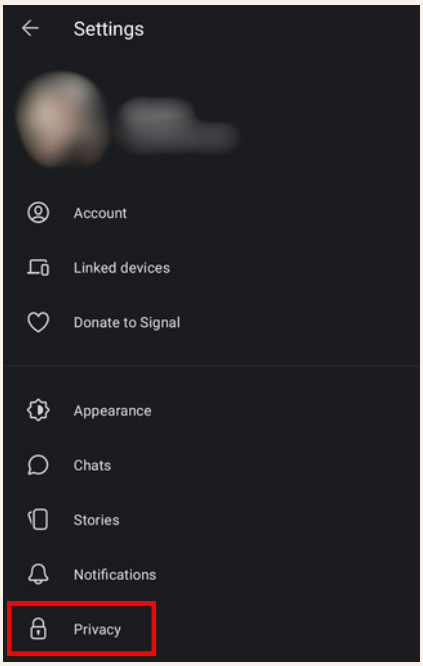


د آواز ضبطولو وروسته د ⏸ تڼۍ کیکاږئ ← د ① تڼۍ انتخاب کړئ ← او بیا د ➤ تڼۍ کیکاږئ.

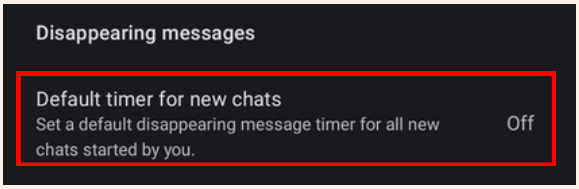
په سیګنال کې د خصوصي حریم د تنظیمولو پرلاوونه

د ورکېدونکو پیغامونو فعالول یا بندول

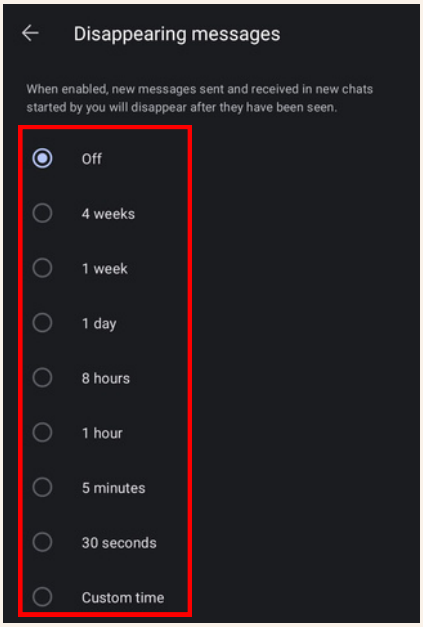
د خپل پروفایل پر عکس باندې کلیک وکړئ ← 'خصوصي حریم'



'ورکیدونکو پیغامونو' ته لاړ شئ او پر 'Default timer for new chats' باندې کلیک وکړئ.

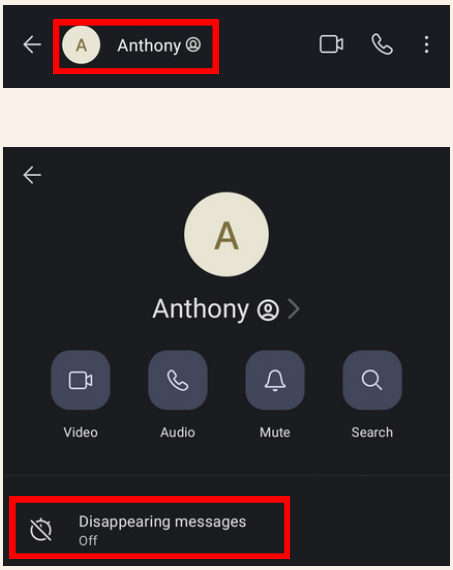


د پیغامونو د ورکېدو (غایبیدو) لپاره خپل د خوښې وړ موده وټاکئ.



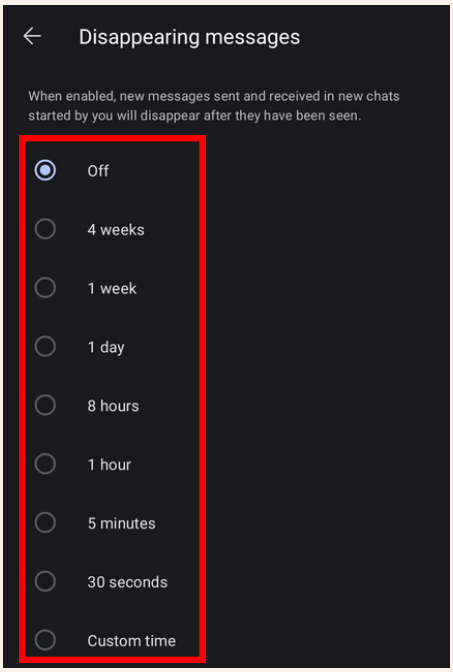
په انفرادي مکالمې (چټ) کې د ورکیدونکو پیغامونو آپشن فعالول

یوه مکالمه (چټ) خلاصه کړئ او د مخاطب کس پر نوم باندې کلیک وکړئ.

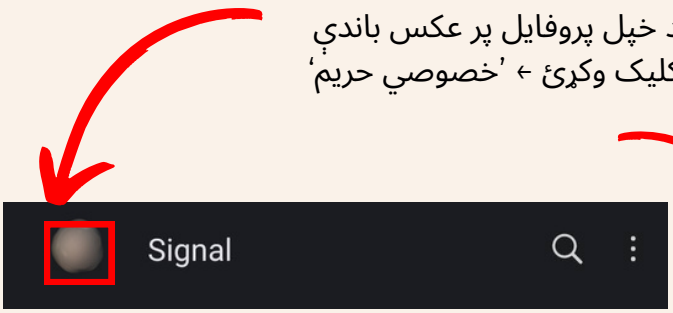


پر ورکیدونکو پیغامونو (Disappearing messages) باندې کلیک وکړئ.

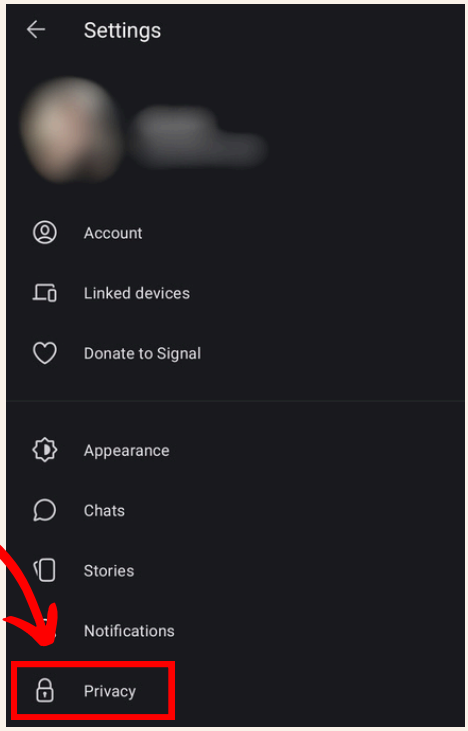
د پیغامونو د ورکېدو لپاره خپله د خوښې وړ موده وټاکئ.



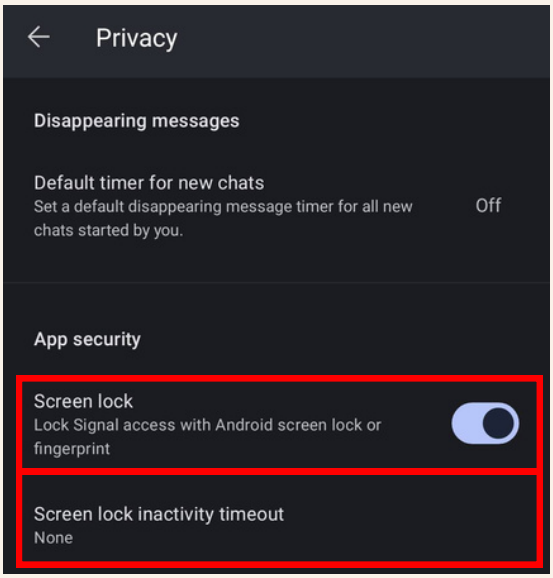
د سیګنال قفل کول (خوندي کول)



د خپل پروفایل پر عکس باندې کلیک وکړئ ← 'خصوصي حریم'



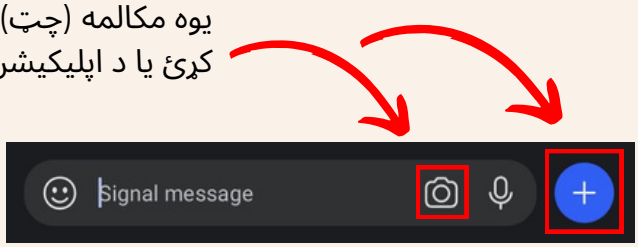
د 'اپلیکیشن د خوندیتوب' یا ''App Security برخې لاندې 'د پاڼې قفل' یا ''Screen Lock تنې بدله کړئ.



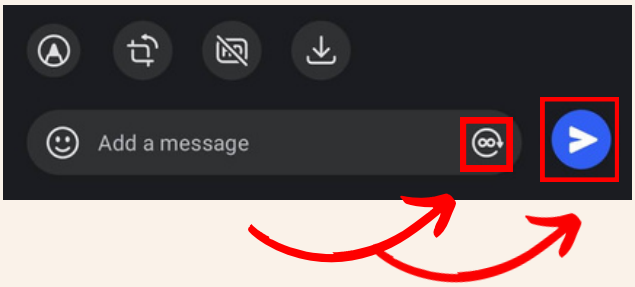
د خپل سیګنال پروګرام بندولو لپاره د 'Screen lock inactivity' تنې کیکاړئ چې پس له دې timeout کاره به ستاسو سیګنال بند شی.

د سیګنال له لارې د ورکیدونکو عکسونو/ ویډیوګانو لېږل

یوه مکالمه (چټ) خلاصه کړئ او یو عکس/ ویډیو انتخاب کړئ یا د اپلیکیشن په کامرې عکس یا ویډیو واخلئ.

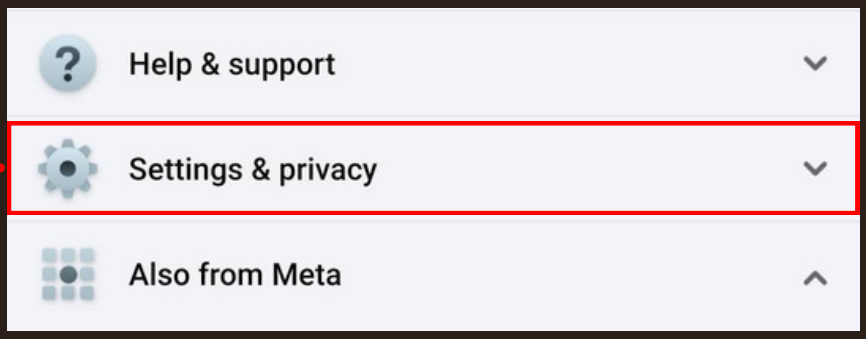


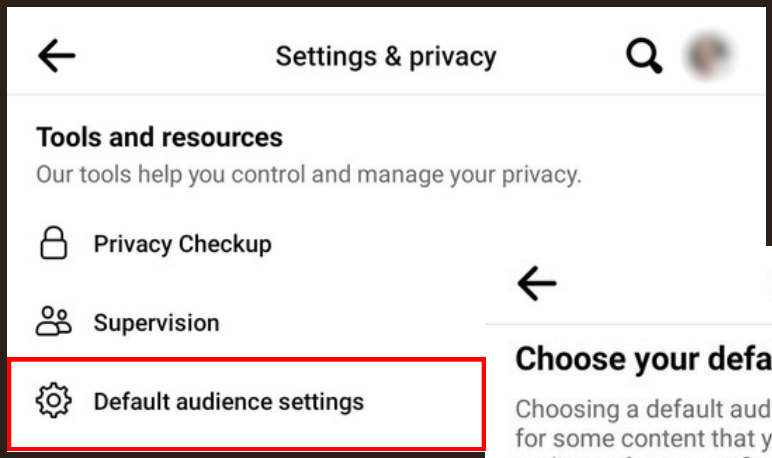
د صفحې په ښکته ښي کونج کې پر تڼۍ باندې کلیک وکړئ او بیا د تڼۍ انتخاب کړئ.



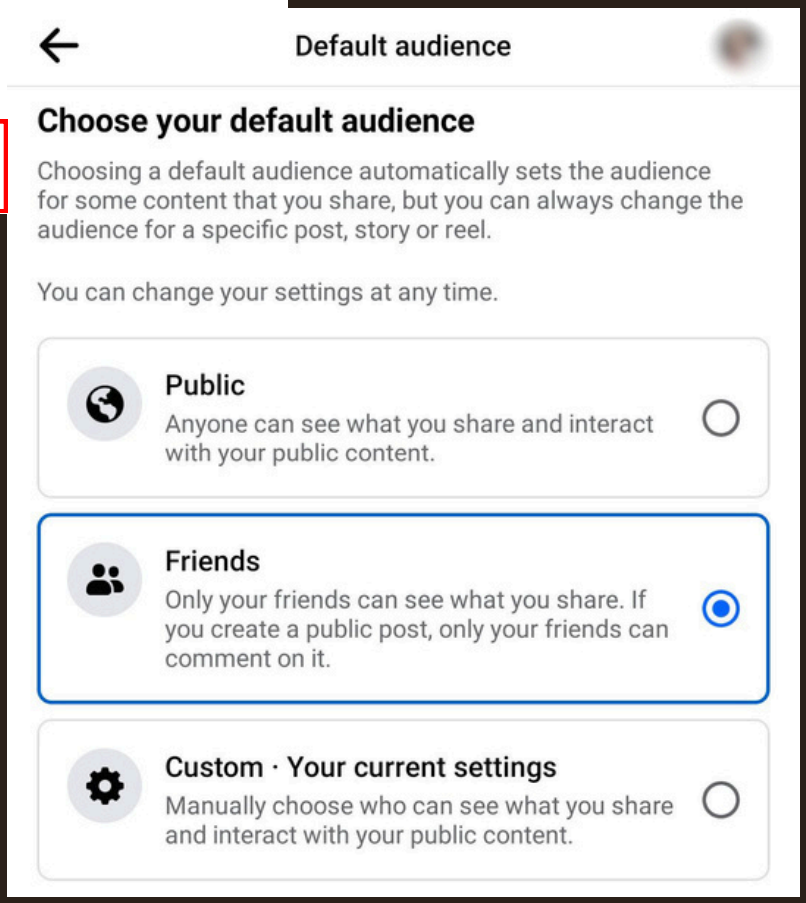
۳. د ټولنیزو رسنیو د اکاونټونو خوندي کول

په فیسبوک کې د خصوصي حریم د تنظیمولو پړاوونه

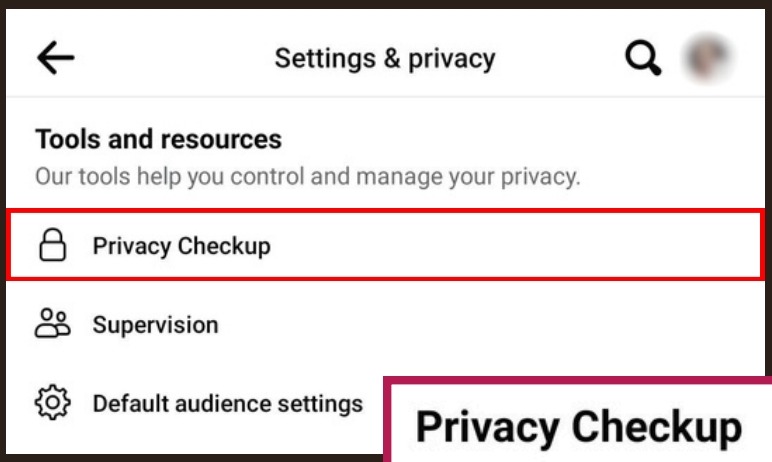


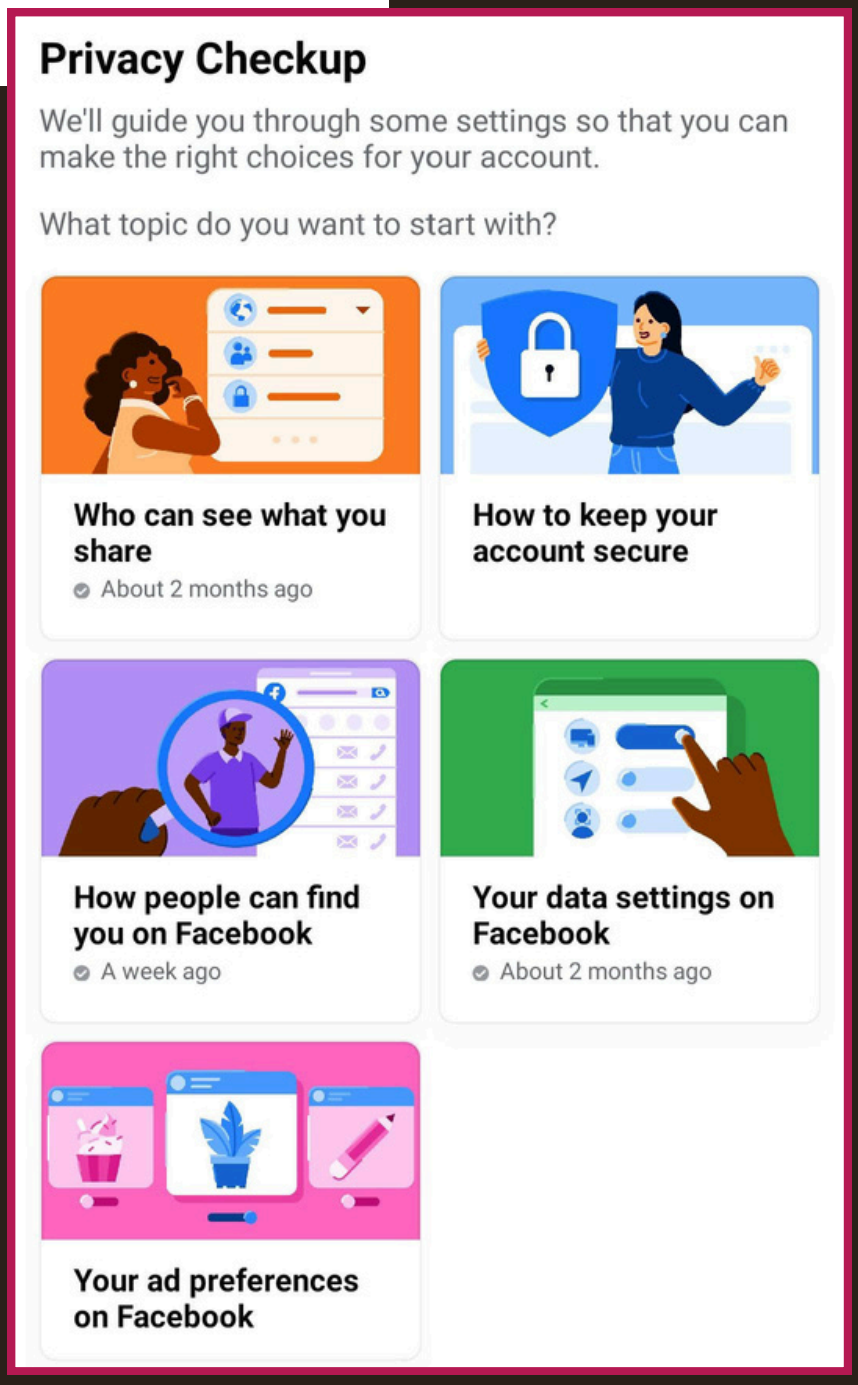


د 'Default audience settings' آپشن تاسو ته دا امکان درکوي ترڅو پریکړه وکړي چې څوک کولای شي ستاسو پوسټونه، لیکنې او نور شیان وګوري.

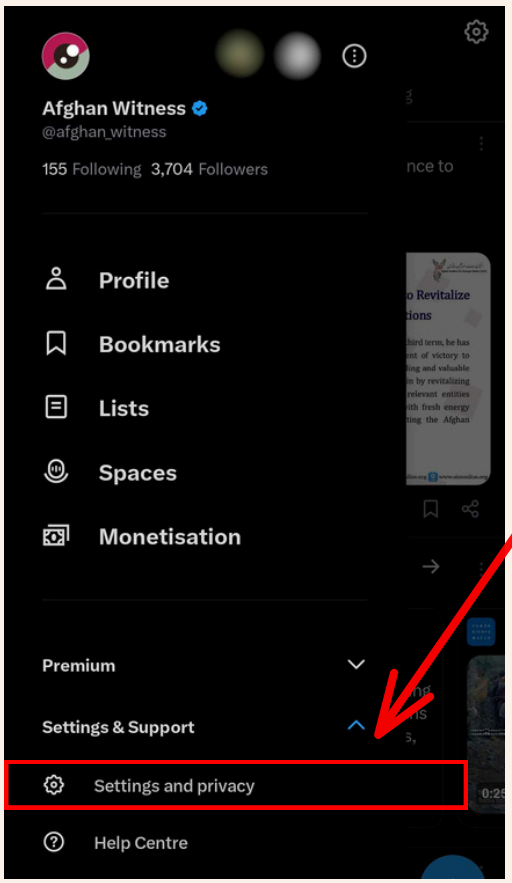


د ''Privacy Checkup ' آپشن تاسو
ته د تنظیماتو په اړه لا ډیر معلومات
وړاندې کوي او تاسو ته دا امکان
برابروي تر څو د خصوصي حریم
تنظیمات لوړې کچې ته ورسوئ.

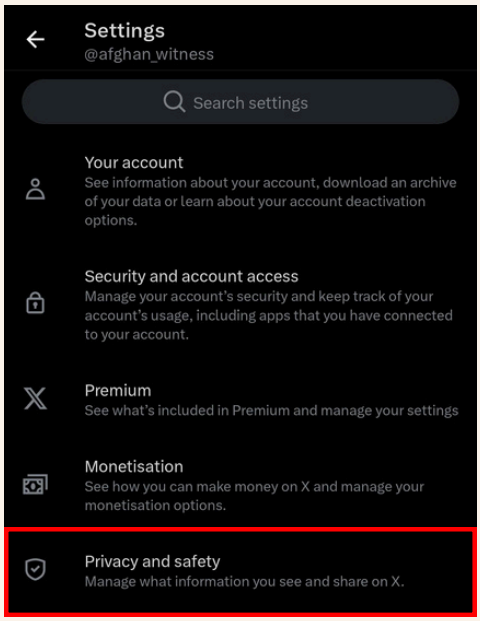




په ایکس/ټویټر پاڼه کې د خصوصی حریم د تنظیمولو پړاوونه



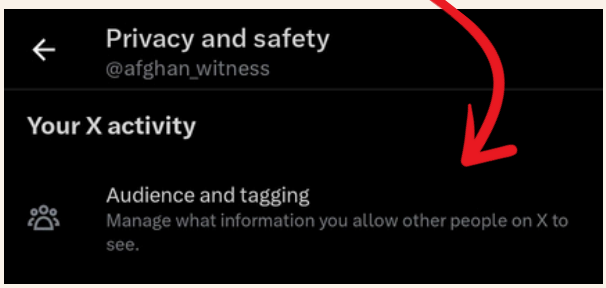
د خپل پروفایل پر عکس کلیک وکړئ، اول په 'Settings & Support' باندې او بیا پر 'Settings and privacy' باندې کلیک وکړئ.

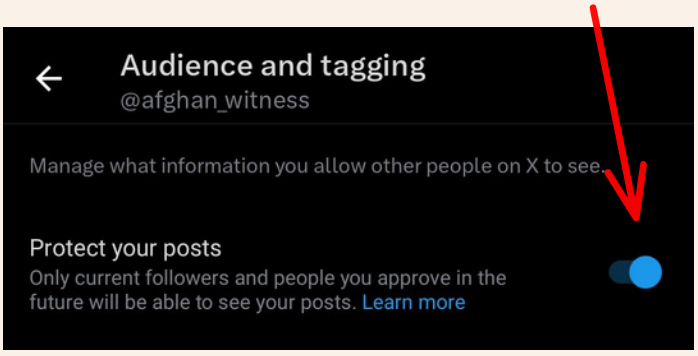


اوس پر 'Privacy and safety' باندې کلیک وکړئ.

د 'Protect your posts' انتخاب فعال کړئ ترڅو یوازې ستاسو پیروان (فالوورز) وکولای شي ستاسو پوسټونه وګوري.

اوس 'Audience and tagging' کیکاږئ.



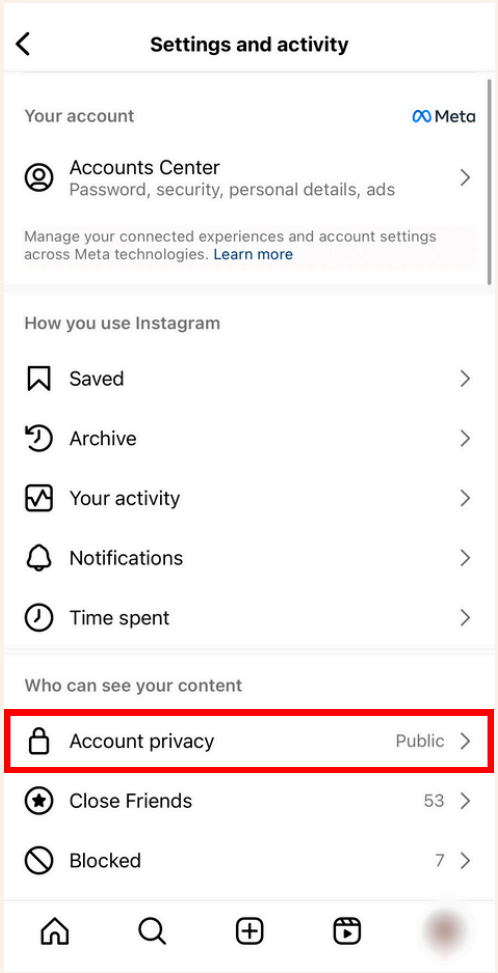


په انسټاګرام کې د خصوصي حریم د تنظیمولو پړاوونه

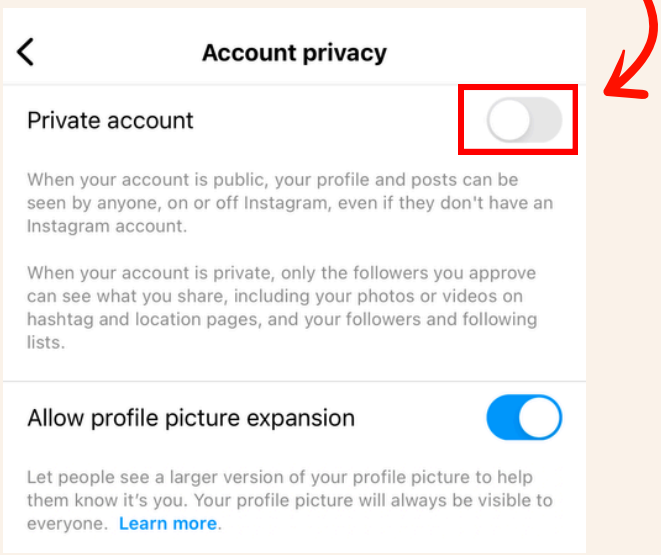
د صفحې په ښکته ښي خوا کې د خپل پروفایل پر عکس کلیک وکړئ.

اوس په پورتنۍ ښي کونج کې په درې کرښو باندې کلیک وکړئ.

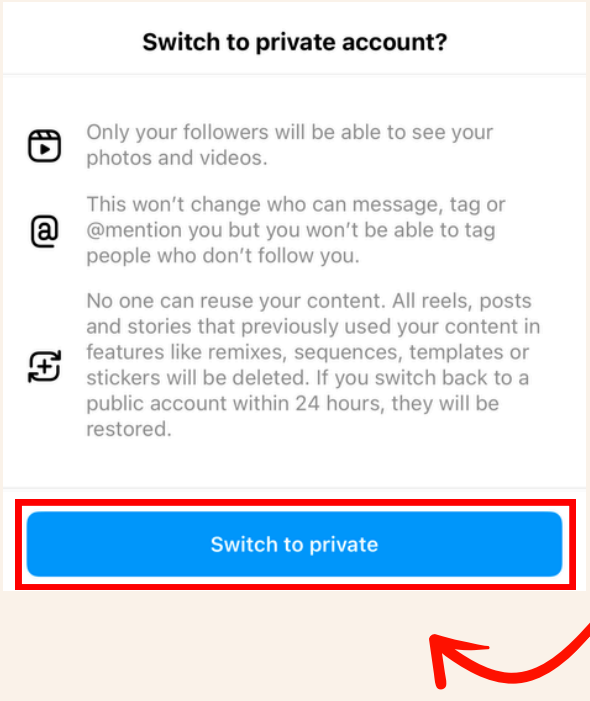
د 'Who can see your content' ټنۍ لاندې د "Account privacy' ' ټنۍ کیکاږئ.



د خپل اکاونټ خصوصي کولو لپاره د 'Private account' ټنۍ ښي خوا ته کش کړئ.



د تایید لپاره په 'Switch to private' باندې کلیک وکړئ.



۴. په انټرنیټ/ویب کې لټون

د خطرونو پېژندنه

په انټرنیټ/ویب کې د لټون پر مهال، تاسو ځان له بیلابیلو خطرونو سره مخامخ کوئ.

کیدای شي تاسو د چارواکو یا آن د کورنۍ غړو لخوا **تعقیب او وڅارل شئ** چې دوی کولای شي ستاسو د انټرنیټ ټول ټرافیک ته لاسرسی ومومي.

کیدای شي تاسو د **وایرسونو او بدو پوستغالو** (malware) د بریدونو له خطر سره مخ شئ چې په دې حالت کې ستاسو دستګاوې د داسې یو وایرس لرونکي سافټویر سره اخته کیږی چې ستاسو معلومات (ډیټا) غلا کوي او ستاسو فعالیتونه ځاري.

کیدای شي تاسو د **فیشینګ برید** موخه واوسئ. دا په دې معنی چې هرکله یو برید کوونکی هڅه وکړي تاسو ته د جعلی پیغامونو، بریښنالیکونو او ویبسایټونو د استولو له لارې چې تاسو ته با اعتباره ښکاري، ستاسو د یوزرنیم (د اکاونټ نوم)، پټنومونو او مالی معلوماتو د ترلاسه کولو لپاره تاسې وغولوي.

همداراز کیدای شي تاسو د معلوماتو د **افشا کېدو یا خپرېدو** ښکار شئ. دا په دې معنی چې د اعتبار وړ د خدمتونو وړاندې کوونکې مراجع هیک کیږي او د دوی معلومات (ډیټا) چې ښایي ستاسو شخصی معلومات هم پکې شامل وي، غلا کیږی.

د ځینو احتیاطي تدابیرو په نیولو سره، تاسو کولای شئ د دغو بریدونو پر وړاندې خپله د **زیانمن کیدو** کچه **راټیټه** کړئ.

مجازي خصوصي شبکې (VPN) او ناپیژانده لټون

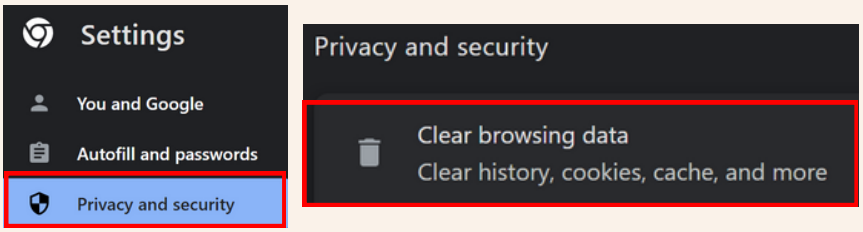
مجازي خصوصي شبکې (VPNs) ستاسو د IP پته پټوي او ستاسو د انټرنیټ اړیکه کوډ کوي چې دا کار د هغه کسانو لخوا ستاسو څارنه خورا ستونزمنوي چې ستاسو د دستګاه یا کور نه ستاسو د انټرنیټ فعالیت ګوري. ښه ده چې د اعتبار وړ مجازي خصوصي شبکې (VPN) براوزر انتخاب کړئ. په داسې حال کې چې د ډیرو مجازی خصوصي شبکو خدمتونه میاشتنی فیس لري، د Proton مجازي خصوصي شبکه تاسو ته غوره وړیا خدمتونه وړاندې کوی.

د لا ډیر خوندیتوب لپاره د تور **Tor** براوزر انتخاب کړئ. دغه براوزر یوه ځانګړې غیر متمرکزه کوډ شوی شبکه کاروي چې د هیڅ حکومت لخوا نه څارل کیږی او وړیا ده. دغه براوزر تاسو ته په آنلاین ډول ترټولو غوره ناپیژانده نوم درکوي. خو تاسو باید خپل شخصي اکاونټونو ته د ننوتلو لپاره د **Tor** براوزر کارولو نه ډډه وکړئ.

په انټرنیټ کې د خپل لټون سابقه/تاریخچه پاکه کړئ

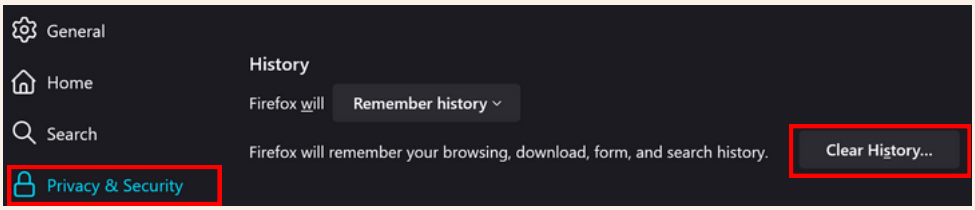
Chrome

‘Settings’ → ‘Privacy and security’ → ‘Clear browsing data’



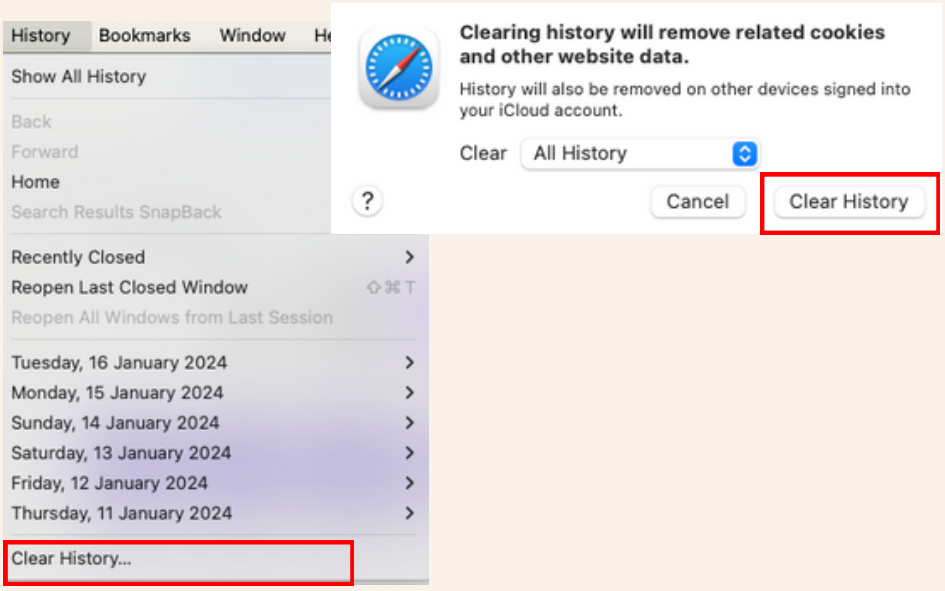
Firefox

‘Settings’ → ‘Privacy & Security’ → ‘History’



Safari

‘Settings’ → ‘Safari’ → ‘Clear History and Website Data’



مجازي خصوصي شبکه (VPN) وکاروئ

مجازي خصوصي شبکه يا VPN ستاسو د IP پتې د پټولو او ستاسو د انټرنيټ ټول ټرافيک کوډ کولو لپاره يوه لاره ده ترڅو هيڅوک و نشي کولای هغه څه وموميِ چې تاسو يې په آنلاين توګه ګورئ.

د لاندې مجازي خصوصي شبکو (VPN) سپارښتنه کيږي:

- Proton VPN (وړيا)
- Tunnelbear (۲ ګيګه وړيا)
- Surfshark ($۲.۴۹ په مياشت کې)
- NordVPN ($۳.۹۹ په مياشت کې)
- Private Internet Access ($۳.۳۳ په مياشت کې)

د کمپيوټر پاکوونکی سافټويِر (PC Cleaning) وکاروئ.

د لاندنيو کمپيوټر پاکوونکو سافټويرونو سپارښتنه کيږي:

CCleaner

BleachBit

د کمپيوټر پاکولو سافټويرونه لکه **CCleaner** او **BleachBit** په اوتوماتيک ډول په اينټرنيټ کې د لټون د تاريخونو پاکولو له لارې ستاسو د کمپيوټر په پاکولو کې، ستاسو د کمپيوټر د اغيزمنتوب او فعاليت د دوام لپاره او ستاسو د محرميت په ساتلو کې مرسته کوي.

خصوصي لټون حالت وکاروئ

د خصوصي لټون لپاره لاندني شارټ کټونه (shortcuts) وکاروئ:

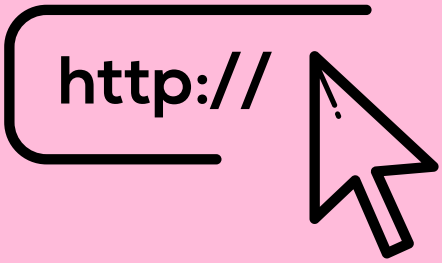
Chrome — Ctrl + Shift + N

Firefox — Ctrl + Shift + P

Safari — Command + Shift + N

خصوصي لټون حالت په ويب براوزرونو کې يوه ځانګړنه ده چې ستاسو د لټون د **تاريخچې، کوکيز (د معلوماتو غير اړين کوچنی فايلونه) او نورو داخلي معلوماتو د راغونډېدو او زيرمه کيدو مخه نيسي** او ستاسو د آنلاين محرميت په ساتلو کې مرسته کوي.

خو دغه حالت د هغه کسانو پر وړاندې چې ستاسو آنلاين فعاليتونه **له بهر څخه** ګوري او ستاسو شبکې ته لاسرسی لري، کومه ګټه **نه کوي** - نو ځکه تاسې بايد نور احتياطي تدابير ونيسئ.



بدیل براوزرونه او د لټون ماشینونه

د محرمیت د نښه خوندي کولو لپاره، کروم (Chrome)، سافاري (Safari) یا ایج (Edge) مه کاروئ او د ګوګل لټون ماشین کارولو څخه ډډه وکړئ.

فایرفاکس (Firefox) یو نښه انتخاب دی، خو په دې شرط چې په سمه توګه يې تنظیم (Configure) کړئ او د خپل محرمیت خوندی کولو لپاره د ویب براوزر د ملاتړ سافټویر (extensions) نصب کړئ.

هغه براوزرونه او ماشینونه چې شپارښتنه يې کیږی

Brave ← هغه براوزر چې د اعلانونو او تعقیبوونکو مخه نیسی

Tor ← هغه سافټویر چې د کوډ شوي شبکې په کارولو سره براوزر ناپیژانده کوي

DuckDuckGo ← د لټون خصوصي ماشین

Startpage ← د لټون خصوصي ماشین

د ویب براوزر د ملاتړ سافټویرونه (Browser Extensions)

د ویب براوزر د ملاتړ سافټویرونه چې د **add-ons** یا **plugins** په نومونو هم پیژندل کیږي، هغه پروګرامونه دي چې د ویب براوزر ملاتړ کوي او تنظیموي يې.

دغه سافټویرونه کولای شي د **دریمو یا ثالثو اړخونو (اشخاصو) په بندولو سره چې ستاسو آنلاین فعالیتونه تعقیبوي**، ستاسو د محرمیت په خوندي کولو کې مرسته وکړي. خو بیا هم احتیاط وکړئ ځکه چې ځینې د ویب براوزر د ملاتړ سافټویرونه (extensions) کیدای شی زیان اړوونکي واوسي.

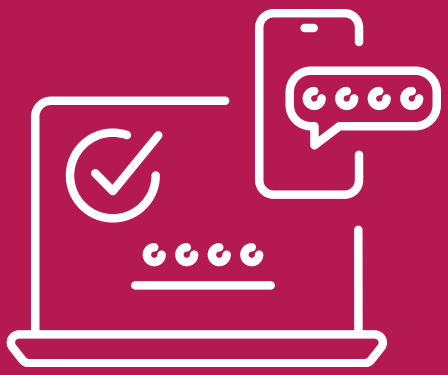
مور د **uBlock Origin** سافټویر نصبولو سپارښتنه کوو چې دغه سافټویر نه یوازې اعلانونه بندوي او ستاسې لټون ګړندی او نښه کوی، بلکې ستاسو د خصوصي حریم نه هم ساتنه کوی او ستاسو تعقیبول ستونزمن کوي.

۵. د پټنوم یا پاسوورډ خوندیتوب

د پټنوم امنیت **د شخصي خوندیتوب او محرمیت ساتلو لپاره اړین دی**.

له بده مرغه، ډیری خلک ضعیف پټنومونه لکه '123456'، "password ' یا نومونه او د زیږیدنې نیټې کاروي چې په آسانۍ سره اټکل او د غلا کیدو له خطر سره مخامخ کیدای شي. همداراز ځینې خلک خپل پټنومونه په خپلو کتابچو یا د خپلې دستګاه په فایل کې ساتي چې هرڅوک یې په آسانۍ سره موندلای شي. ځینې خلک د خپلو ټولو حسابونو لپاره یو ډول پټنوم کاروي.

د پیاوړي پټنوم امنیت په پام کې نیول د حساسو معلوماتو په خوندي کولو کې مرسته کوي او د شخصي اړیکو، ځایونو او فعالیتونو د خصوصي ساتې کیدو په اړه ډاډ درکوي. د پاسوورډ منیجر کارول ستاسو د امنیت او خوندیتوب لوړولو لپاره تر ټولو غوره لاره ده: پاسوورډ منیجر په اوتوماتیک ډول ستاسو د ټولو اکاونټونو لپاره خوندي پټنومونه جوړوی، پداسې حال کې چې تاسې ټولو پټنومونو ته د لاسرسۍ لپاره باید یوازې یو پټنوم په یاد ولرئ.



ښې طريقې:

✅ لږترلږه **۱۵ حروف** وکاروئ.

✅ له حروفو نه جوړ شوي پټنوم پرځای د **کلمو** نه جوړ شوي پټنوم کارولو په اړه فکر وکړئ:

یوه **جمله** یا د **مختلفو کلمو ټولګه یا ترکیب** یو نه ماتیدونکی پټنوم رامنځته کوي، پداسې حال کې چې کولای شو په آسانۍ سره یې په یاد وساتو.

داسې یو څه لکه '**smallfrogsittinginatree**' یا په بشپړ ډول مختلف یو څه لکه '**frozenspouseimperfectjuice**' کارول وآزمایئ.

✅ د غټو او کوچنیو حروفو، شمېرو او سمبولونو د ترکیب کارول کولای شي ستاسو د اکاونټ امنیت پیاوړی کړي

✅ د **خپل پټنوم پیاوړتیا** د پټنوم د آزمویلو آنلاین وسیلې، لکه www.passwordmonster.com په کارولو سره وآزمویئ.

✅ خپل پټنوم هر ۳ تر ۹ میاشتو وروسته یا د اړتیا پر وخت **بدل کړئ**.

✅ د **مختلفو حسابونو** (اکاونټونو) لپاره مختلف پټنومونه وکاروئ.

✅ **پاسوورډ منیجر پروګرام** وکاروئ.

✅ په خپلو اکاونټونو کې **دوه فکتوره تصدیق (FA2)** سیسټم فعال کړئ. د ګرځنده ټیلفون اپلیکیشنونه، لکهGoogle Authenticator هم ښه کار کوي!

بدې طريقې:

🚫 هیڅکله تکراري پټنومونه (پاسوورډونه) مه کاروئ.

🚫 براوزر ته اجازه مه ورکوئ چې پټنومونه وساتي.

🚫 په خپلو پټنومونو کې هیڅ شخصي معلومات مه کاروئ (لکه د زیږیدنې نیټه، د ماشوم یا د کورنیو حیواناتو نومونه او داسې نور).

🚫 د خپلو پټنومونو نوملړ د ساده متن په توګه خپل کمپیوټر کې مه ساتئ.

🚫 د خپلو پټنومونو نوملړ په کاغذ مه لیکئ او مه یې ساتئ.

پاسوورډ منیجرونه
(Password Managers)

پاسوورډ منیجرونه پیاوړي او بې ساري پټنومونه جوړوي او ساتي چې په دې کار سره ډیجیټل خوندیتوب آسانه کیږي. پاسوورډ منیجر پټنومونه په یو خوندي 'والټ' (زیرمتون) کې ساتي او د ماسټر پاسورډ (اصلی پاسورډ) سره یې خوندي کوي. د دې ګټې او ښه والی دا دی چې پټنومونه جوړ، خوندي او په اټوماټیک ډول په دستګاوو کې ساتل کیږي.

د پاسوورډ منیجر ستونزه دا ده چې که چیرې کوم څوک ستاسو پاسوورډ منیجر ته لاسرسی ومومي، نو دوی به ستاسو په ټولو حسابونو (اکاونټونو) کې ستاسو ټولو معلوماتو ته لاسرسی ولري.

دا خورا مهم دی چې خپل پاسورډ منیجر لپاره پیاوړی ماسټر پاسورډ انتخاب کړئ او ډاډ ترلاسه کړئ چې ستاسو وسیله د بدو پوستغالو (malware) پر وړاندې خوندي ده. که چیرې امکان ولري، دوه فکتوره تصدیق سیستم فعال کړئ.

KeePass یو وړیا **پاسورډ منیجر** دی چې د خلاصې سرچینې نه ترلاسه کیدای شی او کارول یې آسانه دی او د کارولو پر وخت یې ویب ته اړتیا نشته.

خپل د پاسوورډ ډیټابیس او ماسټر پاسوورډ جوړولو وروسته، تاسو کولای شئ خپل د ډیټابیس فایل په خپل کمپیوټر یا ټیلفون کې وساتئ او یا کولای شئ خپل فایل د (Cloud) پلټفارم پورې اړوند د فایلونو د زیرمه کولو سرویس (Googl Drive) کې وساتئ او پدې کار سره کولای شئ هر وخت او هرچیرې ورته لاسرسی ولرئ. دا یو ډیر عملي انتخاب دی چې تاسو ته لا ډیر کنټرول او همداراز د پروګرام اپدیټ کولو او د ډیټابیس فایل خوندي ساتلو لپاره ډیر مسؤلیت درکوي.

همداراز دا د **Android** او **iOS** لپاره اپلیکیشنونه لري.

د **BitWarden** پاسورډ منیجر هم په پیسو او هم په وړیا ټوګه ترلاسه کیدای شی. دغه پاسورډ منیجر د KeePass په پرتله د کارونکو د خوښې وړ پاسورډ منیجر دی او بې له دې چې لکه د KeePass پاسورډ منیجر په خپر ډیټابیس تنظیمولو ته اړتیا ولري، ستاسو پټنومونه په سملاسي ټوګه په (Cloud) کې خوندي کوی. دغه پاسورډ منیجر په اتوماتیک ډول اپدیټ کیږي. دا د KeePass په پرتله خورا آسان انتخاب دی.

همداراز دا د **Android** او **iOS** لپاره انتخابونه لري.

۶. فزيکي خوندیتوب

د شخصي دستګاوو ساتنه

وسایل پټ وساتئ: هر کله چې خپل ټیلفون، لپ ټاپ یا ټابلیټ نه کاروئ، له لیدلو نه یې لیرې وساتئ، په ځانګړې توګه په عامه ځایونو کې. دا کار ستاسو د وسیلې د غلا کیدلو او ضبطیدلو خطر کموي.

په دستګاه کې د کوډ کولو ځانګړنه فعاله کړئ: د خپلې ډیټا د خوندي کولو لپاره د وسیلې کوډ کولو ځانګړنه (سیستم) وکاروئ. دا کار ډاډ درکوي چې که چیرې ستاسو دستګاه ورکه یا غلا شی، د سم پاسوورډ پرته ستاسو ډیټا (معلوماتو) ته څوک لاسرسی نشي موندلای. دغه ځانګړنه په پورتني ماډلونو کې په ډیفالټ ټوګه فعاله شوې ده.

د وسیلې ورکیدل

که چیرې ستاسو دستګاه ورکه یا غلا شی، تاسو کولای شئ د Find My Device په کارولو سره (په iPhone ټیلفون کی هم) د خپل دستګاه منځپانګه (محتوا) پاکه کړئ.

د دستګاه د ورکیدو پر وخت د خپلو معلوماتو له لاسه ورکولو څخه د مخنیوی لپاره، په یو خوندي (Cloud) سرویس یا یو کوډ شوې بهرنی درایو کې په منظم ډول د مهم معلوماتو د ساتلو یا (backup) کولو په اړه ډاډ ترلاسه کړئ.

خوندي آنلاین طریقې

په ټولنیزو رسنیو کې په ریښتیني وخت کې د خپل موقعیت شریکولو څخه ډډه وکړئ. د مفصلو معلوماتو شریکولو په اړه محتاط اوسئ ځکه چې ستاسو ځای او موقعیت ښودلای شي او لوړې کچې ته خپل د اکاونټ د محرمیت رسولو په اړه ډاډ ترلاسه کړئ.

د فزیکي ځارنې پیژندل

د هغو ناپیژانده افرادو په اړه هوښیار واوسئ چې ګمان کوئ تاسې ځاري او ګوري. خپل روټین بدل کړئ ترڅو ستاسو د راتلونکي فعالیت په اړه څوک ونه شي کولای پوه شي .

که چیرې تاسې ګمان کوئ چې ځارل کیږئ:

- مستقیماً کور ته **مه ځئ**، له شخص سره د سترګو مستقیم تماس مه نیسئ، یا مستقیما خپل منزل او مقصد په لور مه تښتئ.
- **خپل شاوخوا وڅارئ:** یوې مغازې یا هټۍ ته ننوځئ او په احتیاط سره خپل شاوخوا وڅارئ او هغه کس چې تاسې تعقیبوی، د سترګو له کونجه وڅارئ. د دې کس ځیره او چلند په یاد وساتئ.
- **په عامو سړکونو کې پاتې شئ**: په عامو کوڅو کې تګ ته دوام ورکړئ، د امکان تر حده د ګڼې ګوڼې په لور حرکت وکړئ، او د خپل مسیر بدلولو لپاره موجودې راتلونکې کوڅې کې وګرځئ. دا مرحلې تکرار کړئ تر څو چې له تعقیبوونکي کس نه لاره ورکه شي.
- **نښې وپیژنئ:** په یاد ولرئ چې د یو ځل لپاره د یو څه پیښیدل یوه عادي پیښه ده، دوه ځله د یو څه پیښیدل کیدای شي تصادفي وي، خو که یو څه درې یا دریو ځلو نه ډېر پیښ شول، د یو احتمالي ګواښ نښکارندویي کوي.

د بېړنيو حالاتو کړنلارې

د بېړنيو حالاتو د کړنلارو جوړول کولای شي ستاسو خوندیتوب پام وړ کچې ته لوړ کړي او تاسې او هغه کسانو ته چې ورسره په تماس کې یاست، ذهني هوساینه برابره کړي.

لاندې ځینې اغیزمنې کړنلارې راغلي چې تاسو یې پلې کولای شئ:

<u>خپل د اعتبار وړ کسان د خپلو پلانونو په اړه خبر کړئ.</u>

د خپل سفر پروګرام شریک کړئ:

- یو ځای ته تر تلو مخکې: تل خپل د اعتبار وړ کس سره خپل د سفر منزل، کومې لارې چې تاسې پرې سفر کوئ او منزل ته د رسیدلو احتمالي وخت په ګډون، خپل د سفر پلان شریک کړئ،
- ورځني پلانونه: خپل ورځنی مهالویش شریک کړئ، په ځانګړې توګه کله چې په غونډو کې ګډون کوئ یا ناپیژانده ځایونو څخه لیدنه کوئ.

منظمې اړیکې:

- د مهالویش پر اساس اړیکې ټینګول: خپل د اعتماد وړ کس سره د اړیکو ټینګولو لپاره پر وختونو موافقه وکړئ. دا کار د عاجلې ټیلفوني اړیکې، متني پیغام استولو یا د ټولنیزو رسنیو اپډیټ کولو له لارې ترسره کیدای شي.
- کوډ شوي کلمات: د خپل خوندیتوب د تایید لپاره او د شک پیدا کولو پرته خپل د ناخوښۍ د څرګندولو لپاره هغه کوډ شوي کلمات یا عبارتونه وکاروئ چې مخکې مو ټاکلي وي. د مثال په توګه، یوه جمله لکه "زه سارا خاله سره یم" دا ښیي چې هرڅه سم دي، پداسې حال کې چې یوه جمله لکه "زه خپل د کاکا زوی لیدو ته ځم" ښایي دا وښیي چې تاسې په ستونزه کې یاست.

<u>د بېړني حالت نښې او د ګوابنس پر وړاندې ګامونه</u>

د اړیکې نه ټینګېدل:

- سملاسی (عاجل) اقدام: که چېرې یوه مخکې ټاکل شوې ټیلفوني اړیکه مو میس کړه (له لاسه درنه لاړه)، ستاسو د اړیکې کس باید هڅه وکړي چې د ټولو موجودو وسیلو (ټیلفون، پیغامونو، او داسې نور) له لارې تاسو سره اړیکه وونیسي.
- د الارم فعالول: که ستاسو د تماس کس ونشي کولای له مخکې ټاکل شوي وخت سره سم تاسو سره اړیکه ونیسي، دوی باید د اعتبار وړ اړوندو چارواکو یا د بېړني حالت لپاره ټاکل شویو نورو اشخاصو ته خبر ورکړي. مخکې له مخکې په دې اړه موافقه وکړئ.

د خطر د حالت نښې (سیګنالونه):

- چوپ الارمونه: که چېرې تاسې مرستې ته اړتیا لرئ خو نشئ کولای په آزاده توګه خبرې وکړئ، د اشارې نښې (سیګنالونه) وکاروئ. دا کیدای شي د هوکړه شوي ایموجي (تصویري ژبې) یا کوډ شوي پیغام لیږل وي.
- د مرستې لپاره ټیلفوني اړیکه ونیسئ: که په خطر کې یاست، خپل د اعتبار وړ تماس کس سره ټیلفوني اړیکه ونیسئ او آن که تاسې خبرې هم نشئ کولای، ټیلفوني اړیکه مه بندوئ. پدې کار سره ستاسو د تماس کس کولای شی هغه څه واوري چې تاسو ته پیښیږی او په اړه یې اقدام وکړي.

د سفر یا له پولې (سرحد) څخه تېریدو پر وخت

د خطرونو پېژندنه

د سفر پر مهال، په ځانګړې توګه له پولو څخه د تېریدو پر مهال، امنیتي کارکوونکي په آزاده توګه ستاسو بریښنایي دستګاوې لټوي چې دا کار کولای شي ستاسې حساس معلومات د افشا کیدو له خطر سره مخ کړي. کیدای شي دغه امنیتي کارکوونکي ستاسې دستګاوې ضبط کړي او په دغو دستګاوو کې شته معلومات (ډیټا) کاپي او وڅیړل شي. کیدای شي دغه امنیتی کارکوونکي ستاسو عکسونو، تماسونو او شخصي اړیکو ته لاسرسی وموميِ چې کیدای شي دغه کار نه یوازې تاسو بلکې نور کسان هم له خطر سره مخ کړي.

د احتیاطي تدابیرو په نیولو سره، تاسو کولای شئ د داسې لاسوهنو او خطرونو پر وړاندې ځان خوندي کړئ.

له سفر نه مخکې تیاری

له ځان سره یوه 'پاکه' دستګاه ولېږدوئ: د پاکولو د یو خوندي سافټویر په مرسته ټول غیر ضروري فایلونه پاک کړئ. **داډ ترلاسه کړئ چې ټول معلومات (ډیټا) له جنک (Junk) فولډر نه هم پاک شوي**.

له شخصي اکاونټونو نه لاګ اوټ شئ (ووځئ)، خپل اکاونټ ته د ننوتلو (لاګ این) ساتل شوي معلومات پاک کړئ، خپل ټول زیرمه شوي معلومات (ډیټا) او ټول حساس اپلیکیشنونه پاک کړئ.

خپل معلومات (ډیټا) په یو خوندي ځای، یا په (Cloud) سرویس او یا بل ډرایو یا دستګاه کې چې ستاسو دستګاه سره تړلی نه وي، بک اپ (زېرمه) کړئ. دا کار تاسو سره ستاسو د معلوماتو بیرته ترلاسه کولو کې مرسته کوي ترڅو ستاسو معلومات خوندي وي او یا که چیرې ستاسو وسیله ورکه یا ضبط شی، دا کار تاسو ته دا امکان درکوي چې خپل معلومات بیرته ترلاسه کړئ.

د سفر پر مهال کارولو لپاره لنډمهاله بریښنالیک او ټولنیزو رسنیو اکاونټونه جوړ کړئ او د خپل شخصي اکاونټونو په پټولو سره ځان په اړه شک راتیټ کړئ.

که امکان ولري، د سفر پر مهال ځان سره لنډمهاله تلیفون یا لپ ټاپ ولرئ چې یوازې اړین او خوندي معلومات مو پکې ساتلي وي.

پام وکړئ چې ستاسو دستګاه دومره پاکه نه وي چې خوک درباندې شکمن شي - هڅه وکړئ ترڅو ستاسې ټیلفون عادی ښکاره شي او ځینې عکسونه، پیغامونه او اپلیکیشنونه ولري.

له سفر او پولې څخه تر تېریدو وروسته

خپلې دستګاوې د لاسوهنې د نښو، لکه ناپېژانده اپلیکیشنونو او بدل شویو تنظیماتو د پیدا کولو په موخه وڅیړئ. که چیرې شک لرئ چې ستاسو په دستګاه کې لاسوهنه شوې ده، خپله دستګاه پاکه او معلومات له ساتل شوي (بکاپ شوي) کاپۍ نه بیا ترلاسه کړئ.

د هغو اکاونټونو پټنومونه بدل کړئ چې تاسو د سفر پرمهال جوړ کړي وو. دا کار مرسته کوي تر څو ستاسو پټنومونه د لاسوهنې له خطر سره مخ نشي.

کله چې تاسې په خوندي ځای کې یاست او انټرنیټ ته لاسرسی لرئ، کولای شئ خپل معلومات د خپل بکاپ شوي کاپۍ نه بیرته ترلاسه کړئ.

د اضافي معلوماتو سرچينې

په فارسي/دري، پښتو او انګليسي ژبو

لينکونه

Access Now — Guide to Safer Travel (په انګليسي ژبه)

Chayn — Advanced DIY Privacy for Every Woman (په انګليسي ژبه)

Chayn — DIY Online Safety (په فارسي ژبه)

CiviCert — The Digital First Aid Kit (په فارسي ژبه)

EFF — Surveillance Self-Defense guide (په انګليسي ژبه)

EFF — Street-Level Surveillance project (په انګليسي ژبه)

Freedom of the Press Foundation — Secure communication (په انګليسي ژبه)

Human Rights First — Steps to Protect Your Online Identity from the Taliban: Digital History and Evading Biometrics Abuses (په فارسي او پښتو ژبو)

Privacy Guides — Knowledge Base (په انګليسي ژبه)

Tactical Tech — Resources (په انګليسي ژبه)

The New Oil — The Beginner's Guide to Data Privacy & Cybersecurity (په انګليسي ژبه)

د اصطلاحاتو تعریفونه

کوډ کول: په یو پټ کوډ د معلوماتو بدلول ترڅو یوازې کیلې لرونکي کسان وکولای شي دغه معلومات ولولي او له نورو څخه خوندي وي.

له پایه تر پایه (End-to-End) کوډ کول: په داسې یوه طریقه د پیغامونو لېږل چې یوازې د پیغام لیږونکی او ترلاسه کوونکی وکولای شي پیغامونه ولولي او ډاډه شي چې نور څوک نشي کولای چې دا معلومات وګوري.

خلاصه سرچینه: هغه سافټویر چې هرڅوک یې لیدلای، کارولای، بدلولای او شریکولای شي. د خلاصې سرچینې سافټویر ډیری وختونه د پروګرام جوړوونکو لخوا جوړیږي.

فایروال: یوه امنیتي وسیله چې ستاسو کمپیوټر یا شبکې ته د زیان رسوونکي انټرنیټ ټرافیک د داخلیدو مخه نیسي او ستاسو د معلوماتو د خوندي کولو لپاره د یو خنډ په توګه عمل کوي.

انټي وایرس (د وایرس ضد سافټویر): یو سافټویر دی چې هغه زیان رسوونکي سافټویرونه (وایرسونه) پیدا او له منځه وړي او مخه یې نیسي چې کولای شي ستاسو کمپیوټر ته زیان ورسوي او ستاسو معلومات غلا کړي.

بد پوستغالی (Malware): د وایرسونو، جاسوسي سافټویر (spyware) او (ransomware) په شمول هر هغه سافټویر (پوستکالی) چې ستاسو کمپیوټر ته د زیان رسولو یا ستاسو د معلوماتو د غلا کولو په موخه جوړه شوی دی.

د فیشینګ برید: د غولولو یو خاص ډول چې په هغه کې اشخاص هڅه کوي د جعلي پیغامونو د لیږلو له لارې ستاسو د شخصي معلوماتو غلا کولو په موخه تاسې وغولوي. ډیری وخت دغه پیغامونه داسې ښکاري چې یو د اعتبار وړ شرکت یا شخص لخوا تاسو ته لیږل شوي دي.

د **ټولنیزې انجینرۍ برید:** د رواني چلونو (تیرایستنو) په کارولو سره د خلکو غولول چې په دې ډول برید کې هیکران تاسو ته ځان یو د اعتبار وړ کس ښیي تر څو تاسو نه محرم معلومات غلا کړي.

مجازی خصوصي شبکه (VPN): یوه شبکه ده چې د انټرنیټ له لارې خوندي او خصوصي اړیکه رامینځته کوي، ستاسو آنلاین فعالیتونه پټوي او د جاسوسۍ (څارنې) پر وړاندې ستاسو د معلوماتو ساتنه کوی.

دوه فکتوره تصدیق (2FA) سیستم: اکاونټونو ته د ننوتلو لپاره د خوندیتوب اضافي کچه چې نه یوازې پټنوم بلکه هغه کوډ ته اړتیا لری چې ستاسو ټیلفون ته لیږل کیږی.

پټنوم (پاسوورډ): د هغو شمیرو یا اعدادو ټولګه چې تاسو یې د خپل ټیلفون، کمپیوټر یا اپلیکیشنونو د خلاصولو لپاره کاروئ چې ستاسو د معلوماتو په خوندي ساتلو کې مرسته کوي.

پاسوورډ منیجر (Password Manager): هغه سافټویر دی چې ستاسو پټنومونه په خوندي ډول جوړوی، زیرمه کوي او تنظیموی، ځکه نو تاسې باید یوازې یو ماسټر پټنوم (اصلی پټنوم) په یاد ولرئ.

د اصطلاحاتو تعریفونه

د تعقیبولو کوکیز (د معلوماتو کوچني فایلونه): هغه کوچني فایلونه دي چې ویب پاڼې یې ستاسو په کمپیوټر کې زیرمه کوي ترڅو ستاسو فعالیتونه او لومړیتوبونه په یاد ولري او ډیری وخت د اعلاناتو د خپرولو لپاره ستاسو د لټونونو د تعقیبولو په موخه کارول کیږي.

د خصوصي لټون حالت: په ویب براوزرونو کې یوه ځانګړنه ده چې د معلوماتو کوچني فایلونه (کوکیز) یا ستاسو د لټون نیټې نه زیرمه کوی او په انټرنیټ کې ستاسو د لټون خصوصي ساتلو کې مرسته کوي.

بایومټریک معلومات: هغه معلومات چې د فزیکي ځانګړتیاو پراساس دي، لکه د ګوتو نښې، د مخ پیژندنه یا د سترګو سکن چې د افرادو د پیژندلو او تایید لپاره کارول کیږي.

اعلان بندوونکی سافټویر (adblocker): یوه وسیله یا د ویب براوزر د ملاتړ سافټویرو دی چې په هغو ویب پاڼو کې چې تاسو یې ګورئ د اعلاناتو د خپریدو مخه نیسي او ستاسو لټون تجربه پاکه او ګړندۍ کوي.

د کمپیوټر د پاکولو سافټویر: د CCleaner او BleachBit په څیر پروګرامونه چې ستاسو کمپیوټر پاکوي، ستاسو د کمپیوټر فعالیت نښه کوي او د غیر اړین فایلونو او د لټون تاریخچو د پاکولو له لارې ستاسو د خصوصي حریم ساتنه کوی.

Tor براوزر: یو ځانګړی ویب براوزر دی چې ستاسو آنلاین فعالیت د څو سرورونو سره د وصل کولو له لارې پټوي او د اشخاصو لخوا ستاسو د آنلاین کارونو تعقیبول ستونزمن کوي.

نړیوال موقعیت ټاکونکی سیستم (GPS): یو سیستم دی چې په نقشه کې ستاسو کره موقعیت موندلو او ښودلو لپاره سپوږمکۍ کاروي چې د موقعیت موندنې او د موقعیت پر اساس خدماتو لپاره ګټور دی.

بلوتوت (Bluetooth): یوه ټیکنالوژي چې د ټیلفونونو، هیډفونونو، او کمپیوټرونو په څیر دستګاوو ته اجازه ورکوی تر څو معلومات په بیسیم توګه او په لنډو واټنونو کې وصل او شریک یې کړی.

خوندي پیغام لیږلو اپلیکیشنونه: د سیګنال یا WhatsApp په څیر اپلیکیشنونه چې ستاسو د پیغامونو خوندي کولو لپاره د کوډ ورکونې پیاوړی سیستم کاروي ترڅو یوازې تاسو او هغه څوک یې وکولای شي ولولي چې تاسو ورسره خبرې کوئ.

د معلوماتو افشا: کله چې خصوصي معلومات په ناڅاپی یا قصدي ډول افشا شي او هغه کسان ورته لاسرسی ومومي چې باید ورته لاسرسی ونه لري.

د ویب براوزر د ملاتړ سافټویر (Browser Extention): د سافټویر کوچني پروګرامونه چې تاسو کولای شئ خپل براوزر ته یې د لا ډیرو ځانګړنو ورکولو، لکه د اعلانونو بندولو او د ژبو د ژباړې په موخه ور اضافه کړئ.

#WOMENSAFEONLINE

afghanwitness.org

@afghan_witness

@AfghanWitnessOfficial

@afghan_witness