ډیجیټل امنیت او محرمیت

د فعالینو او د بشري حقونو د مدافعینو لپاره چې په افغانستان کې فعالیت کوي

سپتامبر 2022

د افغانستان د ډیموکراسۍ او پرمختک موسسه
(ADDO)

فهرست

د افغانستان د ډیموکراسۍ او پرمختک موسسه (ADDO) 1
د لارښود په اړه 1
د لنډیزونو لیست 1
د ډیجیټل امنیت او محرمیت 2
د حکومت څارنه 4
ستاسو د انټرنیټ پیوستون خوندي کول 5
د کوډ کولو کارول 5
د NO-LOGS پالیسي سره VPN غوره کړئ 6
د IP پته نقاب کړئ 6
د وړیا VPN خطرونه مه اخلئ 6
د انلاین سانسور بندول 6
امنیت لوړول 6
په نامعلوم ډول انټرنیټ ته لاسرسی ومومئ، د (TOR) شبکه وکاروئ 6
عامه وای فای په خوندي ډول وکاروی 7
ستاسو د کمپیوټر ساتنه 7
یو فایروال فعال کړئ 8
د انټي ویروس سافټویر نصب کړئ 8
د انټي سپایویر کڅوړه نصب کړی 8
پیچلي پاسورډونه وکاروی 9
خپلOS ، APPs، او براوزر تازه کړی 9
اسپم (SPAM) په پام کې ونیسی 9
خپل کمپیوټر بک اپ کړی 10
خپل کمپیوټر بند کړئ 10
خپل شبکه خوندي کړی 10
د کارولو لپاره دوه فکتور تصدیق کړی 10
تاسو ممکن کوډ کول وکاروی 11
ستاسو د سمارټ فون ساتنه 11
غیر محفوظ وائی فای 11
د شبکې سپکاوی 11
فشینګ بریدونه 12
سپایویر 12
مات شوي کریپټوګرافي 12
د ناستې ناسمه اداره کول 13
د ګرځنده امنیت لپاره به بیا کوم ګواښونه راڅرګند شي؟ 13
SMiShing: *13*

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

:BYOD *13*
:The Internet of Things (IoT) *13*
ستاسو د پټنوم (پاسورډ) خوندي کول 13
د پاسورډ بریدونه 14
پروفایل کول *14*
ټولنیزه انجنیري *15*
قاموسی بریدونه *15*
د وحشي ځواک بریدونه *15*
د قوي پاسورډ جوړول 15
د پاسورډ اتومات خوندي کول 16
انټرنیټ اکسپلورر (IE) *16*
موزیلا فایرفاکس *16*
ګوګل کروم *16*
سفاري (SFAFARI) *16*
اتومات ننوتل 17
ستاسو د ویب پاڼې محرمیت خوندي کول 17
براوزرونه 17
د محرمیت ساتلو لپاره غوره براوزر 17
څنګه په خوندي ډول براوزر وکاروئ 18
پاک او کلیک وکړئ *18*
د خپروني بیجر *18*
سایبرګوسټ وی پی ان *18*
د فعالینو لپاره غوره او خوندي براوزرونه 18
تور (Tor) براوزر *18*
EPIC *19*
FIREFOX *19*
د لټون ماشینونه 19
ګوګل څه پوهیږي *19*
د کروم کارولو څرنګوالی *20*
د محرمیت لپاره د غوره لټون انجنونه 20
دک دک ګو (DUCKDUCKGO) *20*
متاجر (METAGER) *20*
استارټر پیج (STARTPAGE) *20*
ستاسو د معلوماتو محرمیت خوندي کول 20
د کلاوډ ذخیره 21
د کلاوډ ذخیره کولو څرنګوالی 21
د معلوماتو شریکول 21
ستاسو د ټولنیزو رسنیو او اړیکو ساتنه 22

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د خوندي اړیکو کارولو څرنګوالی 22
برېښنالیکونه (ایمیلونه) 22
ستاسو د برېښنالیک پېژندنه شخصي ساتل 22
د برېښنالیک خوندیتوب 23

ټولنیزې رسنۍ(SOCIAL MEDIA 23

د مخ پېژندنې په اړه مهم معلومات 23
د ټولنیزو رسنیو ترتیبات بدل کړئ 23
په ټولنیزو رسنیو کې د خوندي حساب ترتیب کول.. 24

د ټولنیزو رسنیو پلیټ فارمونو او ارتباطي وسایلو امنیت او خوندیتوب 24

د ټولنیزو رسنیو پلیټ فارمونو مهم ټکي.. 24
فیسبوک(Facebook 24
ټویټر(Twitter 25
انستاګرام(INSTAGRAM 26
تیک تاک(TikTok 27
یوټیوب(YouTube 28
د ټولنیزو رسنیو د ارتباطي وسایلو مهم ټکي 30
جی میل(Gmail 30
یاهوو(Yahoo 31
مسینجر(Messenger 32
واتساپ(WhatsApp 34
وایبر(Viber 35
ټیلیګرام(Telegram 36
سکایپ(Skype 36
سیګنال(Signal 37

د بیان د آزادۍ په اړه د حکومت قانون چې د ډیجیټل حقونه اغیزمن کوي. 38

حوالې (سرچینې) 40
کتابونه.. 40
ویب سایټونه 40

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د افغانستان د ډیموکراسۍ او پرمختک موسسه (ADDO)

د افغانستان د ډيموکراسی او پرمختک موسسه (ADDO) يوه غير دولتي موسسه ده چې په ۲۰۱۴ کال کې د افغانستان په اقتصاد وزارت کې ثبت شوې ده ADDO. د کابل په ګډون په سهيلي، شمالي او مرکزي افغانستان کې کار کوي. د ADDO ليد د يوې ټولنې رامينځته کول دي چيرې چې د قانون حاکميت ، ډيموکراسي او د بشري حقونو درناوی د ټولنې د حکومتداری اساسات دي او چيرې چې هدف لرونکي ټولنې د ټولنيز او اقتصادي خودمختاری دوامداره کچې ته رسيدلي وي. د دې سازمان موخه د افغان اتباعو د وړتياوو د پیاوړتیا، د مدافع وکيلانو په کارونو او ښځينو کې د ښکيلتيا او په بهر کې د افغانستان د ښه انځور د لوړولو له لارې د ډيموکراتيکو اصولو او بشري حقونو وده ده. د افغانستان په کليوالي او ښاري برخو کې، ADDOد پاليسي جوړونکو، CSOs، د ښځو د حقونو ډلو، او د ځوانانو سازمانونو سره د روزنې، څېړنې، د قانون جوړونې نظارت، مدافع وکيل، ظرفيت لوړولو، او د بشري حقونو او آزاديو د ساتنې له لارې د ډيموکراسی د پياوړتيا لپاره کار کوي.

د لاربښود په اړه

دا لاربښود د ډيجيټل امنيت او خونديتوب په اړه د وروستي معلوماتو په کارولو سره رامينځته شوی. دا د ټولو افغان فعالانو او د بشري حقونو مدافعينو لپاره چې په افغانستان او له پولو هاخوا فعاليت کوي، ګټور لاربښود دی. د بديل په توګه، موږ د هرې موضوع لپاره لينکونه وړاندې کړل چې د هرې لنډيز شوي موضوع لاندې پوښل شوي. ډيری ګټوري ويب پاڼې شتون لري چې کولی شي په لاربښود کې پوښل شوي موضوعاتو په اړه نور معلومات چمتو کړي. د لا زياتو دقيقو او ګټورو معلوماتو لپاره، لوستونکي کولی شي د حوالې سرليک لاندې چمتو شوي ويب پاڼې وپلټي. دا لاربښود د ACCESSNOW د سخاوتمند ملاتړ لخوا ممکن شوی ADDO. د دوی د تمويل ملاتړ او فرصتونو لپاره د لاسرسي ستاينه کوي. دلته څرګند شوي محتويات او نظرونه د اکس نو پر غاړه نه دي، او اړينه نه ده چې خپل نظرونه منعکس کړي ADDO. به د دې لاربښود د مينځپانګې په اړه هر ډول نظرونو ته ښه راغلاست ووايي (په شمول د هر ډول غلطيو اصلاح).

د لنډيزونو ليست

- AES - Advanced Encryption Standard
- BYOD – Bring Your Own Device
- GMIC - Government Media and Information Center – Afghanistan
- HTTPS - Hypertext Transfer Protocol Secure
- IDS - Intrusion Detection System
- IoT - The Internet of Things
- ISP - Internet Service Provider
- NSA - National Security Agency
- OS - Operation System
- PC - Personal Computer
- RFID - Radio Frequency Identification
- SSL - Secure Sockets Layer
- SMS - Short Message Service
- UDHR - Universal Declaration of Human Rights
- VPN - Virtual Private Network

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د ډیجیټل امنیت او محرمیت

بې له شکه، موږ کمپیوټرونه، سمارټ فونونه، او انټرنیټ د معلوماتو لټون، ذخیره کولو او تبادلې لپاره کاروو. له همدې امله، په ډیجیټل نړۍ کې امنیت زموږ د معلوماتو امنیت پورې اړه لري. موږ باید خپل معلومات خوندي کړو چیرې چې دا غلا کیږي، محدود کیږي، جوړ او زیانمن کیږي. په بې کاره سیستم کې، هرڅوک د معلوماتو د لاسرسي او خپرولو لپاره مساوي فرصت لري. په هرصورت، ځینې حکومتونه د معلوماتو جریان کنټرولوي، او کله چې دوی وغواړي، دوی په معلوماتو محدودیتونه وضع کوي. بله ستونزه دا ده چې د انټرنیټ کاروونکي به ناوړه اشخاص تجربه کړي چې د کمپیوټرونو او سمارټ فونونو لپاره ویروسونه رامینځته کوي او د دوی سیستمونو ته هک کوي ترڅو زیانمن کړي او ارزښتناک معلومات غلا کړي.

اوس ګډوډي زموږ ډیجیټل نړۍ اداره کوي. په امید سره، موږ وایو چې هیڅ شی ډاډمن نه دی. په هرصورت، هرڅه ممکن پیښ شي. موږ یو بریښنالیک لیږو، یو چا ته متن ورکوو، د ټولنیزو رسنیو د اړیکو وسیلو کې اسناد لیږو، او یا یو سند لیکو، مګر موږ هیڅکله د ناامنی پایلې په پام کې نه نیسو. بې له شکه، موږ نشو کولی په ډیجیټل چاپیریال کې ډاډمن لوبغاړي ولرو. موږ باید د معلوماتي لویو لارو او ټیکنالوژۍ په نوي دور کې چې راڅرګندیږي د خپلو وړتیاوو او ضعفونو څخه په بشپړ ډول خبر شو. موږ باید پوه شو او مهارتونه ولرو چې ژوندي پاتې شو او په انټرنیټ کې زموږ ورځنۍ کار په خوندي ډول ترسره کړو.

ځینې هیوادونه قانون تصویبوي او نوې ټیکنالوژي معرفي کوي ترڅو د نظارت ډیر ځواک ولري .د مثال په توګه، د ECHELONپروژه د نړیوال څارنې سیستم معرفي کوي چې کولی شي په تلیفون، انټرنیټ او سټلایټ کې زموږ ارتباطات ثبت او پروسس کړي. د پایلې په توګه، د انټرنیټ اتصال نقطو څخه معلوماتو ته د لاسرسي حق او وړتیا محدوده شوې. حکومتونه دې ته چمتو نه وو چې خپلو اتباعو ته حق ورکړي، له هغه څخه یې ګټه پورته کړه او انټرنیټ ته یې د وړیا لاسرسي حق محدود کړ. د هیواد په کچه د فلټر کولو ډیری سیستمونه رامینځته شوي ترڅو د انټرنیټ معلومات محدود او بلاک کړي چې نامناسب او یا د هیواد د قوانینو خلاف ګڼل کیږي.

د نړیوال انټرنیټ محدودیتونه او نظارت مخ په ډیریدو دی. لکه څنګه چې عمومي آنلاین ازادي کمه شوې، په ټوله نړۍ کې حکومتونه د انټرنیټ محدودیت او د څارنې هڅې ګړندۍ کوي.د 2014 کال د جون راهیسې د 65 هیوادونو څخه په نیمایي کې تحلیل شوي آنلاین آزادۍ کې کمښت راغلی. فرانسه، چې د چارلي ابدو د بریدونو په پایله کې یې یو قانون نافذ کړ، یو تر ټولو ناوړه کمښت ولیدل. ایران، سوریه او چین د هغو هیوادونو په توګه لیست شوي چې د آنلاین ازادۍ په اړه خورا سخت محدودیتونه لري. په مجموع کې، 14 هیوادونو د حکومت نظارت زیاتولو لپاره قانون تصویب کړ. د 65 هیوادونو څخه په 42 کې خصوصي شرکتونه مجبور وو چې د انټرنیټ معلومات حذف یا محدود کړي ځکه چې د حکومتي واک په اړه انتقادي څرګندونې د سانسور لامل کیږي. برسیره پردې، ډیری حکومتونو د آنلاین نوم او کوډ کولو لپاره د ټیکنالوژیو په وړاندې په زیاتیدونکي توګه سخت چلند غوره کړی.

چین یو "لوی فایروال" معرفي کړ، کوم چې ټولې نړیوالې مخابراتو ته لاره هواروي. لوی فایروال په رسمي دروازو کې د پراکسي سرورونو له لارې فعالیت کوي. د عامه امنیت وزارت وتوانید چې انفرادي کارونکي او مینځپانګې وپیژني ، حقونه تعریف کړي او په پای کې په دې دروازو کې د هیواد دننه او بهر ترافیک وڅاري .اوس، په چین کې "لوی فایروال" یو بشپړ نسل بدلوي. له هغې وروسته، چین د "طلایی شیلډ" معرفي کړ. دا د پخواني سیستم یو هوښیار جانشین بود.

ګولډن شیلډ په ملي انټرنیټ تکیه کوي او له نړیوال انټرنیټ څخه جلا شوی. د ګولډن شیلډ پروژه باید د هر انټرنیټ کارونکي ډیټابیس وساتي او د ملي امنیت ساتلو کې د مرستې لپاره یې وکاروي. په اصل کې، دا په چین کې د پراخه جاسوسۍ لپاره یو تخنیک و. چین د څارنې استخباراتو شبکه جوړه کړې، چې د لیدلو، اوریدلو او فکر کولو اجازه ورکوي .اوس د مینځپانګې فلټریشن له ملي کچې څخه ملیونونو معلوماتو او مخابراتي وسیلو ته په عامه ځایونو او د خلکو کورونو کې لیږدول شوی. په نهایت کې ، ګولډن شیلډ په زړه پورې پیچلې ټیکنالوژۍ سره سمبال دی .

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

دا محدودیتونه زموږ د انټرنیټ کارولو ورټیا محدودوي او زموږ د پوهې او مخابراتو په تعقیب کې د سرحدونو په اوږدو کې سفر کوي. برسیره پردې، دوی د بشري حقونو د نړیوالې اعلامیې (UDHR) یو شمیر مقرراتو څخه سرغړونه کوي چې د هرچا د محرمیت او د بیان ازادۍ حق تضمینوي .

د څارنې او څارنې تخنیکونه د استخباراتي افسرانو له کنټرول څخه هارډویر او سافټویر سیستمونو ته لیږدول شوي چې دواړه سوداګریزې سوداګرۍ او دولتي سازمانونه پرمخ وړي.

تر دې مخکې د هغه چا جاسوسي کېدله چې ملي امنیت ته ګواښ بلل کېده. د څارنې او فلټر کولو میکانیزمونو له امله چې زموږ حکومتونو په انټرنیټ کې رامینځته کړي، موږ ټول اوس شکمن یو. ټیکنالوژۍ تل د کاروونکو ترمنځ توپیر نه کوي ځکه چې دا زموږ په بریښنالیکونو، پیغامونو، او ویب لټونونو کې د ځانګړو جملو لپاره ګوري، او کله چې دوی کشف کړي، دا د څارنې ټیمونو ته خبرداری ورکوي یا زموږ ارتباطات غیر فعالوي .

د آنلاین محرمیت لپاره د دفاع وروستۍ کرښې یو کوډ کول (encryption) دي. دا موږ ته اجازه راکوي چې خپل مخابرات کوډ کړو ترڅو یوازې مطلوب ترلاسه کونکي یې ولولي. حتی د انټرنیټ په جوړښت کې د خوندي مالي معاملو مالتړ لپاره د کوډ کولو یو پرت شامل دی چې د خوندي ساکټ پرت (SSL) په نوم یادیږي.
دا ټیکنالوژي په ډیری هیوادونو کې له سختو نیوکو سره مخ شوه کله چې دا د غیر مالي معلوماتو خوندي کولو لپاره کارول پیل کړل .
د متحده ایالاتو حکومت په پیل کې غوښتل چې ټول SSL کوډ کول غیرقانوني کړي چې پیچلتیا یې د دوی د کوډ کولو وړتیا څخه زیاته وه[1]. ټول کوډ شوي بریښنالیکونه به احتمال ولري د اضافي ازموینې لپاره د نړیوال نظارت سیسټم لکه ECHELON(یا کوم بل) لخوا راټول شي ، ځکه چې دوی په لومړي ځای کې کوډ شوي و. له همدې امله، د محرمیت هره هڅه به د یو څه پټولو د غوښتنې په توګه تشریح شي.

په خپلو هیوادونو کې فعالان او د بشري حقونو مدافعین ځانګړي ګواښونه لري. د بشري حقونو فعالین په مکرر ډول د څارنې او محدودیتونو موضوع ګرځي. د دوی وړتیا د بیان د آزادۍ حق په منظم ډول محدود دی .

دوی ډیری وختونه د خپل کار د ترسره کولو لپاره له سختو مجازاتو سره مخ کیږي. د دوی لپاره، ډیجیټل عمر دواړه ګټه او لعنت دی. له یوې خوا، دوی اوس د خپلو نړیوالو همکارانو سره ډیر تړلي دي، او د مخابراتو سرعت او د بشري حقونو د سرغړونو راپورونه په چټکۍ سره ویروس کیدی شي. انټرنیټ د خلکو د متحرک کولو لپاره کارول کیږي ، او ډیری ټولنیز نوښتونه آنلاین بدل شوي، په ځانګړي توګه د COVID-19 په جریان کې. برسېره پردې، ډیجیټل ویش په لږ پرمختللو هیوادونو کې ډیری فعالین او مدافعین د نړیوالو خبرو اترو او پوهاوي کې د ګډون څخه منع کړي دي ځکه چې دوی کمپیوټر یا انټرنیټ ته لاسرسی نلري. د دوی د ګرځنده وسایلو ناامني ورځ په ورځ زیاتیږي.

بریښنالیکونه د دوی مطلوب ترلاسه کونکو ته نه رسیږي، د ټولنیزو رسنیو پاڼې هیک شوي، د انټرنیټ اتصالونه پیچلي دي، د ټولنیزو رسنیو د اړیکو وسیلې په کلکه څارل کیږي، د تلیفون خبرې اوریدل کیږي، کمپیوټرونه نیول کیږي، او ویروسونه د کلونو کارونه خرابوي. دا مسایل عادي او ښه پیژندل شوي دي. په آنلاین خپرونو کې د چارواکو مخ په زیاتیدونکي علاقه یو بل تکراري پیښه ده. کله چې "ناغوښتل" مواد د یو فعال او د بشري حقونو مدافع څخه راځي، چارواکي په چټکۍ سره غبرګون ښيي. دوی په فعاله توګه د آنلاین خبرونو سایټونو، ټولنیزو رسنیو پاڼو، او بلاګونو له لارې ګوري.
ډیجیټل ویش، په ډیجیټل ډول تسهیل شوي جبر، د امنیت په نوم سرغړونې، سیستمیک سایبر زیانمنتیا، او ډیجیټل ناامني یوازې یو څو ننګونې دي چې په ټوله نړۍ کې د فعالینو او د بشري حقونو مدافعینو لپاره شتون لري .

د کمپیوټرونو، سمارټ فونونو، او انټرنیټ عملیاتو سره په آشنا کېدو سره، فعالان او د بشري حقونو مدافعین کولی شي د خپل کار په ښه توګه ساتنه وکړي. له همدې امله، دوی به د خپلو حقونو په دفاع کې ډېر بریالي وي او د نورو حقونو ته وده ورکړي چې دوی یې د مرستې هڅه کوي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د حکومت څارنه

حکومتونه د خپلو اتباعو آنلاین فعالیت تعقیبولو لپاره د لوړ ټیکنالوژۍ تجهیزاتو کې ډیرې پانګونې کوي .د ټولنیزو رسنیو د څارنې زیاتیدونکي کارول، کله چې د هغو هیوادونو په شمیر کې د اندیښنې وړ زیاتوالی سره یوځای کیږي چیرې چې د ټولنیزو رسنیو کاروونکي د دوی د آنلاین قانوني فعالیت لپاره توقیف شوي دي، په ډیجیټل پلیټ فارمونو کې د مدني فعالیت لپاره د خوني کمولو ګواښ کوي. ډیری حکومتونه د خپلو اتباعو آنلاین چلند څاري، لکه څنګه چې د دوی استخباراتي خدمتونه کوي. ستاسو د انټرنیټ خدمت چمتو کونکي (ISP) هر هغه څه چې تاسو آنلاین کوئ محرم دي، او چارواکي کولی شي دا مجبور کړي چې ستاسو ډیټا بدل کړي .

د ټولنیزو رسنیو څارنه د فعالانو او د بشري حقونو د مدافعینو لپاره بله ننګونه ده. دا د آنلاین مخابراتي وسیلو له لارې راټول شوي شخصي معلوماتو راټولول او اداره کول شامل دي ، په مکرر ډول د اتوماتیک سافټویر کارولو له لارې چې د ریښتیني وخت راټولول ، مدیریت او د پام وړ میټاډاټا او مینځپانګې تحلیل وړ کوي. د ټولنیزو رسنیو څارنه د لږ مداخلې په توګه نشي رد کیدی ځکه چې دا د سپایویر په پرتله خورا پراخه دی، کوم چې د ځانګړو خلکو وسیلو باندې تمرکز کولو سره د خبرو اترو مخه نیسي. دا ډیجیټل پلیټ فارمونه په ټوله نړۍ کې د ملیاردونو خلکو لخوا کارول کیږي ترڅو د ملګرو او کورنۍ سره وصل شي ، له عزیزانو سره اړیکه ونیسي او خپل سیاسي ، ټولنیز او مذهبي نظرونه څرګند کړي. هغه معلومات چې د دې خدماتو کاروونکو په اړه راټول شوي، جوړ شوي، او اټکل شوي، حتی کله چې دوی په ندرت سره د دوی سره اړیکه لري، د اعلان کونکو او همدارنګه په زیاتیدونکي توګه د قانون پلي کونکو او استخباراتي سازمانونو لپاره خورا ارزښت لري. حکومتونو مسلکي کسان ګمارلي چې د اوږدې مودې لپاره د ټولنیزو رسنیو وینا وڅاري، پشمول د اصلي کاروونکو سره د اړیکو لپاره د جعلي حسابونو ترتیب کول او شبکې ته لاسرسی. ایراني چارواکو د خپل 42,000 پیاوړې داوطلبانو اردو په اړه وياړي چې آنلاین ویناوې څاري. د سایبر پولیسو (FATA) په ویب پاڼه کې، هر وګړی کولی شي د دندې لپاره راپور ورکړي. دې ته ورته، چین د انټرنیټ له لارې په سلګونو خلک ګمارلي دي او چارواکو ته د هر ډول پوښتنې وړ حسابونو یا مینځپانګو په اړه خبرداری ورکوي. چینایي اجنټان په فعاله توګه د لویو شرکتونو سره همکاري کوي ترڅو آنلاین خلکو باندې نظر وساتي. نږدې 364 ملیون چینایي کاروونکو د ټولنیزو رسنیو حسابونه، مخابرات، او شریک شوي فایلونه په یو غیر خوندي ډیټابیس کې موندل شوي چې د امنیتي څیړونکو لخوا د لارښود قانون پلي کولو تعقیب لپاره کارول کیږي. د چین حکومت د مقرراتو د پیچلې ویب له لارې د کاروونکو معلوماتو او میټا ډیټا ته لاسرسی لري ، کوم چې چارواکو ته دا اسانه کوي چې د حساس مینځپانګې خپرونکي اشخاص وپیژني او مجازات کړي.

افغانستان، لکه څنګه چې نن دی، له هغه هېواد سره چې په ۲۰۰۱ کال کې انټرنیټ منع شوی و، ډېر توپیر لري. د سیل ټاورونه په ټول هیواد کې د حکومت لخوا جوړ شوي، چې متحده ایالاتو یې ملاتړ کاوه. د بازار د څیړنې شرکت سټیسټا په وینا، د ګرځنده تلیفون کاروونکو شمیر په 2005 کې یوازې یو ملیون څخه په 2019 کې 22 ملیون ته لوړ شوی. د کارپوهانو په وینا، 70٪ خلک ګرځنده تلیفون ته لاسرسی لري.

طالبانو چې پخوا یې پر انټرنټ بندیز لګولی و، له ټولنیزو رسنیو څخه یې د مخالفانو د ځپلو او د خپلو نظریاتو د خپرولو لپاره د یوې قوي وسلې په توګه کار اخیستی دی. دوی په زرګونو ټویټر حسابونه کاروي، ځینې رسمي او ځینې مستعار. دوی دا ټیکنالوژیکي وړتیا ښیي چې اورپکو د کلونو جګړو په جریان کې وده کړې، او دا په پټه توګه وړاندې کوي چې طالبان څنګه د افغانستان د کنټرول لپاره له دغو سرچینو څخه کار اخلي. خلکو، د ټولنیزو رسنیو کاروونکو خپل عکسونه، پوسټونه لرې کړل او حتی خپل اکاونټونه یې لغوه کړل ځکه چې طالبانو وېرې خپرول. فیسبوک او ټویټر دواړو ژمنه کړې چې د اکاونټونو د ساتنې لپاره به اقدام وکړي. د طالبانو ضد کمپاینونو کې د ګډون کوونکو ټولنیزو رسنیو حسابونه حذف شوي دي. د وخت او بهرنۍ مرستې پرته، نن ورځ به طالبان د بهر څخه د پیغامونو بندول ستونزمن وي، لکه څنګه چې چین او روسیه کوي.

ډیری افغانان، په ځانګړې توګه هغه کسان چې ژوند یا شخصي وضعیت یې د طالبانو لپاره هدف ګرځوي، د دوی د ټولنیزو رسنیو اکاونټونو یا آنلاین شتون په بې رحمۍ سره رنګول یا اپډیټ کول پیل کړل کله چې طالبانو د وسلو لپاره د خلکو تلیفونونه او کورونه لټول پیل کړل. دوی دا کار کوي ځکه دوی پوهیږي چې طالبان د ټولنیزو رسنیو د څارنې سیمه ایز تمایل تعقیبوي ترڅو د پام وړ مخالفانو باندې واک ټینګ کړي. په داسې حال کې چې طالبان له ټولنیزو رسنیو څخه د

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

داستانونو د کنټرول او څارنې لپاره کار اخلي، د متحده ایالاتو په ملاتړ پخوانۍ اداري په وار وار په هیواد کې د WhatsApp او ټیلیګرام په څیر د پیغام رسولو اپلیکیشنونو د بندولو امر کړی و.

اوس د یو فعال او د بشري حقونو د مدافع په توګه، تاسو ممکن د حکومت د څارنې هدف وي که تاسو په مکرر ډول ټولنیز رسنۍ کاروئ، په کنفرانسونو کې خبرې کوئ، یا د مدني ټولنې سازمانونو سره ستاسو د ښکیلتیا په اړه څرګندې خبرې کوئ. دا په ځانګړې توګه ریښتیا ده که تاسو په عامه توګه د اصلاحاتو غوښتنه کړې وي، د بشري حقونو ملاتړ وکړئ، یا احتمالي فساد یا د بشري حقونو سرغړونې افشا کړئ. له بده مرغه، په نبنه شوي څارنې ته اړتیا نشته چې تاسو جرم کړی وي. حکومتونه د مختلفو مسلکیانو د جاسوسۍ لپاره مختلف پیچلي سایبر وسیلې کاروي، په شمول د ژورنالیستانو، اکادمیکانو او حتی حکومتي چارواکو په شمول. دا عمل په هر ځای کې واقع کیږي. چارواکي د څارنې تخنیکونو له لارې وسیلو ته د لاسرسي لپاره پېژندل شوي ، اړیکې بیرته ترلاسه کوي ، پاسورډونه وموميي ، پیغامونه او تلیفون زنګونه تعقیب کړي ، او د فعالینو فعالیت کې مداخله وکړي. حکومتونو د څارنې د میتودونو له لارې راټول شوي معلومات ګټه اخیستې ترڅو فعالین بدنام کړي، د مجرمینو په توګه یې انځور کړي، او تورونه یې په زندان کې واچوي.

ستاسو د انټرنیټ پیوستون خوندي کول

څکه چې ستاسو د انټرنیټ خدمت چمتو کونکی (ISP) ستاسو د انټرنیټ ترافیک اداره کوي ، دا کولی شي د هر هغه څه تعقیب وساتي چې تاسو آنلاین کوئ. ستاسو ISP ممکن ستاسو فایلونه، بریښنالیکونه، پاسورډونه، آنلاین پیرودونه، او حتی هغه پوښتنې چې تاسو یې د خپل سمارټ سپیکر څخه وپوښتئ وګورئ.
څه بدتر دی چې ستاسو ISP ممکن ستاسو په اړه کافي معلومات راټول کړي ترڅو ستاسو د ډیری فعال فعالیتونو سره اړیکه ونیسي، شاید ستاسو په وړاندې د شواهدو راټولولو کې د قانون پلي کولو سره مرسته وکړي ISPs .ټینګار کوي چې دوی ستاسو معلومات د بهرنیو خواوو سره نه شریکوي. په هرصورت، دوی ممکن اړ وي چې ستاسو معلومات دولتي او د قانون پلي کونکو چارواکو ته وسپاري. د مثال په توګه، په آسټرالیا کې ISPs اړ دي چې فدرالي پولیسو ته د کارونکي سرفینګ ډیټا ته لاسرسی ورکړي. ځینې معلومات د دوو کلونو لپاره ساتل کیږي.

د خوندي اړیکو لپاره، د مجازی خصوصي شبکه (VPN) وکاروئ. دلته ځینې VPNs دي چې د سانسور ضد ټریک ریکارډونه لري:

TunnelBear: https://www.tunnelbear.com/download
VPNGate: https://www.vpngate.net
ProtonVPN: https://protonvpn.com
Mullvad: https://mullvad.net/en/download/
Bitmask: https://bitmask.net

ستاسو غوره انتخاب دا دی چې د ISPs VPNs مداخلې سره د مبارزې لپاره په معتبر VPN باندې د پیسو مصرف کولو په اړه فکر وکړئ. بیا، کله چې تاسو آنلاین شئ، یو VPN به تاسو ته یو شخصي، خوندي اړیکه درکړي او ستاسو د آنلاین چلند نامعلوم کولو کې مرسته وکړي. د امنیت ډیری پرتونه د VPNs لخوا کارول کیږي او د تنظیم کولو لپاره نسبتا ساده دي، لکه:

د کوډ کولو کارول

قوي AES 256-(پرمختللي کوډ کولو معیاري) کوډ کول د پریمیم VPNs سره ستاسو د اړیکې ساتلو لپاره کارول کیږي. دا ستاسو د آنلاین چلند څارنې یا جاسوسي کولو څخه ناپاک خلک منع کوي. هغه ویب پاڼې چې تاسو یې ګورئ او هغه خدمتونه چې تاسو یې کاروئ ستاسو ISP یا نورو بهرنۍ خواوو ته د پایلې په توګه نه لیدل کیږي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د NO-LOGS پالیسي سره VPN غوره کړئ

یو VPN غوره کړئ چې په کلکه د نو-لاګ قانون ته غاړه کیږدي نو دا نشي کولی ستاسو د کارونکي هیڅ ډیټا په خپل سرورونو کې زیرمه کړي. ستاسو د لټون کولو تاریخ او شخصي توضیحات پکې شامل دي VPN .به پولیس ته د سپارلو لپاره هیڅ شی ونه لري که دوی ستاسو په اړه کوم معلومات وغواړي.

د IP پته نقاب کړئ

ډیری زرګونه سرورونه په نړۍ کې په لوی VPNs کې موقعیت لري. ستاسو اصلي IP پته پټ وي کله چې تاسو د VPN IPپتې له امله یو سره وصل شئ. دا کار د هر چا لپاره دا ناممکن کوي چې ستاسو آنلاین فعالیتونه تاسو سره وصل کړي .

د وړیا VPN خطرونه مه اخلئ

ډیری وړیا VPNs ادعا کوي چې ستاسو آنلاین محرمیت او مهم معلومات خوندي کوي. ډیری یې د پام وړ نیمګړتیاوې او خطرونه لري، لکه:

-د ډیټا مقدار محدودیتونه چې تاسو یې کارولی شئ او د هغه وسیلو شمیر چې تاسو یې خوندي کولی شئ د دوی په برنامه کې شامل شوي د دریمي ډلې تعقیبونکي لږترلږه سرور اختیارونه:

-د VPN کارولو پر مهال د انټرنیټ اتصال ځنډ
-اډویر او پټ مالویر
-په پاپ اپ اعلانونو کې ښکاري چې ادعا کوي ستاسو معلومات د دریمي ډلې سره شریک شوي

د انلاین سانسور بندول

تاسو شاید نشئ کولی ځانګړو خبرونو ویب پاڼو، اپیسونو، یا ټولنیزو رسنیو ته لاسرسی ومومئ که تاسو په یو هیواد کې اوسیږئ چې سخت آنلاین محدودیتونه لري. په هرصورت، تاسو کولی شئ په هغو هیوادونو کې سرورونو سره وصل شئ چیرې چې ځینې ویب پاڼې او ایپس د باور وړ VPN په کارولو سره بلاک شوي ندي. تاسو کولی شئ په جغرافیه کې محدود شوي مینځپانګې او بې طرفه سرچینو ته لاسرسی ومومئ او حتی د خپل ډیجیټل موقعیت بدلولو سره خپل فعالیت آنلاین همغږي کړئ. په هرصورت، دا سمه ده چې ځیرنه وکړئ چې کوم VPNs ستاسو په سیمه کې خورا اغیزمن دي ځکه چې هر VPN نشي کولی ټول بند شوي مینځپانګې ته لاسرسی ومومي.

امنیت لوړول

پریمیم VPNs په خورا مشهور ډیسکټاپ او ګرځنده عملیاتي سیستمونو کې کارول کیدی شي. حتی سمارټ تلویزیونونه، روټرونه، او یو څو نور ترل شوي وسایل کولی شي دوی وکاروي.

په نامعلوم ډول انټرنیټ ته لاسرسی ومومئ، د (TOR) شبکه وکاروئ

د فعالینو لپاره په خوندي او نامعلوم ډول انټرنیټ ته د لاسرسي لپاره په زړه پورې چلند د) Tor د پیاز روټر یا The Onoion Router)له لارې دی. ستاسو ټول انټرنیټ فعالیت او ډیټا پداسې حال کې چې د تور شبکې سره وصل شوي څو ځله کوډ شوي ، دا ناممکن کوي چې تاسو له دې څخه وپیژنئ.

د محرمیت او محافظت اعظمي کولو لپاره ، موږ مشوره ورکوو چې VPN د Tor سره یوځای کړئ. د Tor سره وصل کیدو دمخه ، تاسو باید د (VPN over Tor(VPN سره وصل شئ.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د دې په کولو سره، نور نوډ به ستاسو د کور IP پته ونه ګوري، او تاسو به د تور شبکې لخوا وړاندیز شوي د محرمیت ټولو محافظتونو څخه ګټه پورته کړئ. په تور کې د VPN کارول اضافي ګټې لري، لکه:

ستاسو د کور شبکه نشي پیژندل کیدی چې تاسو د VPN څخه د کوډ شوي ترافیک له امله تور کاروئ. په هغه ځایونو کې چیرې چې تور محدود دی، VPNکولی شي تاسو ته شبکې ته لاسرسی درکړي. تاسو به نشئ کولی د خپل VPN لخوا تعقیب شئ کله چې د تور شبکې کاروئ. ستاسو VPN ستاسو او هر هغه بګ ترمینځ اضافي امنیت اضافه کوي چې ممکن په تور براوزر کې شتون ولري.

عامه وای فای په خوندي ډول وکاروئ

هغه ټرافیک چې د پرانیستي وای فای شبکې څخه تیریږي معمولا خوندي نه وي، دا د آنلاین سنوپس لپاره ښکاره هدف جوړوي. دا د عامه وای فای کارول خطرناک کوي. دا مهمه ده چې تاسو احتیاط وکړئ که تاسو باید په عامه شبکه کې د فعالیت پورې اړوند فعالیتونو کې برخه واخلئ.

مهرباني وکړئ د عامه وائی فای کارولو پرمهال په پام کې ونیسئ:

-د VPN په کارولو سره خپل معلومات کوډ کړئ ترڅو ستاسو د انټرنیټ فعالیت ناپاک وي او تعقیب یې ناممکن وي.
-یوازې د HTTPS خوندي ویب پاڼو څخه لیدنه وکړئ.
-که تاسو عامه کمپیوټر کاروئ، ډاډ ترلاسه کړئ چې د خپلو ټولو حسابونو څخه لاګ آوټ شئ.
-د نور ویروس د دفاع لپاره خپل فایروال فعال وساتئ.
-د خپل شبکې ارتباط اداره کولو لپاره شخصي پورټ ایبل روټر وکاروئ.
-هیڅکله د باور وړ شبکو سره مه یوځای کیږئ.
-د پټنوم محافظت پرته له شبکې سره مه یوځای کیږئ.

-د خپلو وسیلو لپاره اتوماتیک وای فای اتصال مه فعالوئ.
-کله چې په کارولو کې نه وي، هیڅکله خپل بلوتوث یا وای فای سره وصل مه ساتئ.
-د عامه وای فای په کارولو سره، شخصي معلومات یا اسناد مه توزیع یا اپلوډ کړئ.

ستاسو د کمپیوټر ساتنه

ستاسو په کمپیوټر کې یو ټن شخصي او ارزښتناک معلومات شتون لري. تاسو احتمالا هره ورځ مختلف کمپیوټرونه کاروئ، پشمول د لپ ټاپ، ټابلیټ، سمارټ فون، کور ډیسکټاپ او دفتر ډیسکټاپ. ستاسو د بانک معلومات، بریښنالیکونه، فایلونه، انځورونه، ویډیوګانې، او نور ډیجیټل مخابرات ټول په دې وسایلو کې زیرمه شوي دي. ستاسو د ټولو آنلاین وسیلو او ډیټا خوندي کولو لومړی ګام ستاسو د کمپیوټر خوندي کول دي.
د فعالینو ډیری برخه د مایکروسافټ وینډوز سره کمپیوټرونه د خپل عملیاتي سیسټم په توګه لري. ترټولو پراخه کارول شوي تغیرات وینډوز دي .
ستاسو کمپیوټر باید یو خوندي عملیاتي سیسټم ولري ترڅو د آنلاین بریدونو څخه خوندي شي. د زیانمنونکي کمپیوټرونو په لټه کې چې د ځانګړي امنیت نوي کولو نشتوالی لري، زرګونه هیکران په دوامداره توګه د IP پتې ګوري. د اونۍ امنیتي تازه معلومات باید د وینډوز په ټولو نسخو کې نصب شي، حتی که کمپیوټر نوی وي. که تاسو ورته اجازه ورکړئ، د وینډوز ډیری نسخې به دا پیچ کول په اتوماتیک ډول ترسره کړي. فعالان په انټرنیټ تکیه کوي ترڅو خپل بریښنالیکونه وګوري، کمپاینونه پرمخ بوځي، د خپلو جغرافیایي سیمو څخه بهر حرکتونو سره یوځای شي، آنلاین غونډو کې ګډون وکړي، آنلاین مطالعه وکړي، په ټولنیزو رسنیو کې برخه واخلي، او نور مهم عملیات ترسره کړي - سره له دې چې د حکومتي چارواکو او کمپیوټر هیکرانو لخوا د څارنې شتون شتون لري. بیا هم حتی په لویو سازمانونو کې چې پرمختللي امنیتي محافظتونه لري، موږ ډیری وختونه د پام وړ کمپیوټر لاسوهنو په اړه زده کوو. د خپلو کمپیوټرونو او حساسو معلوماتو د خوندي کولو لپاره لاندې معیاري لارښوونې وکاروئ:

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

یو فایروال فعال کړئ

انټرنیټ ته د لاسرسي دمخه د فایر وال فعال کړئ. د اور وژني وال د شبکې او بهرنی نړۍ ترمنځ د دیوال په توګه کار کوي، بنسټیز امنیت چمتو کوي. ځیني وختونه د فایر وال یو واحد سرور دی، ځیني وختونه، دا یو روټر دی، او بیا هم ځیني وختونه، دا د کمپیوټر سافټویر دی. د اور وژني وال، په هر ډول فزیکي بڼه کې چې دا اخلي، سیسټم ته د ننوتلو او وتلو شبکې ترافیک کنټرولوي. د فایر وال سره په ګډه، یو پراکسي سرور په مکرر ډول د داخلي شبکې IP پته ماسک کولو لپاره کارول کیږي او یو واحد IP پته بهرنیانو ته ښودل کیږي. احاطه د فایروالو او پراکسي سرورونو لخوا خوندي کیږي ، کوم چې ترافیک تحلیل کوي او هغه ځای ته د تګ مخه نیسي چې د مدیر لخوا منع شوی وي. د مداخلې کشف سیسټم (IDS) په مکرر ډول د دې دوه امنیتي اقداماتو بشپړولو لپاره کارول کیږي IDS .یوازې د ترافیک تعقیب ساتي او د هر ډول غیر معمولي فعالیت لټون کوي چې د سرغړونې هڅې ته اشاره کوي.

د انټي ویروس سافټویر نصب کړئ

د وینډوز میشته کمپیوټرونو لپاره ډیری مشهور انټي ویروس برنامې شتون لري. ستاسو کمپیوټر د انټي ویروس پروګرامونو لکهAvast، Bitdefender، Panda Free Antivirus، او Malwarebytes لخوا د ناوړه سافټویر او غیر مجاز کوډ څخه خوندي دی. مالویر او کمپیوټر ویروسونه پراخ دي. ویروسونه ممکن اصلي لامل وي چې ستاسو کمپیوټر ورو چلیږي یا مهم فایلونه له مینځه وړي، یا ممکن لږ څرګند وي. د انټي ویروس سافټویر هر فعالیت څاري او په دوامداره توګه پرمخ ځي. دا هرکله چې تاسو د انټرنیټ څخه فایل ته لاسرسی ومومئ، سافټویر چل کړئ، یا یو سند خلاص کړئ. ټول نوي فایلونه د غوښتنلیک لخوا سکین شوي، او هر هغه څوک چې شکمن وي قرنطین شوي. عموما، تاسو به بیا د اقدام کولو لپاره هڅول کیږي. کله چې ستاسو د انټي ویروس برنامه تنظیم کړئ، دوه خورا مهم فاکتورونه شتون لري چې باید په پام کې ونیول شي. لومړی ګام دا دی چې تایید کړئ چې تازه معلومات ستاسو د انټي ویروس حل کې پلي کیږي. د دې ډاډ ترلاسه کول چې په کمپیوټر کې یوازې یو انټي ویروس محصول نصب شوی دویمه مهمه برخه ده.

که تاسو له یو څخه ډیر انټي ویروس پروګرامونه نصب کړئ، دوی به ستاسو د کمپیوټر کنټرول لپاره یو بل سره سیالي وکړي. تاسو کولی شئ د 2022 لپاره غوره 10 انټي ویروس دلته ومومئ:

https://www.antivirussoftwareguide.com/best-windows-antivirus

د انټي سپایویر کڅوره نصب کړی

سپایویر یو ځانګړی ډول سافټویر دی چې په پټه توګه د اشخاصو یا سازمانونو ډاټا ګوري او راټولوي .ځیني سپای ویر د پاسورډونو او نورو حساسو مالي معلوماتو ته د لاسرسي لپاره هر کیسټروک لاګ کوي. د کمپیوټر ټول فعالیتونه د سپایویر پروګرامونو لخوا څارل کیدی شي، او دریمې ډلې کولی شي دې ډاټا ته په مختلفو لارو لاسرسی ومومي. ترټولو عام تخنیک د ټروجن آس کاروي. سربیره پردې، که تاسو په ساده ډول یو ځانګړی ویب پاڼه لیدئ، مالویر ممکن په شالید کې ډاونلوډ پیل کړي. خوشبختانه، دلته ډیری سافټویر پروګرامونه شتون لري چې هدف یې د سپایویر موندلو او له مینځه وړل دي، لکه څنګه چې د سپی ویئر ډیری غوښتنلیکونه شتون لري. خوشبختانه، دلته د ډیرو سافټویر پروګرامونه شتون لري چې هدف یې د سپاییویر موندلو او له مینځه نښه دي، لکه څنګه چې د سپاییورونو بیلابیلو اپلیکشنونه شتون لري. که څه هم antispywareیوازې په دې ګواښ تمرکز کوي، دا په مکرر ډول د ویبروټ، McAfee، او نورتون په څیر شرکتونو څخه په مشهور انټي ویروس کڅوړو کې شامل دي. د ریښتیني وخت امنیت د antispyware محصولاتو لخوا چمتو شوی ، کوم چې ټول راتلونکي ډیټا معاینه کوي او ګواښونه ودروي.

سربیره پردې، دا غوښتنلیکونه په مکرر ډول ارزانه دي. د عمل غوره لاره چې تاسو یې کولی شئ د خپل کمپیوټر د اخته کیدو څخه د سپایویر مخه ونیسئ، البته، هیڅکله د انټرنیټ څخه هیڅ شی ډاونلوډ نه کړئ چې د خورا معتبر او باوري ویب

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

پاڼي څخه سرچینه نه اخلي. ډیری اوسني انټي ویروس پروګرامونه یا د انټي سپایویر سره معیاري راځي یا دا د اختیاري اضافه په توګه وړاندیز کوي. تاسو کولی شئ دلته د 2022 لپاره د انټي سپی ویئر په شمول 10 غوره انټي ویروس ومومئ:
https://www.antivirussoftwareguide.com/best-windows-antivirus

پیچلي پاسورډونه وکاروئ

د کمپیوټر په مؤثره توګه کارول د قوي پاسورډونو کارولو ته اړتیا لري. یو قوي پاسورډ د هر سیسټم خورا مهم برخه ده کله چې دا ډیجیټل امنیت ته راځي. ترټولو پرله پسې لاره چې هیکران او برید کونکي ستاسو د معلوماتو سیسټمونه په نښه کوي د تاریخ په وینا د کریک کولو پاسورډونو له لارې دي. د پاسورډ مدیر وکاروئ، لکهDashlane ، Sticky Password، LastPass، یا د پاسورډ باس. د وینډوز قوي پاسورډ ولرئ، مګر ستاسو د معلوماتو خوندي ساتلو لپاره د وینډوز پاسورډونو پورې اړه مه کوئ. دوی په چټکۍ سره ویجاړ شوي. د لنډ، څرګند پټنوم کارولو پر ځای، دا غوره ده چې خپل پاسورډونه ولیکئ او په خوندي ډول یې خوندي کړئ. هر ځل یو مختلف پاسورډ وکاروئ او ډاډ ترلاسه کړئ چې خوندي پاسورډونه ستاسو د ګټو یا د ژوند له لارې سره نږدې ندي. هیڅکله خپل کلیدي پاسورډونه هیچا ته مه ښکاره کوئ یا افشا مه کوئ. په هرو دریو یا شپږو میاشتو کې، خپل پاسورډونه بدل کړئ. په یاد ولرئ چې یو شمیر وړیا آنلاین وسیلې شتون لري چې تاسو سره ستاسو د وینډوز پاسورډ موندلو کې مرسته کوي، د بې سیم شبکې کوډ کول، او د کمپیوټر بل هر ډول پټنوم چې تاسو یې لرئ.

خپلOS ، APPs، او براوزر تازه کړئ

ستاسو د عملیاتي سیسټم او انټي ویروس سافټویر نوي کول خورا ستونزمن ندي. دا خصوصیت لا دمخه په اوسني محصولاتو کې د ډیفالټ لخوا فعال شوی. په هرصورت، دا ممکنه ده چې ځینې سافټویر پروګرامونه چې تاسو یې په خپل کمپیوټر کې ځای پر ځای کړي دي امنیتي تازه معلومات نه ترلاسه کوي.
ویب براوزرونه، جاوا، اډوب ریډر، او ډیری نور پروګرامونه د دې کټګورۍ لاندې راځي. د دې پروګرامونو تازه کول اړین دي. تاسو شاید دمخه یادونه کړې وي چې اډوب ریډر تاسو ته د هرکله چې تاسو د پی ډی ایف فایل خلاص کړئ برنامه تازه کولو ته هڅوي. ځینې اپ ګریډونه هغه نیمګړتیاوې حل کوي چې د ناوړه سافټویر لپاره دا امکان ورکوي چې په دې برنامو برید وکړي. سمدلاسه د نوي عملیاتي سیسټم تازه معلومات نصب کړئ. ډیری تازه معلومات د امنیتي پیچونو سره راځي چې هیکرز د خپلو موخو لپاره ستاسو ډیټا ته د لاسرسي او کارولو مخه نیسي. اطلاقات توپیر نلري. د نن ورځې ویب براوزرونه ډیر او هوښیار کیږي ، په ځانګړي توګه د محرمیت او امنیت شرایطو کې. د ټولو تازه تازه معلوماتو پلي کولو سربیره، په یاد ولرئ چې د خپل براوزر امنیتي ترتیبات وګورئ. د مثال په توګه، تاسو کولی شئ د خپل براوزر په کارولو سره خپل آنلاین محرمیت زیات کړئ ترڅو ویب پاڼې ستاسو د حرکتونو تعقیبولو مخه ونیسي. په بدیل سره، د دې خوندي ویب براوزرونو څخه یو وکاروئ.

اسپم (Spam) په پام کې ونیسئ

ډیری لوستونکي شاید د سپیم په اړه اوریدلي وي. سپیم ناغوښتل شوی، ناغوښتل شوی بریښنالیک دی چې ډیری ترلاسه کونکو ته ویشل شوی. که څه هم دا په مکرر ډول د بازار موندنې موخو لپاره کارول کیږي، دا د ډیرو تیارو پایونو لپاره د ناوړه ګټه اخیستنې وړتیا هم لري. د مثال په توګه، سپیم د ویروس یا کیم د خپریدو لپاره یو ځانګړی میتود دی. د ترلاسه کونکي د هویت د غلا کولو لپاره، سپیم د بریښنالیکونو لیږلو لپاره هم کارول کیږي چې دوی د فشینګ ویب پاڼو لیدلو ته هڅوي. په اصل کې، سپیم د مالویر، ویروسونو، ورمونو، او فشینګ بریدونو په شمول د مالویر لپاره تر ټولو غوره یو ناورین دی او په بدترین ډول د رسولو طریقه ده. له همدې امله، د هغه چا څخه چې تاسو یې نه پیژنئ د ضمیمو خلاصولو یا په بریښنالیکونو کې لینکونو کلیک کولو په وخت کې خبرداری ورکړئ. د سپیم انباکس فلټرونه د خورا څرګند سپیم په نیولو کې ښه کیږي.

په هرصورت، ډیر پیچلي فشینګ بریښنالیکونه چې ستاسو ملګري، همکاران، او باوري سازمانونه (لکه ستاسو بانک) په نښه کوي مشهور شوي، نو د هر هغه څه لپاره چې شکمن ښکاري یا غږ کوي خبرداری ورکړی.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

خپل کمپیوټر بک اپ کړئ

ستاسو د معلوماتو بیک اپ درلودل اړین دي که چیرې هیکرز ستاسو سیسټم مات او ویجاړ کړي. تل ډاډ ترلاسه کړئ چې تاسو کولی شئ ژر تر ژره روغ شئ که تاسو د معلوماتو له لاسه ورکولو یا پیښې تجربه کوئ.

د وینډوز فایل تاریخ او macOS وخت ماشین سره د بیک اپ برنامو سره پیل کړئ. دا اسانتیاوې هم په بهرني بیک اپ هارډ ډیسک کې د کافي ظرفیت سره په مؤثره توګه کارول کیدی شي.

دا انګیرنه چې "هیڅ شی به غلط نه شي" په مکرر ډول ستاسو د کمپیوټر مینځپانګې بیک اپ کاپي جوړولو اړتیا ته لومړیتوب ورکوي. موږ په خپل ځان او زموږ ټیکنالوژۍ باندې حساب کوو ترڅو د معلوماتو د هیرولو، له لاسه ورکولو یا زیان رسولو مخه ونیسو.
ستاسو د معلوماتو بیک اپ ډول، حجم او فریکونسۍ په اړه فکر وکړئ. تاسو کولی شئ په iCloud او Dropbox کې د خپلو ټولو معلوماتو او اسنادو یوه کاپي ولرئ، مګر تاسو ممکن د هر څه یوه کاپي سره د USB حافظې سټیک ولرئ. ستاسو په سازمان کې د سرور کمپیوټر د سافټویر او سیسټم تنظیماتو منظم بیک اپ ته اړتیا لري سربیره پردې هغه اسناد چې کاروونکي یې ساتي.

خپل کمپیوټر بند کړئ

ډیری سازمانونه په دوامداره توګه "ټول سیستمونه ځي،" په ځانګړې توګه هغه څوک چې ویب سرورونه چلوي. په هرصورت، که تاسو د انټرنیټ پر بنسټ یو پیچلي سازمان نه چلوئ، خپل کمپیوټر د شپې یا د اوږدې مودې لپاره بند کړئ پداسې حال کې چې تاسو یې نه کاروئ. ستاسو د کمپیوټر بندول هر هغه اړیکه لرې کوي چې یو هیکر ممکن ستاسو د شبکې سره رامینځته کړې وي او د احتمالي زیان پیښیدو مخه نیسي ځکه چې ستاسو کمپیوټر پریښودل دا ډیر څرګند او د هیکرانو هدف ګرځوي.

مهرباني وکړئ په یاد ولرئ چې د دې تخنیکونو څخه کوم یو د ناوړه لوبغاړو لخوا کارول کیدی شي چې ستاسو د بریښنالیک حسابونو ته د لاسرسي لپاره فعالین په نښه کوي.

خپل شبکه خوندي کړئ

ډیری روټرونه د لوړې کچې امنیت فعال شوي سره نه لیږدول کیږي. کله چې خپله شبکه تنظیم کړئ، روټر ته لاسرسی ومومئ او د کوډ شوي، خوندي تنظیم په کارولو سره رمز دننه کړئ. دا هکران ستاسو شبکې ته د لاسرسي او ستاسو تنظیماتو بدلولو مخه نیسي.

د کارولو لپاره دوه فکتور تصدیق کړئ

د کمپیوټر هیکرانو په وړاندې ستاسو لومړنی دفاعي کرښه یو پاسورډ دی، مګر د بل پرت اضافه کول امنیت زیاتوي. ډیری ویب پاڼې تاسو ته اجازه درکوي چې دوه فکتور تصدیق کړئ، کوم چې د ننوتلو په وخت کې ستاسو د پاسورډ سربیره د شمیرې کوډ چمتو کولو ته اړتیا لري. دا کوډ ستاسو تلیفون یا بریښنالیک آدرس ته لیږل کیږي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

تاسو ممکن کوډ کول وکاروئ

کوډ کول کولی شي هېکران ستاسو هرډول ډیټا ته د لاسرسي مخه ونیسي، حتی که دوی ستاسو شبکې او فایلونو ته لاسرسی ولري. تاسو کولی شئ هر هغه USB فلش ډرایو کوډ کړئ چې حساس معلومات لري ، خپل وینډوز یا macOS هارډ ډرایو د BitLocker Windowsیا FileVault Mac سره کوډ کړئ، او د ویب ترافیک خوندي کولو لپاره VPN وکاروئ. یوازې د خوندي ویب پاڼو څخه پیرود وکړئ؛ تاسو کولی شئ دوی سمدلاسه د "HTTPS" په آدرس بار او د تړل شوي پیډ لاک آیکون له لارې جلا کړئ.

ستاسو د سمارټ فون ساتنه

په کمپیوټرونو کې د ګرځنده وسیلو (Mobile) کارول ورځ په ورځ زیاتیږي. د ګرځنده وسیلو امنیت ته ګواښونه مخ په ډیریدو دي. د 1 ملیون څخه ډیرو کاروونکو وسیلو کې، کاسپرسکای په 2014 کې د مالویر شاوخوا 3.5 ملیون ټوټې کشف کړې.د کاسپرسکای په لابراتوار کې د کشف الګوریتمونه د 2017 تر پایه هره ورځ 360,000 ناوړه فایلونه پروسس کوي. برسیره پردې، د دې فایلونو 78٪ د مالویر پروګرامونه وو، چې د 280,000 مالویر فایلونو د ورځني کشف کچه اندازه کوي، چې ډیری یې د ګرځنده وسیلو لپاره دي. دلته د ګرځنده وسیلې ځینې ګواښونه او د راتلونکي لپاره وړاندوینې دي.

غیر محفوظ وائی فای

کله چې د بې سیم هټ سپاټونو ته د لاسرسي وړ وي، هیڅ څوک نه غواړي خپل ګرځنده ډیټا وکاروي، بیا هم وړیا وای فای شبکې په مکرر ډول ناامنه وي. درې برتانوي سیاستوال چې د وړیا وای فای امنیت تجربې کې برخه اخیستو رضایت درلود، د سایبر متخصصینو لخوا په اسانۍ سره جوړ شوي و.

د دوی VoIP چیټونه، د PayPal لیږدونه، او د ټولنیزو رسنیو حسابونه ټول جوړ شوي او هیک شوي. د خوندیتوب لپاره په خپل ګرځنده وسیله کې وړیا وای فای په احتیاط سره وکاروئ. سربیره پردې، دا هیڅکله شخصي یا محرم خدماتو ته د لاسرسي لپاره مه کاروئ، لکه د بانکداري یا کریډیټ کارت توضیحات.

د شبکې سپکاوی

په لوړه ترافیکي عامه ځایونو کې لکه د کافي شاپونو او هوایي ډګرونو کې ، هیکرانو د جعلي لاسرسي نقطې رامینځته کړي، هغه اړیکې چې داسې ښکاري چې د وای فای شبکې وي مګر جالونه دي.

د دې لپاره چې خلک وصل شي، سایبر مجرمین د لاسرسي ځایونو ته پیژندل شوي نومونه ورکوي لکه "د وړیا هوایی ډګر وائی فای" یا "کافي هاؤس." حتی برید کونکي کاروونکو ته اړتیا لري چې د "حساب" لپاره راجستر شي، د دې وړیا خدماتو ته د لاسرسي لپاره د پټنوم سره ډک شي.

هېکرانو کولی شي د کاروونکو بریښنالیک، ای کامرس، او نورو خوندي معلوماتو ته لاسرسی ومومي ځکه چې ډیری کاروونکي د ډیری خدماتو لپاره ورته بریښنالیک او پاسورډ ترکیب کاروي. هیڅکله شخصي معلومات مه ورکوئ کله چې وړیا وای فای سره وصل شئ، د احتیاط سربیره. او تل یو ځانګړی پاسورډ جوړ کړئ هرکله چې تاسو د دې کولو غوښتنه وکړئ، که دا د Wi-Fi یا کوم بل پروګرام لپاره وي. د نورو معلوماتو لپاره مهرباني وکړئ لیدنه وکړئ:

https://www.techtarget.com/searchsecurity/definition/IP-spoofing

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

فشینګ بریدونه

وسایل د ډیری فشینګ بریدونو هدف دی څکه چې دوی په دوامداره توګه روان دي. څکه چې دوی په مکرر ډول خپل بریښنالیک په ریښتیني وخت کې ګوري ، د رسیدو سره سم بریښنالیکونه لوستل او خلاصول ، د ګرځنده کارونکي ډیر افشا کیږي. د ټیټ سکرین اندازې ته، په ګرځنده وسیلو کې د بریښنالیک پروګرامونه لږ معلومات ښکاره کوي، کاروونکي ډیر زیانمنونکي کوي. د مثال په توګه، پرته لدې چې تاسو د سرلیک معلوماتو بار پراخ کړئ، یو بریښنالیک ممکن د لیږونکي نوم حتی د خلاصیدو وروسته هم وښیي. هیڅکله په بریښنالیکونو کې لینکونو باندې کلیک مه کوئ چې تاسو یې نه پیژنئ. اجازه راکړئ څواب یا عمل توکي تر هغه وخته پورې انتظار وباسئ چې تاسو په کمپیوټر کې یاست که ستونزه عاجل نه وي. دلته د فشینګ بریدونو او د دوی د مخنیوي څرنګوالي په اړه نور معلومات شتون لري:

https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

سپایویر

که څه هم ډیری ګرځنده کاروونکي د مالویر په اړه اندیښمن دي چې بیرته هکرانو ته د ډیټا جریان لیږل کیږي، سپایویر یو ډیر سمدستي ګواښ دی. کاروونکي باید ډیری وختونه د شریکانو، همکارانو، یا کارګمارونکو لخوا ګمارل شوي سپایویر په اړه اندیښمن وي چې غواړي د نامعلوم برید کونکو څخه د مالویر پرځای د دوی حرکتونه او چلند وڅاري. ډیری دا پروګرامونه، چې ډیری وختونه د سټیکرانو په نوم یادیږي، د هدف په سمارټ فونټ کې د دوی د پوهې یا رضایت پرته نصب شوي دي. دا ډول غوښتنلیک د نورو مالویر په پرتله یو څه مختلف اداره کولو ته اړتیا لري څکه چې دا څنګه ستاسو وسیله او هدف ته ننوځي. په دې توګه یو بشپړ انټي ویروس او مالویر کشف سویټ باید د سکین کولو متخصص تخنیکونه وکاروي. د نورو معلوماتو لپاره مهرباني وکړئ لیدنه وکړئ:

https://www.malwarebytes.com/spyware

مات شوي کریپټوګرافي

کله چې د اپلیکیشن پراختیا کونکي د کوډ کولو غیر مؤثر تخنیکونه کاروي یا په ناسمه توګه قوي کوډ کولو ځای په ځای کوي ، نو کریپټوګرافي مات کیدی شي. په لومړي سناریو کې د اپلیکیشن پراختیا پروسې ګړندي کولو لپاره، پراختیا کونکي ممکن د دوی منل شوي امنیتي نیمګړتیاو سره سره د کوډ کولو پیژندل شوي تخنیکونه وټاکي. د دې له امله ، هر ټاکل شوی برید کونکی کولی شي د نیمګړتیاوو څخه ګټه پورته کړي ترڅو پاسورډ مات کړي او لاسرسی ترلاسه کړي.

په دویمه قضیه کې، پروګرام کونکي خورا خوندي الګوریتم ګماري مګر اضافي "شاته دروازې" د لاسرسي وړ پریږدي چې د دوی اغیزمنتوب کموي. د مثال په توګه، هکران ممکن د پاسورډونو اټکل ونه کړي، مګر که پراختیا کونکي په کوډ کې کیګونه معرفي کړي چې برید کونکي اجازه ورکوي د لوړې کچې اپ ځانګړتیاوې بدل کړي - لکه د متن پیغامونو لیږل یا ترلاسه کول - دوی ممکن حتی د مسلو رامینځته کولو لپاره پاسورډونو ته اړتیا ونلري.

مخکې له دې چې اپس (اپلیکېشنونه) خپور شي، دا د شرکتونو او پراختیا کونکو مسؤلیت دی چې د کوډ کولو معیارونه پلي کړي. د نورو معلوماتو لپاره مهرباني وکړئ لیدنه وکړئ:

https://knowledge-base.secureflag.com/vulnerabilities/broken_cryptography/broken_cryptography_category.html

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د ناستي ناسمه اداره کول

ډېری اپس "ټوکنونه" کاروي، کوم چې کاروونکو ته اجازه ورکوي چې ډېری عملیات ترسره کړي پرته له دې چې خپل پیژندنه بیا تایید کړي ترڅو د ګرځنده وسیلو لیرد لپاره د لاسرسي اسانتیا مالتړ وکړي.

ټوکنونه د وسیلو پیژندلو او تصدیق کولو لپاره د اپسونو لخوا رامینځته شوي، لکه څنګه چې پاسورډونه د خلکو لپاره دي. د هرې لاسرسي هڅې یا "غونډې" سره، خوندي اپس نوي نښې رامینځته کوي چې باید شخصي وساتل شي. منیفیسټ ادعا کوي چې د سیشن نامناسب اداره کول هغه وخت پیښیږي کله چې برنامه په غیر ارادي ډول د سیشن نښې شریکوي ، لکه د ناوړه لوبغاړو سره چې بیا د دوی سره د ریښتیني کاروونکو په توګه راپورته کیدی شي. دا په مکرر ډول د یوې ناستې په پایله کې پیښیږي چې لاهم فعال وي وروسته له دې چې کارونکي اپلیکیشن یا ویب پاڼه پریږدي. یو سایبر مجرم به ویب پاڼ او ستاسو د ګمارونکي شبکې نورو اړوندو ساحو ته غیر محدود لاسرسی ولري که چیرې ، د مثال په توګه ، تاسو د خپل ټابلیټ څخه د کار ځای انټرانیټ سایټ ته ننوتل. او کله چې تاسو دنده پای ته ورسوله لاګ آوټ کول هیر کړل.

د ګرځنده امنیت لپاره به بیا کوم ګواښونه راڅرګند شي؟

سره له دې چې د هکرانو لپاره غوره هدف ګرځېدلی، د ګرځنده امنیت ته د شبکې او کمپیوټر امنیت په څیر ورته لومړیتوب نه ورکول کیږي. حتی د ګرځنده اکوسیستم دننه، د هارورډ سوداګری بیاکتنې تحلیل سره سم، د ګرځنده اپلیکیشن پراختیا په پرتله امنیتي پانګه اچونه په دوامداره توګه کمه وه. لکه څنګه چې په ګرځنده وسیلو زموږ تکیه زیاتیږي، د ډیټا ارزښت هم لوړیږي، کوم چې هیکرانو ته ډیر هڅوي. د اضافي ګواښونو په لټه کې اوسئ چې په لاندې دریو لویو اغیزو ساحو کې په نښه شوي د ګرځنده امنیت خطرونو سربیره چې موږ یې بحث کړل.

:SMiShing

سایبری جنایتکاران SMiShing کاروي، د فشینګ سکیمونو په څیر یو تخنیک، هڅه کوي چې کاروونکي د مالویر ډاونلوډ کړي، په زیان رسوونکو لینکونو کلیک وکړي، یا شخصي معلومات ښکاره کړي. د بریښنالیک پرځای ، د SMiShing برید د متن پیغامونو له لارې پیل شوی.

:BYOD

لکه څنګه چې شخصي ګرځنده وسیلو ته د لوړې کچې لاسرسی د کارپوریټ کاروونکو لپاره چمتو شوی ، سمارټ فونونه او ټابلیټونه په لازمي ډول د ډېری سوداګری عملیاتو لپاره د ډیسټکاپ کمپیوټرونو ځای نیسي. په هرصورت، شخصي ګرځنده وسیلې د مربوط امنیت یا کنټرول ورته کچه نه وړاندې کوي لکه د ډیسټاپ کمپیوټرونو په څیر چې د شرکت ملکیت لري چې دوی یې ځای په ځای کوي.

:The Internet of Things (IoT)

څکه چې د سمارټ وسیلو مختلف ډولونه په چټکۍ سره پراخیږي، د RFID چپس څخه ترموسټات او حتی د کور وسایلو ته، دا تل د کاروونکو یا انټي ویروس پروګرامونو لپاره امکان نلري چې په دوی باندې نظر وساتي. د دې له امله، IoTوسیلې د هیکرانو لپاره مطلوب هدف دی چې دوی لویو شبکو ته د ننوتلو نقطو په توګه کاروي.

ستاسو د پټنوم (پاسورډ) خوندي کول

ستاسو پاسورډونه ترټولو مکرر میتود دی چې د کمپیوټر هیکر به تاسو ته زیان رسولو لپاره کاروي. آنلاین شرکتونه په مکرر ډول له موږ څخه غوښتنه کوي چې زموږ د ننوتلو معلومات تازه کړئ او هغه پاسورډونه غوره کړئ چې د سخت امنیت معیارونو سره سمون لري. کله چې هغه پټنوم چې تاسو یې کارول غواړئ خورا لنډ وي او یو ځانګړی کرکټر، شمیره، او لوی لیک نلري، دا کیدای شي

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

مایوسه وي. که څه هم امنیتي لاربښوونې ممکن ناامنه وي، دوی ستاسو د ساتنې لپاره شتون لري. تاسو باید د خوندي پاسوردونو په اهمیت پوه شئ مخکې لدې چې موږ دې اړتیاو ته ساده ځوابونه وړاندې کړو. د خپل پټنوم ترتیبولو پر مهال:

-د خپل معلومات خوندي ساتلو لپاره د وینډوز پاسوردونو تکیه مه کوئ. دوی په چټکۍ سره ویجاړ شوي.
-داسې پاسوردونه جوړ کړئ چې لږترلږه اته حروف اوږد وي. یو لنډ جمله ستاسو د پټنوم په توګه هم کارول کیدی شي.
-د لنډ، ښکاره پاسورډ کارولو پر ځای، دا غوره ده چې خپل پاسوردونه ولیکئ او په خوندي ډول یې خوندي کړئ.
-خپل پټنوم د سمبولونو، لوړو لیکو، کوچنیو لیکو او عددونو څخه جوړ کړئ.
-هر ځل مختلف پاسورډ وکاروئ.
-خوندي پاسوردونه وکاروئ چې ستاسو شخصي ګټو یا د ژوند طریقې سره نږدې نه وي.
-هېڅکله خپل کلیدي پاسوردونه له چا سره مه ښکاره کوئ.
-په هرو دریو یا شپږو میاشتو کې خپل پاسورډ بدل کړئ.
-په یاد ولرئ چې تاسو سره ستاسو د وینډوز پاسورډ، د بې سیم شبکې کوډ کولو، او د کمپیوټر بل هر ډول پټنوم چې تاسو یې لرئ په موندلو کې د مرستې لپاره ډیری وړیا آنلاین وسیلې شتون لري.

د پاسورډ بریدونه

زموږ څخه ډیری د پیژندل شوي سافټویر برنامو لخوا وړاندیز شوي امنیتي دندو څخه کار اخلي. تاسو کولی شئ د مایکروسافټ، Quicken، Adobe، او نورو شرکتونو څخه د فایل یا سافټویر خوندي کولو لپاره پاسورډ وکاروئ. د مایکروسافټ دفتر پروګرامونه لکه مایکروسافټ ورډ د دې یو عام مثال دی. دا د کلمې پروسیسر یو امنیتي ځانګړتیا وړاندې کوي چې تاسو ته اجازه درکوي د هر سند پټنوم خوندي کړئ. هر هغه څوک چې د سند خلاصولو هڅه کوي د پټنوم لپاره هڅول کیږي، او تر هغه چې سم پاسورډ داخل شوی نه وي، په سند کې به هیڅ مینځپانګه ونه لیدل شي. یوازې صادق خلک به د دې امنیتي اقدام لخوا لرې وساتل شي ، کوم چې یوازې یوه طبقه ده. پټنوم د دوو تخنیکونو څخه یو په کارولو سره اخیستل کیدی شي. د کمپیوټر په مؤثره توګه کارول د قوي پاسوردونو کارولو ته اړتیا لري. که دا د بریښنالیک حساب وي، د شبکې ننوتل، یا آنلاین بانکداري، دوی اړین خدمت ته د لاسرسي تصدیق کولو سره د امنیتي خنډ په توګه کار کوي. تاسو ته اجازه درکول کیږي چې د مختلف حسابونو لپاره مختلف پاسوردونه وکاروئ. دا کار کول ډیر ننګونکي کوي. د دې له امله، په تخنیکي لحاظ، هغه معلومات چې ستاسو پاسوردونه دفاع کوي باید د قیمتي خوندي په څیر خوندي وي. یو قوي پاسورډ د هر سیسټم ترټولو مهم برخه ده کله چې دا ډیجیټل امنیت ته راځي. ترټولو پرله پسې لاره چې هیکران او برید کونکي ستاسو د معلوماتو سیسټمونه په نښه کوي د تاریخ په وینا د کریک کولو پاسوردونو له لارې دي.

پروفایل کول

پروفایل کول د هغه شخص په اړه چې د حقایقو او شخصي معلوماتو په راټولولو سره پاسورډ لري د زده کړې اټکل رامینځته کوي. زموږ پاسوردونه عموما د هغه څه استازیتوب کوي چې زموږ لپاره په یاد ساتل اسانه دي، لکه زموږ د زیږون کال، د یو ځانګړي کس نوم، زموږ ښارګوټی، زموږ د فوټبال غوره ټیم، او نور. دا او ورته نور حقایق د پروفایلرانو لخوا په پام کې نیول شوي. دوی ممکن ستاسو د کتابچه کې کتابونه وګوري که دوی ستاسو دفتر ته لاسرسی ولري. له هغه ځایه چې ډیری پاسوردونه شتون لري تاسو کولی شئ په یاد ولرئ چې یاد ساتل ستونزمن دي او تاسو سره هیڅ اړیکه نلري. په هرصورت، په سیسټم کې د ماتولو لپاره ترټولو مشهوره طریقه چې د ټاکل شوي هیکرانو لپاره خورا اغیزمنه پاتې کیږي د کارونکي په اړه د شخصي معلوماتو په پوهیدو سره د پټنوم اټکل کول دي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

ټولنیزه انجنیري

په هوښیار ډول جوړ شوي سناریوګانو او پوښتنو له لارې، ډیری خلک د دوی د رمزونو په افشا کولو کې دوکه شوي. دا ممکن ستاسو د ISP څخه د تلیفون کال بڼه واخلي، څوک چې ادعا کوي د سرور اپ ګرېډ کوي او ستاسو پټنوم ته اړتیا لري ترڅو ډاډ ترلاسه کړي چې تاسو په پروسه کې هیڅ بریښنالیک له لاسه نه ورکوئ.

یو څوک کولی شي ستاسو د شرکت د مختلف څانګې څخه د همکارانو په توګه وښیي او د شریک بریښنالیک حساب ته د پټنوم غوښتنه وکړي پدې دلیل چې مالک اوس مهال ناروغ دی او اړتیا لري چې شیان ژر تر ژره واستوي. دې تمرین ته ټولنیز انجینری ویل کیږي. دا لاهم د هیکرانو لپاره د اعتبار وړ لاره ده چې هڅه وکړي سیسټم ته ننوځي.

قاموسی بریدونه

د لغت برید په قاموس لغات کې هره کلمه د پاسورډ په توګه داخلول شامل دي ترڅو د پاسورډ خوندي کمپیوټر ، شبکې یا نورو IT سرچینو ته لاسرسی ومومي. د قاموس برید هم د دې لپاره کارول کېدی شي چې د ارتباط یا سند په اړه هڅه وکړي چې کوډ شوی وي. د احتمالي پاسورډونو لیست به پدې برید کې د سند برید لپاره وکارول شي. د لغتونو یو شمیر سیټونه وړیا آنلاین ډاونلوډ لپاره شتون لري، او دا لیست د لغت په نوم پیژندل کیږي.

د وحشي ځواک بریدونه

په ډیری مواردو کې، دا برید به د پنځو ثانیو څخه لږ وخت کې پای ته ورسیږي. دا طریقه د احتمالي پاسورډونو دمخه بار شوي لیست باندې تکیه نه کوي. پرځای یې، دا به هر پټنوم هڅه وکړي - په شمول د لیکونو، شمیرو، او ځانګړي حروفونو سره - دا ممکنه وي. که څه هم دا ممکن ناشونی ښکاري، د پروسس کولو لوی ځواک په پام کې ونیسئ چې دا مهال په هر کمپیوټر کې شتون لري. اپلیکیشن د ځلورو څخه تر لسو حروفونو سره د پاسورډونو هڅه کولو لپاره ډیزائن شوی دی ځکه چې ډیری پاسورډونه له ځلورو څخه کم نه لري. د مثال لپاره، دا ممکن د لاندې پاسورډونو په هڅه کولو سره برید پیل کړي.

د قوي پاسورډ جوړول

موږ اوس پوهیږو چې پاسورډونه لکه "منه،" "مایکل،" او حتی "کیله 4" نامنه دي. آنلاین خدمتونه د دې له امله ډېر خوندي اعتبار ته اړتیا لري. ډیری ویب پاڼې به داسې پاسورډ ته اړتیا ولري چې لږترلږه اته حروف اوږد وي او یو شمیر او یو ځانګړی کرکټر ولري. ځینې به په لوی لیک باندې هم ټینګار وکړي. دا به ننګونه وي چې د داسې پټنوم سره راشي چې د یادولو لپاره دواړه ساده وي او د دې معیارونو سره سمون ولري. زه د مستقیم جوړښت سره د یو لړ پاسورډونو کارولو مشوره کوم. فرض کړئ چې تاسو د خپل آنلاین بانکي حسابونو لپاره د پټنوم تازه کول غوره کړي او دا چې تاسو باید د پاسورډ امنیتي معیارونو سره مطابقت ولرئ.

که تاسو باید په پټنوم کې "ایپل" شامل کړئ، د "Orange23$%18No" کارولو په اړه فکر وکړئ. د پاسورډونو رامینځته کولو لپاره ډیری لارې شتون لري چې دواړه یې اټکل کول سخت او په یاد ساتل ساده دي. د پټنوم مدیران غوره انتخابونه دي. مهرباني وکړئ وګورئ. د پاسورډ مدیرانو لپاره پیچلي پاسورډ وکاروئ. د پاسورډ مدیر وکاروئ، لکهDashlane ، Sticky Password، LastPass، یا د پاسورډ باس.

ستاسو پټنوم په مکرر ډول ستاسو د معلوماتو د ساتنې لومړی او خورا مهم تضمین دی. دا ستاسو کور ته د ننوتلو په توګه کار کوي. دا لکه د خراب پاسورډ کارولو لپاره ټوله شپه دروازه خلاصه پریږدي یا هیڅ شی نه. شاید هیڅوک به داخل نشي، یا شاید یو څوک به ستاسو هرڅه غلا کړي. د دې په اړه ډېر محتاط اوسئ چې تاسو خپل پاسورډونه څنګه جوړوئ او چیرته یې ذخیره کوئ.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د پاسورډ اتومات خوندي کول

ډېری برنامه او عملیاتي سیستمونه د دوی ساده کارولو لپاره ترټولو غوره هڅه کوي. د پاسورډونو لپاره د اتوماتیک خوندي کولو اختیار وړاندیز کول یوه لاره ده چې ویب براوزرونه او نور اطلاقات دا ترسره کوي. د مثال په توګه، ډېری ویب براوزرونه به تاسو څخه وغواړي چې پټنوم خوندي کړئ کله چې تاسو ویب پاڼې سره وصل شئ او آنلاین حساب ته ننوځئ. تاسو براوزر ته اجازه ورکړې چې په خپل کمپیوټر کې پټنوم خوندي کړي کله چې تاسو دا اختیار غوره کړئ او خپل پټنوم داخل کړئ. د دې نه کوډ شوي ډېټا څخه دا پاسورډونه بیرته ترلاسه کولو لپاره ډېری برنامې رامینځته شوي. دلته یو اسانه حل دی. هیڅکله سافټویر ته اجازه مه ورکوئ چې ستاسو پاسورډونه پخپله خوندي کړي. تاسو کولی شئ دا تعدیل کړئ که ستاسو ویب براوزر اوس مهال تاسو ته ننوځي کله چې تاسو ویب پاڼې toته په اتوماتیک ډول لیدنه وکړئ وروسته له دې چې تاسو ورته د خپل پټنوم خوندي کولو اجازه درکړه. زه به تشریح کړم چې څنګه د انټرنیټ اکسپلورر، موزیلا فایرفوکس، ګوګل کروم، او سفاري څخه ستاسو پاسورډونه پاک کړم، حتی که زه نشم کولی د هر غوښتنلیک لپاره دا څنګه ترسره کړم. د وینډوز، ماک او لینکس لپاره غوره څلور ویب براوزرونه دلته لیست شوي دي.

انټرنیټ اکسپلورر(IE)

د مینو بار څخه "وسیلې" غوره کړئ، او بیا "انټرنیټ اختیارونه" غوره کړئ. دا به د یو شمیر انتخابونو سره نوې کړکۍ راوړي. په "عمومي" ټب کې د "لټون تاریخ" لاندې "ړنګول" تڼۍ کلیک وکړئ. ستاسو لنډمهاله فایلونه، تاریخ، کوکیز، خوندي شوي پاسورډونه، او د ویب فارمونو ډاټا ټول به د پایلې په توګه حذف شي.

موزیلا فایرفاکس

په مینو بار کې "وسیلې" او بیا "اختیارونه" کلیک وکړئ. تاسو باید د "امنیت" مینو لاندې د "پاسورډونو" لیبل یوه برخه وګورئ. یوه نوې کړکۍ به پرانستل شي کله چې تاسو "خوندي پاسورډونه" کلیک وکړئ، په هغه کمپیوټر کې ټول خوندي شوي پاسورډونه ښکاره کوي. تاسو کولی شئ د "ټول لرې کړئ" په کلیک کولو سره کوم خوندي شوي پاسورډونه حذف کړئ. کله چې پای ته ورسیږي، "بند" کلیک وکړئ او په "اختیارونو" کړکۍ کې، "د سایټونو لپاره پاسورډونه په یاد وساتئ" غیر چیک کړئ.

ګوګل کروم

د سکرین په پورتنۍ ښي کونج کې موقعیت لرونکي مینو بار کې "ترتیبات" کلیک وکړئ. دا به د یو شمیر انتخابونو سره یو نوی پاڼه راوړي. هلته د سکرول کولو وروسته د پاڼې په پای کې "پرمختللي ترتیبات وښایاست" کلیک وکړئ. نور اختیارونه، د پاسورډونو لپاره د یوې برخې په ګډون، د پایلې په توګه به پورته شي. "ذخیره شوي پاسورډونه اداره کړئ" انتخاب کیدی شي. تاسو به وکولی شئ دا کار وکړئ ترڅو خپل رمزونه له ذخیره کولو څخه لرې کړئ. په راتلونکي کې د ډېری پټنوم بریدونو څخه د ځان ساتلو لپاره، وروسته له دې چې تاسو یې ترسره کړئ "د پټنومونو ساتلو وړاندیز وکړئ چې په ویب کې یې ټایپ کړئ" په څنګ کې بکس خلاص کړئ.

سفاري(SFAFARI)

په مینو بار کې د "سفاري" کلیک کولو وروسته د مینو څخه "ترجیحات" غوره کړئ. یوه نوې کړکۍ به ښکاره شي چې ډېری اختیارونه لري. تاسو کولی شئ د "پاسورډونو" انتخاب په غوره کولو سره خپل ټول خوندي شوي رمزونه وګورئ. د دې کړکۍ په پای کې د "ټول لرې کړئ" تڼۍ موندل کیدی شي. کله چې تاسو دا کلیک وکړئ، خوندي شوي پاسورډونه ړنګ شوي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

اتومات ننوتل

عملیاتي سیستمونه تاسو ته د خپل پټنوم خوندي کولو او په اوتومات ډول ننوتلو انتخاب هم درکوي. دا دواړه په زړه پورې ګټور او خورا خطرناک دي. دا ممکن د منلو وړ وي که ستاسو کمپیوټر یوازینی کاروني کې وي او سیسټم په داسې ځای کې تړل شوی وي چې یوازې تاسو ورته لاسرسی لرئ. مګر که نور خلک کله ناکله ستاسو کمپیوټر ته لاسرسی ولري، دا ممکن خطرناک وي. ستاسو ټول اسناد او شخصي معلومات ستاسو په کمپیوټر کې زیرمه شوي دي. هیڅ شی ستاسو د معلوماتو د غلا کولو څخه یو څوک نه منع کوي که ستاسو کمپیوټر په اوتومات ډول لاګ ان شي لکه څنګه چې تاسو یې چالان کړئ. په خپل کارن حساب کې د پټنوم فعالولو سره، تاسو کولی شئ دا نور ننګوني کړئ.

ستاسو د ویب پاڼې محرمیت خوندي کول

براوزرونه

ستاسو د انټرنیټ پیوستون معلومات او آنلاین فعالیت په منظم ډول د ویب براوزرونو لخوا راټولیږي. په منظم ډول یو معیاري ویب براوزر ستاسو د پیوستون او آنلاین فعالیتونو په اړه معلومات راټولوي او خوندي کوي. دا لاندې معلومات هغه ویب پاڼو ته لیږي چې تاسو یې ګورئ.

-ستاسو IP پته
-ستاسو د وسیلې ډول،
-ستاسو د براوزر نوم،
-ستاسو د کوکي تنظیمات
-ستاسو د براوزر اضافه کول،
-ستاسو د موږک کلیکونه او حرکتونه،
-ستاسو ځای او د وخت زون
-ستاسو د سکرین ریزولوشن او د بیټرۍ کچه ځینې اضافي اساسي توضیحات دي.

د دې ډیټا ډیری برخه ممکن غیر مهم ښکاري، مګر کله چې راټول شي، دا یو واحد ډیجیټل ګوتو نښان تولیدوي چې ویب پاڼې ممکن تاسو آنلاین پیژني او څارنه وکړي. ستاسو د براوزر د ګوتو نښان به ویب پاڼو او د دریمې ډلې تحلیلونو ته ښکاره شي حتی که تاسو خپل کوکیز لرې کړی وي (کوچني ډیټا فایلونه چې ویب پاڼې ستاسو په وسیله ذخیره کوي)، تاریخ، او کیچ یا یو پټ/شخصي کړکۍ کاروي. دا ممکن ستاسو او ستاسو د فعالیت تر مینځ روښانه اړیکې رامینځته کړي. تاسو شاید باور ولرئ چې ټول هغه څه چې د تعقیب مخه نیسي ستاسو د براوزر محرمیت ترتیباتو کې یو ساده بدلون دی. په حقیقت کې، دا ممکن ستاسو د براوزر د ګوتو نښې ځانګړتیا زیاته کړي.

د محرمیت ساتلو لپاره غوره براوزر

ډیری براوزرونه شتون لري. غوره لاندې اوه دي، مګر ترټولو خوندي د کروم، ایج، سفاري، اوپرا، زړورتیا، او انټرنیټ اکسپلورر په پرتله فایرفوکس دی.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

څنګه په خوندي ډول براوزر وکاروئ

پاک او کلیک وکړئ

په یوه کلیک سره، هر هغه براوزر بند کړئ چې تاسو یې اوس مهال لرئ. پدې کې د فارم ډیټا، کوکیز، کیچ، پاسورډونه چې تاسو دمخه خوندي کړي، او ستاسو د براوزر او ډاونلوډ تاریخ شامل دي.

د خپروني بیجر

ټریکرونه بند کړئ او په سمدستي توګه په هغه ویب پاڼو کې شکمن فعالیت پیژنئ چې تاسو یې ګورئ. هر هغه څه چې د کارونکي رضایت خلاف وي بند شوي دي.

سایبرګوسټ وی پی ان

تاسو کولی شئ د VPN خدمت په مرسته خپل IP پته پټ کړئ. دا د هیڅ فعالیت لاګ نه ساتي او ټول آنلاین تعقیب غیر فعالوي.

که تاسو نه غواړئ ویب براوزرونه بدل کړئ، ستاسو په آنلاین فعالیت کې د تعقیب او ډیټا ذخیره کمولو لپاره نورې لارې شتون لري، لکه: د کوکیز شمیر محدودول چې تاسو یې منئ؛ ستاسو د براوزر تنظیم کول ترڅو د تعقیب اعلاناتو او نه لیدل کیدونکي ټریکرونه بند کړي، او په منظم ډول ستاسو زیرمه او کوکیز پاک کړئ ترڅو ستاسو د تعقیب کیدو خطر کم کړي.

دا کړنالرې ګټورې دي، مګر دوی به ستاسو د براوزر د ګوتو نښان د پام وړ بدل نه کړي. لکه څنګه چې مخکې یادونه وشوه، د یو څو ترتیباتو بدلول ممکن په حقیقت کې ستاسو د براوزر ډیجیټل ګوتو نښان د هغو ویب پاڼو لپاره چې تاسو یې ګورئ نور هم ځانګړي ښکاري.

د تور شبکې کارول ستاسو د براوزر د ګوتو چاپ کیدو چانس کمولو لپاره ښه لاره ده. مهمه نده چې کوم وسیله یا عملیاتي سیسټم کارول کیږي، د تور هر کارونکي باید دقیق ورته د براوزر ګوتې نښه ولري. تاسو کولی شئ د تور براوزر وکاروئ یا د تور شبکې ته د لاسرسي لپاره براوزر بدل کړئ.

د فعالینو لپاره غوره او خوندي براوزرونه

تور (Tor) براوزر

د مخکینۍ ترتیب شوي امنیتي میکانیزمونو او ریلي سرورونو په مرسته، Tor، د دلیل په توګه د محرمیت ترټولو مشهوره متمرکز براوزر، د غیرقانوني جاسوسۍ مخه نیسي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

EPIC

د محرمیت لپاره ډیفالټ اختیار فعال دی. براوزر به کوکیز، تعقیبونکي، او اعلانونه غیر فعال کړي کله چې د شخصي لټون انجن DuckDuckGoکاروي. ستاسو د ننوتلو معلومات، د لټون کولو تاریخ، او نور معلومات هم ذخیره شوي ندي.

FIREFOX

د محرمیت محافظت څخه مننه کوم چې تاسو د تعقیب ، ویروسونو او کریپټومینرونو پروړاندې ساتي ، دا یو له خورا خوندي براوزرونو څخه دی. سربیره پردې، دا په مکرر ډول تازه کیږي ترڅو د ګواښونو کنټرول کې مرسته وکړي.

د لټون ماشینونه

ستاسو هر انټرنیټ حرکت د ګوګل او نورو لټون انجنونو لخوا تعقیب کیږي. دوی په مکرر ډول او ممکن د کاروونکو ډیټا دریمې ډلې ته لیږدوي. ګوګل او نور د لټون انجنونه ستاسو په اړه څومره معلومات لري شاید تاسو حیران کړي. دوی یو ټن معلومات راټولوي ترڅو هدف شوي اعلانونه چمتو کړي او ستاسو ویب لټون تنظیم کړي.

ګوګل څه پوهیږي

ستا په اړه

ګوګل ستاسو نوم، عمر، جنس، د مخ او غږ پیژندني ډاټا، د فټنس معلوماتو، سیاسي نظرونو، او مذهب څخه خبر دی. دا څنګه پوهیږي، د ګوګل، ګوګل لټون، ګوګل فټ، او ګوګل معاون لپاره د راجستر کولو پروسې له لارې.

چیرته یې؟

ګوګل ستاسو د اوسني موقعیت او همدارنګه ستاسو د تیر، اوسني او راتلونکي ځای څخه خبر دی. ستاسو د ترانسپورت طریقه او د موقعیت پوښتني ګوګل ته هم پیژندل کیږي. دا څنګه پوهیږي، د Waze او Google Maps له لارې.

تاسو له چا سره خبرې کوئ

ستاسو خبرې اترې، ملاقاتونه، انځورونه، فلمونه، او نور هغه څه چې تاسو ډرایو ته ځړول ټول ګوګل ته معلوم دي. حساس معلومات، په شمول د مارچ لارې، د بایکاټ یا اعتصاب پلان، لیک او غوښتنلیکونه، ټول ممکن ګوګل ته د لاسرسي وړ وي. دا څنګه پوهیږي، د ګوګل ډرایو، ګوګل کیلنډر، ګوګلHangouts ، او Gmail له لارې.

ته څوک یې

ګوګل د هغو کتابونو، مقالو، او فلمونو څخه خبر دی چې تاسو یې لوستل، لیدلي، پیرودلي او لټون یې کړي دي. دا څنګه پوهیږي، د ګوګل نیوز، یوټیوب، ګوګل لټون، او د ګوګل شاپینګ اعلاناتو، د ګوګل کتابونو له لارې.

هغه څه چې تاسو یې لټون کوئ

ګوګل د هغو ویب پاڼو له تاریخ څخه خبر دی چې تاسو یې لیدلي، په شمول د هر ډول خوندي شوي کارن نومونه او پاسورډونه.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د کروم کارولو څرنګوالی
تاسو باید خبر اوسئ چې د لټون ډیری انجنونه د قانون پلي کونکو یا حکومتي چارواکو لخوا ستاسو د لټون او لټون کولو تاریخ بدلولو ته اړ ایستل کیدی شي.

په پام کې ونیسئ چې دا به ستاسو لپاره د یو فعال په توګه څه شی وي که تاسو په مکرر ډول د مخالفانو او حکومتي شخصیتونو او همدارنګه د حقوقي مرستو او نړیوالو سازمانونو په اړه معلومات ګورئ. موږ پوهیږو چې ګوګل د لټون ترټولو مشهور انجن دی. مګر کله چې دا د کاروونکو معلوماتو تعقیب او راټولولو لپاره راځي، دا یو له بدترین څخه دی. اسوشیټیډ پریس پدې وروستیو کې وموندله چې ګوګل ستاسو د موقعیت تعقیب ته دوام ورکوي حتی که تاسو د "ځای تاریخ" اختیار بند کړئ.

د محرمیت لپاره د غوره لټون انجنونه

دک دک ګو(DUCKDUCKGO)
دا د کارولو لپاره محرم او ساده دی. نه کوکیز او نه هم د کاروونکي معلومات د دې لخوا راټول شوي. سربیره پردې، دا د سرورونو IPالاګونه پاکوي. تاسو کولی شئ DUKDUCKGO ته لاسرسی ومومئ:

https://duckduckgo.com/?va=b&t=hc.

متاجر(METAGER)
د آلمان څو ژبو لټون انجن د کارونکي د محرمیت په ساتلو باندې ډیر ټینګار کوي او نه د خپلو کاروونکو په اړه پروفایلونه او معلومات راټولوي. د میټاجر مستقیم لاسرسي لپاره تور وکاروئ. تاسو کولی شئ MetaGer ته لاسرسی ومومئ:

https://metager.org

استارتر پیج(STARTPAGE)
دا د تعقیب پرته د ګوګل ټیکنالوژۍ په کارولو سره د آرامۍ مګر شخصي سرفینګ تجربه وړاندې کوي Startpage. د کارونکي هیڅ معلومات نه ثبتوي یا یې بهر ګوندونو ته نه افشا کوي. تاسو کولی شئ د پیل پاڼې ته لاسرسی ومومئ:

https://www.startpage.com

ستاسو د معلوماتو محرمیت خوندي کول

فعالین په مکرر ډول حیاتي معلومات لري، او ډیری یې ډیری موادو ته لاسرسی لري چې ممکن د دوی اهدافو ته وده ورکړي. دا شتمنی، چې د معلوماتو په بڼه ساتل کیږي، د ټولو اړخونو لخوا د ناوړه بریدونو لپاره حساس دي. ستاسو د معلوماتو خوندي ساتلو لپاره یو بدیل په کوډ شوي فلش ډرایو (میموري سټیکونو) یا هارډ ډیسکونو کې دی، مګر داسې کول ممکن ستاسو معلومات حتی د غلا، ضایع کیدو یا تخنیکي ستونزو سره حساس پریږدي. د فزیکي وسایلو ذخیره کولو ظرفیت هم محدود دی.

د Cloud Storage د پایلې په توګه خورا مهم شوي. په Cloud کې معلومات هم د شریکولو وړ دي، کوم چې د فعالینو لپاره خورا مهم دی چې د خپلو الملونو لپاره د معلوماتو خپرولو ته اړتیا لري.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د کلاوډ ذخیره

د پام وړ بادل ذخیره کولو ډیری چمتو کونکي ممکن ستاسو ډیټا ته د قانون پلي کونکو لاسرسي ته اړتیا ولري.

تاسو باید خبرداری ورکړئ چې ستاسو د کلاوډ ذخیره چمتو کونکی د ډیټا کوډ کولو وړاندیز کوي پدې معنی ندي چې ستاسو محرمیت تضمین شوی. اډمینټ څارنوالان ممکن لوی بادل یا کلاوډ شرکتونه همکاری ته اړ کړي، او یوازې کوډ کول به د دې په وړاندې ساتنه ونه کړي څکه چې ځینې خدمتونه په متحده ایالاتو کې د ملي امنیت اداری (NSA) په څیر د دولتي جاسوس سازمانونو سره د معلوماتو او فایلونو تبادله کولو لپاره پیژندل شوي.

د کلاوډ ذخیره کولو څرنګوالی

د کلاوډ ذخیره چمتو کونکي په غوره کولو سره چې ستاسو فایلونه په محلي ډول ستاسو په وسیله کوډ کوي مخکې لدې چې دوی کلاوډ ته اپلوډ شي، تاسو کولی شئ خپل کلاوډ ذخیره خوندي کړئ (لکه د فایلونو سره مخالف چې کلاوډ ته په لیږد کې کوډ شوي وي). په یاد ولرئ چې چمتو کونکي ممکن د کوډ کولو کیلي ته لاسرسی ولري او ممکن ستاسو فایلونه ډیکریپټ کړي یا چارواکو ته د اړتیا په صورت کې ورکړي.

دا په کلکه سپارښتنه کیږي چې تاسو خپل ډیټا د کلاوډ خدمت ته سپارلو دمخه په لاسي ډول کوډ کړئ. تر هغه چې تاسو هیڅکله د خپلو فایلونو سره د کوډ کولو کیلي نه اپلوډ کوئ ، تاسو به یوازینی څوک یاست چې ستاسو د ډیټا ډیکریپټ کولو کیلي لرئ.

دلته ډیری سوداګریز او وړیا کوډ کولو برنامې شتون لري ، مګر ډاډ ترلاسه کړئ چې دوی ستاسو د وسیلو او ستاسو د کلاوډ ذخیره چمتو کونکي سره مطابقت لري. ډاډ ترلاسه کړئ چې برنامه له پای څخه تر پای پورې کوډ کول کاروي، کوم چې ډاډ ورکوي چې ستاسو فایلونه له هغه شیبې څخه کوډ شوي چې دوی ستاسو سمارټ فون پریږدي تر هغه چې تاسو یوځل بیا دوی ته لاسرسی ومومئ.

د معلوماتو شریکول

[اپلیکشن](https://veracrypt.fr/)Veracrypt (https://veracrypt.fr/) کاروونکو ته اجازه ورکوي چې کوډ شوي فولډرونه په هارډ ډرایو او آنلاین ذخیره کولو، ګوګل ډرایو یا ډراپ باکس کې خوندي کړي، کوم چې بهرنیانو ته د نورمال یا

سیسټم فایلونو په څیر ښکاري. دا د آنلاین شریکولو او ذخیره کولو لپاره د اپلوډ کولو دمخه ستاسو په کمپیوټر کې د ذخیره کولو پرمهال ستاسو د اسنادو امنیت ډاډمن کولو لپاره ترسره کیږي. د دې لپاره چې برنامه د خبرتیا راجلبولو مخه ونیسي، د ویراکریپ کارولو وروسته غوښتنلیک حذف کول غوره کړئ ترڅو د دې په څیر سند کوډ کړئ حتی له کڅافاتو څخه. د فایل شریکولو لپاره د خوندي پای څخه تر پایه کوډ شوي بدیلونو لپاره، لاندې انتخابونه وګورئ:

https://cryptpad.fr/drive
https://ufile.io
https://send.tresorit.com
https://send.tresorit.com

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

ستاسو د ټولنيزو رسنيو او اړيکو ساتنه

د خوندي اړيکو کارولو څرنګوالی

فعالين په مکرر ډول د نورو فعالينو، ډلو، وکيلانو او ژورناليستانو سره شخصي معلومات تبادله کوي. د ريښتيني شخصي چټ ترسره کولو ترټولو لويه لاره د مخابراتو مخابراتو ده، مګر دا په څرګنده توګه ټل امکان نلري.

دا غوره ده چې د کوډ شوي مخابراتي خدماتو لکه سيګنال، تار او کيبيس څخه کار واخلئ کله چې آنلاين خبرې وکړئ. په دې طريقه کې، د پای څخه تر پای پورې کوډ کول د هغه څه د ساتنې لپاره کارول کيږي چې تاسو يې وايئ.

مهرباني وکړئ په ياد ولرئ چې ټيليګرام د ډيټا سرغړونې درلودې او دا چې له پای څخه تر پای پورې کوډ کول د "شخصي چيټونو" او آډيو او ويډيو تليفونونو استثنا سره په ډيفالټ فعال ندي. د بريښناليک خدماتو چمتو کونکي ممکن مجبور وي چې چارواکو ته ستاسو معلومات ورکړي. تاسو ممکن د ټولنيزو رسنيو د محرميت پاليسيو سره مخ شئ.

بريښناليکونه (ايميلونه)

ډيری پيژندل شوي بريښناليک شرکتونه خورا خوندي دي او د ډيټا ليکونو پروړاندې د ساتنې لپاره سخت ميکانيزمونه لري. په هرصورت، دا پروسيجرونه له خطا پاک او يا د ناکامۍ ثبوت نه دي. دا امکان نلري چې امنيتي تدابير به تاسو خوندي وساتي که ستاسو د بريښناليک چمتو کونکی د حکومتي چارواکو لخوا ستاسو په بريښناليکونو کې د معلوماتو بدلولو ته اړتيا ولري.

ستاسو د برښناليک پيژندنه شخصي ساتل

تاسو بايد د خپل محرميت ساتلو لپاره اضافي احتياطي تدابير ونيسئ ترڅو د دې احتمال کم کړئ چې دولتي ادارې به ستاسو د ليک له لارې تيريږي. ترټولو عملي لاره د شخصي بريښناليک خدمت کارول دي لکه پروټون ميل، فسټ ميل، يا زوهو ميل ځکه چې د بريښناليکونو کوډ کول وخت او هڅې اخلي.

رايس اپ او اکتيوکس، د فعالينو لپاره رامينځته شوي خوندي بريښناليک خدمتونه وړيا دي ځکه چې دوی د بسپنې لخوا ملاتړ کيږي. په هرصورت، دوی ممکن د سوداګريز چمتو کونکو په توګه د ډيری خوندي شوي بريښناليکونو ملاتړ ونه کړي، نو تاسو ممکن د اضافي بريښناليک مديريت وغواړئ، لکه د خوندي کلاوډ ذخيره کولو اسانتيا کې د زړو بريښناليکونو آرشيف کول.

ډيری پيژندل شوي بريښناليک شرکتونه خورا خوندي دي او د ډيټا ليکونو پروړاندې د ساتنې لپاره سخت ميکانيزمونه لري. په هرصورت، دا پروسيجرونه له خطا پاک او يا د ناکامۍ ثبوت نه دي. دا امکان نلري چې امنيتي تدابير به تاسو خوندي وساتي که ستاسو د بريښناليک چمتو کونکی د حکومتي چارواکو لخوا ستاسو په بريښناليکونو کې د معلوماتو بدلولو ته اړتيا ولري.

دا غوره ده چې خپل شخصي بريښناليک حسابونه او بريښناليک حسابونه په جلا توګه د فعاليت لپاره وساتئ. دا د هغه حساب مخه نيسي چې ستاسو شخصي، د پيژندلو وړ معلومات لري له هغه حساب (حسابونو) سره نښلول کيږي چې تاسو يې د پيښو پلان کولو يا د نورو فعالينو سره اړيکه ونيسئ.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

د بریښنالیک خوندیتوب

فشینګ د درغلۍ یوه بڼه ده کله چې آنلاین بدکاران یا نور جاسوسان د باور وړ سوداګرۍ یا اشخاصو ښکارندوی کوي چې تاسو یې پیژنئ، په ځانګړي توګه د بریښنالیک له لارې. موخه دا ده چې کاروونکو ته اجازه ورکړي چې خپل شخصي بریښنالیکونه یا نور معلومات افشا کړي. د دې لپاره چې تاسو قانع کړئ چې ناوړه سافټویر ډاونلوډ کړئ یا په لینکونو کلیک وکړئ چې داسې ښکاري چې مشروع وي، د هنرمندانو کولی شي تاسو هم جذب کړي. ډاډ ترلاسه کړئ چې د بریښنالیک پته د دوه ځله چک کول.

ټولنیزې رسنۍ(SOCIAL MEDIA)

د خورا مشهور ټولنیزو اپیسونو او سایټونو شاته شرکتونه د تناقض سره مخ شوي ، په ځانګړي توګه د محرمیت او امنیت په اړه. د دې حقیقت سره سره چې ټولنیز رسنۍ د فعالینو لپاره ځینې خورا ګټورې وسیلې وړاندې کوي - د حرکتونو او لاملونو لپاره ډله ایز ښکیلتیا، د پیښو ترویج، یا پوهاوی او کمپاین، د بیلګې په توګه.

د مثال په توګه، په وروستیو کلونو کې د کیمبرج انالیټیکا تناقض روښانه کړه چې څنګه فیسبوک د ملیونونو کاروونکو څخه د شخصي معلوماتو راټولولو اجازه ورکړه. د محرمیت دا ډول سرغړونه په ګوته کوي چې ټولنیز رسنۍ ستاسو په اړه څومره معلومات لري. هغه معلومات چې تاسو په دې شبکو کې ښکاره کوئ په ښکاره ډول شخصي ندي لکه څنګه چې تاسو باور لرئ.

جیوټاګینګ په مکرر ډول په ټولنیزو رسنیو کې ستاسو دقیق موقعیت په ګوته کولو لپاره کارول کیږي. فیسبوک یوازې ستاسو د موقعیت څخه ډیر څه تعقیبوي؛ دا ستاسو پیرودونه، ویب لټونونه، او اړیکې هم ثبتوي. پلیټ فارم په دوامداره توګه ستاسو اړیکو ته د لاسرسي غوښتنه کوي، د تلیفون تاریخ، او SMS د دې له امله.

د مخ پیژندنې په اړه مهم معلومات

پراخه او غیر ارادي د مخ نښه کول د ځارنې خطر زیاتوي. د مخ پیژندنې سافټویر د ټولنیزو رسنیو عکس شریکولو سیسټمونو کې ځای په ځای شوی. پلیټ فارمونه د لوی کارونکي مخ عکسونو راټولول راټولوي.

د ټولنیزو شبکو سایټونه معمولا چارواکو ته د مخ پروفایل معلومات وړاندې کوي. یوځل چې تاسو عکس اپلوډ کړئ، دا د پلیټ فارم ملکیت کیږي. د اوسني مخ پیژندنې سیسټمونو څخه د وتلو کومه لاره نشته. تاسو یوځل دننه یاست چې تاسو دننه یاست.

ستاسو شخصي معلومات د فیسبوک یا نورو ټولنیزو رسنیو پلیټ فارمونو سره خوندي ندي، لکه څنګه چې دوی په وار وار ښودلي. ستاسو محرمیت په خطر کې دی هغه نور شخصي معلومات چې تاسو یې په ټولنیزو رسنیو کې پوسټ کوئ. د مشهورو کمپاینرانو لپاره، د ګډون او لید تر منځ غوره کول دوه مخې توره ده.

د ټولنیزو رسنیو ترتیبات بدل کړئ

د فعال په توګه د غوره نوم نه ښودلو تضمین کولو لپاره، تاسو باید تل د پلیټ فارم ډیفالټ څخه خپل محرمیت تنظیمات بدل کړئ. تاسو به دا کنټرول کړئ چې څوک کولی شي ستاسو پروفایل، پوسټونه، موقعیت، عکسونه، او د اړیکو توضیحات وګوري، په بیله بیا خلک کولی شي تاسو په نښه کړي یا تاسو د دې له امله د پروفایل لټونونو کې وموموئ.

تاسو کولی شئ په خپلو ټولنیزو رسنیو حسابونو کې د امنیت ترتیبات هم ښه کړئ. تاسو کولی شئ دلته دوه فاکتور تصدیق تنظیم کړئ ، د کارونکي پروفایلونه بند کړئ ، او د خبرتیاو لپاره لاسلیک وکړئ کله چې ستاسو حساب ته د لاسرسي لپاره غیر مجاز هڅه وشي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

په ټولنيزو رسنيو کې د خوندي حساب ترتيب کول

که تاسو په ټولنيزو رسنيو کې خوندي حساب غواړئ:

- هيڅکله خپل بشپړ يا ريښتينی نوم مه کاروئ.
- کله چې تاسو راجستر کوئ د خپل اصلي آدرس څخه بل بريښناليک وکاروئ.
- يوازې هغه معلومات ورکړئ چې اړتيا وي.
- د پروفايل عکس غوره کړئ چې نه په فزيکي توګه او نه د ميټا ټاګونو له لارې ستاسو يا ستاسو موقعيت په ګوته کولو لپاره کارول کيدی شي.
- دوه فکتور تصديق تنظيم کړئ او خوندي پټنوم غوره کړئ.
- د پټنوم د بيرته ترلاسه کولو ساحو لپاره جعلي ځوابونه غوره کړئ، بيا خپل انتخابونه د پاسورډ مدير کې خوندي کړئ.
- د براوزر توسيع نصب کړئ چې د دريمې ډلې کوکيز او ټريکر غير فعالوي.

تاسو ممکن د خپلو ټولنيزو رسنيو تنظيماتو په سمه توګه درک کولو لپاره شرايطو او شرايطو يا د محرميت قواعدو ته اړتيا ولرئ، کوم چې وخت نيسي او ستونزمن کيدی شي.

هغه برخې چې تشريح کوي چې ستاسو معلومات څنګه کارول کيږي کله چې دريم اړخ ته ورکړل شي او پليټ فارم څنګه د قانون پلي کونکو غوښتنو ته عکس العمل ښيي، دا بايد په پام کې ونيول شي، خورا مهم دي.

همچنان، په ياد ولرئ چې د محرميت تنظيمات بدل کيدی شي. د تازه معلوماتو لپاره وګورئ چې دا معلومه کړئ چې ايا کوم پخوانی شخصي معلومات اوس شريک کيدی شي، مګر د کوم نوي اختيارونو لپاره هم وګورئ چې تاسو ته د محرميت ډير کنټرول درکوي.

د ټولنيزو رسنيو پليټ فارمونو او ارتباطي وسايلو امنيت او خونديتوب

موږ د ټولنيزو رسنيو ځينې پليټ فارمونه او د مخابراتو وسيلې په ګوته کوو چې په پراخه کچه په دې کټګورۍ کې په افغانستان کې کارول کيږي. زموږ د مثبتو چاراوکو په پليټ فارمونو او د مخابراتو په ګوته کوي چې د دې کچې کچه په دې کې د افغانستان په کټګورۍ کې کارولې ده. جی ميل، ياهو، ميسنجر، واټساپ، وايبر، ټيليګرام، سکايپ، زوم او سيګنال د ټولنيزو رسنيو تر ټولو مشهوره وسيلې دي. د دې سرليک لاندې، موږ په دې لارښود کې د پورتنيو مهمو ټکو له تکرار څخه ډډه کوو. مهرباني وکړئ په دې لارښود کې د ټولو فصلونو له لارې ولولئ که تاسو غواړئ لاندې لست شوي د ټولنيزو رسنيو پليټ فارمونه او د مخابراتو وسيلې په خوندي ډول وکاروئ او خپل محرميت وساتئ، ځکه چې موږ به د نورو فصلونو ډيری مهم ټکي له سره تکرار نه کړو.

د ټولنيزو رسنيو پليټ فارمونو مهم ټکي

فيسبوک(Facebook)

-دوه فکتور تصديق کول ستاسو د فيسبوک حساب خوندي کولو کې مرسته کوي. دا يو امنيتي خصوصيت دی چې ستاسو د حساب خوندي کولو او ننوتلو لپاره ډيزاين شوی. څنګه فعال کړئ: https://www.facebook.com/help/148233965247823

-تاسو کولی شئ کنټرول کړئ چې څوک په فيسبوک کې تاسو ومومي. تاسو کولی شئ د لټون انجنونه او د فيسبوک لټون کنټرول کړئ. د فعالولو څرنګوالی https://www.facebook.com/help/1718866941707011 :

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

-تاسو کولی شئ په فیسبوک کې خپل ځای بند کړئ. د فعالولو څرنګوالی :
https://www.facebook.com/help/275925085769221

-که تاسو په فیسبوک کې نور محرمیت ته اړتیا لرئ، خپل پروفایل بند کړئ. د فعالولو څرنګوالی:
https://www.facebook.com/help/196419427651178

-د پټنوم مدیر وکاروئ او پیچلي پاسورډ وکاروئ. په تصادفي ډول، خپل پټنوم بدل کړئ. هیڅکله په ډیرو ویب پاڼو کې ورته پاسورډ مه کاروئ. ګټور پاسورډ مدیران:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

خپل فیسبوک حساب ته په خوندي ډول ننوتئ که چیرې یو کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. د یاد پاسورډ انتخاب مه انتخابوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه لاګ آوټ شئ.

-د فشینګ بریدونو په لټه کې اوسئ. هیڅکله اجازه مه ورکوئ چې جعلي حسابونه تاسو د خپل حساب د ننوتلو معلوماتو په ورکولو کې تیر کړي. دوی معمولا جعلي پیغامونه لیږي چې د پټنوم بیا تنظیم کولو غوښتنه کوي.

-خپل پټنوم بدل کړئ که ستاسو حساب سره جوړجاړی شوی وي. د مرستې لینک ته لاړ شئ که تاسو نشئ کولی خپل پټنوم بدل کړئ. نور معلوماتhttps://www.facebook.com/help/203305893040179 :

-مهرباني وکړئ خپل تلیفون خلاص مه پریږدئ یا بل چا ته یې ورکړئ. د فیسبوک حسابونه په ډیری تلیفونونو کې د لاسرسي وړ دي. له همدې امله، هرڅوک چې ستاسو ګرځنده تلیفون ته لاسرسی لري کولی شي ستاسو حساب ته لاسرسی ومومي.

-د فشینګ درغلۍ او په هر ډول شکمن لینک کلیک کولو څخه ډډه وکړئ. پرځای یې، یوازې د هغې د اعتبار تصدیق کولو وروسته په لینک باندې کلیک وکړئ. نور معلومات:
https://www.facebook.com/help/166863010078512

ټویټر(Twitter)

-دوه فکتور تصدیق ستاسو د ټویټر حساب خوندي کولو کې مرسته کوي. دا ستاسو د ټویټر حساب لپاره د امنیت اضافي پرت دی. د فعالولو څرنګوالیhttps://help.twitter.com/en/managing-your-account/two-factor-authentication : مهرباني وکړئ خپل تلیفون خلاص مه پریږدئ یا بل چا ته یې ورکړئ پداسې حال کې چې تاسو دوه فاکتور تصدیق فعال کړی وي.

-د پټنوم مدیر وکاروئ. یو پیچلی پاسورډ جوړ کړئ او په مکرر ډول یې بدل کړئ. هیڅکله د څو اکاونټونو لپاره زوړ پاسورډ او ورته پاسورډ مه کاروئ. ګټور پاسورډ مدیران:

https://www.dashlane.com
https://www.stickypassword.com

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

-خپل ټویټونه اداره کړئ، که عامه وي یا شخصي. تاسو کولی شئ د خپلو ټویټونو محرمیت کنټرول کړئ.

https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public
https://help.twitter.com/en/safety-and-security/public-and-protected-tweets

-د خپل ټویټ موقعیت کنټرول کړئ او د خپل حساب هیواد موقعیت پټ کړئ.
https://help.twitter.com/en/using-twitter/tweet-location

https://help.twitter.com/en/managing-your-account/how-to-change-country-settings

-خپل ټویټر اکاونټ ته په خوندي ډول ننوتئ که چیرې داسې کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. د یاد پاسورډ اختیار انتخاب مه کوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه لاګ آوټ شئ.

-که ستاسو حساب سره جوړجاړی شوی وي، مګر تاسو بیا هم ننوتلی شئ، تاسو به وکولی شئ خپل حساب خوندي کړئ او د ناوړه چلند مخه ونیسئ. که تاسو نشئ کولی خپل حساب ته ننوځئ، د احتمالي هیک شوي حساب سره مرستې ته لاړ شئ. دا څنګه وکړو:
https://help.twitter.com/en/safety-and-security/twitter-account-compromised

-د ډیفالټ په توګه، کاروونکي کولی شي په ټویټر کې ستاسو د موندلو لپاره ستاسو بریښنالیک آدرس او د تلیفون شمیره وکاروي. سربیره پردې، د لټون انجنونه هم کولی شي ستاسو ټویټر کشف کړي. تاسو کولی شئ د بریښنالیک ، تلیفون ، او د لټون انجنونو له لارې خپل کشف کنټرول کړئ. څنګه فعال کړئ:
https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings

https://help.twitter.com/en/safety-and-security/remove-twitter-profile-from-google-search

-تاسو کولی شئ خپل ټویټونه کنټرول کړئ او ټویټر په خوندي ډول د فعالولو او غیر فعالولو له لارې وکاروئ) ټاګ کول، کشف کول، اضافه کول او ډیټا تعقیب کول، د کیفیت فلټر کول، حساس مینځپانګې پټول، حسابونه بندول او خاموش کول، ټکي خاموش کول، خپل DMs بندول او د راپور ورکولو حسابونه .(څنګه فعال او غیر فعال کړئ :
https://help.twitter.com/en/safety-and-security/control-your-twitter-experience

انسټاګرام(INSTAGRAM)

دوه فاکتور تصدیق ستاسو د انسټاګرام حساب او ستاسو رمز خوندي کولو کې مرسته کوي. دا یو امنیتي خصوصیت دی چې ستاسو د حساب امنیت لپاره اړین دی. څنګه فعال کړئ:
https://help.instagram.com/566810106808145

-د پټنوم مدیر وکاروئ. یو پیچلی پاسورډ جوړ کړئ او په تصادفي ډول یې بدل کړئ. هیڅکله د څو اکاونټونو لپاره زوړ پاسورډ او ورته پاسورډ مه کاروئ. ګټور پاسورډ مدیران:
https://www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

https://www.passwordboss.com

-کنټرول کړئ چې څوک په انسټاګرام کې تاسو تعقیبوي، څوک ستاسو د انسټاګرام عکسونه ګوري، او څوک کولی شي په دوی تبصره وکړي. سربیره پردې، تاسو کولی شئ کنټرول کړئ څوک ستاسو انسټاګرام حساب ته لاسرسی لري. څنګه فعال او غیر فعال کړئ https://help.instagram.com/116024195217477 :

-ستاسو د محرمیت ترتیبات او معلومات کنټرول کړئ. څنګه یې وکړو:
https://help.instagram.com/196883487377501

https://help.instagram.com/377830165708421/?helpref=hc_fnav

-که ستاسو حساب سره جوړجاړی شوی وي. ډیری ګامونه شتون لري چې تاسو یې کولی شئ د ویب پاڼې یا ایپ په کارولو سره د خپل حساب خوندي کولو لپاره ترسره کړئ که تاسو باور لرئ چې ستاسو حساب هیک شوی یا جوړ شوی. دا څنګه وکړو :
https://help.instagram.com/149494825257596

-تاسو کولی شئ په انسټاګرام کې کاروونکي بلاک کړئ. په انسټاګرام کې د یو فرد بلاک کولو لپاره ډیری لارې شتون لري.
https://help.instagram.com/426700567389543/?helpref=hc_fnav

-تاسو کولی شئ د سپیمونو، نامناسب پوسټونو، تبصرو، یا اشخاصو راپور ورکړئ چې د انسټاګرام ټولنې پالیسي څخه سرغړونه کوي پداسې حال کې چې تاسو د انسټاګرام د جوړ شوي راپور ورکولو ځانګړتیاو په کارولو سره دوی ته پام کوئ. دا څنګه وکړو :
https://help.instagram.com/165828726894770/?helpref=hc_fnav

تیک تاک(TikTok)

-د TikTok کارولو دمخه، تاسو کولی شئ د هغې څلور د خوندیتوب لارښوونې ولولئ، اعلانونه او ستاسو ډاټا، د هوساینې لارښود، د نوي کاروونکي لارښود، او د ساتونکي لارښود. تاسو دلته لارښود موندلی شئ https://www.tiktok.com/safety/en/ :

-دوه مرحلې تصدیق، کوم چې TikTok فعالوي، دا اړینه کوي چې هرکله چې تاسو لاګ ان شئ اضافي تایید چمتو کړئ. دا ستاسو حساب او پټنوم خوندي ساتي. دلته د دوه مرحلې تصدیق فعالولو څرنګوالی دی https://www.tiktok.com/safety/youth-portal/keep-your-account-secure?lang=en :

-د پټنوم جوړولو لپاره، د پټنوم مدیر وکاروئ. یو پیچلی پاسورډ جوړ کړئ او معمولا یې بدل کړئ (https://support.tiktok.com/en/log-in-troubleshoot/log-in/reset-password). هیڅکله د څو اکاونټونو لپاره زوړ پاسورډ او ورته پاسورډ مه کاروئ. د پټنوم مدیران، کوم چې تاسو سره مرسته کولی شي:

https://www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

-تاسو کولی شئ یو شخصي حساب ولرئ، مګر یوازې هغه کسان چې تاسو ته اجازه درکوي تاسو تعقیب کولی شي، ستاسو ویډیوګانې، ژوندۍ ویډیوګانې، بایو، خوښې، او همدارنګه ستاسو د پیروانو او پیروانو لیست وګورئ. نور کارونکي به ونه شي کولی خپل ویډیوګانې ډویټ ، سټیچ یا ډاونلوډ کړي که تاسو شخصي حساب ولرئ. دلته دا دی چې څنګه خپل حساب شخصي او یا عامه کړئ: https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/making-your-account-public-or-private

-تاسو کولی شئ محدود کړئ چې څوک کولی شي تاسو په TikTok او د لټون انجنونو لټون وکړي. د خپل پروفایل په پورتنۍ ښي کونج کې د ترتیباتو اختیار ته لاړشئ که تاسو غواړئ محدود کړئ چې څوک ستاسو د ټیک ټیک حساب ته لاسرسی کولی شي. https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/suggested-accounts

-د نور محرمیت لپاره، تاسو اړتیا لرئ خپل ځای په TikTok کې بند کړئ. دلته په TikTok کې د موقعیت خدمات بندولو څرنګوالی دی:
https://support.tiktok.com/en

-د فشینګ درغلۍ څخه ډډه وکړئ. برید کوونکي ډیری وختونه جعلي پیغامونه کاروي، چې د فشینګ په نوم هم پیژندل کیږي، ترڅو قربانیان وهڅوي چې حساس معلومات لکه پاسورډونه، د کریډیټ کارت شمیرې، ټولنیز امنیت شمیرې، او نور شخصي معلومات ښکاره کړي. بریښنالیک، ایس ایم ایس (متن پیغام)، په اپلیکیشن کې مخابرات، او د پیغام رسولو اپیسونه ټول د جعلي پیغامونو لیږلو لپاره کارول کیدی شي. تاسو دلته موندلی شئ چې څنګه د فشینګ څخه مخنیوی وکړئ:
https://support.tiktok.com/en/safety-hc/account-and-user-safety/avoid-fraudulent-message-attacks-on-tiktok

یوټیوب(YouTube)

ستاسو د یوټیوب حساب په ګډون ستاسو د ګوګل حسابونو خوندیتوب او امنیت زیاتولو لپاره دوه فاکتور تصدیق یا دوه مرحلې تصدیق وکاروئ. د دې کولو په واسطه، تاسو کولی شئ د خپل حساب امنیت پیاوړی کړئ په هغه صورت کې چې ستاسو پټنوم جوړ شوی وي. یو ځل چې فعال شو، تاسو کولی شئ د خپل تلیفون یا خپل پټنوم په کارولو سره خپل حساب ته لاسرسی ومومئ. دلته د دې کولو څرنګوالی دی: https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3Ddesktop

-په یوټیوب کې د خوندیتوب حالت تنظیم کولو په ټایپ کولو سره د یوټیوب خوندیتوب حالت فعال کړئ. دا فنکشن کولی شي د احتمالي اعتراض وړ بالغ مینځپانګې فلټر کولو کې مرسته وکړي چې تاسو یا ستاسو د وسیلو نور کارونکي ممکن د لیدو څخه ډډه وکړي. دلته د دې کولو څرنګوالی دی :
https://support.google.com/youtube/answer/174084?hl=en&co=GENIE.Platform%3Ddesktop

-د پټنوم مدیر وکاروئ او یو پیچلی پټنوم جوړ کړئ. په تصادفي توګه، خپل پټنوم بدل کړئ. هیڅکله په ډیرو ویب پاڼو کې ورته پاسورډ مه کاروئ. د پټنوم مدیران چې کولی شي تاسو سره د قوي پاسورډ په درلودلو کې مرسته وکړي:

https://www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

-خپل یوټیوب اکاونټ ته په خوندي ډول ننوتل که چیرې یو کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. د یاد پاسورډ اختیار انتخاب مه کوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه لاګ آوټ شئ.

-د یوټیوب حساب سره جوړجاړی حل کیدی شي. یوټیوب د ګوګل ملکیت دی. که تاسو ګومان کوئ چې په ګوګل کې ستاسو یوټیوب حساب ممکن هیک شوی وي، اخیستل شوی وي، یا په یو ډول سره جوړ شوی وي، ستاسو د Gmail یا ګوګل حساب بیرته ترلاسه کولو لپاره، تاسو کولی شئ د بیرته ترلاسه کولو لپاره ځینې لارښوونې تعقیب کړئ. دلته د دې بیرته ترلاسه کولو څرنګوالی دی :

https://support.google.com/youtube/answer/76187?hl=en

-یوټیوب د ګوګل ملکیت دی. تاسو کولی شئ د خپل یوټیوب حساب خوندیتوب ته وده ورکړئ ستاسو د یوټیوب سره تړل شوي ستاسو د Gmail حساب امنیت او خوندیتوب پیاوړي کولو سره .

https://support.google.com/youtube/answer/76187?hl=en#zippy=%2Crequired—step-verification-for-creators-in-the-youtube-partner-program

-خپل اکاونټ له تورو اړیکو او معلوماتو څخه خوندي کړئ. فشینګ هغه وخت دی چې یو هیکر د شخصي معلوماتو غلا کولو لپاره د باور وړ شخص په توګه وړاندې کوي. شخصي معلومات کېدای شي عبارت دي له:

- مالي معلومات
- د ټولنیز امنیت شمیره/ملي ID
- په کریډیټ کارتونو کې شمیرې
- هیکران کیدای شي بریښنالیکونه، متنونه، یا ویب پاڼي د سازمانونو، خپلوانو، یا همکارانو په توګه وښيي.

په یاد ولرئ چې ستاسو پټنوم، بریښنالیک آدرس، یا کوم بل حساب معلومات به هیڅکله د یوټیوب لخوا نه غوښتل کیږي. که چیرې یو څوک تاسو سره اړیکه ونیسي چې د یوټیوب څخه کار کوي، د هغې لپاره مه مه کوئ.

https://support.google.com/youtube/answer/9701986?hl=en&ref_topic=7071231

-که تاسو ناامنه او ناامنه احساس کوئ، خپل یوټیوب چینل پټ کړئ او یا یې رنګ کړئ تاسو د خپل چینل په بشپړ ډول رنګولو یا په لنډمهاله توګه په دې کې د ځینې مینځپانګې پټولو اختیار لرئ. په یاد ولرئ چې ستاسو د ټولنې پوسټونه، تبصرې، او ځوابونه به د تل لپاره حذف شي که تاسو د یوټیوب چینل پټ یا غیر فعال کړئ.

https://support.google.com/youtube/answer/55759?hl=en&ref_topic=7071231

-په نهایت کې، لکه څنګه چې پورته یادونه وشوه، ستاسو د یوټیوب حساب خوندي ساتل د دې یا ستاسو د چینل د هک کیدو، په واک کې اخیستلو یا موافقت کیدو خطر کموي. زده کړئ چې څنګه خپل حساب خوندي کړئ که تاسو باور لرئ چې دا تړون شوی دی. لاندې ستاسو د حساب خوندي کولو لپاره خورا مهم ګامونه دي:

- یو پیچلی پاسورډ جوړ کړئ او په یاد ولرئ.
- د هیکرانو په وړاندې خپل پټنوم خوندي کړئ.
- خپل پاسورډونه تعقیب کړئ.
- زوړ پاسورډ مه کاروئ.
- د ګڼو اکاونټونو لپاره ورته پاسورډ مه کاروئ.
- هیڅکله د خپل لاسلیک توضیحات مه ښکاره کوئ.
- د معمول امنیتي معایناتو ترسره کول.
- د حساب بیرته راګرځولو لپاره اختیارونه تازه کړئ یا اضافه کړئ

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

- د ۲ مرحلې تایید پیل کړئ.
- له خپل حساب څخه مشکوک کاروونکي لرې کړئ او غیر ضروري ویب پاڼې او پروګرامونه لرې کړئ
- خپل سافټویر تازه کړئ، او د حساب بیک اپ جوړ کړئ
- له شکمنو غوښتنو لرې اوسئ
- له شکمنو ویب پاڼو څخه لیرې اوسئ
- د فشینګ یا سپیم راپور.

د ټولنیزو رسنیو د ارتباطي وسایلو مهم ټکي

جی میل(Gmail)

-په خپل جی میل اکاونټ کې د خپل بشپړ نوم کارولو څخه ډډه وکړئ. تاسو باید خپل لومړی او وروستي نومونه په Gmail کې شخصي وساتئ. یو غلط نوم یا ستاسو د قلم نوم باید چمتو شي.

https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop

-د پټنوم مدیر وکاروئ او یو پیچلی پټنوم جوړ کړئ. په تصادفي ډول، خپل پټنوم بدل کړئ. هیڅکله په ډیرو ویب پاڼو کې ورته پاسورډ مه کاروئ. د پاسورډ مدیران چې کولی شي تاسو سره د قوي پاسورډ په درلودلو کې مرسته وکړي:

https://www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

-د ګوګل په ټولو خدماتو کې ستاسو د آنلاین محرمیت اداره کول ستاسو لومړیتوب دی. ستاسو په ګوګل حساب کې ځینې معلومات عامه یا شخصي کیدی شي. بیا تاسو کولی شئ پریکړه وکړئ چې څوک کولی شي معلوماتو ته لاسرسی ومومي لکه ستاسو د زیږون یا تلیفون شمیره په ټولو ګوګل خدماتو کې.

https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop

-دوه فکتور تصدیق کول ستاسو د جی میل او یا ګوګل حسابونو خوندي کولو کې کلیدي فاکتور دی. د خپل ګوګل حسابونو خوندي کولو لپاره دوه مرحلې تایید/ دوه فکتور تصدیق وکاروئ. د هکرانو د ساتلو لپاره خپل حساب ته د محافظت بل پرت اضافه کړئ. کله چې تاسو لاسلیک کوئ، د ۲ مرحلې تایید ستاسو د شخصي معلوماتو محرمیت، امنیت او خوندیتوب ډاډمن کولو کې مرسته کوي.

-خپل جی میل اکاونټ ته په خوندي ډول ننوتئ که چیرې داسې کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. په شخصي توګه براوز. د یاد پاسورډ اختیار انتخاب مه کوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه ننوتل. د نورو معلوماتو لپاره؟https://support.google.com/accounts/answer/2917834 :

-یو جوړ شوی Gmail حساب تنظیم کیدی شي. که ستاسو جی میل هیک شوی وي، اخیستل شوی وي، یا یو څه جوړ شوی وي، ستاسو د جی میل بیرته ترلاسه کولو لپاره تاسو کولی شئ د بیرته ترلاسه کولو لپاره ځینې لارښوونې تعقیب کړئ. دلته د دې بیرته ترلاسه کولو څرنګوالی دی :
https://support.google.com/accounts/answer/6294825?hl=en

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

-خپل جی میل حساب د فشینګ په وړاندې خوندي کړئ. فشینګ د جعلي بریښنالیکونو، پیغامونو، اعلاناتو، یا ویب پاڼو کارول دي چې مشروع ویب پاڼې نقلوي چې تاسو ډیری وختونه د شخصي معلوماتو غلا کولو یا آنلاین حسابونو ته د لاسرسي په هڅه کې لیدنه کوئ. دوی معمولا:

- د خپل مالي یا شخصي توضیحاتو په اړه پوښتنه وکړئ.
- له تاسو څخه وغواړئ چې سافټویر ډاونلوډ کړئ یا په ویب پاڼو کلیک وکړئ.
- د یو معتبر شرکت په توګه انځور کړئ، لکه ستاسو بانک، د ټولنیزو رسنیو پلیټ فارم چې تاسو یې کاروئ، یا ستاسو د کار ځای.
- د یو فرد په توګه چې تاسو یې پیژنئ، لکه یو خپلوان، آشنا یا همکاران.
- بالکل د یو پیغام په څیر چې تاسو به د یوې سرچینې څخه ترلاسه کړئ چې تاسو یې باور لرئ.
- د ګمراه کوونکو غوښتنو او پیغامونو څخه په پاکولو کې ستاسو سره د مرستې لپاره دا لارښوونې وکاروئ.
- د ګوګل خبرداریو ته پام وکړئ.
- کله چې غوښتل کیږي شخصي معلومات مه ورکوئ.
- هیڅکله د پیغام لینک کلیک کولو وروسته خپل پټنوم مه داخل کړئ.
- د هغو خبرو اترو څخه محتاط اوسئ چې عاجل ښکاري یا خورا ښه وي چې ریښتیا وي.
- مخکې له دې چې تاسو کلیک وکړئ، ودریږئ او فکر وکړئ.
- د فشینګ بریښنالیکونو موندلو لپاره، جی میل وکاروئ.
- د کروم د خوندي لټون کولو ځانګړتیا وکاروئ.
- کوم شکمن خوندي شوي پاسورډونه تایید کړئ.
- د خپل ګوګل اکاونټ پاسورډ د ۲ مرحلې تایید په ترتیبولو سره خوندي کړئ.
- که تاسو یو فشینګ بریښنالیک ترلاسه کړی نو ګوګل ته راپور واستوئ.

https://support.google.com/mail/answer/8253?hl=en

مهرباني وکړئ په یاد ولرئ چې ګوګل او یاهو خورا خوندي بریښنالیک خدمتونه نه وړاندې کوي. له دوی څخه هیڅ یو ستاسو پیغامونه له پای څخه تر پای پورې نه کوډ کوي.

یاهوو(Yahoo)

-په خپل یاهو اکاونټ کې د خپل بشپړ نوم کارولو څخه ډډه وکړئ. تاسو باید خپل لومړی او وروستي نومونه په یاهو کې شخصي وساتئ. یو غلط نوم یا د لیږلو نوم باید چمتو شي. په یاهو میل کې، د لاندې ګامونو په کارولو سره خپل د لیږلو نوم بدل کړئ:

- یاهو میل ته ننوتل.
- د ترتیباتو مینو آیکون باندې کلیک وکړئ
- میل باکسونه ټیک کړئ.
- هغه حساب غوره کړئ چې ترمیم ته اړتیا لري.
- د خپل لیږلی نوم بدلولو یا لرې کولو لپاره، "ستاسو نوم" لینک کلیک وکړئ.
- ذخیره کړئ فشار ورکړئ.

https://help.yahoo.com/kb/SLN28072.html

* د هکرانو او جعلکارانو په وړاندې ستاسو د دفاع لومړی کرښه یو قوي پاسورډ دی. دلته د قوي پاسورډ جوړولو لپاره ځینې ګټورې اشارې دي چې ستاسو معلومات خوندي ساتي. د قوي پاسورډ جوړولو لپاره:

- بې ساري کلمې وکاروئ
- یا ډیر حروف ولرئ

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

- د شخصي معلوماتو لکه ستاسو نوم، ستاسو د یاهو ID ، ستاسو د زیږون نیټه، او داسې نور په کارولو سره ښکاره مه کوئ.
- د ترتیبونو یا تکرار حروفونو څخه ډډه وکړئ.
- د هر حساب لپاره مختلف پاسورډ وکاروئ.
- پاسفریج وکاروئ
- زوړ پاسورډونه بیا مه استعمالوئ
- د خپل کمپیوټر لپاره د انټي ویروس سافټویر وکاروئ.
- خپل پټنوم په منظم ډول بدلولو سره تازه وساتئ.
- د ننوتلو لپاره yahoo.com ته وګورئ.
- محتاط اوسئ - که له تاسو څخه د خپل پټنوم بدلولو غوښتنه کیږي.
- په بریښنالیک کې د لینک کلیک کولو پر ځای د خپل براوزر په پته بار کې URL ټایپ کړئ.
- د یاهو اکاونټ کیلي وکاروئ - که تاسو د خپل پټنوم د غلا کیدو په اړه اندیښنه لرئ.

https://in.help.yahoo.com/kb/SLN3012.html

* یاهو ستاسو د محرمیت حق ته ارزښت ورکوي. تاسو کولی شئ ډیری اړخونه وګورئ او اداره کړئ چې څنګه ستاسو معلومات د یاهو محصولاتو سره د محرمیت ډشبورډ له لارې کارول کیږي.
https://in.help.yahoo.com/kb/viewing-managing-account-data-sln28671.html

* کله چې د نوي وسیلې یا براوزر څخه د ننوتلو هڅه ترسره کیږي ستاسو د پټنوم سربیره د کوډ غوښتنه کولو لپاره دوه مرحلې تایید فعال کړئ. د ۲ مرحلې تایید کارولو لپاره، تاسو باید د یاهو اکاونټ کیلي غیر فعال کړئ که تاسو دا اوس د ننوتلو لپاره کاروئ.

https://help.yahoo.com/kb/SLN5013.html

* خپل یاهو اکاونټ ته په خوندي ډول ننوتئ که چیرې داسې کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. د یاد پاسورډ اختیار انتخاب مه کوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه ننوتل. د نورو معلوماتو لپاره:
https://ph.help.yahoo.com/kb/sln5283.html?redirect=true

* تاسو فکر کوئ چې ستاسو حساب سره جوړجاړی شوی، د خوندي کولو لپاره لاندې ګامونه تعقیب کړئ.
- سمدستي، خپل پټنوم بدل کړئ.
- د اپلیکیشن پاسورډونه لرې کړئ چې تاسو یې تایید نه کړئ.
- وګورئ چې وګورئ ستاسو د بیا رغونې اختیارونه تازه دي.
- که بدل شوی وي نو خپل د بریښنالیک ترتیبات بیرته واخلئ.
- ډاډ ترلاسه کړئ چې تاسو په خپل کمپیوټر کې د انټي ویروس سافټویر نصب او تازه کړی.
- د حساب کیلي یا دوه مرحلې تصدیق وکاروئ ترڅو ډاډ ترلاسه کړئ چې ستاسو حساب اضافي امنیت لري.

https://help.yahoo.com/kb/SLN2090.html

مهرباني وکړئ په یاد ولرئ چې ګوګل او یاهو خورا خوندي بریښنالیک خدمتونه نه وړاندې کوي. له دوی څخه هیڅ یو ستاسو پیغامونه له پای څخه تر پای پورې نه کوډ کوي.

مسینجر(Messenger)

په خپل میسنجر کې له پای څخه تر پایه کوډ کول وکاروئ. په خبرو اترو کې، له پای څخه تر پای پورې کوډ کول اضافي امنیت او محافظت زیاتوي ترڅو یوازې تاسو او بل کس کولی شي هغه پیغامونه وګوري، واوري یا ولولي او هغه تلیفونونه

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

چې تاسو يې تبادله کوئ. میسنجر نور د وینش موډ ملاتړ نه کوي. د پای څخه تر پایه کوډ شوي چټ کې، کاروونکي لاهم کولی شي ورک شوي پیغامونه واستوي.

https://www.facebook.com/help/messenger-app/1084673321594605

* په میسنجر کې، تاسو کولی شئ خپل محرمیت په دې پریکړه کولو سره اداره کړئ چې څوک ستاسو فعال حالت لیدلی شي، ستاسو د کیسې لپاره لیدونکي غوره کړئ، د پټو خبرو اترو په کارولو سره، او نور. دلته ستاسو د میسنجر محرمیت اداره کولو څرنګوالی دی.

https://www.facebook.com/help/messenger-app/408883583307426?helpref=faq_content

* تاسو کولی شئ کنټرول کړئ چې څوک ستاسو د خبرو لیست ته راسي. تاسو به د پیغام غوښتنه ترلاسه کړئ که چیرې یو څوک تاسو ته په فیسبوک کې پیغام واستوي، مګر تاسو ورسره تړلي نه یاست. په یاد ولرئ چې د پیغام غوښتنې ته ځواب ویل ستاسو او لیږونکي ترمینځ اړیکه رامینځته کوي او هر هغه مینځپانګه رامینځته کوي چې تاسو یې لیږلي وي. ومومئ چې څنګه محدود کړئ چې په میسنجر کې څوک کولی شي ستاسو سره نوې خبرې پیل کړي.

https://www.facebook.com/help/936247526442073?helpref=related&source_cms_id=907368596013605

https://www.facebook.com/help/messenger-app/2258699540867663?helpref=faq_content

* که داسې کسان وي چې تاسو یې نه غواړئ واورئ، بند کړئ، پټ کړئ، یا خاموش کړئ. تاسو کولی شئ د ټولو خبرو اترو لپاره د میسنجر خبرتیاوې کنټرول کړئ. په میسنجر کې د اشخاصو د خاموش کولو، سترګې پټولو یا بلاک کولو څرنګوالی ومومئ.

https://www.facebook.com/help/messenger-app/204908296312159?helpref=faq_content

https://www.facebook.com/help/messenger-app/1245152242249842?helpref=faq_content

https://www.facebook.com/help/messenger-app/330627630326605?helpref=faq_content

* د ځواب ویلو څخه ډډه وکړئ او میسنجر ته د درغلی راپور ورکړئ که تاسو داسې څه ولیدل چې تاسو فکر کوئ چې درغلي وي.

https://www.facebook.com/help/messenger-app/833709093422928?helpref=faq_content

* په خپل سمارټ فون کې، تاسو کولی شئ اپلیکیشن بند کړئ. تاسو کولی شئ د خپل Android یا iOS وسیلې لپاره د میسنجر ایپ لاک فیچر فعال کړئ ترڅو ستاسو میسنجر حساب اضافي امنیت او محرمیت چمتو کړي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

https://www.facebook.com/help/messenger-app/2585155295072006?locale=en_US&helpref=faq_content

* د لا زیاتو امنیت او د میسنجر خوندیتوب لپاره مهرباني وکړئ لیدنه وکړئ
https://www.facebook.com/help/messenger-app/1064701417063145/?helpref=hc_fnav

یادونه: تاسو کولی شئ د خپل فیسبوک حساب په کارولو سره میسنجر ته لاسرسی ومومئ ځکه چې دا له فیسبوک سره تړلی دی. میسنجر او فیسبوک دواړه د میټا ملکیت دی. مهرباني وکړئ د خپل میسنجر د امنیت او خوندیتوب په اړه د نورو معلوماتو لپاره د فیسبوک توضیحاتو ته مراجعه وکړئ.

واتساپ(WhatsApp)

* هیځکله خپل د WhatsApp تایید کوډ هیچا ته مه ورکوئ. ستاسو د تلیفون شمیرې ته صادر شوی د SMS تایید کوډ اړین دی چې ستاسو حساب کنټرول کړي که چیرې څوک د دې کولو هڅه وکړي. د دې کوډ پرته، هر څوک چې هڅه کوي ستاسو د تلیفون شمیره تصدیق کړي نو نشي کولی دا کار وکړي او په WhatsApp کې ستاسو شمیره وکاروي. دا پدې معنی ده چې ستاسو د WhatsApp حساب لاهم ستاسو په کنټرول کې دی https://faq.whatsapp.com/619670298808780/?locale=en_US .

* دوه مرحلي تایید فعال کړئ او خپل بریښنالیک آدرس دننه کړئ نو تاسو ممکن یادونه ترلاسه کړئ که تاسو خپل PIN له لاسه ورکړی.

https://faq.whatsapp.com/585667085685460/?locale=en_US

* تاسو کولای شئ د وسیلي کوډ ترتیب کړئ. دا اړینه نده چې خپل تلیفون وصل وساتئ تر څو په یو وخت کې تر څلورو پورې وصل شوي وسیلو کې WhatsApp وکاروئ. په WhatsApp کې، په یو وخت کې یو تلیفون وصل کیدی شي.
https://faq.whatsapp.com/381777293328336/?locale=en_US
* WhatsApp د ټولو هغو پیغامونو لپاره چې تاسو یې لیږئ او ترلاسه کوئ د پای څخه تر پای پورې کوډ کول وړاندیز کوي ترڅو ډاډ ترلاسه کړي چې یوازې تاسو او هغه څوک چې تاسو ورسره خبرې کوئ ستاسو شخصي پیغامونه لوستل یا اوریدلی شئ. دلته د فعالولو څرنګوالی دی:
https://faq.whatsapp.com/629089898272226/?locale=en_US

* لاندې لست شوي ګامونه کولی شي تاسو سره ستاسو د WhatsApp حساب ته د لاسرسي بیرته ترلاسه کولو کې مرسته وکړي که تاسو د خپل WhatsApp کوډ افشا کولو کې دوکه شوي یاست او دې ته لاسرسی له لاسه ورکړی.

https://faq.whatsapp.com/690494414810591/?locale=en_US

* تاسو کولی شئ په WhatsApp کې چیټونه پټ کړئ که تاسو اړتیا لرئ. تاسو کولی شئ د آرشیف چیټ فیچر په کارولو سره ستاسو د چیټ لیست څخه د ځانګړي انفرادي یا ډله ایز چټ پټولو سره خپلې خبرې په ښه توګه تنظیم کړئ.

https://faq.whatsapp.com/154568698849853/?helpref=search&query=hide%20chats&search_session_id=a71f37c78ad24eb384f8975249d20c9f&sr=8

* په WhatsApp کې ستاسو د چیټونو د خوندیتوب او خوندیتوب په اړه د نورو جزیاتو لپاره مهرباني وکړئ لیدنه وکړئ :
https://faq.whatsapp.com

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

وایبر(Viber)

* وایبر د ډیفالټ له مخې له پای څخه تر پای پورې کوډ کولو ځانګړتیاوې لري. ستاسو وسیله د ترلاسه کونکي وسیلې ته د کوډ شوي کوډ په توګه پیغامونه لیږي چې یوازې هغه وسیله کولی شي د کوډ کولو کیلي په کارولو سره د ساده متن په توګه څرګندولو لپاره ډیکریپټ کړي. یوازې د کارونکي وسیلو کې او بل چیرې د کوډ کولو کیلي شتون نلري. له همدې امله، هیڅوک نشي کولی ستاسو پیغامونه وګوري، نه حتی وایبر.

https://www.viber.com/en/security/

* وایبر د ورکیدو پیغامونو فیچر فعال کړی دی. په خپل چیټ کې د هر پیغام لپاره د ځان ویجاړولو ټایمر ترتیب کړئ ترڅو داډ ترلاسه کړئ چې دا په اوتومات ډول د وایبر چیټ څخه پاک شوی کله چې د ټولو ښکیلو خواو لخوا لوستل شي. هغه کړنې چې سکرین شاټونه پکې شامل وي په خبرو اترو کې به راپور شي پداسې حال کې چې دا فعال وي.

https://www.viber.com/en/security/

* د ټولو پیغامونو ترمیم او رنګول ممکن دي. دا د یو پیغام لیږلو لپاره مایوسه کیدی شي چې ټایپ پکې وي، مګر اندیښنه مه کوئ - یوازې د سمدستي سمولو لپاره پیغام اوږده کړئ. که تاسو اوس هم غواړئ، حتی که دا دمخه لیدل شوی وي، هغه پیغام پاک کړئ چې په خبرو اترو کې ټولو ته لیږل شوی. هغه څه چې تاسو یې ښکاره کوئ ستاسو پورې اړه لري.

https://www.viber.com/en/security/

* په وایبر کې، تاسو کولی شئ د پټ شمیرې چټ وکاروئ. کله چې تاسو په یوه ګروپ کې له نویو اشخاصو سره وینئ نو سمدلاسه خوندي خبرې پیل کړئ یا دوی د نوم لټون له لارې په وایبر کې ومومئ پرته لدې چې ستاسو یا د دوی تلیفون شمیرې ښکاره یا تبادله کړئ.

https://www.viber.com/en/security/

* تاسو کولی شئ په وایبر کې د پټو چیټونو څخه په اغیزمنه توګه کار واخلئ. تاسو نه غواړئ چې څوک په غیر ارادي ډول ستاسو چیټ واوري او یا په قصدي ډول ستاسو تلیفون چیک کړي. چیټونه ستاسو د چیټ لیست څخه پټ کیدی شي او هر وخت د PIN په کارولو سره لاسرسی کیدی شي. تاسو هغه څوک یاست چې کولی شئ PIN ترتیب کړئ.

https://www.viber.com/en/security/

* که تاسو یو سپیمر ګورئ، تاسو اختیار لرئ چې هر هغه څوک چې تاسو فکر کوئ سپیمر یا درغلي کوونکی وي بلاک او راپور ورکړئ. د آټو سپیم چیک فعال کړئ ترڅو وائبر فعال کړي ترڅو د هغو اړیکو څخه ترلاسه شوي ناوړه مینځپانګې لپاره پیغامونه وګوري چې ستاسو د اړیکو لیست کې ندي.
https://help.viber.com/en/article/protect-yourself-and-your-privacy-on-viber

* خپل د وایبر حساب غیر فعال کړئ که تاسو غواړئ ستاسو ټول معلومات چې د بل چا په وسیله خوندي شوي وي لرې کړئ. تاسو به سمدلاسه حذف شوي ټولې خبرې اترې ومومئ چې تاسو له هرچا سره ستاسو د وسیلې او د دوی دواړو څخه لرئ.

https://help.viber.com/en/article/deactivate-or-uninstall-viber-on-your-phone

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

ټيليګرام(Telegram)

*تاسو کولای شئ خپل تليفون شميره په ټيليګرام کې پټ کړئ. تاسو کولی شئ پرته له دې چې خپل تليفون شميره ښکاره کړئ په ټيليګرام کې په ګروپونو او شخصي چيټونو کې پيغامونه واستوئ. په ډيفالټ کې، يوازې هغه اړيکې چې تاسو يې په خپل پته کتاب کې اضافه کړي دي څکه چې اړيکې کولی شي ستاسو د تليفون شميره وګوري. په هرصورت، تاسو کولی شئ دا پټ کړئ.
https://telegram.org/faq

*په ټيليګرام کې، تاسو کولای شئ پټې خبرې وکړئ. د هغه کارن پروفايل چې تاسو غواړئ اړيکه ونيسئ بايد خلاص شي. "..." کليک وکړئ او بيا "پټ چټ پيل کړئ." په ياد ولرئ چې د ټيليګرام شخصي چيټونه د وسيلې لپاره ځانګړي دي. ستاسو په يوه وسيله کې، که تاسو او يو ملګري شخصي خبرې پيل کړئ، يوازې دا وسيله به ورته لاسرسی ولري. يوځل چې تاسو چيک آؤټ کړئ ستاسو ټولې شخصي چيټونه به ورک شي. تاسو کولی شئ د ورته تماس سره ډيری مختلف شخصي چيټونه وکړئ لکه څنګه چې تاسو غواړئ.
https://telegram.org/faq#q-how-are-secret-chats-different

* تاسو کولای شئ په ټيليګرام کې له پای څخه تر پايه کوډ کولو څخه خوند واخلئ. برخه اخيستونکي وسايل د کوډ کولو کيلي تبادله کولو لپاره د Diffie-Hellman کيلي تبادله کاروي کله چې پټ چيټ رامينځته کيږي.
د خوندي پای څخه تر پای پورې اړيکې رامينځته کولو وروسته، موږ يو ګرافيک رامينځته کوو چې ستاسو د خبرو لپاره د کوډ کولو کيلي نمايندګي کوي.
کله چې تاسو دا انځور د خپل ملګري سره پرتله کړئ، که چيرې دوه عکسونه يو شان وي، تاسو ممکن ډاډه اوسئ چې پټې خبرې اترې خوندي دي او دا چې يو سړی په منځ کې بريد نشي بريالی کيدی.
https://telegram.org/faq#q-how-do-i-start-a-secret-chat

* ټيليګرام دوه مرحلې تاييد لري، او تاسو کولی شئ دا فعال کړئ. که څه هم د ننوتلو لپاره د ايس ايم ايس کوډ کارول د پيغام رسولو صنعت معيار دی، که تاسو نور محافظت غواړئ يا د خپل ګرځنده کيرير يا حکومت په اړه د شکمن کيدو دليل لرئ، تاسو کولی شئ خپل کلاوډ چيټونه د اضافي پاسورډ سره خوندي کړئ.
https://telegram.org/faq#q-how-does-2-step-verification-work

* هرڅوک کولی شي تاسو په ټيليګرام کې وومومي او ستاسو پروفايل او عکسونه وګوري. هرڅوک چې د ډلې غړی وي کولی شي ستاسو نوم د غړو په ليست کې وګوري. تاسو کولی شئ د هر چا څخه پيغامونه ترلاسه کړئ.
https://telegram.org/faq#q-do-you-have-a-privacy-policy

سکايپ(Skype)

*د پټنوم مدير وکاروئ او يو پيچلی رمز جوړ کړئ. په تصادفي توګه، خپل پټنوم بدل کړئ، هيڅکله زوړ پټنوم مه کاروئ. د پټنوم مديران چې کولی شي تاسو سره د قوي پاسورډ په درلودلو کې مرسته وکړي:
https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

* تاسو کولای شئ په سکايپ کې له پای څخه تر پايه کوډ کول وکاروئ. غږ، ويډيو، د فايل ليږد، او د سکايپ څخه تر سکايپ کاروونکو ترمنځ فوري پيغامونه ټول کوډ شوي دي. دا تاسو د ناوړه اشخاصو لخوا د تصور وړ اوريدلو څخه ساتي. ستاسو د زنګ برخه چې د PSTN (د تليفون دوديز شبکه) څخه تيريږي کله چې تاسو د سکايپ څخه ګرځنده او لينډين تليفونونو ته زنګ وهئ کوډ شوی نه وي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

https://support.skype.com/en/faq/FA31/does-skype-use-encryption

* سکایپ د مایکروسافټ ملکیت دی. د مایکروسافټ دوه مرحلې تایید امنیت خصوصیت ستاسو د سکایپ حساب خوندي ساتلو لپاره کار کوي ترڅو د غیر مجاز کاروونکو لپاره ستاسو مایکروسافټ حساب ته لاسرسی سخت کړي. دلته د دې فعالولو څرنګوالی دی:
https://answers.microsoft.com/en-us/skype/forum/all/skype-login-two-factor-authentication/303d1b3b-8827-49b4-bdaa-ea7f823d971c

* ستاسو حساب سره جوړجاړی شوی او یا هیک شوی، مهرباني وکړئ لیدنه وکړئ څنګه د مایکروسافټ هیک شوي یا جوړ شوي حساب بیرته ترلاسه کړئ.
https://support.microsoft.com/en-us/account-billing/how-to-recover-a-hacked-or-compromised-microsoft-account-24ca907d-bcdf-a44b-4656-47f0cd89c245
* خلک کولی شي ستاسو سره د نښلولو لپاره ستاسو د تلیفون شمیره په کارولو سره ستاسو لټون وکړي او خبرې پیل کړي که تاسو د تلیفون شمیره کاروئ ترڅو د ننوتلو یا سکایپ ته ننوځئ یا که تاسو په خپل پروفایل کې لیست شوي یاست. که تاسو د خپل تلیفون شمیره د لټون وړ نه کول غوره کړئ، تاسو کولی شئ دا په هر وخت کې ترسره کړئ.
https://support.skype.com/en/faq/FA34934/can-people-find-me-with-my-phone-number-in-skype

*تاسو کنټرول لرئ چې څوک کولی شي ستاسو د سکایپ پروفایل توضیحاتو او شتون حالت ته لاسرسی ومومي. ځینې معلومات عامه دي، مګر که تاسو نه غواړئ چې دا ستاسو په پروفایل کې ښکاره شي، تاسو کولی شئ خالي پریږدئ.
ستاسو بریښنالیک آدرس په سکایپ کې نه ښودل کیږي. هیڅوک نشي کولی دا وګوري کله چې ستاسو پروفایل وګورئ.
ستاسو د بریښنالیک آدرس د ملګرو پرته د بل چا لخوا د موندلو لپاره نشي کارول کیدی چې دمخه یې پیژني.
https://support.skype.com/en/faq/FA34745/who-can-see-my-skype-profile-and-presence-status

*خپل سکایپ اکاونټ ته په خوندي ډول ننوتل که داسې یو کمپیوټر کاروئ چې ستاسو نه وي. تاسو کولی شئ د انټرنیټ د ډیرو شخصي کارولو لپاره مجازی خصوصي شبکه (VPN) وکاروئ. لومړی، د براوزر امنیت تایید کړئ. د یاد پاسورډ اختیار انتخاب مه کوئ. یوځل چې تاسو پای ته ورسیږئ، د حساب څخه ننوتل.

سیګنال(Signal)

د ډیفالټ له مخې له پای څخه تر پای پورې کوډ کول ځانګړتیاوې لري. سیګنال هیڅکله د شخصي معلوماتو راټولولو یا ذخیره کولو لپاره جوړ شوی. د سیګنال زنګونه او مخابرات تل له پای څخه تر پای پورې کوډ شوي، شخصي او خوندي وي، نو نه سیګنال او نه کوم بل دریم اړخ ورته لاسرسی کولی شي.

https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private-

* د پاکو اړیکو تاریخ ساتلو لپاره، ورک شوي پیغامونه وکاروئ. یوځل چې شمیرنه پای ته ورسیږي ، پیغام به ستاسو له وسیلو څخه لرې شي. دا د هغو قضیو لپاره ندي چیرې چې ستاسو اړیکه ستاسو مخالف وي؛ په هرصورت، یو څوک چې ورک شوی پیغام ترلاسه کوي ممکن تل د پیغام ورکیدو دمخه د سکرین عکس اخیستلو لپاره بله کیمره وکاروي که چیرې دوی واقعیا د دې ریکارډ غواړي. دلته د دې کولو څرنګوالی دی:
https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

* په سیګنال کې د ټولو پیغامونو ترمیم او ړنګول ممکن دي. که تاسو لاهم غواړئ هغه پیغام له مینځه ویسي چې په خبرو اترو کې هرچا ته لیږل شوی و، تاسو کولی شئ دا ترسره کړئ حتی که لیدل کیږي. دلته د دې کولو څرنګوالی دی:
https://support.signal.org/hc/en-us/articles/360007320491-Delete-messages-alerts-or-chats

* په سیګنال کې د لاک سکرین تنظیم کړئ. د سیګنال د سکرین لاک خصوصیت ستاسو په تلیفون کې د پن ، پاسفریج یا بایومیټریک تصدیق کاروي) د مثال په توګه ، د ګوتو نښه ، TouchID، یا .(FaceID دلته د دې فعالولو څرنګوالی دی:
https://support.signal.org/hc/en-us/articles/360007059572-Screen-Lock

* سیګنال PIN یو کوډ دی چې د ځانګړتیاوو لکه پیژندونکي ملاتړ کوي چې د تلیفون شمیرو پراساس ندي. دا پدې مانا ده چې که تاسو کله هم وسایل له لاسه ورکړئ یا بدل کړئ، ستاسو PIN ستاسو د پروفایل، ترتیباتو، اړیکو، او بلاک شوي کاروونکو بیرته ترلاسه کولو کې مرسته کولی شي. د راجسټریشن یو اختیاري قفل چې PIN کاروي کولی شي بل څوک ستاسو په استازیتوب ستاسو د شمیرې ثبتولو مخه ونیسي. د نورو معلوماتو او د PIN بدلون لپاره، لیدنه وکړئ:
https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN

* سیګنال ستاسو په ګرځنده وسیله کې موجود کیبورډ یا د ان پټ میتود ایډیټر (IME) چلوي. تاسو کولی شئ پټ کیبورډ فعال کړئ ترڅو ستاسو د مجازی کیبورډ سافټویر ستاسو د ټایپینګ نمونو نظارت کولو مخه ونیسي او د دې معلوماتو کارولو لپاره د دې خدمت ګټلو لپاره که تاسو اندیښنه لرئ. دلته د دې فعالولو څرنګوالی دی:
https://support.signal.org/hc/en-us/articles/360055276112-Incognito-Keyboard

* تاسو کولی شئ د سیګنال په کارولو سره په عکسونو کې مخونه تور کړئ. ستاسو د محرمیت ساتلو لپاره ټول پروسس په محلي توګه ستاسو په خپل وسیله ترسره کیږي. د دې ترلاسه کولو لپاره ، "د مخونو تور" ته لاړشئ او مخونه به په اوتومات ډول کشف او پټ شي.

د بیان د آزادئ په اړه د حکومت قانون چې د ډیجیټل حقونه اغیزمن کوي.

د ۲۰۲۱ کال د سپټمبر په ۱۹مه طالبانو د خبري سازمانونو او خبریالانو لپاره د ۱۱ مقرراتو یو لست خپور کړ. له دې مقرراتو څخه نهه د رسنیو او فعالینو په فعالیت اغیزه لري. د دې مقرراتو له مخې، دا د قانون خلاف دی چې د لاندې څخه کوم یو خپور یا پوسټ کړئ:
* د اسلام سره په ټکر کې د موضوعاتو خپرول.
* په رسنیو کې د ملي شخصیتونو سپکاوی.
* ملیت او د هر چا شخصي محرمیت ته سپکاوی.
* د رسنیو او خبریالانو لخوا د خبرونو محتوا تحریف کول.
* په خپله لیکنه کې د ژورنالیزم اصولو ته درناوی نه کوي.
* په خپرونو کې توازن نه ساتل.
* د هغو موضوعاتو په خپرولو کې محتاط نه وي چې اعتبار یې نه وي معلوم او د نورو لخوا تایید شوی نه وي.
* د داسې موضوعاتو په خپرولو کې محتاط نه وي چې د خلکو په افکارو منفي اغیزه وکړي یا د خلکو روحیه خرابه کړي.
رسنۍ دې د خبرونو په خپرولو کې خپله بې طرفي نه ساتي او هر څه چې ریښتیا وي خپاره نه کړي. * GMICهڅه کوي د رسنیو او خبریالانو سره همکاري وکړي او د رسنیو راپورونه چمتو کړي او د دوی اړوند ځانګړي چمتو کولو سره په همغږۍ کې راپور ورکړي.

دوی د نظریاتو او طرزالعملونو پر بنسټ یو تنظیمي چوکاټ رامینځته کړی چې د مسلک په توګه د ژورنالیزم سره مطابقت نلري. لومړی درې مقررات، چې ژورنالیستان د هغه موادو له خپرولو منع کوي چې "د اسلام خلاف وي"، "ملي شخصیتونو ته سپکاوی کوي،" یا "د محرمیت څخه سرغړونه کوي"، د افغانستان د پخوانیو موجودو ملي رسنیو قانون پراساس دي، چې

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

یو شرط هم پکې شامل دی. د نړیوالو معیارونو، لکه د مدني او سیاسي حقونو نړیوال میثاق، او د بشري حقونو د نړیوالې اعلامیې د ۱۹ مادې مراعات کول.

په نویو مقرراتو کې د دې مکلفیت نشتوالی د سانسور او جبر لپاره ځای پریږدي ځکه چې دا څرګنده نده چې څوک پریکړه کوي - یا په کوم اساس - چې یوه تبصره یا کیسه د اسلام یا عامه شخصیت سپکاوی کوي .

درې واړه مقررات ژورنالستان ته لارښوونه کوي چې هغه څه تعقیب کړي چې اخلاقي معیارونه ګڼل کیږي. دوی باید "ژورنالیستي ارزښتونه تعقیب کړي،" "د خبر د موادو د بدلولو هڅه ونه کړي،" او "دا ډاډ ترلاسه کړي چې د دوی راپور ورکول متوازن دي." په هرصورت، دا لارښووني ممکن د منلو وړ نړیوالو نورمونو ته د حوالې د نشتوالي له امله په بالقوه توګه ناوړه ګټه پورته کړي یا په خپل سري ډول تشریح شي.

د مقرراتو په چوکاټ کې 7 او 8 مادې د خبرونو محدودیت یا کنټرول بیا ځای پرځای کول اسانه کوي چې په تیرو 20 کلونو کې په افغانستان کې شتون نلري. د دوی د مقرراتو له مخې، "هغه شیان چې د خپرولو په وخت کې د چارواکو لخوا تایید شوي نه وي باید په احتیاط سره چلند وشي،" او "هغه مسایل چې د خلکو په روحیه ناوړه اغیزه کولی شي یا مورال اغیزمن کړي باید د نشر یا خپریدو په وخت کې په دقت سره اداره شي ".

وروستي دوه مقررات (10 او 11) په ګوته کوي چې" GMIC یو ځانګړی چوکاټ ډیزاین کړی ترڅو د رسنیو سازمانونو او ژورنالیستانو لپاره دا اسانه کړي چې خپل راپورونه د مقرراتو سره سم چمتو کړي" او دا چې پرمخ ځي، رسنی باید "د GMICسره په همغږۍ کې مفصل راپورونه چمتو کړي،" کوم چې د خبر کنټرول یا مخکیني سانسور ته د بیرته راستنیدو خطر زیاتوي. موږ لاهم نه پوهیږو چې دا "تفصیلی راپورونه" څه دي.

نهم قاعده، کوم چې دا امر کوي چې رسنی "په هغه څه کې چې دوی یې خپروي د بې پرېتوب مفهوم ته غاړه کیږدي" او "یوازې حقیقت راپور ورکوي" په مختلفو لارو تعبیر کیدی شي او ژورنالیستان د خپل سري غچ اخیستنې سره مخ کوي.

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

حوالي (سرچيني)

کتابونه

* Chuck Easttom, 2019, Computer Security Fundamentals, Third Edition,
* Michael Bazzell, 2018, Personal Digital Security, New Version
* Carla Mooney, 2015, Online Privacy An Social Media
* Melody Karle, 2020, A Social Media Survival Guide
* S.M. Iacus G. Porro, 2021, Subjective Well-Being and Social Media
* Kevin Mitnick and Robert Vamosi, 2017, The Art of Invisibility
* Christopher J. Hadnagy, 2018, Social Engineering: The Science of Human Hacking

ويب سايټونه

https://www.accessnow.org
https://rsf.org/en/
https://www.mei.edu/
https://www.techtarget.com
https://www.politico.com
https://basecreative.co.uk
https://www.ssl.com
https://www.ssl.com
https://freedomhouse.org/
https://www.cyberghostvpn.com/
https://www.kaspersky.com/
https://www.tunnelbear.com/download
https://www.vpngate.net
https://protonvpn.com
https://mullvad.net/en/download/
https://bitmask.net
https://cryptpad.fr/drive
https://ufile.io
https://send.tresorit.com
https://send.tresorit.com
https://veracrypt.fr/en/Home.html
https://www.dropbox.com
https://www.techtarget.com
https://www.expressvpn.com
https://www.vpn-mentors.com
https://www.cloudflare.com
https://www.microsoft.com
https://www.antivirussoftwareguide.com
https:/www.dashlane.com/

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.

https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com
https://whatismyipaddress.com
https://www.tripwire.com
https://www.malwarebytes.com
https://knowledge-base.secureflag.com
https://owasp.org
https://www.ibm.com
https://securityboulevard.com
https://www.techadvisor.com
https://www.hypr.com
https://www.businessinsider.com
https://duckduckgo.com
https://metager.org
https://www.startpage.com
https://account.proton.me/login
https://www.fastmail.com
https://www.zoho.com/mail
https://account.riseup.net
https://en.exp.activix.ca/users/sign_in
https://www.facebook.com
https://help.twitter.com
https://help.instagram.com https://www.tiktok.com/safety
https://support.google.com
https://help.yahoo.com
https://faq.whatsapp.com
https://www.viber.com
https://telegram.org/faq
https://support.skype.com
https://support.signal.org

Copyright © 2022 Afghanistan Democracy Development Organization. All rights reserved.