اړیکو لارښود

د افغانستان د مدني ټولنې لپاره

2024

RIGHT TO CONNECT
RTC

د اړیکو لارښود

د افغانستان د مدني ټولنې لپاره

د دې لارښود د پراختیا لپاره، RTC په افغانستان او جلاوطنۍ کې د افغانستان د CSO له بېلابېلو استازو، HRDs، او خبریالانو سره مرکې وکړې. موږ دا لارښود د هغو ګڼو ننګونو په ځواب کې جوړ کړی چې د افغانستان د بشری حقونو د سازمانونو، بشری حقونو او خبریالانو په مسلکی چاپېریال او جلاوطنۍ کې ورسره مخ دی. RTC د کوم تخنیکی لارښود مسؤلیت په غاړه نه اخلی چې دلته چمتو شوی. دا لارښوونې ګټورې دی که تاسو په افغانستان کې کار کوئ. د دې لارښوونو سره ، تاسو ښه موقعیت لرئ ترڅو وضعیت په دقیق ډول پوه شئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د مسؤلیت رد کول

دلته څرګند شوي نظرونه د لیکوال نظرونه دي او حتمي نه ده چې د RTC او زموږ د بسپنه ورکوونکیو نظر دې منعکس کړي. سره له دې چې د دې رسالې معنوي حق له RTC سره خوندي دی، افراد او موسسې کولای شي یوازې د غیر تجاري، زده کړو یا علمي موخو لپاره، د اصلي سرچینې له تایید او نوم ذکر کولو وروسته، د دې رسالې له منځپانګې ګټه پورته کړي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د محتویاتو جدول

مخففات............ 1

لومړۍ برخه: د نادولتي موسسو اړیکې............ 2

د نادولتي موسسو اړیکې څه شی دي؟............ 3

د نادولتي موسسو د اړیکو برخې............ 3
۱. کورنۍ اړیکې:............ 3
۲. بهرنۍ اړیکې:............ 4
۳. د کمپاینونو او عدالت غوښتنې اړیکې:............ 4
۴. د کړکیچ او بیړنیو حالاتو اړیکې:............ 4
۵. د ذینفع بنسټونو ګډون:............ 4
۶. ډیجیټل اړیکې:............ 4
۷. روڼتیا او ګذارش ورکونه:............ 5
په افغانستان کې د انلاین اړیکو د رامنځ ته کولو پر مهال د نادولتي موسسو اصلي او اساسي ننګونې کومې دي؟............ 5
۱. د رسنیو کنټرول او سانسور:............ 5
۲. د ډیجیټلی اړیکو او انټرنیت محدودیتونه:............ 5
۳. امنیت او محرم والی:............ 6
۴. د عامه ګډون محدودیت:............ 6
۵. د نظریاتو د وړاندې کولو څخه د ناسم برداشت خطر:............ 6
۶. د ذینعفو بنسټونو ګډون:............ 6

څه ډول کولای شو په افغانستان کې د اړیکو ننګونو ته ځواب ووایو؟............ 6

له ننګونو سره څه دول چلند غوره کول (۱) د رسنیو سانسور او کنترول (۲) د ډیجیټل اړیکو او انټرنیټ محدودیتونه او (۳) د امنیت او محرم والی:...... 6

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

لومړۍ لاره - د خصوصي مجازي شبکو نه ګټه پورته کول (VPN): 6
دویمه لاره - د اړیکو اپلیکشنونو په برخه کې له کوډ شویو هغو او د ایمیل له خوندي خدمتونو ګټه واخلئ: 8
درېیمه لاره - ځان مه ځلوئ او له عامه پام څخه لرې اووسئ: 8
څلورمه لاره - له فرهنګي حساسیتونو ډډه وکړئ: 8
پنځمه لاره. د سایبري امنیت په برخه کې کارکوونکیو ته منظمه روزنه: 9
شپږمه لاره. د ډیجیټل امنیت تازه او اپډیټ لارې چارې وڅارئ او وڅېړئ: 9
اوومه لاره. د انټرنیټي خطرونو ځواب ته یوه بېړنۍ طرحه چمتو کړئ: 9
اتمه لاره. حساسه ډیټا کوډ او ذخیره کړئ: 9
نهمه لاره. په دفتر کې موجود د اړیکو اسناد او مدارک: 9
لسمه لاره. د قوي پاسورډونو او کوډنو رامنځته کولو پالیسۍ اړتیا: 9
یوولسمه لاره - له 2FA څخه ګټه پورته کړئ: 11
دولسمه لاره - د غیر متوقع پېښو لپاره د غبرګون پلان رامنځ ته کول: 11
دولسمه لاره - له TOR ګټه پورته کول: 11
۲ . د عامه ګډون د محدودیت موضوع ته څه ډول ځواب ووایو؟ 13
۳ . د خپرونو او نظرونو څرګندولو د ناسم برداشت له خطر سره څنګه مقابله وکړو؟ 15
لومړۍ لاره - د حساسیتونو په برخه کې پوهه او ګاهي: 15
دویمه لاره - له رسمي ژبو دقیقه ګټه اخیستنه: 15
درېیمه لار - له دیني مشرانو (ملا امامانو) سره تعامل: 16
څلورمه لار - په سیمه ییزو جوړښتونو کې د نړېوالو بشري حقونو دود او رواجول: 16
پنځمه لاره - سیمه ییزه خبررسونه 16
شپږمه لاره - د ځانګړي او عمومي اړیکو تر منځ توپیر: 16
اوومه لاره - منظمه څارنه: 16
اتمه لاره - د ټولنیزو رسنیو کنترول: 16
۴. څنګه کولای شو په افغانستان کې د ګټه اخیستونو د ګډون پر وړاندې ننګونو سره، سم چلند غوره کړو؟ 17
لومړۍ لاره - د خوندي اړیکو لپاره له ټکنالوژۍ ګټه پورته کول: 17
دویمه لاره - له مولټي میډیا څخه په احتیاط ګټه پورته کول: 17
درېیمه لار - له مجازي نړۍ څخه تعامل: 17
څلورمه لار - نړېوالې شبکې او له هغوی سره ګډون: 17

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

پنځمه لار - له افغانستانه بهر د منځګړي ګمارل:... 17

د نادولتي موسسولپاره د اړيکو خوندي وسيلې کومې دي؟ 18

نادولتي موسسو ته د اړيکو تر ټولو خوندي وسيلي کومې دي؟ 20

٩ م شکل: نادولتي موسسو ته د ايميل د خدمتونو تر ټولو خوندي وراندي کوونکي... 21

امن ترین ابزارهای کنفرانس تصویری برای موسسات غیردولتی کدام ها اند؟ 22

موسسات غیردولتی هنگام برقراری ارتباطات از چه اصطلاحاتی باید اجتناب کنند؟ 24

١ . ګټې 26
لومړی ګټه ـ تعامل او لاسرسی: 26
دويمه ګټه ـ عدالت غوښتنه او شبکه جوړول:.. 26
درېيمه ګټه - مستقيمې اړيکې:.. 27
څلورمه ګټه - د مالي مرستو راجلبول: 27
پنځمه ګټه - د مطالبو خپرول: 27
شپږمه ګټه ـ د اړيکو او پوهاوي کچه پراخول:... 27
٢ . زيانونه 28
لومړی زيان - امنيتي خطرونه: 28
دويم زيان - څارنه او سانسور: 28
درېيم زيان - غلط او نيمګړي معلومات:.. 28
څلورم زيان - د خصوصي حريم اړوند اندېښنې:.. 28
پنځم زيان - د ډيټا د امنيت ژمنې او خطرونه: 28
شپږم زيان - د مالي مرستو په برخه کې د امنيتي ننګونو سروې:... 29
اووم زيان - د باور قوي کول: 29

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

دویمه برخه: د ټولنیزو غونډو سوله ییزې اړیکې 31

۱ . له غونډې مخکې اړیکې: 32
۲ . د غونډې په بهیر کې اړیکې: 32
۳ . له غونډې وروسته اړیکې: 32
۴ . خپلمنځي یا داخلي اړیکې: 33
۵ . بهرنۍ اړیکې: 33
۶ . بېړنۍ اړیکې: 33
۷ . رسنیزې اړیکې: 33
لومړۍ لاره - د قانون مراعاتول: 33
دویمه لاره - پر وضعیت څارنه: 34
درېیمه لاره - د داخلي اړیکو ستراتېژۍ جوړول: 34
څلورمه لاره - د بهرنیو اړیکو ستراتېژي جوړول: 34
پنځمه لاره - د بېړنیو اړیکو ستراتېژي جوړول: 34
شپږمه لاره - له پولې پورې افغاني او بهرنیو رسنیو سره د اړیکو ساتنه: 34
اوومه لاره - له ګډونوالو سره اړیکه: 35
اتمه لاره - د بشري حقونو له سازمانونو او نادولتي موسسو سره همغږي: 35
نهمه لاره - د اړیکو خوندي چینلونه په نظر کې ولرئ. 35
لسمه لاره - له نړېوالو رسنیو او سازمانونو سره تعامل: 35
یوولسمه لاره - مجازي غونډو ته مخه کړئ: 35
دولسمه لاره - د بینرونو او نښو ښودل: 35
دیارلسمه لاره - د کلیمو او شعار ورکولو په برخه کې دقیق اووسئ: 36
څوارلسمه لاره - له سوله ییزو خبرو اترو کار واخلئ: 36
پنځلسمه لاره. له ټولنیزو رسنیو ګټه واخلئ خو په ژوندۍ بڼه مه ښکاره کېږئ: 36
شپاړلسمه لاره - بېړنۍ اړیکې: 36
اوولسمه لاره - د وضعیت مدیریت کول تر څو له عامه پام او لیدنې نه خوندي پاتې شئ: 36
اتلسمه لاره - د تنظیموونکیو تر منځ اړیکې: 36
نولسمه لاره - د نورو پام ځان ته مه راواړوئ: 37

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

شلمه لاره - له خپل حالته خپل نږدې خپلوان او ملګري خبر کړئ: 37
یوویشتمه لاره - لنډ وضاحت: 37
دوه ویشتمه لاره - په ټولنیزو رسنیو کې پام او احتیاط: 37
درویشتمه لاره - پر وضعیت څارنه: 37
څلورویشتمه لاره - بېړنۍ طرحه: 37
پنځه ویشتمه لاره. له غونډې وروسته خبرې اترې: 37
شپږویشتمه لاره - د معلوماتو دقیق خپرول: 38
اوویشتمه لاره - ملاتړ او تعقیب: 38
۱ . ګټې: 39
لومړۍ ګټه - پوهاوی او راټولېدنه: 39
دویمه ګټه - د معلوماتو شریکول: 39
دریيمه ګټه - راټولېدنې رامنځ ته کول: 39
څلورمه ګټه - د نړېوالې ټولنې پام: 39
پنځمه ګټه - لاسرسی / ترلاسه کول او تعامل: 39
شپږمه ګټه - عدالت غوښتنه او شبکه جوړول: 40
اوومه ګټه - مخامخ یا مستقیمه اړیکه: 40
اتمه ګټه - د اطلاعاتو خپرول: 40
نهمه ګټه - د اړیکو او پوهاوي پراخول: 40
۲ . زیانونه: 40
لومړی زیان - د چارواکیو له لوري څارنه او ځپل: 40
دویم زیان - ناسم او نیمګړي معلومات: 41
دریيم زیان. تاوتریخوالی او هڅونه: 41
څلورم زیان – خوربېدل /خواره کېدل: 41
پنځم زیان. امنیتي ګواښونه: 41
شپږم زیان - سانسور او څارنه: 41
اووم زیان - ناسم معلومات او نیمګړي معلومات: 41
اتم زیان - د خصوصي حریم اړوند اندېښنې: 42
لومړۍ لاره - لومړی امنیت: 42

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

دویمه لاره - ناپېژانده ګزارش: 42
درېیه لاره - خوندي شبکې: 42
څلورمه لاره - په غوره توګه شریکول: 42
پنځمه لاره - د مناسب وخت ټاکنه: 43
شپږمه لاره - له کورنیو او بهرنیو رسنیو سره ګډون: 43
اوومه لاره - مستند شواهد: 43
اتمه لاره. کنټرول شوې خپرېدنې: 43
نهمه لاره - له هغو چینلونو ګټه واخلئ چې د حساسې منځپانګې له پروتوکولونو سره تړلې وي: 43
لسمه لاره - د وړاندیزونو او نیوکو حلقه: 43
یوولسمه لاره - د ډیټا یا معلوماتو د ساتنې تدابیر: 43
دولسمه لاره - د خصوصي حریم ترتیبول: 44
دیارلسمه لاره - روزنه او پوهاوی: 44
۱ . پایله یا نتیجه ګیري: 45
۲ . لارښوونې: 45
۳ . د سوله ییزه وتو اسانتیا: 45
۴ . وضعیت وڅارئ: 45
۵ . له غونډې وروسته اړیکې: 45
۶ . غونډه مستنده کړئ: 45

سرچینې 46

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

مخففات

2FA	*Two-Factor Authentication*
AI	*Artificial Intelligence*
CSO	*Civil Society Organization*
DVD	*digital versatile disc*
GDPR	*General Data Protection Regulation*
HRD	*Human Rights Defender*
ID	*Identity*
IDP	*Internal Displaced Person*
ITA	*Interim Taliban Authorities*
NGO	*Non-Governmental Organization*
PIN	*Personal Identification Number.*
QR Code	*Quick Response Code*
SEO	*Search Engine Optimization*
SMT	*Senior Management Team*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
TOR	*The Onion Router*
UN	*United Nations*
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

لومړۍ برخه: د نادولتي موسسو اړیکې

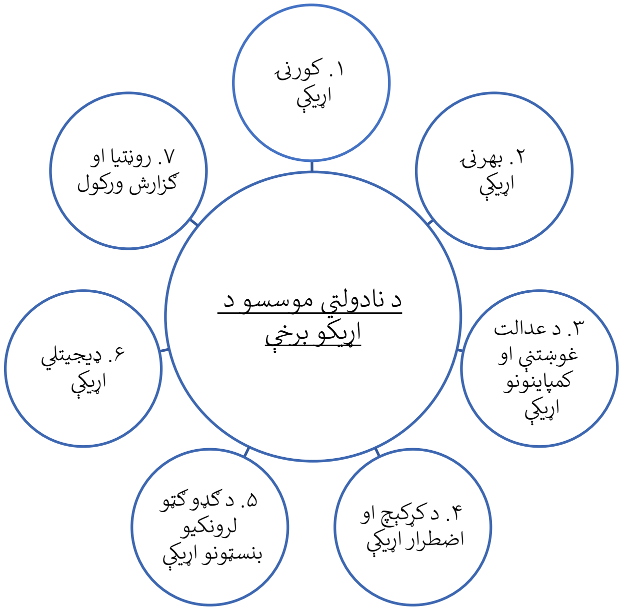
Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د نادولتي موسسو اړيکې څه شی دي؟

د نادولتي موسسو اړيکې هغو ستراتیژیو او میتودونو یا لارو چارو ته اشاره ده چې دا موسسې د معلوماتو شريکولو، د مختلفو لوريو/ اړخونو سره د اړيکو، د موخو شريکولو، د خپلو فعاليتونو پلي کولو او لاسته راوړنو په برخه کې ورڅخه ګټه پورته کوي. د ملاتړ تر لاسه کولو، د سرچينو راټولولو، پر پالیسیو اغیز ښندنه او خپلو موخو ته د رسېدو لپاره، د نادولتي موسسو لپاره اغېزناکې اړيکې درلودل ډېر مهم دي. د نادولتی موسساتو د اړيکو لمن پراخه، د کورني او بهرني ابعادو درلودونکې او د تغير په حال کې ده، څکه چې د رسنيو او تکنالوژۍ له پرمختګ سره، د چارواکيو تحولات، د بسپنه ورکوونکيو او تمويلونکيو په پالیسیو کې تغيرات او د مخاطبانو کړه وړه تغير يا وده کوي، نو اړينه ده چې د چارواکيو، تمويلوونکيو او د مخاطبينو د ارزښتونو په برخه کې ژور درک او ورتيا ولرو. د دغه ډول ورتياوو او مهارتونو په ترلاسه کولو، نادولتي موسسې کولای شي له ګټه اخيستونکيو سره خپلې اړيکې غښتلې کړي، له خونديتوبه يې ډاډ تر لاسه کړي، د دوی نظریات او اغېزمنتوب ډېر او په مناسبه او حسنه توګه خپلې کارنده موخې تر لاسه کړي.

د نادولتي موسسو د اړيکو برخې

دلته به تاسې ته د نادولتي موسسو د اړيکو په هکله ځينې برخې تعريف شي، خو نشو کولای چې ټولې برخې تر همدې ځایه محدودې کړو:



۱. کورنۍ اړيکې:

ناودلتي موسسې بايد ډاډه اوسي چې غړي، کارکوونکي او رضاکاران يې خوندي، اګاه، هڅانده، څواب ورکوونکي او د ورسپارل شويو دندو او موخو تر لاسه کولو په برخه کې ژمنتيا لري. د کورنۍ اړيکو د پراختيا لپاره، نادولتي موسسې له مختلفو وسيلو او لارو چارو ګټه پورته کوي، لکه ايميل، خبرپاڼه، ورځينۍ انلاين او حضوري غونډې، د ډله ييزو غونډو پلاټفورمونو لکه Jitsi، Slack يا Microsoft Teams. د نادولتي موسسو د اړيکو کورنۍ برخې لکه داخلي حساب ورکونه، تازه معلومات شريکول، د روزنيزو برنامو ترسره کول، په داخلي پالیسیو کې تغير يا اصلاح راوستل، او د غړو، کارکوونکيو او رضاکارانو تر منځ په ورځينيو بحثونو او نظرونو څرګندولو کې، اسانتيا رامنځ ته کول دي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

شکل ۱: د نادولتي موسسو د اړیکو برخې

۲. بهرنۍ اړیکې:
د نادولتي موسسو بهرنۍ اړیکې، د بسپنه ورکوونکیو یا تمویلوونکیو، د ګټه اخیستونکیو سازمانونو، چاروکو، رسنیو او عامه خلکو سره هر ډول ممکنه او د هوکړې وړ اړیکې تضمینوي. ناودلتي موسسې د بهرنیو اړیکو لپاره له مختلفو لارو چارو کار اخلي، له دې جملې څخه، له ویبسایټونو، د ټولنیزو رسنیو له پلاټفورمونو، د اړیکو له وسیلو، د مدني درېځ او رسنیزو ویناوو، ایمیلونو، ویلاګونو، او ډلیزو رسنیو څخه ګټه پورته کوي. د بهرنیو اړیکو برخې د ډېرو عواملو له امله متفاوته دي چې دموسسو د کار او بودیجې تر لاسه کولو اړوند د عامه پوهاوي لوړولو لپاره کمپاینونه، کاري ګذارشونه او پر ټولنه د دغه فعالیتونو اغېزې، د ګټه پورته کوونکیو په ژوند کې د مثبت تغیر روایتونه وړاندې کولو، د بنسټ د موقعیت تثبیت، د عدالت غوښتنې یا ایډووکسي پیغامونه او پرمختیایي مواد رانغاړي.

۳. د کمپاینونو او عدالت غوښتنې اړیکې:
نادولتي موسسې پر عامه افکارو، پالیسیو او د خپلو موخو او کاري ماموریت په اړونده قوانینو اغېز ښندونکې دي. دوی له مختلفو وسیلو او روښونو څخه ګټه پورته کوي، لکه د سوله ییزو غونډو، لابي ګرۍ، غوښتنلیکونو، د ټولنیزو رسنیو کمپاینونو، د عامه اعلامیو د خپرولو او په ټولنیزو رسنیو کې د انفلوئنسرانو یا اغېز ښندونکو اشخاصو سره د ګډون له لارې. نادولتي موسسې د واضح او قانع کوونکیو پیغامونو له لارې، د خپلې موخې وړ مخاطبینو او خپلو ملاتړو ته د رسېدو او د هغوی د راټولېدو د مناسبو چینلونو د ترکیب او انتخابولو له لارې، هڅه کوي چې ستراتېژیک اووسي.

۴. د کړکېچ او بیړنیو حالاتو اړیکې:
د نادولتي موسسو هدف پر ورځینو چارو او موخو د کړکېچونو د منفي اغېزو د کمښت مدیریت دی. د دې امر د تحقق لپاره، دوی له مختلفو لارو چارو لکه د کړکېچ د اړیکو طرحه چمتو کول، د چټک غبرګون د ټیم رامنځ ته کول، د کړکېچ پر وخت د ښکاره او رڼو اړیکو رامنځ ته کول او له کړکېچ څخه وروسته د ارزونې د راپور له چمتو کولو ګټه پورته کوي.

۵. د ذینفع بنسټونو ګډون:
نادولتي موسسې هغو افرادو او موسساتو سره د مثبتو اړیکو رامنځ ته کولو او خوندیتوب ته ژمن دي چې د نادولتي موسسو په عمومي فعالیتونو یا په پروژو کې علاقه لري او یا پې برخوال دي. موسسات له مختلفو لارو چارو ګټه اخلي، د منظمو تازه معلوماتو شریکول، په پروژو یا نورو پروګرامونو کې د ګډون بلنې، د اطلاعاتو د راټولولو سروی او د دغه بنسټونو ملاتړ تر لاسه کول.

۶. ډیجیټل اړیکې:
نادولتي موسسې له ډیجیټلي اړیکو ګټه پورته کوي، ځکه چې په نننۍ نړۍ کې، مخاطبانو ته په پراخه کچه د ګټورې او ارزانه لاسرسۍ په موخه، ډیجیټلي پلاټفورمونو ته ډېره اړتیا ده، دوی د پراخه کچې ستراتېژیو او وسیلو نه کار اخلي، لکه د انلاین ښه لیدو لپاره د پلټنې د اصلاح کولو ماشین یا SEO (Search Engine Optimization) د دوی د کاري منځپانګې د ودې، په انځوریزو بڼو د روایتونو بیانول، بریښنایي خبرپاڼو او همدارنګه پر ټولنه د خپلو کاري اغېزو د اندازه کولو او تعامل لپاره.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۷ . روڼتیا او ګذارش ورکونه:

نادولتي موسسې د خپلو فعالیتونو په ښکاره توګه د شریکولو او ښکاره کولو، د مالي امورو د پایلو، دولتي تنظیموونکیو د ځواب ورکونې ښکاره کولو، مرسته ورکوونکیو او د شریکانو او ګډو کټو لرونکیو له لوري ډاډ تر لاسه کوي. دوی د ځواب ورکونې له مختلفو ګذارشونو او میکانیزمونو، لکه شپږ میاشتني او کلني ګذارشونو، مالي حسابونو، د پروژې ګذارشونو، سازماني ګذارشونو، مالي پلټنو او د اغېزو له ارزونو ګټه پورته کوي چې ډېر ځله د نادولتي سازمان په ویب سایټ او په بعضو برخو کې د ټولنیزو رسنیو له لارې خپرېږي.

په افغانستان کې د انلاین اړیکو د رامنځ ته کولو پر مهال د نادولتي موسسو اصلي او اساسي ننګونې کومې دي؟

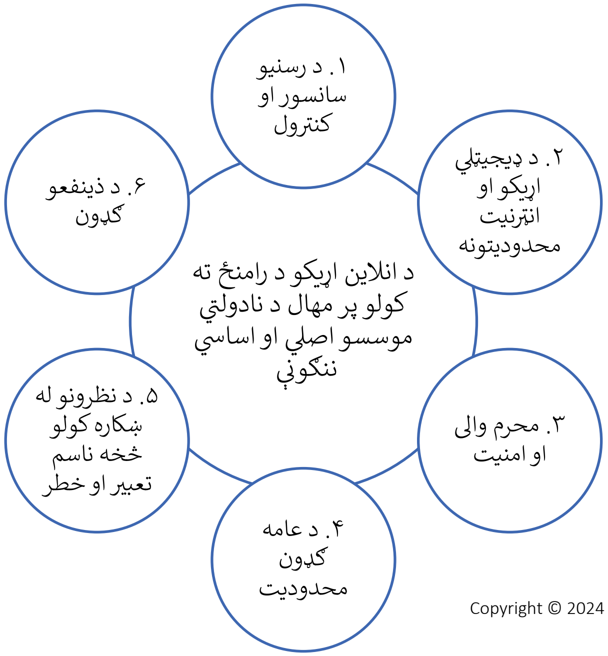
په افغانستان کې د نادولتي موسسو اړیکې له مختلفو ننګونو سره مخ دي. دوی (نادولتي موسسې) په یوه حساس او محدود چاپېریال کې فعالیت ترسره کوي. د نادولتي موسسو د فعالیت چاپېریال د دوی د امنیت، اړیکو او د پیچلیو ټولنیزو او سیاسي شرایطو سره د حساسیت له امله، ستراتیژیک او انعطاف منونکي چاپېریال ته اړتیا لري. دا یو نازک توازن دی چې نادولتي موسسې یې باید په احتیاط سره په پام کې ونیسي. دلته هغو سترو ننګونو ته یوه کتنه کوو چې د نادولتي موسسو پر اړیکو اغېز لرونکي دي:

۱ . د رسنیو کنټرول او سانسور:

د بیان پر ازادۍ او ډله ییزو رسنیو موجود شدید کنټرول، په مستقیمه توګه له خلکو سره د نادولتي موسسو پر اړیکو، اغېز ښندي. د طالبانو د موقتي اداري د پام وړاوښتو د مخنیوي او د دوی د منفي دید له امله، د نادولتي موسسو تر منځ د ځان سانسورۍ فضا حاکمه شوې ده.

۲ . د ډیجیټلي اړیکو او انټرنیټ محدودیتونه:

انټرنیټ ته لاسرسی، له ډیجیټل پلاټفارمونو ګټه اخیستل او ټولنیزې رسنۍ له یوې مخې تر ځارنې لاندې او په بعضو مواردو کې محدود شوې دي. (۳) نادولتي موسسې باید د خپلو کارکوونکیو، ګټه اخیستونکیو او خپلو فعالیتونو ته د وړپېښ خطر د مخنیوي په موخه، د دې ډول محدودیتونو په شتون کې، له ډېر پام او احتیاط نه کار واخلي.



شکل ۲: د انلاین اړیکو د رامنځ ته کولو پر مهال د نادولتي موسسو اصلي او اساسي ننګونې

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۳ . امنیت او محرم والی:

د نادولتي موسسو د اړیکو فعالیتونه د طالبانو د موقتي اداري تر سختې څارنې لاندې دي (۴) نادولتي موسسې باید د خپلو کارکوونکیو او موسسې ته خدمات وړاندې کوونکیو هویت پټ ساتلو او ډاډمن خوندیتوب ته لومړیتوب ورکړي. په دې ډول حالاتو کې خوندي مخابراتي چینلونه او د کوډ شویو پیغام رسوني خدمات خورا اړین او حیاتي ارزښت لري.

۴ . د عامه ګډون محدودیت:

په افغانستان کې د عامه ګډون او عدالت غوښتنې په کمپاینونو کې د پام وړ کموالی رامنځ ته شوی دی. نادولتي موسسې مجبوره دي چې خپلې عامه اړیکې محدودې کړي او په دې توګه کمرنګه فعالیتونه ترسره کوي، تر څو د چارواکیو پام ور وا نه وړي.[1]

۵ . د نظریاتو د وړاندې کولو څخه د ناسم برداشت خطر:

هغه اړیکې چې د طالبانو د موقتي اداري پر وړاندې نیوکې پکې موجودې وي او یا د بشر د حقونو په هکله خبرې چې د طالبانو د اصولو خلاف او پخپله خوښه یې په شریعت ورګډوي او دفاع ترې کوي، له خطره خالي نه دي. نادولتي موسسې باید خپل اظهارات په ډېر پام سره بیان کړي تر څو خپل کارکوونکي او فعالیتونه له خطر سره مخ نه کړي.

۶. د ذینعفو بنسټونو ګډون:

له نړېوالو تمویلونکیو، مرستندویه ادارو او نړیوالې ټولنې سره تعامل ورځ تر بلې پیچلې کېږي. (۶) نادولتي موسسې باید له سیمې څخه د پېښو ګذارش ورکولو، د نړیوالو بنسټونو څخه د ملاتړ تر لاسه کولو په موخه عدالت غوښتنه او پر خلکو د خپل اغېز شکاره کولو لپاره د اړیکو ساده او خوندي لارې پیدا کړي.

څه ډول کولای شو په افغانستان کې د اړیکو ننګونو ته ځواب ووایو؟

له ننګونو سره څه ډول چلند غوره کول (۱) د رسنیو سانسور او کنترول (۲) د ډیجیټل اړیکو او انټرنیټ محدودیتونه او (۳) د امنیت او محرم والی:

لومړی لاره - د خصوصي مجازي شبکو نه ګټه پورته کول (VPN):

[1] https://press.un.org/en/2023/sc15222.doc.htm

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د خصوصي مجازي شبکو نه ګټه پورته کول (VPN)په خوندي توګه انټرنیټ ته د لاسرسي او د سانسور او محدودیتونو لرې کولو لپاره مناسبه لاره حسابیږي. دا کار ستاسي د انلاین هویت د خوندیتوب او انټرنیټي ترافیک په برخه کې له تاسي سره مرسته کوي. خو دا په یاد ولرئ چي (VPN)خدمتونو وړاندې کوونکیو ټولو کمپنیو باندې باور کول نه دي په کار. بعضې دولتونه د VPN له شرکتونو د خپلو اړتیا وړ موادو ته د لاسرسي پیدا کولو لپاره، ګټه اخلي. دلته د VPN خدمتونو وړاندې کوونکې شتون لري چي کولای شئ ګټه ورځخه پورته کړئ.

نوم	خدمات وړاندې کوونکې	ښېګڼې	عیبونه	کوربه هېواد
ProtonVPN	Proton Technologies AG	امنیت او دخصوصي حریم خوندیتوت ته قوي ژمنه، په سویس کې مېشت د مطلوبه خصوصي حریم قوانینو خوندیتوب، سیستم ته د نه ورننوتلو پالیسي، Secure Core یا د لا ډېر امنیت لپاره ځانګړنې.	کېدای شي د درنو کوډکېدو له امله یې سرعت کم وي	Switzerland
	وبسایت	https://protonvpn.com/		
Mullvad	Amagicom AB	د خصوصي حریم په خوندیتوب متمرکز، له ګذارش پرته پالیسي، د کریډیټ کارډ د لارې د ناپېژاندو تادیاتو ملاتړ، د WireGuard پروتوکول څخه ملاتړ او له سانسور څخه د خلاصون په برخه کې د پل په څېر حالت	رابط کاربری/ د نښلولو لیکه یا (Interface) کېدای شي د بعضو کاروونکو لپاره لږ څه دوستانه وي.	Sweden
	وبسایت	https://mullvad.net/en		
ExpressVPN	Express VPN International Ltd	رابط کاربر پسند، سرعت قابل اعتماد، رمزگذاری قوی، فناوری TrustedServer برای بهبود امنیت.	هزینه بالاتر، بر اساس حوزه قضایی Five Eyes.	British Virgin Islands
	وبسایت	https://www.expressvpn.com/		

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

NordVPN	Tefincom & Co., S.A	د پراخه سرور شبکه، قوي شوي کوډونه، د لا ښه امنيت او ګډوډۍ تخصصي سرورې، دوه VPN د لا خونديتوب لپاره	په کال ۲۰۱۸ کې د (14-Eyes) په يوه هېواد کې پې يوه امنيتي پېښه درلوده.	Panama
	وبسايت	https://nordvpn.com/		
CyberGhost	Kape Technologies	د کاروونکو د خوښې برنامې، قوي کوډ شوي، له څو وسيلو يا دستګاوو څخه ملاتړ، د تورنت او خپرولو لپاره ځانګړي سرورونه	د خصوصي حريم د خونديتوب سياست پې د نورو ارايه کوونکيو په څېر غښتلی نه دی. سرعت پې په مختلفو سرورونو کې توپير لري.	Isle of Man
	وبسايت	https://www.cyberghostvpn.com/		

۳ م شکل: د VPNخدمتونو مشهور ارايه / وراندي کوونکي

دويمه لاره - د اړيکو اپليکشنونو په برخه کې له کوډ شويو هغو او د ايميل له خوندي خدمتونو ګټه واخلئ:

د کورنۍ او بهرنيو اړيکو لپاره د اړيکو له کوډ شويو برنامو او د ايميل له خوندي خدمتونو ګټه پورته کړئ. دلته د اړيکو د کوډ شويو قابليت درلودونکي او د ايميل د خوندي خدمتونو اپليکيشنونه موجود دي. (۸ او ۹ شکلونو ته مراجعه وکړئ).

درېيمه لاره - ځان مه ځلوئ او له عامه پام څخه لرې اووسئ:

که په افغانستان کې کار کوئ، هغه لارې وکاروئ چې د ډېرو خلکو پام نه دراوړي او د دې چارې په ساتلو سره په اړيکو او عمومي فعاليتونو تمرکز ولرئ. په ټولنيزو رسنيو کې د ډېر فعاليت او تلويزيوني مصاحبو کې له راڅرګندېدو ډډه وکړئ. دا کار کولای شي تاسې د چارواکيو له سختې ځارنې خوندي کړي او که داسې و نه کړئ، کېدای شي د طالبانو موقته اداره ستاسې کار او فعاليت حساس او مشکل رامنځ ته کوونکې وګڼي.

څلورمه لاره - له فرهنګي حساسيتونو ډډه وکړئ:

د خپلو برنامو د طرحه کولو په برخه کې له افغان کارپوهانو سره له مشورې وروسته ډاډ تر لاسه کړئ چې ټولې اړيکې او د اړيکو برنامې له فرهنګي پلوه حساسيت پارونکې نه دي. دغه ډول مشوره او ځان ډاډه کول د حاکمو ډلو د منفي پام درګرځېدا، خطر کموي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

پنځمه لاره. د سایبري امنیت په برخه کې کارکوونکیو ته منظمه روزنه:

خپلو کارکوونکیو ته په محدودو او امنو سیمو کې د ډیجیټل امنیت او د خوندي اړیکو لارو چارو په هکله منظمې روزنې ورکړئ. که ستاسې موسسه د دغه ډول روزنې وړتیا نه لري، له موسسو یا هغو افرادو چې د ډیجټلي امنیت په برخه کې تخصص لري، مرسته وغواړئ. دوی کولای شي تاسې ته مناسبه مشوره درکړي، تازه او اپډیټ معلومات درسره شریک کړي او د ډیجیټلي ننګونو په برخه کې لارې چارې در په ګوته کړي. ډېرې موسسې شته چې کولای شي ستاسې سره په دې برخه کې مرسته وکړي.

شپږمه لاره. د ډیجیټل امنیت تازه او اپډیټ لارې چارې وڅارئ او وڅېړئ:

په منظمه توګه د ډیجیټل امنیت نوې او اپډیټ لارې چارې وڅارئ، د څارنې تکنالوژۍ په پرلپسې توګه مخ پر وده روانه ده. په پایله کې، په منظمه توګه د ډیجیټلي امنیتي اقداماتو له سره کتنه وکړئ تر څو نوي ګواښونه په نخښه او مقابلې ته یې چمتووالی ونیسئ او د اړیکو لپاره له پرمختللې تکنالوژۍ له تازه او اپډیټ شویو لارو چارو څخه ګټه پورته کړئ.

اوومه لاره. د انټرنیټي خطرونو ځواب ته یوه بېړنۍ طرحه چمتو کړئ:

وار له مخه د خپلو اقداماتو لپاره یوه بېړنۍ او روښانه طرحه جوړه کړئ، چې که انټرنیټي خدمات ټکني کېږي نو د ډیجیټل سرویلانس مقابلې یا موافقت کوونکي ډیجیټل وسیلې کارنده وسائل شي،. د دغه ډول طرحو شتون دا تظمینوي چې کارکوونکي د خپلو او په موسسه کې دخیلو افرادو اطلاعات خوندي کړي او په چټکه او امنه توګه غبرګون وښایي.

اتمه لاره. حساسه ډیټا کوډ او ذخیره کړئ:

د مناسبو پلاټفورمونو نه په ګټه اخیستنه، خپله حساسه ډیټا کوډ او ذخیره کړئ او له هغو پلاټفورمونو ګټه واخلئ چې قوي امنیتي امکانات ارایه کوي. د ډیټا د بشپړوالي او د نورو لاسونو ته د لاسرسی نه د خوندیتوب او یا هم په ناقانونه توګه له لاسه ورکولو امکان د پېښېدو له وېرې، د کنترول د قابلیت لرونکیو وړ او امنو میتودونو څخه ګټه واخلئ.

نهمه لاره. په دفتر کې موجود د اړیکو اسناد او مدارک:

له ډیجیټلي امنیټ سربېره، په دفتر کې د حساسو اطلاعاتاتو لرونکي توکیو له شتونه ځان ډاډه کړئ. دې ډول اسنادو ته د لاسرسی او ځای پر ځای کولو په برخه کې له سختو پالیسیو ګټه پورته کړئ.

لسمه لاره. د قوي پاسورډونو او کوډنو رامنځته کولو پالیسی اړتیا:

- هغه پالیسي رامنځ ته او پلې کړئ چې د فرد پورې اړوند ټولو حسابونو او خدماتو ته قوي او ځانګړي پاسورډونو ته اړتیا لري.د پاسورډ غوره کولو پر مهال.
- د یوه لنډ او روښانه پاسورډ کارولو پر ځای، یو نوی، پېچلی او قوي پاسورډ وکاروئ.
- د خپل پاسورډ د خوندي کولو لپاره د غټو حروفوونو، ورو حرفونو، علامو او نخښو او اعدادو څخه ګټه واخلئ.
- د وینډوز په پاسورډ ډېره ملا مه تړئ، ډېر نازک او په بېړه له منځه تلونکی دی.
- د خپل پاسورډ لپاره کم تر کمه له اتو کرکټرونو یا نخښو کار واخلئ.
- د تغیر ورکولو پر مهال، تل له یوه نوي پاسورډ څخه کار اخلئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

- له يوه داسې خوندي پاسورډ څخه ګټه واخلئ چې ستاسې له شخصي ژوند او سرګرميو سره هيڅ ډول اړه يا اړيکه و نه لري.
- هره يوه مياشت او يا هم درې مياشتې وروسته خپل پاسورډ بدل کړئ.
- خپل کارکوونکي وهڅوئ چې د خپل پاسورډ د لا ښه خونديتوب لپاره د پاسورډ د مديريت کولو له اپليکيشنونو څخه ګټه واخلي.

دلته نادولتي موسسو ته د پاسورډونو د مديريت د تر ټولو خوندي اپليکيشنونو څو برخې درسره شريکوو:

کوربه هېواد	مناسب والی	د خدماتو وړاندې کوونکي نوم	نوم
متحده ايالات	رونتيا ته لومړيتوب، له ډيجټلي امنيت نه اګاه کاروونکيو لپاره ايډيال. دا اپليکيشن د پرانيستې پاسورډ سرچينه، پراخه او ارزانه خدمات وړاندې کوي.	8bit Solutions	Bitwarden
	https://bitwarden.com/	وبسايت	
متحده ايالات	د څو لاملونو له امله د خوښې وړ او د هويت د تصديق او د خوښې وړ او د ځانګړو خوندي لارو لرونکی. هغوی چې راحت او همکاری ته ارزښت قايل دي، ډېر مناسب دی.	LogMeIn, Inc	LastPass
	https://www.lastpass.com/	وبسايت	
کانادا	د قوي امنيتي ځانګړتياوو لرونکی، د سفر پر مهال د لا ډېر خونديتوب ورتيا، د سرغړونو د څارنو لپاره د څار برج يا ټاور، د هغو کسانو لپاره چې د ټوليز امنيت او خونديتوب په لټه کې دي، ايډيال دی.	AgileBits Inc	1Password
	https://1password.com/	وبسايت	
متحده ايالات	پر تياره ويب، VPN او پاسورډ بدلولو څارنه ترسره کوي. هغو کاروونکيو ته چې د لا ښه امنيت او خونديتوب لپاره د ټېر پاسورډ په لټه کې دي، ګټور دی.	Dashlane Inc	Dashlane
	https://www.dashlane.com/	وبسايت	

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

KeePassXC	KeePassXC Development Team	هغوی ته ډېر کټور او بهتره دی چې د خصوصي حریم کنترول ته لومړيتوب ورکوي، د پاسورډ د سیمه ییز رایګان مدیریت او سرچینې بازار ته وړاندې کوي.	آلمان
	وبسایت	https://keepassxc.org/	

۴ م شکل: نادولتي سازمانونو ته د مدیریت د پاسورډ بهترین اپلیکیشنونه

یوولسم لاره - له 2FA څخه ګټه پورته کړئ:

پخپلو ټولو حسابونو کې د هویت د تصدیق دوه مرحله ییز (2FA)تطبیق کړئ. د امکان په صورت کې، د هویت د تصدیق دوه مرحله ییز توکې په حسابونو کې د یوه امنیتي او خوندي توکي په توګه وکاروئ، په تېره هغو حسابونو کې چې د موسسې په فعالیتونو کې تړي ګټه اخلئ.

دولسمه لاره - د غیر متوقع پېښو لپاره د غبرګون پلان رامنځ ته کول:

د احتمالی امنیتي سرغړونو یا ډیټا لیک کېدو پر وړاندې، د غیر مترقبه پېښو پر وړاندې د غبرګون یوه روښانه او د اجرا وړ طرحه رامنځ ته کړئ. په دې طرحه کې باید د مهارولو، ارزونې، خبرتیاوو او بېرته تر لاسه کولو لارې چارې په ګوته شوي وي. که ستاسې ویب سایټ هیک شو او یا مو د حسابونو پاسورډونه له خطر سره مخ شول، چمتووالی ولرئ. تاسې باید دغو ټولو سناریوګانو ته بشپړ چمتووالی ولرئ.

دولسمه لاره - له TOR څخه ګټه پورته کول:

په هغو موقعیتونو کې د ناپېژانده پاتې کېدو ته یې اړتیا لرئ، چې د خپلو اړیکو لپاره له ناپېژندل شویو ډیزاین شویو توکیو لکه TOR څخه د حساسو خبرتیاوو، د ډیټا د انتقال یا انټرنیټ ته د لاسرسي لپاره ګټه ورڅخه اخلئ. دلته تاسې ته د څو تر ټولو مناسبو هغو په هکله معلومات درکوو او درپېژنوو یې:

نوم	نام ارائه دهنده خدمات	مناسب والی	کوریه هېواد
Tor Browser	The Tor Project	د TOR شبکې ته د لاسرسی په برخه کې او ډېر کاریدونکې او ډېر پېژندل شوی. دا د هغو کاروونکیو لپاره چې د ویب د لیدو پر مهال ناپېژانده پاتې کېدو او د خصوصي حریم خوندیتوب ته ډېره اړتیا لري، ایډیال دی.	نړیوال (مرکز یې د امریکا متحده ایالات)
	وبسایت	https://support.torproject.org/tbb/	

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

Brave Browser with TOR	Brave Software	له TOR سره سره، د خصوصي حریم د خوندیتوب او د تبلیغاتو د بندولو ورتیاوې له ځانه سره لري. د هغو کاروونکیو لپاره چې د TOR له ادغام سره بدیل براوزر غواړي، ډېر مناسب دی.	متحده ایالات
	وبسایت	https://community.brave.com/	
Whonix	Whonix Project	Whonix د خصوصي حریم لپاره متمرکز عملیاتي سیستم دی چې د یوه مجازي ماشین په منځ کې ترسره کېږي او د TOR شبکې له لارې د انټرنیټ ټول ترافیک ته لارښوونه کوي. هغو کسانو ته چې د خپل خصوصي حریم د لا ښې اوخوندي حللارې په لټه کې دي، مناسب دی.	نړیوال
	وبسایت	https://www.whonix.org/	
Tails (The Amnesic Incognito Live System)	Tails Project	Tails د یو ژوندي سیستم لرونکی عمل دی چې د USB یا DVD سره طراحي شوی دی او د انټرنیټ ټول ترافیک ته د TOR له لارې لارښوونه کوي. دا د هغو کسانو لپاره ګټور او ښه دی چې غواړي ناپېژانده پاتې شي او په کوربه سیستم کې یې هیڅ ډول نښه پاتې نشي	نړیوال
	وبسایت	https://tails.net/	
Orbot/Orfox	The Guardian Project	Orbot د پروکسي یوه برنامه ده چې ستاسې د ګرځنده تلیفون دستګاه ته د TOR د شبکې له لارې لارښوونه کوي، په داسې حال کې چې Orfox رسمي ویب د انډروايد لپاره د TORرسمي پروژه ده. دوی د هغو کاروونکیو لپاره چې پخپلو ګرځنده تلیفونونو کې د TOR د نه پېژندنې دستګاه ته اړتیا لري، مناسب دی.	متحده ایالات
	وبسایت	https://guardianproject.info/apps/info.guardianproject.orfox/	

۵ م شکل: بعضي مناسب او ګټور TOR

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۲ . د عامه ګډون د محدودیت موضوع ته څه ډول ځواب ووایو؟

د عامه ګډون د محدودیت ستونزې ته ځواب ورکونه دا ایجابوي چې نادولتي موسسې نوښتګر چال چلند غوره کړي تر څو وشي کولای خپلو هڅو ته په ډېر پام او هوښیارۍ سره دوام ورکړي. د ښو ستراتېژیو په تنظیم سره پر خپل ښه والي، امنیت او له سیمه ییزو شبکو څخه د ګټې اخیستې اړوند د ښه تمرکز لپاره، نادولتي موسسې کولای شي له خلکو سره ښه تعامل او د دوی (خلکو) د موخو ملاتړ ته دوام ورکړي. نادولتي موسسې معمولاً د شوراګانو، جرګو او سیمه ییزو مشرانو له لارې له خپلو ګټو اخیستونکیو سره اړیکې نیسي او خپل خدمات وړاندې کوي. په افغانستان کې شورا ګانو او جرګو په نوم د مدني ټولنې بنسټونه شتون لري. دا سنتي سیمه ییزې شوراګانې دي چې په لرې پرتو سیمو کې پې کلي او قومونه رامنځ ته کوي، تر ډېره په راپیدا شویو مسایلو کې د یو ځای د ګټو استازیتوب کوي. جرګې او شوراګانې تصمیم نیونکې سیمه ییزه بنسټونه دي چې په افغانستان کې د مدني ټولنې تر ټولو دودیز واحدونه حسابېږي. دغه ادرسونه په عمومي توګه د لرې پرتو سیمو له مشرانو څخه رامنځ ته شوي او په نارسمي ډول (یعنې د غیر ثبت شویو ډلو په توګه) فعالیت ترسره کوي.

نادولتي موسسې په مستقیم ډول او یا هم د شوراګانو، جرګو یا د ټولنې د مشرانو له لارې له خپلو ګټه اخیستونکیو سره اړیکې ټینګوي. د نادولتي موسسو ګټه اخیستونکې د ټولنې مختلف قشرونه دي، لکه:

مېرمنې او نجونې	نادولتي موسسې ډېر ځله د ښځو پر حقونو، د ښځو په پیاوړتیاوو، زده کړې او روزنې، روغتیایي خدمتونو ته پام کولو او د توپیري چلند او تاوتریخوالي پر وړاندې په مقابله تمرکز کوي
ماشومان	نادولتي موسسې د ماشومانو د زده کړو ته د لاسرسي پر ښه والي، روغتیایي پاملرنې، خواړو او خوندیتوب لپاره هڅې کوي.
کورني بېځایه شوي (IDPs)	نادولتي موسسې هغو افرادو او کورنیو ته چې په هېواد کې دننه د جګړې یا طبیعي پېښو له امله بې کوره شوي وي، د سرپناه، زده کړو ته د لاسرسي، روغتیایي پاملرنې، د خوراک څښاک او د ژوند نورو اړتیاوو برابرولو په برخه کې مرسته کوي.
کډوال	نادولتي موسسې په افغانستان کې له کډوالو او راستنېدونکیو د ملاتړ پروګرامونه پر مخ وړي او خدمات ورته وړاندې کوي، په دې برخه کې د نویو کورونو لپاره زمینه مساعدول، زده کړه، روغتیایي پاملرنې او د ژوند پر مخ بیولو لپاره فرصتونه او اسانتیاوې برابروي.
څنډې ته شوې ټولنې	نادولتي موسسې د ډول ډول برنامو او خدماتو له لارې، څنډې ته شوې ډلې لکه قومي لږه کې، معلولیت لرونکې افراد او هغه افراد چې په لرې پرتو سیمو کې مېشت یا له کورنۍ جګړې نه اغېزمن شوي وي، خپله موخه ټاکي.
د طبیعي پېښو قربانیان	نادولتي موسسې له طبیعي پېښو لکه سیلاب، وچکالي، زلزلې او واورې خوئېدنې یا برف کوچ نه اغېزمن شوي افرادو ملاتړې دي او مرسته ورسره کوي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د افغانستان د مدني ټولني لپاره د اړیکو لارښود

نادولتي موسسې د روغتیایي پاملرنې له سیستمونو، روغتیایي خدماتو، د زیربناوو جوړول، روغتیایي او درملیزه روزنه او د عامه پوهاوي کمپاینونو څخه ملاتړ کوي.	د روغتیا ساتنې یاروغتیا ته له پاملرنې ګټه اخیستونکي

۶م شکل: په افغانستان کې د نادولتي سازمانونو ګټه اخیستونکي.

نادولتي موسسې باید د خپلو ګټه اخیستونکیو سره د اړیکو لپاره، له شوراګانو، سیمه ییزو جرګو او همدارنګه ملاامانو او مذهبي، ټولنیزو او سیمه ییزو مشرانو سره اړیکې ټینګې کړي. دغه ډله مدني بسټونه او افراد کولای شي د معلوماتو په خپرولو او په اغېزمنه توګه له بدلون ملاتړ تر لاسه کولو کې مهم رول ولوبوي، په ځانګړي ډول هغه معلومات چې له فرهنګي پلوه حساس وي، تر څو لړ پام ورواوړي.

دا ډله هغه افراد دي چې د جومات د جماعت د امام په توګه، په مدرسو او جوماتونو کې روزونکي او په کار بوخت مذهبي کارپوهان دي. په سیمه کې ملایان له استوګنو سره په اړیکو کې پېژندل شوي او اګاه خلک دي. دوی ته په جومات کې د کلونو خدمت له امله، د همدې سیمې د جومات پورې اړوندو خلکو لیدلوری ښه ورمعلوم دی. که نادولتي موسسې غواړي له وړ او مستحقو ګټه اخیستونکیو سره اړیکه ټینګه کړي، باید له دغو مذهبي مشرانو سره کاري اړیکه رامنځ ته کړي.	مذهبي مشران (ملا امامان)
په کلیو او بانډو کې ملکان یا خانان د خلکو د استازو په نوم چارې ترسره کوي او د کلي دننه او له کلي بهر د خپل کلي د ګټو استازولي کوي. دا خلک د خپلو سیمو له ټولو خلکو سره ښې اړیکې لري او په چارو پوه خلک دي. نادولتي موسسې چې د یو کلي یوې ځانګړې برخې ته د خدماتو وړاندې کولو په لټه کې دي، متوجه به شي چې خان او ملک کولای شي په اړیکو کې اغېزناکه اسانتیا رامنځ ته کړي.	سیمه ییز مشران (خان او ملک)
دګذر وکیل په ښاري سیمو کې استازی دی چې د خلکو لخوا د یوې ځانګړې دورې لپاره په ښاروالۍ کې ټاکل کېږي. دغه اګاه خلک دي او ګټه اخیستونکیو سره د خپلو اړیکو له لارې، له نادولتي موسسو سره په مرسته کې کلیدي رول لوبوي.	د ګذر وکیل

۷م شکل: په افغانستان کې وړ او مستحقوو افرادو ته د لاسرسي لپاره، کلیدي کسان.

پام مو وي: په یاد ولرئ چې د دغه ډول خلکو اغېز کېدای شي د دوی د انفرادي چلند له مخې، توپیر ولري.

په داسې حال کې نادولتي موسسې باید:

- د ټولنې په کچه اړتیاوو ته په کتو او نشتو امکاناتو په موجودیت کې له کم شمېر ګډونوالو نه ګټه پورته کړئ. د پراخه او سترو کمپاینونو پر ځای، پر وړو برنامو تمرکز وکړئ چې د ډېر شور او ځوړ لرونکي نه وي. ښوونیز او روزنیز ورکشاپونه، خبرې اترې او هغه روزنیزې غونډې چې په ځانګړي چاپېریال کې ترسره کېږي، کولای شي د خلکو د پام دراووښتو پرته، تعامل او پوهاوي ته قوت ورکړي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

- د عدالت غوښتنې لپاره د نامستقيمو اړيکو تاکتيکونه غوره کړئ. د ارزښتمنو موضوعاتو اړوند د کيسو ويل او کلتوري پېښې په نامستقيمه توګه د خپلو پيغامونو د اړيکو ساتلو لپاره وکاروئ. دا لارې ګودرې خپلول کولای شي تاسې د نورو له منفي مقابلې وژغوري او هغو چاروکيو ته چې ستاسې کاري ساحه محدودوي، د منلو وړ وګرځي.
- له ګټو اخيستونکيو سره د خپلو اړيکو لارې چارې قوي کړئ او له هغوی سره د مستقيم تعامل لپاره، د قوي اړيکو ليکې امنې او خوندي کړئ. پر وخت خبرتياوې، کوډ شوې برنامې او مستقيمې ليکې د ځانګړو اړيکو په برخه کې اسانتيا راولي، له دې سره سره، هغوی کولای شي له تاسې ملاتړ وکړي او سرچينې او اطلاعات به له دې چې د نورو لاسونو ته ولوېږي، تاسې ته درکړي.

۳ . د خېرونو او نظرونو څرګندولو د ناسم برداشت له خطر سره څنګه مقابله وکړو؟

په افغانستان کې د خېرونو او نظرونو څرګندولو له ناسم برداشت له خطر سره مقابله، په ځانګړې توګه کله چې په احتمالي توګه د طالبانو موقتي اداري ته نيوکه متوجه وي او يا هم له بشري حقونو څخه دفاع چې د طالبانو پخپله خوښه شريعت سره سماوی و نه لري، يو ستراتېژيک او محتاط چلند ته اړتيا پيښېږي. نادولتي موسسې بايد له دغه ډول پارووڼکي وضعيت څخه اګاه وي تر څو بې له دې چې خپل فعاليت ترسره، او خپل کارمندانو له پېښېدونکيو ګواښونو نه خوندي، او خپلې چارې پر مخ يوسي. د دغه ډول ستراتېژيکو تګلارو په پلي کولو سره، نادولتي موسسې کولای شي په افغانستان کې پېچلی او له خطره ډک چاپېريال کنټرول کړي او د خپلو نظريو د څرګندولو په برخه کې د رامنځ ته شوي ناسم پوهاوي احتمالي بدو پايلو کچه راکمه کړي او وشي کولای خپلو موخو ته د رسېدو او خپلو ګټو اخيستونکيو ته د خدمتونو ترسره کولو ته دوام ورکړي.
ا ست .

لومړی لاره - د حساسيتونو په برخه کې پوهه او ګاهي:

په افغانستان کې د سياسي او فرهنګي حساسيتونو په هکله پوهېدا او اګاهي، د موضوعاتو ژورو ته د کښته کېدو لپاره د کلي حيثيت لري. دغه پوهه او اګاهي کولای شي د پيغامونو جوړښت ته داسې لارښوونه وکړي چې په سيمو کې مثبت غبرګون رامنځ ته کړي او ورسره د نادولتي موسسو موخو ته پرمختګ او پراختيا ورکړي. د ۲۰۲۱ کال د اګست له مياشتې راپدېخوا چې د طالبانو د موقتي اداري لخوا کوم فرمانونه، حکمونه، متحدالمال مکتوبونه، سپارښتنې او پرېکړې صادرې شوي او ستاسې په کاري چاپېريال پورې اړه ولري، مرور کړئ چې په افغانستان کې له نويو بدلونونو او حساسيتونو نه باخبره اووسئ. د خپلو چارو د لا ښه سنبالولو په موخه، د دغو فرمانونو، حکمونو، متحدالمال مکتوبونو، سپارښتنو او پرېکړو په هکله د معلوماتو ترلاسه کولو لپاره بايد له اړونده ادارو، وزارتونو او د طالبانو له موقتي اداري سره په اړيکه کې شئ. د طالبانو موقته اداره چې کومې ملاحظې لري، دوی دغه ډول اسناد په هيڅ يوه ويب سايټ کې نشر ته نه دي سپارلي.

دويمه لاره - له رسمي ژبو دقيقه ګټه اخيستنه:

د اړيکو په رامنځ ته کولو کې له رسمي ژبو څخه ګټه اخيستل، يو بل کارنده او مهم فکتور دی چې د ګډو انساني ارزښتونو او موخو سره تړاو لري. سربېره پر دې، د افغانستان دننه نادولتي موسسې بايد په خواله رسنيو، ټولنيزو او ډليزو رسنيو او په غونډو کې له ستېجونو او دريځونو له لارې له سياسي ويناوو يا هغه ډول ننګونې يا مستقيمې نيوکې چې حساسيت راپاروي، ډډه وکړي. که غواړې چې د افغانستان په خبر هېواد کې بدلون رامنځ ته کړئ، نو وې منئ چې مسلکي کېدل د فعال کېدو په پرتله، څو چنده خوندي دي. په خواله رسنيو، ډليزو او ټولنيزو رسنيو او د خلکو تر مخ د طالبانو په هر ډول پرېکړې نيوکه، د طالبانو په موقتي اداري نيوکه ګڼل کېږي چې دا ډول کار طالبان د شريعت خلاف عمل بولي او دغه ډول حالت د نيوکې کوونکې موسسې فعاليت ناممکنه کوي. نو د دغه دليل له مخې بايد ستراتېژيک چلند غوره کړئ او په مسلکي ډول کارونه مخ ته يوسئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

درېیمه لار - له دیني مشرانو (ملا امامانو) سره تعامل:

له دیني مشرانو (ملا امامانو) سره تعامل هم باید په هغه صورت کې، چې د بشرپاله مسایلو په برخه کې ګډ لید لوری ولري، یو ګټور ګام دی. د دوی ملاتړ او ګډون کولای شي د نادولتي موسسو نوښتونو ته په کلتوري چوکاټ کې لا ډېر اعتبار وروبخښي او د نامطلوبو تفسیرونو خطر او بدې پایلې کمې کړي.

څلورمه لار - په سیمه ییزو جوړښتونو کې د نړیوالو بشري حقونو دود او رواجول:

په یوه سیمه ییز جوړښت کې د بشري حقونو دودول او ترویج، د ناسمو انګېرنو پر وړاندې ګټوره چاره ده. نادولتي موسسې باید خپلې پرمختیایي موخې او د بشري حقونو موضوعاتو بحثونه د ارزښتونو او سیمه ییزو دودونو په چوکاټ کې تنظیم کړي. ښکاره یې کړئ چې دغه نوښتونه څه دول د ټولنې له ښه والي سره ورته والی لري او د توپیرونو پر ځای، په ګډو جوړښتونو، ګډ تمرکز لري.

پنځمه لاره - سیمه ییزه خبررسونه:

سیمه ییز پیغامونه هم یو ارزښتمن عامل دی، خپل پیغامونه د سیمې لیدلوریو او روایتونو ته په کتو تنظیم کړئ. له هغو روایتونو او بېلګو نه ګټه واخلئ چې د سیمې تجربو او ارمانونو ته انعکاس ورکړي، اړخ لګوونکي پیغام وي او د ناسم پوهاوي احتمال له منځه یوسي.

شپږمه لاره - د ځانګړي او عمومي اړیکو تر منځ توپېر:

د عمومي اړیکو تر منځ، چې کېدای شي تعمیم یا عمومي کولو ته یې دقیقه اړتیا وي، او ځانګړي اړیکې چې کېدای شي د ډلو تر منځ په خوندي او تړلې سیمه کې مخامخ بحثونه ترسره شي، توپیر ته قایل اوسئ.

اوومه لاره - منظمه څارنه:

د افغانستان د مختلفو قشرونو خلکو په منځ کې د خپلو اړیکو وضعیت په منظمه توګه وڅارئ او خپلې ستراتېژۍ د نظر غوښتنو په اساس تنظیم کړئ تر څو د خلکو له لورې د خپلو پام وړ پیغامونو په هکله ډاډ تر لاسه کړئ.

اتمه لاره - د ټولنیزو رسنیو کنټرول:

ټولنیزو شبکو ته د هر څه ورلېږلو پر وخت، محتاط اووسئ. د ټولنیزې رسنۍ لپاره د څه لیکلو پر وخت، د لیکنې ټول بعدونه په نظر کې ونیسئ. هیڅکه اجازه مه ورکوئ چې کارکوونکي د اداري له تایید پرته، څه خپاره کړي. که بودیجه او توان یې لرئ، د ټولنیزو رسنیو د اړیکو لپاره یو کارپوه په کار وګومارئ.

پاملرنه: تاسې تر موږ ډېر د خپلو فعالیتونو، پروژو او ګټه اخیستونکیو په هکله معلومات او ژور درک لرئ او د دې ډول ستراتېژیو د ناګټورتیا په صورت کې، کولای شئ د نظرونو د څرګندولو د ناسم پوهاوي د مخنیوي او خپلو خپرونو لپاره نورې ممکنه لارې پیدا کړئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۴. ځنګه کولای شو په افغانستان کې د ګټه اخیستونو د ګډون پر وړاندې ننګونو سره، سم چلند غوره کړو؟

په افغانستان کې د ګټه اخیستونکیو د ګډون د پېچلتیاوو له امله، په ځانګړې توګه داسې حالاتو کې چې پراخه موانع ستاسې اړیکې اغېزمنې کولای شي، نادولتي موسسې اړتیا لري چې نوښتګر او ستراتېژیک کره چلندونه رامنځ ته کړي. دغه ستراتېژیک نوښتونه باید په اغېزمنه توګه عملي واقعیتونه له نورو سره شریک کړي، د هغوی ملاتړ تر لاسه کړي او د خپل کار اغېزې له نړېوالو تمویلوونکیو، شریکباڼو او نړېوالې ټولنې ته څرګندې او ښکاره کړي.

لومړۍ لاره - د خوندي اړیکو لپاره له تکنالوژۍ ګټه پورته کول:

د نړېوالو شریکانو سره د تازه معلوماتو او راپورونو د شریکولو لپاره، د اړیکو خوندي او کوډ شوي وسیلې وکاروئ. د سیګنال یا خوندي برېښنالیک (ایمیل) خدمتونه کولای شي محرمانه مراسلاتو ته لاسرسی اسانه او ډاډ تر لاسه شي چې حساس معلومات له خطر سره نه مخامخ کېږي. (مهرباني وکړئ، د لا ډېرو خوندي اړیکو وسیلو او د ایمیل د خدمتونو لپاره ۸ م او ۹ م شکلونو ته مراجعه وکړئ)

دویمه لاره - له مولتي میډیا څخه په احتیاط ګټه پورته کول:

د خپلو فعالیتونو د مستند کولو لپاره له مولتي مډیا ګټه پورته کړئ، خو که د خطر احساس کوئ، له خپله ادرسه یې مه خپروئ. کیسې او جذاب انځورونه کولای شي له نړۍ سره رامنځ ته شوې تشه، ډکه کړي. خو محتاط اوسئ، د اغېزښندونکیو ویډیوګانو رامنځ ته کول، مقالو، انځورونو او هغه اینفوګرافیک چې د خلکو د ورځینې ژوند واقعیتونه، د نادولتي موسسو هڅې او د خلکو کیسې راڅرګندوي، کولای شي ګټه پورته کوونکي له لوی خطره سره مخامخ کړي. حتی که دوی له ډېرو خوندي لارو له نړیوالو بنسټونو سره چې کېدای شي د عدالت غوښتنې لپاره یو ځای شوي وي، او فعالیتونه یې خپاره شي، ښایي له ګواښ نه خالي نه وي.

درېیمه لار - له مجازي نړۍ څخه تعامل:

کله چې د مخامخ او حضوري لیدو امکان شتون و نه لري، له نړېوالو همکارانو سره د مجازي نړۍ د پلاټفورمونو له لارې تعامل ولرئ، خو له خوندي پلاټفورمونو څخه ګټه پورته کړئ. له نړېوالو تمویلوونکیو او همکارانو سره د اړیکو لپاره مجازي غونډې، وېبنارونه او کنفرانسونه تنظیم کړئ. دا ویبنارونه کولای شي ستاسې د پینل په کوربه توب، د فعالانو، ګټه اخیستونکیو او ستاسې د همکارانو د استفادې وړ وګړېو او د افغانستان د وضعیت په هکله لومړي لاس نظرونه ارایه کړي. (مهرباني وکړئ، د خوندی پلاټفورمونو په برخه کې د لا ډېرو معلوماتو لپاره ۸ م او ۱۰ م شکلونو ته مراجعه وکړئ).

څلورمه لار - نړېوالې شبکې او له هغوی سره ګډون:

له نړېوالو شبکو او له هغوی سره له ګډونه ګټه پورته کړئ، خو له هغوی سره اړیکه مو مه ښکاره کوئ، کېدای شي ستاسې کارکوونکیو، ګټه اخیستونکیو او هغو خلکو ته چې تاسې ورته خدمات ترسره کوئ، د خطر سبب شي. له نادولتي نړېوالو موسسو، د بشري حقونو مدافع ډلو او د ملګرو ملتونو له دفترونو سره د ګډون له لارې، د نادولتي موسسو د غږ قوي کولو لپاره ګټه پورته کړئ. دغه همکاري کولای شي د عدالت غوښتنې د ګډو هڅو سبب شي او په پراخه کچه د مخاطبانو ملاتړ تر لاسه کړي.

پنځمه لار - له افغانستانه بهر د منځګړي ګمارل:

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

له افغانستان څخه بهر د خپل باور وړ افراد د خپلو منځګړو په توګه وګمارئ. په بهرني هېوادونو کې د افغانستان په زړهاوو جلاوطنه، د بشري حقوقو مدافعان او مدني فعالان شتون لري چې کولای شي تاسې سره مرسته وکړي او د منځګړي په توګه ستاسې په موسسو کې وګمارل شي. له هغوی ګټه پورته کړئ چې په ازاده توګه د افغانستان دننه نادولتي موسسو او نړېوالو موسسو تر منځ اړیکې ټینګې کړي او وشي کولاي تاسې له تمویلونکیو سره وصل کړي. دا افراد کولای شي ستاسې د پیغام رسوونکیو او ستاسې د ملاتړو په توګه، له نړېوالو موسسو سره د خبرو اترو اسانتیا رامنځ ته کړي.

د نادولتي موسسولپاره د اړیکو خوندي وسیلې کومې دي؟

له څو مواردو پرته، له دې وسیلو څخه یې یوه هم په بشپړه توګه خوندي نه ده، دغه وسیلې د خپلو اړیکو د حساسیت پر بنسټ غوره کړئ.

وسیلې	کوډ کول	د ډیټا خصوصي حریم	امنیتي ځانګړتیاوې
Signal	دټولو پیغامونو، اړیکو او ګډو رسنیو په برخه کې د ډیفالټ سره سم، له پیله تر پایه کوډ کول او دخلاصو سرچینو پروتوکول کاروي.	لږ تر لږه د کاروونکي پر خصوصي حریم د تمرکز له مخې، د کاروونکي ډیټا راټولوي. خپلو سرورنو ته د سیګنال د پیغام سپارلو وروسته هغه نه ذخیره کوي.	د پیغامونو د محو کولو وړتیا، د نمایش د صفحې امنیت لرونکي (له سکرین شاټ څخه مخنیوی) او د نوم لیکنې بندوونکي (PIN د حساب د خوندیتوب په موخه) خدمات وړاندې کوي
Wire	په ډیفالټ ډول له پیله تر پایه پورې له پیغامونو، اړیکو، غږیزو او انځوریزو پیغامونو کوډ کولو کې ګټه پورته کوي او د سیګنال د خلاصو سرچینو پروتوکول، د دې د برخورد ګټه ده.	د کاربېدونکي وسیلې ځینې برخې، لکه نوم او نور مشخصات، د تلیفون شمېره (که ارایه شي) ، او د ایمیل یا بریښنالیک ادرس (که ارایه شي) د حساب د مدیریت د موخو لپاره راټولوي.	د یوې مودې لپاره د پیغامونو د خوندیتوب له ځانګړتیاوو ملاتړ کوي په اتومات ډول له یوې تعین شوې دورې وروسته له منځه ځي او د خصوصي حریم برخه پراخوي. سربېره پر دې، د Man-in-the-Middle د حملو د مخنیوي لپاره، د کاربدونکي وسیلې وړتیا هم ډېروي.
Threema	د متن، غږ، ویډیو او فایلونو سرتاسري کوډ کېدو لپاره د سیګنال د پروتوکول پر مخ جوړشوي پروتوکول Proteus نه ګټه پورته کوي. ټولو اړیکو لکه، پیغامونو، اړیکو، تلیفون او فایلونو ته له سرتاسري کوډ شویو توکیو نه ګټه اخلي. د NaCl له کوډ کېدو نه ګټه اخلي او د اړیکو پر وخت یوازې کاروونکي کولای شي پیغامونه ولولي.	د ډیټا په کارولو کې د کم لګښت لپاره طراحي شوی، د بریښنالیک یا تلیفون شمېرې ثبتولو ته اړتیا نه پیښېدل. هر کاروونکي ته په تصادفي توګه د Threema ID رامنځ ته کوي او د نه پېژندنې وړتیا ډېروي. د مخاطبینو او ډلو اطلاعات د کاروونکي په دستګاه کې ذخیره کېږي، نه د دې اپلیکیشن په سرورونو کې.	د شخص د ځانګړتیا پورې منحصر دی چې کاروونکي ته دا امکان ورکوي چې مخاطبان په کیو آر کودونو تایید کړي او د یو امنیتي پوخ/ پردې له لارې د هویت د احتمالي جعل یا Man-in-the-Middle د حملو د مخنیوي وړتیا اضافه کړي

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

غیر متمرکز جوړښت اود TOR لوری پیدا کوونه، نه یوازې دا چې د خصوصي حریم قوي ډیټا راکوي، بلکه د شبکې د څارنې او سانسور پر وړاندې هم انعطاف منونکې ده. په Session کې د مرکزي سرورونو نشتون په دې معنی ده چې هیڅ ډول مرکزي نقطه شتون نه لري چې وشي کولای د کاروونکي اطلاعاتو په هکله وړاندیز وکړي یا یې هک کړي.	له نوم لیکنې وروسته، د (PII) هیڅ ډول معلومات نه راټولوي او یوازې د کاروونکي د پېژندنې لپاره، د ناستې په برخه کې پوهاوی تر لاسه کوي، دا طریقه د تلیفون شمیرو یا بریښنالیک پتې سره د حسابونه نه تړلو له امله د خصوصي حریم ساحه پراخوي. دا په داسې بڼه ډیزاین شوی چې د کم ترکمو ډیجیټلي نښې نښانې د راپیدا کولو وړ کرځوي او د کاروونکي پټ پاتې کېدا چانس تر کافي حده پورته وړي.	د پیغامونو لپاره د سیګنال د پروتوکول پر اساس، له پیله تر پایه له کوډکولو ګټه اخلي. هغه څه چې Session له نورو جلا کوي، د هغې د TOR پروتوکول دی چې د معلوماتو تولګه یا پراخه معلومات له پېژندنې پټ ساتي او د دې تشخیص چې څوک له چا سره په اړیکه کې دی، پټ ساتي.	Session
په اتومات ډول د پیغامونو د له منځه وړلو ورتیا لري او په ستګاه کې د یوې نوې برنامې لپاره، د کوډ پین ته اړتیا لري.	د WhatsApp یا Messenger په پرتله محدوده ډیټا راټولوي او کاروونکي په خصوصي حریم تمرکز لري، د تلیفون شمېرې ته اړتیا لري.	د پیغامونو او اړیکو لپاره د ډیفالټ له مخې، له پیله تر پایه پورې کوډ کول چمتو کوي.	Viber
دوه مرحله ییز تایي ارایه کوي، خو د میټا ډیټا د مدیریت چارې او کړنې د انعکاس او څارنې له خطر سره مخ دي.	له کوډ کولو سره سره، د واټس اپ او نورو پلیټفارمونو تر منځ یې د معلوماتو شریکولو په اړه اندېښنې شتون لري،د تلیفون شمېره حتمي ده.	د سیګنال له پروتوکول نه په ګټه اخیستنه، پیغامونو او اړیکو ته له سره تر پایه په ډیفالټ توګه کوډ کول ارایه کوي.	WhatsApp
په مخفي چټونو کې د پیغامونو د تخریب وړتیا ارایه کوي. او د یو ثالث شخص د برنامو لپاره یو پرانیستی API لري چې کېدای شي لا ډېر امنیتي ملاحظات رامنځ کړي.	پخپلو سرورونو کې ډیټا ذخیره کوي تر څو د دستګاګانو تر منځ د همغږي زمینه مساعده کړي. پراخه ډیټا ته لاسرسی لري، د تلیفون شمېره حتمي ده.	یوازې په مخفي چټونو کې سر تر پایه کوډ کول خوندي کوي خو نه په معمولي پیغامونو کې.	Telegram
د خصوصي حریم کنترول یې د خپلو سیالانو په پرتله کم دي.	د ډیټا د راټولولو میتودونه یې چندان واضح نه دي او د کاروونکیو د خصوصي حریم اړوند اندېښنې رامنځ ته کوي.	د انځوریزو او غږیزو اړیکو لپاره د کوډ کولو قابلیت ارایه کوي خو د پیغامونو په کوډ کولو کې روڼتیا نه لري.	IMO
مخفي اختیاري مکالمې وړاندې کوي، خو په ډیفالټ توګه، مکالمې نه کوډ کېږي.	د فیسبوک د ایکو سیستم یوه برخه ده، د هدفمند تبلیغاتو پلاټفورمونو کې یې د ډیټا شریکولو امکان شته دی.	یوازې په (مخفي مکالمو) کې له سره تر پایه کوډ کول وړاندې کوي. معمولي پیغامونه او	Messenger (Facebook Messenger)

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

	اړیکي کوډ کېږي، خو فیسبوک کولای شي لاسرسی ورته ولري.		
Delta Chat	له Autocrypt څخه د نورو کاروونکيو د اړیکو ټینګولو پر مهال، د ایمیل په اتومات ډول کوډ کولو له نور ورتیا لرونکیو Autocrypt نه ګټه پورته کوي.	د ایمیل په پرتوکولونو تکیه لرونکې او یو غیر متمرکز سیستم وړاندې کوي. پیغامونه د ایمیل په سرورنو کې ذخیره کېږي خو کوډ کېږي نه.	له مرکزي سرور پرته، غیرمتمرکزه طراحي، معمولاً پر برېښنايي اړیکو متمرکزه ده
Element (formerly Riot)	د اړیکو او چټونو د سر تر پایه کوډ کولو لپاره د Matrix د پروتوکول له لارې ګټه پورته کوي.	ګډونوال کولای شي خپلو سرورونو ته کوربه توب ورکړي او د خصوصي حریم کنټرول ډېر کړي. پدې توګه، ستاسې خوندیتوب، ستاسې د سرورونو په تنظیمولو پورې اړه لري.	د کوډ شویو ډله ییزو پیغامونو، د ډیټا د ډول ادغام او د اصلاح کولو اختیارونو ملاتړ کوي.

۸ م شکل: نادولتي موسسو ته د اړیکو تر ټولو خوندي وسیلي.

نادولتي موسسو ته د اړیکو تر ټولو خوندي وسیلي کومې دي؟

له څو مواردو پرته، له دوی څخه یو ایمیل هم خوندي نه دی. تاسې يې د خپلو اړیکو د اهمیت او حساسیت له مخې ځان ته غوره کړئ.

وسیلې	کوډکول	د خصوصي حریم معلومات	امنیتي ځانګړتیاوې
Riseup	Riseup د مدني حرکتونو مشرانو او فعالانو ته د اړیکو د خوندي وسیلو په وړاندې کولو او د کاروونکیو د نه پېژندنې په هکله خپله قوي ژمنتیا لري.	Riseup چې د خپلو کاروونکیو خصوصي حریم خوندي ساتلو او د نه پېژندلو ورتیا ته ژمن دی، د خپلو کاروونکیو پورې اړونده هیڅ ډول شخصي اطلاعات نه ذخیره کوي او په منظمه توګه اطلاعات ړنګ او له منځه وړي. دغه پلاټفورم ثالثو اشخاصو سره د ډیټا نه شریکولو په برخه کې د خپل قوي دریځ له امله پېژندل شوی پلاټفورم	په دې پلاټفورم کې VPN خدمتونه شامل دي چې په انلاین بڼه د کاروونکیو د خصوصي حریم په لا خوندي کېدو کې مرسته کوي. همدارنګه Riseup پخپلو خدمتونو یا چوپړتیاوو کې FA2 هم ورزیاتوي تر څو حساب ته د لاسرسي لپاره یو بل امنیتي پوخ یا پرده شتون ولري.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

		دی. خو که د قانون د حکم سره سم مجبور کړای شي.	
	وبسایت		https://riseup.net/en/email
Autistici/Inventati (A/I)	د کوډشویو برېښنالیک مخابراتو لپاره د PGP د کارولو وړاندیز کوي، د دوی خدمات، د برېښنا لیک او ویب کوربه توب سره، په انتقال کې د معلوماتو لپاره SSL/TLS کوډکولو اسانتیا او چمتووالی برابروي.	د کاروونکیو د خصوصي حریم خوندیتوب ته ژمن دی، نه یې تعقیبوي او نه یې له ګواښ او خطر سره مخامخوي.	د دې خدمتونه د هغو فعالانو او کسانو لپاره ډیزاین شوي چې د خصوصي حریم په هکله اندېښمن دي، VPN او TOR له لارې د نه پېژندنې خدمتونه وړاندې کوي.
	وبسایت		https://www.autistici.org
ProtonMail:	ایمیلونه ته سر تر پایه کوډ وړاندې کوي او ډاډ درکوي چې یوازې لېږونکی او تر لاسه کوونکی کولای شي منځپانګه ولولي.	د کوډ کولو په برخه کې، صفر ته له لاسرسي ګټه اخلي، په دې معنی چې: حتی ProtonMail هم نشي کولای ستاسې د ایمیلونو منځپانګې ته لاسرسی ولري.	د ProtonMail سرورونه چې د سوئیس د خصوصيحریم د خوندیتوب تر قوانینو لاندې کار کوي، په سوئیس کې رامنځ ته شوي چې د خصوصي حریم د قوي خوندیتوب له امله پېژندل شوی او ډېر ګټور دی.
	وبسایت		https://proton.me/mail
Tutanota	ایمیلونه او ضمیمې په اتومات ډول کوډ کوي او اړیکې لا ډېرې خوندي کوي.	حد اقل شخصي اطلاعات راټولوي او د نه پېژندنې په برخه کې د برترو ځانګړتیاوو لاسرسی مساعدوي.	دا پلاټفورم په المان کې دی، او د اروپا GDPR د سختو مقرراتو درلودونکی دی چې د کاروونکیو د خصوصي حریم په خوندیتوب باندې تاکید کوي.
	وبسایت		https://tuta.com
Disroot	پر خصوصي حریم متمرکز یو پلاټفورم چې فعالانو او نادولتي موسسو ته ایمیل، د ذخیره کولو فضاء او نور خدمتونه وړاندې کوي.	د ډېټا د خوندیتوب او د ځارنې پر وړاندې اړیکو او د کوډ کولو او امنیتي اقداماتو اړوند تاکید کوي.	د ټولنې په کچه د یو پلاټفورم په توګه، د روڼتیا لپاره Disroot، د بیان ازادۍ او خصوصي حریم ته ارزښت قایل دی او د فعالانو اړتیاوې پوره کوي.
	وبسایت		https://disroot.org/en

۹ م شکل: نادولتي موسسو ته د ایمیل د خدمتونو تر ټولو خوندي وړاندې کوونکي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

امن ترین ابزارهای کنفرانس تصویری برای موسسات غیردولتی کدام ها اند؟

له څو مواردو پرته، د ویډیو کانفرانس له دغو وسیلو هیڅ یوه پې خوندی نه ده. تاسې پې د خپلو اړیکو د حساسیت له مخې د ځان له پاره وټاکئ.

وسیلې	امنیتي ځانګړتیاوې	د خصوصي حریم معلومات	کوډ کول
Jitsi Meet	ویډیویي کنفرانسونو ته د سرتاسري کوډ کول ارایه کوي او د اړیکو خوندي او امن کانالونه تظمینوي.	د پرانیستي سرچینې پلاټفورم له ځانګړتیا سره سره وړیا هم دی، کاروونکي کولای شي د خصوصي حریم د لا خوندیتوب لپاره، کوربه توب وکړي.	د پټ نوم خوندي شوي خونې وړاندې کوي، په دې خونو کې د ګډونوالو د لید کنټرولولو سره، کاروونکي غونډې ته د ننوتلو لپاره باید پاسورډ ولري.
	وبسایت	https://meet.jit.si	
BigBlueButton	له کوډ شویو ورننوتو ملاتړ کوي او د غونډو د او شخصي حریم د خوندیتوب لپاره ځانګړې اسانتیاوې لري،	دا پلاټفورم د زده کړې او روزنې لپاره طراحي شوی، همدارنګه د غږ ثبتولو کنټرول شوی لاسرسی او خاصې ځانګړتیاوې ارایه کوي.	دغه پلاټفورمونه د لاسرسي او په خپلخوښې توګه غونډو ته د ورننوتلو وړتیاوې وړاندې کوي، د غونډو کنټرول د اسانچارې په لاس کې دی، او اسانچارې ته د تختې پر مخ د لیکلو لپاره مرستندویه وسیلې هم اماده کوي.
	وبسایت	https://demo.bigbluebutton.org	
Whereby	په پلاټفورم کې ترسره کېدونکیو ټولو غونډو او اړیکو ته سرتاسری پاسورډ وړاندې کوي.	غونډو ته د ننوتو پاسورډ د تنظیم امکان او کنټرول ته د لاسرسي وړتیا برابروي.	د ننوتو لپاره د ورکړل شوي‌کوډ له لارې، د مجازي غونډې خونې او د انتظار د خونې ځانګړتیاوې په امنه توګه خوندي شوې وي.
	وبسایت	https://whereby.com	
Blue Jeans	د غونډو د بهیر په دمه یا وقفه کې کوډ ورکول او په عین حال کې د تلیفونونو او کنفرانسونو په بهیر کې د کاروونکي ډیټا خوندي کوي.	د خصوصي حریم د خوندیتوب ځانګړتیاوې لکه د ډیټا پوښښ او د غونډې د ګډونوالو کنټرول شوی ګډون ته زمینه سازي کوي.	د ګډون ځانګړتیاوې، د خصوصي حریم کنټرول او د غونډو د امنیت د څارنې کنټرول ته زمینه برابروي.
	وبسایت	https://www.bluejeans.com	
GoToMeeting	د اړیکو او کانفرانس په بهیر کې د ډیټا د خوندیتوب لپاره، د کوډ کولو له قوي پروتوکول نه ګټه اخلي	د ډیټا د خوندیتوب د مقرراتو رعایت کوي، خو کېدای شي د کاروونکي ډیټا د خدمتونو د شبه والې لپاره راټوله شي.	د غونډو د بندولو یا ترلو د ځانګړتیاوو لرونکې ده. په انټرنیټي پاڼو کې د وړاندې کولو محدودیت رامنځ ته کوي او تاسې ته دا حق درکوي چې څوک له اجازې پرته داخل نشي.
	وبسایت	https://www.goto.com/meeting	

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

Facetime/iMessage (Apple)	د ایپل په ایکو سیستم کې د پیغامونو، غږیزو او انځوریزو اړیکو د سر نه تر پایه پورې د کوډ کولو قابلیت.	د ایپل کوډ شویو معیارونو په دلیل، له خصوصي حریم د قوي خوندیتوب قابلیت او د کاروونکي خصوصي حریم ته شوې ژمنه.	د مخاطبانو د بندولو قابلیت لرونکې، برنامو ته د هویت تصدیق یا Face ID/Touch ID او په اتومات ډول د iMessages بشپړول.
	وبسایت	https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web	
Google Meet	G Suite ټولو کاروونکیو ته د سر تر پایه کوډ کولو سره سره د خوندي انځوریز کنفرانس وړاندې کول.	Google امنیتي معیارونه د ډیټا د خوندیتوب ضمانت کوي، خو کېدای شی د کاروونکي خصوصي حریم، د تجارتي تبلیغاتو لپاره د ډیټا د راټولنې تر اغېز لاندې راشي.	د غونډو د ترلو یا قفل کولو ورتیا لرونکی، د خصوصي حریم کنترول او د غیر مجاز لاسرسي د مخنیوي اقدامات.
	وبسایت	https://meet.google.com	
Duo (Google)	د اړیکو او ویدیویي چټونو لپاره له سر تر پایه کوډ کولو نه ګټه پورته کوي، او اړیکې د دریېمګړي له لاسرسي نه خوندي ساتي.	پر خصوصي حریم د Google د امنیتي ستنډردونو رعایتولو سره سم، د خدمتونو د ښه والي لپاره د کاروونکي ډیټا راټولوي.	ویدیویي اړیکې کوډ کېږي تر څو د اړیکو پر وړاندې له مداخلې مخنیوی وشي او د دوه مرحله یي هویت د تصدیق لپاره د Face Match ورتیا لرونکی.
	وبسایت	https://meet.google.com/calling/	
Microsoft Teams	د کوډ کولو د پراخه پروتوکول سره، د خوندي ذخیرې او د انتقال ورتیا لرونکی	د کاروونکیو لپاره د پرمختللي کنترول او تنظیم له مخې، د ډیټا د خصوصي حریم لپاره د سختو مقرراتو درلودونکی.	د غونډو او اړیکو د کوډ کولو ورتیا لرونکی، د دوه مرحله ییز هویت تصدیق،خوندي چینلونه او د تطبیق وړ ستنډرډونه.
	وبسایت	https://www.microsoft.com/en-ca/microsoft-teams/log-in	
Xspace	Xspace د ویدیویي اړیکو لپاره سر تر پایه کوډ کول برابروي او د غونډو په بهیر او فضايي خصوصي اړیکو کې، د اړیکو د خوندی انتقال تضمین کوي.	د کاروونکي د ډیټا خوندیتوب ته لومړیتوب ورکوي او د خصوصي حریم د قوانینو سره سم د ډیټا تضمین کوي.	د غونډو خوني د ورننوتو په کوډ سره خوندي کېږي، غونډو ته د لاسرسي په برخه کې اسانچاری په مطلقه توګه برلاسی دی او د اسنادو د شریکولو لپاره خوندی ځانګړتیاوې لري.
	وبسایت	https://twitter.com/	
Clubhouse	Clubhouse د سر تر پایه پورې د کوډ کولو د ورتیا د نه شتون له امله له نیوکو سره مخ شوی، چې د پلاټفورم په غږیزو چټونو کې د خصوصي حریم د خوندیتوب په هکله یې اندېښنې راپارولې دي.	کاروونکي د ډیټا د خوندیتوب د میتودونو د دلیل او مخکنیو پېښو کې چې، پې له بلنې د افرادو د ګډون له امله خصوصي مکالمو ته لاسرسی پیدا کوي، د خصوصي حریم اړوند یې اندېښنې راولاړې کړې دي.	د کانفرانس د عملیاتي سیستمونو په پرتله د خبرو اترو د اسانه کولو او کنټرول لپاره محدودې وسیلې لري، چې کولای شي د کاروونکیو خوندیتوب اغېزمن کړي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

	وبسایت	https://www.clubhouse.com/
Zoom	په لومړیو وختو کې د لومړني کوډ کولو په اړه له نیوکې سره مخ شوی، خو له هغه وخته راهیسې یې د ټولو غونډو او پیغام رسوني او د سر تر پایه کوډ کولو په برخه کې خپلو امنیتي پروتوکولونو ته وده ورکړه.	په دې پلاټفورم کې د روڼتیا او دقیقي پلټنې وروسته، د ډیټا د خصوصي حریم د میتودونو ښه والی او خوندیتوب، د کاروونکیو لپاره د معلوماتو او د امنیتي ترتیباتو د کنټرول لپاره واکونه چمتو کول. د امنیتي ځانګړتیاوو پراخه زمینه مساعدول لکه د کوډ یا پټنوم خوندیتوب، د انتظار خونې، د اسانچارۍ کنټرولول او د کاروونکي د خوندیتوب لپاره له پیله تر پایه، د اړیکو خوندیتوب.
	وبسایت	https://zoom.us/

۱۰م شکل: نادولتي موسسو ته د انځوریز کانفرانس تر ټولو خوندي وسیلې.

موسسات غیردولتی هنگام برقراری ارتباطات از چه اصطلاحاتی باید اجتناب کنند؟

کله چې نادولتي موسسې اړیکې ټینګوي،په ځانګړې توګه په هغه چاپېریال کې چې د منځپانګې څارنه عامه وي، د ځینو اصطلاحاتو نه کارول کولای شي د خطرونو کچې کمېدو او پر دوی د څارنې اړیکو سره مرسته وکړي. ځینې هېوادونه شته چې د څارنې د ورتیا ودې ورکولو ته له پرمختللې تکنالوژۍ ګټه اخلي. له ۲۰۱۴ کال راهیسې دغې موضوع د تکنالوژۍ له پرمختګ سره پراختیا موندلې او د څارنې هر اړخیز او پېچلې میتودونو کارولو امکان یې برابر کړی دی. په اوس وخت کې، د یادولو وړ ده چې د انلاین فعالیتونو په څارنه کې د مصنوعي ځیرکتیا نه ګټه اخیستلو د خصوصي حریم د خوندیتوب په برخه کې نوې اندېښنې رامنځ ته کړې دي.

د څارنې بنو د استخباراتي ایجنټانو د کارې ساحې څخه، سوداګریزو او دولتي هارډویز او سافټویر سیستمونو ته لار پیدا کړې او ور انتقال شوي دي. له دې مخکې، هغه خلک څارل کېدل چې ملي امنیت ته د خطر پیدا کېدو اندېښنه به موجوده وه. خو اوس، د حکومت لخوا د انټرنیټ د څارنې او فلټر کولو سیستمونو له امله، مور ټول په احتمالی توګه، د شکمنو او مظنونینو په کتار کې حسابېږو.

کارېدونکې تکنالوژۍ د کاروونکیو تر منځ توپیر نه مني او د هر چا پر وړاندې یو ډول چلند ترسره کوي، ایمیلونه، پیغامونه او زموږ د ویب سایټونو براوزرې د ځانګړو کلیمو او لیکنو لپاره سکن کوي. د شکمنو مواردو په پېژندلو، یا د څارنې ټیمونو ته خبر ورکوي او یا مو هم اړیکې پرې کوي. د (encryption) کوډ کېدل د خصوصي حریم لپاره انلاین اخرنی مورچل او سنګر دی چې موږ ته ادا ورتیا راکوي چې خپلې اړیکې خوندی او امنې کړو تر څو یوازې د نظر وړ او مطلوب تر لاسه کوونکي وشي کولای هغه کوډ کړې او وې لولي.

په ټوله نړۍ کې نادولتي موسسې د پام وړ خطرونو سره مخ دي، له دې جملې څخه دوړل څارنه او محدودیتونه چې د دوی اړیکې محدودوي او ډېرې وختونه د دوی د ملاتړ په برخه کې د سختو پایلو سبب ګرځي. سربېره پر دې، د دوی د ډیجټال وسیلو امنیت په پراخه کچه له خطر سره مخ دی. ایمیلونه مقصد ته نه رسېږي، د ټولنیزو رسنیو حسابونه

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

له خطر سره مخ او هیک کېږي، انټرنیټي اړیکې د باور وړ نه دي، د دوی اړیکې په دقت سره څارل کېږي، د دوی ځیرک تلیفونونه او کمپیوټري دستګاګانې يې ضبطېږي او انټرنیټي Malware یا بدافزار د دوی ارزښتمنه ډیټا له منځه وړي.

دغه ډول ننګونې، پر انلاین منځپانګې د چارواکیو سختو څارنو او څېړنو په شمول او د نادولتي موسسو لخوا د نامطلوبو اړیکو ګړندی غچ اخیستل، په ټوله مانا مستند شوي مسایل دي. نادولتي موسسې تل په ډیجیټل پلاټفورمونو لکه خبري سایټونو، ټولنیزو رسنیو او ویبلاګونو کې څارل کېږي. دوی له ډېرو موانعو سره مخ دي، لکه ډیجیټل ویش یا Digital divide، د ډیجیټل وسیلو له لارې د جبر او زیاتي فعالېدل، له ملي امنیت د سرغړونې په پلمه د حقونو سرغړونه او نقض، د پراخه سایبري زیانونو او په ټوله کې د ډیجټال عمومي ناامنیو سره مخ دي. د کمپیوټر، ځیرک موبایلونو او له انټرنیټ سره اشنايي او مهارتونو په تر لاسه کولو کې فعالان او د بشري حقونو مدافعین کولای شي له خپلو نوښتونو څخه په ښه توګه ساتنه وکړي او په اغېزناکه توګه له خپلو حقونو او د هغو خلکو له حقونو چې دوی يې د ملاتړ اراده لري، دفاع وکړي.

پر ټولنیزو رسنیو د څارنې Freedom House د ګذارش پر اساس، په ټوله نړۍ کې دولتونه، له مستبدو رژیمونو نیولې د ټیټې کچې تر دولتونو، په ټولنیزو رسنیو کې د خلکو د ډله ییزې څارنې لپاره د پرمختللې تکنالوژۍ په برخه کې، په ډېره کچه پانګونه کوي. دا عمل چې د دودیز جاسوسي وسیلو (Spyware) په پرتله پراخه، په اتومات ډول د ډیټا راټولول، د ډیټا د پراخه حجم د ډیجیټل ارتباطي پلاټفورمونو تنظیم، تحلیل او تجزیه کول دي. د شخصي او سیاسي موخو لپاره د دغه پلاټفورمونو نه ګټې تر لاسه کولو ته په پام سره، خلک پر ټولنیزو رسنیو څارنه پرغلیزه چاره ګڼي. د چین او ایران په څېر هېوادونو کې، چاروا‌کیو په زرهاوو اشخاص د خلکو پر انلاین فعالیتونو څارنې او د نظام د مخالفینو په هکله ګزارش ورکولو ته راټول کړي او په کار ګومارلي دي. سر بېره پر دې، د (AI) مصنوعي ځیرکتیا پرمختګ د څارنې سیستمونو ورتیا لوړه کړې چې کولای شي اړیکې تحلیل او تجزیه کړي او کولای شي د کاروونکیو د احساساتو او موقعیتونو معلومولو ساحه پراخه کړي او ښايي د انسان له ورتیا پورته، ببلګې او معلومات راڅرګند کړي.[2]

په افغانستان کې د طالبانو موقته اداره، بهرنیو هېوادونو سره د افغانانو د اړیکو د کنټرول په برخه کې له خنډونو سره مخ ده، دا کار د چین او ایران هېوادونو د نه ملاتړ او د تکنالوژۍ په برخه کې پرمختګ نه کولو له امله ډېر وخت ته اړتیا لري او ننګونکې ده. لکه په ایران، چین او روسیې کې د اقداماتو په څېر پر ټولنیزو رسنیو څارنه، د طالبانو د موقتي ادارې لپاره یوه استراتېژیکه وسیله ګرځېدلې چې د دوی د مخالفینو غږونه کنټرول او وځاري. په اوس وخت کې، د طالبانو موقته اداره د خپلو ځانګړو ستراتېژیو نه ګټه اخلي او د خپل ځواک د پیاوړي کولو لپاره پر ټولنیزو رسنیو د څارنې له مخې، د سیمه ییزو نورمونو په کارولو سره ورته تکتیکونه کاروي. د نادولتي موسسو د استازو او هغو فعالانو په وینا چې په دې اړوند مرکې ورسره ترسره شوي دي، د طالبانو موقته اداره کټ مټ لکه د ایران او چین ستراتېژۍ کاروي چې په افغانستان او له افغانستانه بهر افغانانو د ټولنیزو حسابونو، ادرسونو او شبکو د څارنې په موخه يې په زرهاوو تنه ګومارلي او هر څه څاري او تعقیبوي يې. د یوې نادولتي موسسې په توګه چې په داسې شرایطو کې فعالیت کوي، د مدني ټولنې د موضوعاتو اړوند په خواله رسنیو کې د فعالیتونو ډېروالی ښايي تاسې د طالبانو د موقتي ادارې له څار سره مخ کړي.

> د حکومتونو د سختې څارنې یوه بېلګه د چین د سرو زرو ډال یا ګولډن شیلډ دی چې د یوې پرمختللې تکنالوژۍ په توګه عمل کوي او د نورې نړۍ له ویب څخه په جلا یو انټرنیټي زیربنا باندې کار کوي تر څو د مرکزي ډیټابیسونو او هر اړخیزې څارنې له لارې خپل ملي امنیت خوندي کړي. هیڅ ډول ډیټا له فلټر کولو پرته نشي ننوتلای، د سرو زرو ډال په شبکه کې د پراخه څارنې ورتیا په یو ځای کولو سره، د منځپانګې فلټر مختلفو عامه او خصوصي معلوماتي وسیلو ته غځېدلې او د اغېزناک کنټرول او څارنې لپاره، د پېچلې ټیکنالوژۍ کارولو ورتیا لري.

[2] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

په رسنیو یا عمومي غونډو کې ویناء، د بشر له حقونو څخه دفاع یا له اداري فساد سره مبارزه د څارنې او تعقیب چانس ډېروي. مهم ټکی دا دی چې یوه هدفمنده څارنه جرمي فعالیت ته اړتیا نه لري، ځکه چې په ټوله نړۍ کې دولتونه د پېچلیو سایبري الګوریتمونو له لارې، پر متخصصینو لکه فعالانو، خبریالانو او نادولتي موسسو باندې د څارنې لپاره ګټه پورته کوي. دولتونو ته د څارنې په پایله په لاس ورغلې ډیټا دوی د فعالانو د سپکاوي لپاره کاروي، په لاس جوړ شویو یا خودساخته تورونو یا د دوی د نیولو په تنظیمولو کې ترې ګټه اخیستل کېږي، او همدارنګه دغه لاس ته ورغلې ډېټا د ثبوت په توګه کارول کېږي او د مدني ټولنو د بنسټونو په مشروع او برحقه برنامو کې، د دولتونو لخوا ستر ګواښ او نا عادلانه لاسوهنې ته زمینه مساعدوي. په دې توګه، افغانستان کې د اړیکو ټینګولو پر مهال، نادولتي موسسې باید ډېر پام وکړي چې د هغو اصطلاحاتو کارولو څخه چې د سپکاوي سبب کېږي او یا غلطې تعبیرېدای شي، ډډه وکړي. په یاد ولرئ چې که غواړئ په افغانستان کې مثبت تغیرات رامنځ ته کړئ، د مسلکي چلند غوره کول د فعال یا محوره چلند په پرتله، خوندي او امن دی.

ایا نادولتي موسسو ته د ټولنیزو رسنیو له پلاټفورمونو ګټه اخیستل خوندي دي؟

په افغانستان کې د نادولتي فعالو موسسو لپاره د ټولنیزو رسنیو له پلاټفورمونو نه ګټه اخیستل کېدای شي هم ګټور او هم ننګوونکي وي. د ټولنیزو رسنیو خطرونو د کچې کمولو او د کارولو د ګټو په برخه کې، نادولتي موسسې باید د ټولنیزو رسنیو لپاره امنیتي پروټوکولونه باید ولري، د ټولنیزو رسنیو لپاره روښانه پالیسي رامنځ ته کړي، د ډیجیټال امنیت په برخه کې باید خپل کارکوونکي وروزي، او په دې پلاټفورمونو کې باید په عاقلانه او مسولانه توګه له خلکو سره په اړیکه کې اوسي. دلته مدني بنسټونو ته د ټولنیزو رسنیو کارولو څو ګټې او زیانونه درپېژنو.

ا . ګټې

لومړۍ ګټه ـ تعامل او لاسرسی:

د ټولنیزو رسنیو پلاټفورمونه نادولتي موسسو ته یوه ارزښتناکه وسیله ده چې په سمه توګه کارولو سره یې کولای شي د خپل لاسرسي ساحه پراخه کړي، او د نړۍ له خلکو سره د مستقیم تعامل له لارې د دوی د موخو د پوهاوي په برخه کې، خپل معومات ډېر کړي. ټولنیزو رسنیو ته د پراخه لاسرسي او تعاملي ماهیت نه به ګټه اخیستنه، نادولتي موسسې کولای شي په اغېزناکه توګه له خپلو کارکوونکیو سره اړیکې ټینګې کړي، اغېزناکه کیسې او روایتونه شریک کړي او د مختلفو مخاطبانو له منځه د ځان لپاره ملاتړ تر لاسه کړي. دغه ډیجیټالي بڼه خپلول نه یوازې دا چې د دوی پیغامونو ته قوت وربخښي، بلکه د دوی د ملاتړو په منځ کې د اړیکو او ګډون احساس ته وده ورکوي او بې له ځنډه تعامل ممکنوي. په پایله کې، ټولنیزې رسنۍ د نادولتي موسسو لپاره د یو متحرک ګتلست په توګه کار کوي چې غواړي مثبت بدلون رامنځ ته کړي او خپلو نوښتونو ته پراخه پاملرنه راواړوي.

دویمه ګټه ـ عدالت غوښتنه او شبکه جوړول:

د ټولنیزو رسنیو پلاټفورمونه نادولتي موسسو ته د ټولنیز بدلون د ملاتړ لپاره، د دوی د موخو د ملاتړ لپاره، د همفکره او همغږو موسسو تر منځ د اړیکو رامنځ ته کولو لپاره او د تمویلوونکو یا بسپنه ورکوونکیو تر منځ، څو اړخیزه وسیلې چمتو کوي. نادولتي موسسې کولای شي د ټولنیزو رسنیو د ځواک نه په ګټه اخیستنه، په ارزښتناکه مسایلو کې د خلکو

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د پوهاوي لپاره، په اغېزناکه توګه ګټه پورته کړي، له کمپاینونو نه د خلکو ملاتړ پراخه کړي، او د ګډون هغه لارې رامنځ ته کړي چې د خپلو فعالیتونو کارنده اغېز ډېر کړي. دغه ډیجیټلي لیدلورى نه يوازې دا چې د پیغامونو د خپرولو لپاره د یوه پلاټفورم په توګه کار کوي، بلکه یوه شبکه یېزه ټولنه هم رامنځ ته کوي چې د مثبتو تغیراتو په رامنځ ته کولو او د ډلیزو موخو په پرمخ بیولو کې، ټولنیز نفوذ او اغېز ته وده ورکوي.

درېیمه ګټه - مستقیمې اړیکې:

له اوربېدونکیو سره مخامخ او مستقیمې اړیکې درلودل، د نادولتي موسسو د موخو په تر لاسه کولو کې مهم رول لري. د ویب سایټونو پر خلاف چې ډېرى وختونه له لیدونکیو سره اړیکې ټینګوي، ټولنیزې یا خواله رسنۍ د ملاتړو او تمویلوونکیو سره د دوه اړخیز تعامل اسانتیا رامنځ ته کوي او اجازه ورکوي چې په سمدستي او فعاله توګه اړیکه ټینګه شي. د دودیزو معلوماتو سره سم، د اړیکو دغه وسیلې په مستقیمه توګه کولای شي د پوهاوي لوړولو نه نیولې د مطلوب فعالیت تر ترلاسه کولو پورې، د ادارو کاري بهیر ته په اغېزناکه توګه چټکتیا او پرمختګ ورکړي.

څلورمه ګټه - د مالي مرستو راجلبول:

په افغانستان کې ټولنیزې رسنۍ د نادولتي موسسو د پروژو په برخه کې د مالي مرستو، د بسپنې ورکوونکیو د ګډون او دخلکو د تمویل د کمپاینونو د همغږي کولو او د طرحو د جلبولو د اسانتیا لپاره، یوه حیاتي وسیله ګڼل کېږي. له دې پلاټفورمونو نه ګټه اخیستل نادولتي موسسو ته دا فرصت په لاس ورکوي چې د اړیکو متقابلو اسانتیاوو ته پراخه لاسرسی ولري، د خپلو کیسو او روایتونو له لارې د احتمالی ملاتړ کوونکیو پام راجلب کړي او له تمویلوونکیو سره اړیکې ټینګې کړي تر څو د خپلو بشردوستانه او خیر ښېګڼو برنامو پلي کولو ته مالي سرچینو ته لاسرسی پیدا او ګټه ترې پورته کړي.

پنځمه ګټه - د مطالبو خپرول:

د اطلاع رسونې په ستراتېژۍ کې د ټولنیزو رسنیو ځای پر ځای کول او شاملول، نادولتي موسسو ته دا زمینه مساعدوي تر څو حساس موضوعات په ټاکلي وخت، ارزښتناکه او ګټوري سرچینې، بېړنۍ اعلامیې او روزنیز موضوعات په اغېزناکه توګه خلکو ته خپاره کړي. نادولتي موسسې کولای شي د ټولنیزو رسنیو د پلاټفورمونو له لارې په چټکۍ سره مهم اطلاعات خپاره کړي، له خپلو اوربېدونکیو سره په اړیکه کې اووسي، پېښېدونکیو حالاتو ته اغېزناک او موثر ځواب ورکړي او ډاډ تر لاسه کړي چې د دوی اړیکې نه یوازې دا چې پر خپل وخت دي، بلکه پراخه او اغېزناکه هم دي.

شپږمه ګټه . د اړیکو او پوهاوي کچه پراخول:

ټولنیزې رسنۍ د اړیکو په برخه کې د یوې قوي وسیلې په توګه کار کوي او د پوهاوي لوړولو لپاره د اغېزناک او ګټور پلاټفورم په توګه، اغېزناک رول لوبوي. دا وسیلې نادولتي موسسو ته دا وړتیا وربخښی او توان ورکوي چې په میلونونو هغو خلکو سره چې د نورو خلکو، بنسټونو او هغو موخو سره چې د دوی له شوق او علاقې سره ورته والی لري او د اړیکو ټینګولو په لټه کې یې دي، اړیکې ټینګې کړي. ټولنیزې رسنۍ د انځورونو او معلوماتو په شریکولو سره، د نورو بنسټونو په اړه خپل نظرونه وړاندې کوي او د همدې وسیلو له لارې خپل پیغامونه په ځیرتیا سره څرګند او خپروي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۲ . زیانونه

لومړی زیان - امنیتي خطرونه:

د افغانستان په څېر جګړه ځپلو سیمو کې د ټولنیزو رسنیو د ستراتېژۍ پلي کول کولای شي د کارکوونکیو د ښکېلو، ګټه اخیستونکیو، او د فعالو موسسو د شتمنیو پر وړاندې امنیتي ننګونې رامنځ ته کړي. د ټولنیزو رسنیو د پلاټفورمونو نه د ګټې اخیستنې پر مهال، نادولتي موسسې باید له امنیتي پلوه په دغه ډول بې ثباته چاپېریال کې د حساسو معلوماتو خپرولو پر وخت، د کارکوونکیو یا ګټه اخیستونکیو د په نخښه کولو نه لاس په سر شي او د خپلو مهمو سرچینو د خوندیتوب لپاره تل حالات وڅاري.

دویم زیان - څارنه او سانسور:

د افغانستان په ګډون، ډېرو هېوادونو کې چې نادولتي موسسې فعالیت کوي، کېدای شي نادولتي موسسې د ټولنیزو رسنیو د چینلونو کارولو پر مهال د انټرنیټ د سانسور، د څارنې له کړنو او د بیان د ازادۍ په برخو کې له خنډونو او محدودیتونو سره مخ شي. د دغه خنډونو پراخول لکه پر انلاین محتوی سخت کنټرول، د څارنې اقدمات ډېرول چې دا کار د خلکو د خصوصي حریم امنیت له ګواښ سره مخامخوي او په ډیجیټل پلاټفورمونو کې په ښکاره توګه د اړیکو ټینګولو پر ازادۍ محدودیتونه دي. دغه ډول لید لوری پېچلې ننګونې رامنځ ته کوي چې نادولتي موسسې باید په افغانستان کې د ټولنیزو رسنیو د کارولو پر وخت ورته پام ولري، او خپلې د تطبیق وړ اړتیاوې په ځیرتیا سره وڅاري او له خوندي لارې د اغېزناکو اړیکو ستراتېژۍ تضمین او ډاډ تر لاسه کړي.

دریم زیان - غلط او نیمګړي معلومات:

د ټولنیزو رسنیو پلاټفورمونه د ناسمو او نیمګړیو معلوماتو د خپرولو او پروپاګنډې د چینلونو په توګه کار کوي او دغه ډول چاره د نادولتي موسسو موقف او اعتبار ته زیان رسوي او له خطر سره یې مخامخ کوي. د دغه چینلونو له لارې د ګمراه کوونکي منځپانګې او مطالبو لرونکې موضوعات خپرول د نادولتي موسسو اعتبار ته زیان واړوي، د خلکو باورونه کمزوري او ټیټ کوي او د دوی د فعالیتونو او ماموریت دقیق انځور تت او کمزوری راڅرګندوي. په پایله کې، نادولتي موسسې باید د ټولنیزو رسنیو لید لوری وڅاري، د ناسمو معلوماتو پر وړاندې اغېزناکه مبارزه وکړي خپله ډیجیټلې بشپړتیا خوندي وساتي.

څلورم زیان - د خصوصي حریم اړوند اندېښنې:

نادولتي موسسې باید د حساسو معلوماتو خپرولو پر مهال د خصوصي حریم ډیټا، د سایبري زیانونو او د اطلاعاتو د امنیتي ګواښونو اړوند له احتیاطه کار واخلي. د دغه ډول معلوماتو خپرول د معلوماتو سرغړونو، په غیر مجاز او ناقانونه توګه لاسرسي او د خرابکارو ادرسونو له لورې لاسوهنې ته زمینه مساعدوي، نو د حساسو معلوماتو ساتلو او په ډیجیټل برخه او ساحه کې د دوی دعملیاتي بشپړتیا ساتلو خوندیتوب لپاره، د قوي پروتوکولونو درلودو پر اهمیت او ارزښت باندې ټینګار کوي.

پنځم زیان - د ډیټا د امنیت ژمنې او خطرونه:

د ټولنیزو رسنیو خدمتونو نه د ګټې اخیستنې پر مهال، د ډیټا د مدیریت کنټرول او امنیت ستاسې د موسسې له لاسه وځي او د پلاټفورم د معنوي ملکیت په توګه حسابېږي. دغه پلاټفورمونه ستاسو داخلې ډیټا او هغو معلوماتو ته لاسرسی لري چې د بهرنیو سرچینو په توګه د کاروونکیو له حساب ور ها خوا، لکه په پلاټفورمونو، لکه فیسبوک کې شریک

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

شوي انځورونو او همدارنګه ستاسې شخصي او مالي جزئیاتو ته لاسرسی لري. دې پلاټفورمونو او موسسو لپاره دا ډېر مهم دي چې د خپلې، شریکانو او ګټه اخیستونکیو د ډیټا د مدیریت په برخه کې، نړېوالو قوانینو او مقرراتو ته ژمن اووسي. د ټولنیزو رسنیو یو سایټ ته په لاسرسي سره، موسسې د خپلې ډیټا د یوې برخې کنټرول له لاسه ورکوي نو باید چې په هوښیارتیا او ځیرکتیا سره له دغو پلاټفورمونو ګټه پورته کړي او د خپلې ډیټا د خوندیتوب ساحه پراخه کړي.

شپږم زیان - د مالي مرستو په برخه کې د امنیتي ننګونو سروې:

د ټولنیزو رسنیو په پلاټفورمونو کې مالي معاملات یا د نادولتي موسسو لپاره د مالي مرستو راټولونه، امنیتي ننګونې رامنځ ته کوي. په داسې حال کې چې د فیسبوک په څېر پلاټفورمونه د مالي مرستو لپاره وسیلې برابروي، خو ستاسې حساسې مالی ډیټا ته اړتیا لري، همدارنګه دوی د ونډې یا بسپنې ورکولو په برخه کې خپل محدودیتونه لري او د پلاټفورمونو په امنیت کې د کاروونکیو پر باور باندې تکیه کوي. په مقابل کې یې، د SSL جواز لرونکې ویبسایټونه، تمویلوونکیو ته د کنټرول وړ او خوندي چاپېریال وړاندې کوي او په ډیسک ټاپ او موبایل په نسخو کې د معلوماتو د خوندیتوب او د مالی سرچینو د مدیریت به برخه کې، په غوره توګه تضمین کوي.

اووم زیان - د باور قوي کول:

د ټولنیزو رسنیو پلاټفورمونه په طبیعي توګه ذاتي باور، د ویب پاڼې د ډومین د پراختیا په پرتله نه ارایه کوي. په دې برخه کې د یو ډاډمن او د باور وړ ویب سایت لکه org درلودل ګټور دي، چې په پراخه کچه د ګډو ګټو په دلیل یا د علاقې وړ موسساتو د راغونډولو او یوځای کولو سره، د مثبت بدلون اغېزو د هڅو د پیاوړتیا لپاره پېژندل شوی دی. په دې کچه باور او پوهاوی، چې د بنسټ د درک لپاره ډېر مهم دی، داسې څه دي چې ځینې نور رسنیز چینلونه یې په ساده ګۍ نشي ترسره کولای.

نادولتي موسسې څنګه کولای شي په خوندي توګه له ټولنیزو رسنیو ګټه پورته کړي؟

نادولتي موسسې کولای شي د ټولنیزو رسنیو د خطرونو د مخنیوي لپاره، د ځینو کړنو د ترسره کولو سره په خوندي او اغېزناکه توګه خپله ډیټا او انلاین شتون خوندي کړي او د انلاین متقابل عمل سره موجود احتمالي خطرونه راکم کړي.

لومړی لاره - له ډیټا نه د خوندیتوب تدابیر:

نادولتي موسسې باید په ټولنیزو رسنیو کې د خپلو حساسو معلوماتو خپرولو امنیت ته، لومړیتوب ورکړي. په فرد پورې اړوند، د اغېزناکو اقداماتو په ترسره کولو لکه قوي او ځانګړي پاسورډونه رامنځ ته کول، د هویت د تصدیق د لا ډېر خوندیتوب لپاره د دوه مرحله ییز (2FA) فعالول، او د اداري رسمي حسابونو ته د لاسرسی محدودول، په ځانګړې توګه باوري او مسلکي پرسونل ته. نادولتي موسسې په اغېزناکه بڼه کولای شي د ناقانونه لاسرسی، د معلوماتو سرغړونو او د محرمو معلوماتو څخه د احتمالی ناوړه ګټې اخیستنې خطر کم کړي.

دویمه لاره - د خصوصي حریم تنظیمول:

د ټولنیزو رسنیو د پلاټفورمونو لخوا چمتو شوي محرمیت کارول، د نادولتي موسسو د انلاین شتون د کنټرول لپاره ډېر مهم دي. د پوستونو، پیغامونو او پروفایل او د توضیحاتو او د دې تنظیمانو د ښه اداره کولو په برخه کې، نادولتي موسسې کولای شي د خپلو حساسو معلوماتو او د عامه لاسرسی وړ خبرو اترو په ښه شان ساتنه وکړي. د دغه ډول فعالې

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

طریقې په کارولو سره نادولتي موسسې کولای شي خپل خصوصي حریم خوندي وساتي، حساس معلومات او ډیټا خوندي کړي او د ټولنیزو رسنیو په پلاټفورمونو کې د خپلو اړیکو د چینلونو ملاتړ راجلب کړي.

دریمه لاره - پوهاوی او روزنه:

د ډیټا د خوندیتوب لپاره د کارکوونکیو پراخه روزنه او چمتو کول، د خصوصي حریم پروتوکولونه او د ټولنیزو رسنیو لارښوونې نادولتي موسسو ته له حده ډېر ضروري دي تر څو وشي کولای په اغېزناکه توګه په تعاملاتو او انلاین اړیکو کې موجود خطرونه راکم کړي. نادولتي موسسې خپلو کارکوونکیو ته د احتمالي خطرونو پېژندلو او ځواب ورکولو د روزنې، د سایبري امنیت د سرغړونې پر وړاندې دفاعي سیستم، له خصوصي حریم نه د سرغړونې او ناسمو معلوماتو خپرولو په برخو کې روزنه ارزښتناکه او تر ډېره د خطرونو کچه راکموي. وار له مخه د دغسې کړنو لپاره چمتووالی دا تظمینوي چې کارکوونکي په ښه شان اماده دي چې په خوندي توګه په ډیجیټل سیستمونو کې مخکې ولاړ شي، حساسه ډیټا خوندي او په انلاین ډګر کې د موسسې باور او اعتماد وساتي.

څلورمه لاره - د ځواب او څارنې طرحه:

د نادولتي موسسو د ټولنیزو رسنیو حسابونو لپاره، د څارنې د دقیقو پروتوکولونو رامنځ ته کول ډېر ضرور او مهم دي چې په چټکۍ سره وشي کولای ناقانونه لاسرسی وپېژني، مشکوک فعالیتونه معلوم کړي او نا مناسبه محتوی یا منځپانګه بررسي کړي. د منظمو ارزونو په تر سره کولو او پېښو یا امنیتي سرغړونو ته په چټکۍ سره ځواب وئیلو، نادولتي موسسې کولای شي په اغېزناکه توګه خپل انلاین شتون خوندي او د اړیکو چینلونو بشپړتیا او د خپلو لیدونکیو باور له ځانه سره وساتي. د یوه ځواب ویونکي او ښه تعریف شوي پلان درلودل دا تضمینوي چې نادولتي موسسې کولای شي په ګټه اخیستنه یې د ټولنیزو رسنیو موجود خطرونه راکم کړي، احتمالي زیان محدود کړي او د خپلو ګټه ا خیستونکیو لپاره د خوندي او بااعتباره ډیجیټل چاپېریال ملاتړ وکړي.

پنځمه لاره - منظم او اپډیټ معلومات او اړوند موضوعات شریکول(Patches):

د وروستي او نویو امنیتي پیچونو او سافټویر د تازه معلوماتو له لارې، د ټولنیزو رسنیو حسابونو ساتل د نادولتي موسسو لپاره خورا مهم او ارزښتناکه دي چې د سایبري برید ګرو د احتمالي زیانونو او ناقانونه ګټې اخیستنې مخه پرې ونیسي. د امنیتي ترتیباتو ساتلو او په چټکۍ سره د تازه معلوماتو په خپرولو سره، نادولتي موسسې کولای شي د خپلو ډیجیټل شتمنیو امنیت لا خوندي او پیاوړی کړي، د امنیتي سرغړونو خطر کم کړي او د خپلو حساسو شریک شویو معلوماتو په ښه شان ساتنه وکړي.

شپږمه لار - د پیوندونو او پیغامونو تائید او ملا تړ:

نادولتي موسسې باید دې ته لومړیتوب ورکړي چې د ټولنیزو رسنیو د چینلونو له لارې تر لاسه شویو لینکونو، پیغامونو او غوښتنو مشروعیت تصدیق کړي تر څو وشي کولای د درغلیو یا(phishing)او تقلب خطرونه راکم کړي. د کارکوونکیو تر منځ پام او احتیاط ته په وده ورکولو سره، د نامعلومو اړیکو د ځېړلو پر اهمیت ټینګار کولو او د شخصي او اداري معلوماتو له شریکولو څخه ډډه کولو په مراعتولو سره، نادولتي موسسې کولای شي د سایبري ګواښونو او د معلوماتو د احتمالي سرغړونو پر وړاندې چمتووالی ولري او خپله دفاع لا پسې قوي کړي. دغه ډول یوه فعاله کړنلاره درلودل دا تضمینوي چې نادولتي موسسې د سایبري امنیت موضوع ته په جدیت پام کوي، حساس معلومات خوندي کوي او په اسانۍ کولای شي د خپل ډیجیټل امنیت پر وړاندې د ناوړه او مخربو هڅو اغېز، کم کړي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

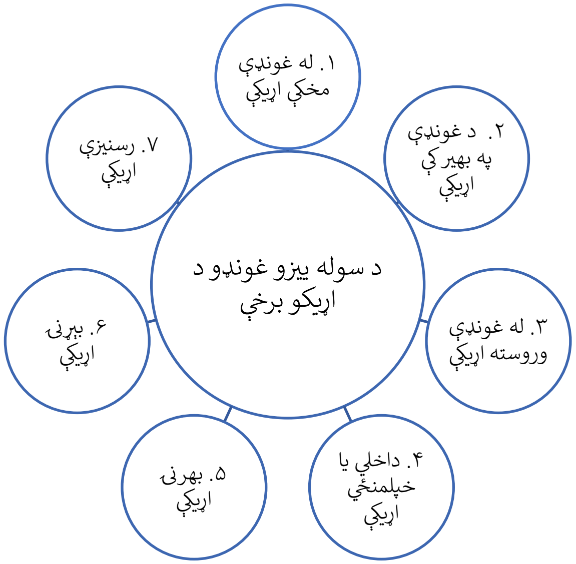
دویمه برخه: د ټولنیزو غونډو سوله ییزې اړیکې

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د سوله ییزو غونډو اړیکې څه شی دي؟

د سوله ییزو غونډو اړیکې هغو لارو چارو او میتودونو ته اشاره کوي چې د تنظیموونکیو، رضاکارانو او د غونډو د ګډونوالو لخوا، د غونډې په بهیر کې د معلوماتو او خبرونو شریکولو، د پلان جوړونې او لوژستیکي مسائیلو، په سوله ییزو غونډو،لاریونونو او راټولېدنو کې د اړونده پیغامونو په رسولو کې ترې ګټه اخیستل کېږي. دغه ډول اړیکې د سوله ییزو فعالیتونو په اغېزناکه توګه همغږي کولو کې اړین دي، د ګډونکوونکیو د خوندیتوب او د غونډو په بهیر کې د پېښو په هکله خبرولو کې ضرور دي. دغه اړیکې، د غونډې څخه مخکې، د غونډې په بهیر کې او له غونډې وروسته اړیکې دي چې باید پام ورته وشي.

د سوله ییزو غونډو د اړیکو برخې کومې دي؟



۱۱ م شکل: د سوله ییزو غونډو د اړیکو برخې

۱ . له غونډې مخکې اړیکې:

د پوهاوي د لوړتیا، د ملاتړ راجلبولو او د غونډې د وخت، ځای او موخو شریکولو لپاره د ټولنیزو رسنیو،ایمیل او ویبسایټونو په څېر ډیجیټلي پلاټفورمونو نه ګټه اخیستل.

۲ . د غونډې په بهیر کې اړیکې:

د مختلفو وسایلو کارونه لکه لاوډسپیکر، ګډونوالو ته د شخصي نښو نښانو او وسیلو انتقال او غونډې ته اغېزناکه سپارښتنې. د ډله ییزو یا ټولنیزو رسنیو پیغامونو رسول هم کولای شي چې سم له واره د غونډې اداره کولو، لوژستیکي مسایلو او نامعلومو حالاتو ته د ځواب ورکولو په برخه کې اسانتیا راولي.

۳ . له غونډې وروسته اړیکې:

د ګډونوالو سره د تعامل خوندي کولو او پر وقت د اعلانونو، پیغامونو، وضاحتونو او خپرونو له لارې چې د غونډې موخه او پایله خلاصه کوي، له ګډونوالو له مننې کولو سربیره، د راروانو فعالیتونو او کړنو په هکله هم هر څه روښانه کړئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۴ . خپلمنځي یا داخلي اړیکې:

د یوې سوله ییزې غونډې د اړیکو په برخه کې ټولې هغه ستراتېژۍ او وسایل شامل دي چې د تظیموونکیو، رضاکارانو او ګډونوالو تر منځ د همغږۍ رامنځ ته کولو لپاره کارول کېږي چې په مستقیمه توګه د غونډې په تنظیمولو کې ښکېل او برخوال دي. اغېزناکه داخلي اړیکې لکه د غونډې د اغېز خوندیتوب، د امنیت د تضمین او د غونډې په بهیر کې د وضعیت د بدلون سره مطابقت، ډېر ضرور دی.

۵ . بهرنی اړیکې:

له رسنیو او نورو بهرنیو بنسټونو سره اړیکه لرل داګته رسوي چې په پراخه کچه د غونډې پیغام خپور او فعالیت په ښه او مناسبه توګه انځور کړل شي.

۶ . بېرنی اړیکې:

د سوله یزو غونډو په بهیر کې بېړنی اړیکه له مخکې تعریف شویو ستراتژیو ته ویل کېږي چې د بېړنیو مسلو په اړه د معلوماتو او پیغامونو د رسولو لپاره کارول کېږي، همدارنګه د تنظیموونکیو، امنیتي پرسونل، رضاکارانو او ګډونوالو تر منځ د غبرګون د همغږي کولو لپاره ورڅخه مناسبه ګټه اخیستل کېږي. د اړیکو دغه بڼه او ډول د احتمالي کړکېچ د اداره کولو او د دخیلو ټولو افرادو د خوندیتوب د تضمین لپاره ضروري چاره ده.

۷ . رسنیزې اړیکې:

له رسنیو سره د اړیکو اداره کول او مدیریت څکه مهم ګڼل کېږي چې تر څو دا ډاډ تر لا سه شي چې د غونډې موخه، کیسې او روایتونه په سمه توګه درک شوي او راپور شوي دي. له رسنیو سره اړیکې، ډاډ راکوي او هغه اړیکې تضمینوي چې رسنیزې اعلامیې، د واړ له مخه ټاکل شویو ویاندویانو مصاحبې او د غونډې له پیل مخکې او له غونډې وروسته کره معلومات، په ښه توګه په رسنیو کې خپاره شي.

څرنګه کولای شو د غونډې له پیل مخکې، د غونډې په بهیر او د غونډې په پای کې اړیکې ټینګې کړو؟

په افغانستان کې د یوې سوله ییزې غونډې پر مهال اغېزمنې اړیکې، د امنیت د تامین او د سیمه ییزو قوانینو او کلتوري نورمونو د رعایت لپاره ځانګړې پاملرنې ته اړتیا لري، دلته د غونډې له پیل مخکې، په بهیر کې او له غونډې وروسته د خبرو اترو لپاره باید له ځینو ځانګړو لارو چارو کار واخیستل شي.

لومړی لاره - د قانون مراعاتول:

د طالبانو موقتي اداري مقرراتو، د کورنیو چارو وزارت له اجازې پرته د سوله ییزو غونډو تنظیمول منع کړي دي. د دې اداري د کورنیو چارو وزارت څخه اجازه تر لاسه کول سخته او ننګونکې ده او تر ډېره امکان نه لري، خو که غونډه د دوی په ملاتړ او ګټه وي، بیا هر څه اسانه دي. تاسې باید ځان له خطر سره مخ نه کړئ او هیڅ ډول هڅه باید و نه کړئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د یوې سوله ییزې غونډې د ملاتړ او تائید لپاره د طالبانو د موقتي اداري له استازو سره خبرې اترې، ښايي هيڅ ډول مثبته پایله او اغېز و نه لري، نو، ځانونه او په غونډه کې شريک او دخيل نور افراد په لومړۍ مرحله کې له خطرونو سره مه مخامخ کوئ.

دویمه لاره - پر وضعیت څارنه:

ډاډ تر لاسه کړئ چې د سوله ییزې غونډې په برخه کې مو د باور وړ معلومات راټول کړي دي. د بشري حقونو بنسټونو ګزارشونه او د خبري سرچینو تازه معلومات وڅارئ.

درېیمه لاره - د داخلي اړیکو ستراتېژۍ جوړول:

د غونډې د تنظیموونکیو، رضاکارانو او ټولو هغو شریکانو تر منځ چې په مستقیمه توګه د غونډې په تنظیمولو کې دخیل دي، د همغږۍ، اړيکو ټينګولو او د خوندي او کارول شوي ارتباطي وسیلو پېژندلو لپاره د داخلي ستراتېژۍ رامنځ ته کول یوه اساسي اړتيا ده. اغېزناکه داخلي اړيکې د غونډې د موثریت ساتلو، د ښکېلو یا شریکو کسانو د خوندیتوب او د غونډې په بهیر کې د بدلېدونکیو موقفونو سره د مطابقت لپاره خورا مهم دي. مهرباني وکړئ، د داخلي اړيکو تر ټولو خوندي او غوره وسيلو او پلاټفورمونو لپاره ۸ م ۹ م او ۱۰ م شکلونه وګورئ.

څلورمه لاره - د بهرنیو اړیکو ستراتېژۍ جوړول:

له رسنیو او نورو بهرنیو بنسټونو سره د اړیکو د څرنګوالی په برخه کې تعامل او د بهرنیو اړیکو ستراتېژۍ چمتو کول یوه اساسي اړتیا ده چې له لارې یې باید د غونډې پیغام په پراخه کچه خپور، رسنیز او په مطلوبه بڼه انځور شي. مهرباني وکړئ، د بهرنیو اړیکو تر ټولو خوندي او غوره وسیلو او پلاټفورمونو لپاره ۸ م ۹ م او ۱۰ م شکلونه وګورئ.

پنځمه لاره - د بېړنیو اړیکو ستراتېژۍ جوړول:

د یوې سوله ییزې غونډې له پیل مخکې، د تنظیموونکیو، امنیتي پرسونل او رضاکارانو تر منځ د غبرګونونو د همغږۍ کولو لپاره د اړیکو بېړنۍ ستراتېژۍ جوړول حتمي او ضروري ده. دغه ستراتېژۍ د ټولو حاضرو افرادو د امنیت د خوندیتوب او د احتمالي کړکېچونو د مدیریت لپاره ضرور ده.

شپږمه لاره - له پولې پورې افغاني او بهرنیو رسنیو سره د اړیکو ساتنه:

سیمه ییزې رسنۍ د خپلو رسنیو د خبریالانو د امنیت د خوندیتوب په دلیل، هیڅکله ستاسې سوله ییزو غونډو ته خبري پوښښ نه ورکوي، ځکه چې دغه رسنۍ د طالبانو د موقتې اداري لخوا غونډو ته د خبري پوښښ ورکولو په برخه کې منع کړل شوي دي. خپلې اړیکې له بهرنیو رسنیو او له پولې پورې غاړې رسنیو سره ټینګې وساتئ، تر څو ډاډه شئ چې د سوله ییزې غونډې موخې، روایتونو او کیسو په سمه توګه انعکاس موندلی او ګزارش یې ورکړل شوی دی. په دې ډول اړیکو کې تاسې کولای شئ له مطبوعاتي اعلامیو، د ټاکل شویو ویاندویانو له مصاحبو او له غونډې وروسته د رسنیو له مختصرو راټولېدنو ګټه پورته کړئ. د امنیتي اقداماتو لپاره، مهرباني وکړئ، په افغانستان کې د مدني ټولنې سوله ییزو غونډو لارښود چې زموږ لخوا پخوا چاپ شوی، وګورئ او ګټه ترې پورته کړئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

اوومه لاره - له ګډونوالو سره اړیکه:

داډ تر لاسه کړئ چې د غونډې ټول ګډونوال د امنیتي لارښوونو په برخه کې پوهاوی لري. دا ډېره مهمه ده چې د مناسب چلند د ساتلو ، اقداماتو ته د ځواب ورکونې او له توافق شویو کوډونو او طرزالعمل نه د اطاعت کولو پر اهمیت ټینګار وشي. سربېره پر دې، ټول وهڅوئ چې په ځیرتیا سره هر څه ته پام وکړي او هر ډول فعالیت چې کېدای شي د غونډې په بهیر کې ورسره مخ شي، ګزارش او راپور دې پې کړي. د امنیتي اقداماتو لپاره، مهرباني وکړئ، په افغانستان کې د مدني ټولنې سوله ییزو غونډو لارښود چې زموږ لخوا پخوا چاپ شوی، وګورئ او ګټه ترې پورته کړئ.

اتمه لاره - د بشري حقونو له سازمانونو او نادولتي موسسو سره همغږي:

د امکان په صورت کې، له نړیوالو نادولتي موسسو او د بشري حقونو سازمانونو سره اړیکه ونیسئ تر څو د افغانستان د اوسنیو شرایطو په هکله، د دوی نظریات معلوم او معلومات مو پراخه کړئ. دوی د پېښو او اړینو امنیتي تدابیرو اړوند کافي تجربه او پوهه لري.

نهمه لاره - د اړیکو خوندي چینلونه په نظر کې ولرئ.

که په یوه غونډه کې د ګډون هوډ لرئ یا یې تنظیموئ، د اړیکو ټینګولو په خوندي لارو چارو فکر وکړئ. د کوډ شویو پیغام رسونې خدمتونه کولای شي د ګډونوالو او تنظیمووونکیو لپاره د خصوصي حریم او ډاډمن امنیت په برخه کې لا ډېر ګټور تمام شي. په غونډه کې د ګډون پر مهال هیڅکله له خپل تلیفون څخه ګټه مه پورته کوئ، مهرباني وکړئ د اړیکو د خوندي وسایلو تر لاسه کولو لپاره ۸ م، ۹ م، او ۱۰ م شکلونو ته مراجعه وکړئ.

لسمه لاره - له نړیوالو رسنیو او سازمانونو سره تعامل:

ډاډ تر لاسه کړئ چې د بشري حقونو نړیوال سازمانونه او رسنۍ د غونډې له ترسره کولو خبر دي. کله کله په ناامنو هېوادونو کې، نړیوال بنسټونه کولای شي تر څه حده پورې تاسې له خطرونو وژغوري. مهرباني وکړئ، د بهرنیو ادارو سره د خبرو اترو په موخه د خوندي او غوره وسیلو او پلاټفورمونو موندلو لپاره، ۸ م، ۹م، او ۱۰، شکلونه وګورئ.

یوولسمه لاره - مجازي غونډو ته مخه کړئ:

وې ارزوئ چې که چېرې یوه حضوري غونډه له امکانه لرې وي او تاسې له خطر سره مخامخ کوي، د انلاین پلاټفورمونو له لارې چې کولای شي بې له کومې اندېښنې او خطره تاسې خپلو موخو ته ورسوي، مخه کړئ او وې کاروئ. مهرباني وکړئ، د یوې مجازي غونډې ترسره کولو په موخه د خوندي او غوره وسیلو او پلاټفورمونو موندلو لپاره، ۸ م، ۹م، او ۱۰، شکلونه وګورئ.

دولسمه لاره - د بیرغونو او نښو ښودل:

د خپلو پیغامونو لېږدولو لپاره له نښو، بیرغونو یا علامو څخه کار واخلئ. دغه وسیلې کولای شي ناظرینو، رسنیو یا چارواکیو ته ستاسې د موخې یا غوښتنو په رسولو کې مهمه ونډه ولري، خو په جوړولو کې یې دومره افراط مه کوئ چې تاسې له خطر سره مخ کړي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

دیارلسمه لاره - د کلیمو او شعار ورکولو په برخه کې دقیق اووسئ:

په هغو شعارونو کې چې د غونډې موخه منعکسوي،همغږي اوسئ. دا تاسې ته د یو ځای کېدو او یو اوسېدو احساس درکوي، د خپل پیغام اغېزو ته وده ورکړئ، خو د هر ډول خطر رامنځ ته کوونکې او حساسو کلیمو کارولو چې د طالبانو موقته اداره یې پر وړاندې تند غبرګون ښايي، ډډه وکړئ. همدارنګه، په شعارونو کې د داسې کلیمو کارولو چې کېدای شي ناسم و انګېرل شي او تاسې له جدي ګواښ او خطر سره مخامخ کړي، ډېر احتیاط وکړئ.

څوارلسمه لاره - له سوله ییزو خبرو اترو کار واخلئ:

که په ناڅاپي توګه د طالبانو د موقتي اداري چارواکیو یا د مخالفو اعتراض کوونکیو سره مخ کېږئ، هڅه وکړئ چې د سوله ییزو خبرو اترو له لارې مخکې ولاړ شئ، له هر ډول تاوتریخوالي څخه ډډه وکړئ او د مناسبې لارې په پیدا کولو له سیمې ووځئ.

پنځلسمه لاره .له ټولنیزو رسنیو ګټه واخلئ خو په ژوندۍ بڼه مه ښکاره کېږئ:

د غونډې په بهیر کې، په ژوندۍ بڼه تویټ او په رسنیزو پلاټفورمونو کې معلومات مه خپروئ یا په بله اصطلاح په ژوندۍ بڼه مه راخرګندېږئ. د غونډې له بهیره د انځورونو، ویډیوګانو او بیانیو خپرول ستاسې د لیدونکیو په جلب او پوهاوي په لوړولو کې مرسته کوي، خو ټول له خطر سره مخامخ کوي. که غواړئ چې څه شی شریک او خپاره کړئ، دا کار له پېښې وروسته تر سره کړئ. په همدې حال کې، په ټولنیزو شبکو کې د انځور یا فلم شریکولو په برخه کې ډېر پام وکړئ، د مستعار یا بدل حساب له لارې، د ګډونوالو د څېرو نتولو او نه ښکاره کولو او VPN او TOR نه د ګټې اخیستنې جدی سپارښتنه در ته کېږي. د مهربانۍ له مخې، د ښه او ګټور VPN او TOR تر لاسه کولو ته د ۳ م او ۵ م شکلونو ته مراجعه وکړئ.

شپاړلسمه لاره - بېړنۍ اړیکې:

ډاډه شئ چې د بېړنیو اړیکو شمېرې مو پخپل تلیفون کې خوندي کړي دي او یا مو یادښت اخستی او له ځانه سره مو ساتلي دي. په همدې حال کې، ستاسې سره په تلیفون یا کاغذ کې د یوې بېړنۍ اړیکې درلودل کولای شي ستاسې ملګري له ترینګلتیا او خطر سره مخ کړي.

اوولسمه لاره - د وضعیت مدیریت کول تر څو له عامه پام او لیدنې نه خوندي پاتې شئ:

د خلکو پام نه دراوړېدو مخنیوی ته، د سوله ییزې غونډې پر مهال په ښکاره او په نخښه شوي توګه مه راڅرګندېږئ. له افراطي اعلامیو، په لاوډ سپیکر کې له ډېرو وېناوو او په روښانه بڼه د بینرونو له کارولو ډډه وکړئ.

اتلسمه لاره - د تنظیموونکیو تر منځ اړیکې:

د غونډې په بهیر کې د تنظیم کوونکیو تر منځ د خبرو اترو او اړیکو یوه محتاطانه کړښه وساتئ چې د کارونو د همغږۍ او غیر متوقع شرایطو ته ځواب ویوونکي اووسئ. که مو پام شو چې څوک د برېښنايي اړیکو څارنه کوي، نو له فرعي او نرمو سیګنالونو ګټه واخلئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

نولسمه لاره - د نورو پام ځان ته مه راړوئ:

د غونډې له پای ته رسېدو وروسته، ډاډه شئ چې نور په هغو جامو کې چې په غونډه کې مو اغوستي وې یا مو د غونډې لپاره کوم توکي کارولي وي، د هغو نخښو سره مه راځرګندېږئ او د غونډې د سیمې پورې تړلې هیڅ ډول نخښه یا علامه له ځانه سره مه ساتئ.

شلمه لاره - له خپل حالته خپل نږدې خپلوان او ملګري خبر کړئ:

د یوې خوندي ارتباطي وسیلې له لارې، چې په ټولنیزو رسنیو کې له پیله تر پایه کوډ کول وړاندې کوي، له کورنۍ یا ملګرو سره اړیکه ونیسئ. هغوی ته خبر ورکړئ چې تاسې خوندي یاست. که پوهېږئ چې خوندي نه یاست، د خپل ځای په هکله ورسره خبره مه شریکوئ.

یوویشتمه لاره - لنډ وضاحت:

د غونډې لپاره د ګډوانولو سره په یوه ځای کې مه راټولېږئ. که تاسې خوندي هم یاست، د غونډې د پرمخ بیولو لپاره هر ډول اړین او ضروري کړنې پلان کړئ. د سیګنال په څېر د ټولنیزو رسنیو ډاډمنه وسیله وکاروئ چې سل سلنه د کوډ کولو وړتیا لري، د تلیفون له لارې خبرې مه کوئ.

دوه ویشتمه لاره - په ټولنیزو رسنیو کې پام او احتیاط:

د هغه څه په هکله چې تاسې یې په ټولنیزو رسنیو کې خپروئ، ډېر پام وکړئ. کله کله هغه معلومات چې موږ خپروو، کولای شي موږ او زموږ د څنګ ملګرو ته د احتمالي خطرونو پېښېدو سبب شي. که حتمي وي چې په ټولنیزو رسنیو کې څه خپاره کړئ، له یوه ناپېژانده حساب یا ادرس او یو VPN نه ګټه واخلئ.

درویشتمه لاره - پر وضعیت څارنه :

د غونډې له پای ته رسېدو وروسته، د خبري سرچینو له لارې د خپلې سیمې له پېښو ځان باخبره او اګاه کړئ. دا تاسې سره مرسته کوي چې د غونډې د پایلو په برخه کې د رامنځ ته شوي تغیر په هکله چې ښایي ستاسې امنیت اغېزمن کړي، تاسې باخبره وساتي.

څلورویشتمه لاره - بېړنۍ طرحه:

ډاډ تر لاسه کړئ چې که سوله ییزه غونډه کې ګډوډي رامنځ ته کېږي یا د امنیتي ځواکونو له لورې خورېږي، تاسې ورته وار له مخه اټکل کړی او پلان ورته لرئ. ښه به دا وي چې له ضرورت او اړتیا پرته سفر و نه کړئ او په ننګونکې سیمه کې پاتې نشئ. د پاتې کېدو لپاره مناسب ځای پیدا کړئ. یوازې په هغه صورت کې د خپل ځای په هکله نور خبر کړئ چې تاسې ډاډه یاست چې څوک به مو د طالبانو موقتې ادارې ته و نه سپاري. په خوندي ځای کې اووسئ او هیڅ ډول تلیفون یا تلیفوني دستګاه له ځانه سره مه انتقالوئ.

پنځه ویشتمه لاره .له غونډې وروسته خبرې اترې:

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

د غونډې د پایلې او لاس ته راغلو تجربو اړوند بحث لپاره د غونډې له کلیدي تنظیمووَنکیو سره یوه لنډه جلسه ونیسئ. ډاډ تر لاسه کړئ چې دا کار په خصوصي توګه او خوندیتوب کې ترسره کولای شئ. د حضوري راغونډېدو پر ځای، د اړیکو لپاره د ټولنیزو رسنیو خورا خوندي وسیلې چې د کوډ شویو پیغام رسونې خدمتونه ارایه کوي، وکاروئ او مجازي ناسته تنظیم کړئ. د مهربانۍ له مخې، د خپلو اړیکو ټینګولو او د خوندي وسیلو کارولو لپاره ۸ م، ۹ م او ۱۰ م شکلونو ته مراجعه وکړئ.

شپږویشتمه لاره - د معلوماتو دقیق خپرول:

که د غونډې اړوند معلومات په عمومي ډول شریکوئ (د بېلګې په توګه، د ټولنیزو رسنیو یا رسنیو له لارې) د هغه څه په هکله چې شریکېږي، په ډېر پام او احتیاط سره باید شریک شي چې د احتمالي خطرونو کچه کمه کړي. انځورونه باید د غونډې په سوله ییزو اړخونو تمرکز ولري، نه دا چې چاړواکي ستاسې پر وړاندې راوپارېږي. په همدې حال کې، د ټولو ګډونوالو مخونه باید تت رنګه او له پېژندو ووځي تر څو و نه پېژندل شي. که داسې و نه شي، د ټولو ګډونوالو څېرې چې په انځور یا ویډیو کې ښکاره کېږي او نشر ته سپارل کېږي، کولای شي ټول له خطر سره مخ کړي.

اوویشتمه لاره - ملاتړ او تعقیب:

د چاړواکیو له لوري د هر ډول عواقبو او اقداماتو په صورت کې، له ګډونکوونکیو ملاتړ وکړئ. د بشري حقونو د کورنیو او بهرنیو سازمانونو نه د همکارۍ کولو غوښتونکي شئ.

د سوله ییزې غونډې په بهیر کې د کولو اصطلاحاتو له کارولو ډډه باید وشي؟

په افغانستان کې د یوې غونډې نه مخکې، په بهیر کې یې او له غونډې وروسته، مهمه ده چې د ځینو هغو اصطلاحاتو چې حساسیت پاروونکي یا نامناسبه ګڼل کېږي، له کارولو ډډه وشي. د دې اصطلاحاتو پېژندنه یو څه ګران کار دی، خو هر هغه څه چې د طالبانو د موقتي اداري د ایډیالوژۍ د موضوعاتو سره په ټکر کې وي، په ښه نه ورته کتل کېږي. په دغه ډول چاپېریال کې د اړیکو ټینګولو پر مهال، د سیمې رواجونو او ادابو ته په پام کولو سره، فرهنګي نورمونه او رفتار او سیاسي چاپېریال په نظر کې لرل خورا مهم دی. په دې هکله چې د طالبانو موقتي اداري لخوا، د دغه ډول اصطلاحاتو کارولو د څرنګوالي او څارنې په هکله د دوی دریځ لا روښانه شي، مهرباني وکړئ، نادولتي موسسې باید د اړیکو پر وخت د کومو اصطلاحاتو له کارولو ډډه وکړي، په دې برخه کې له حساسو اصطلاحاتو اړوند، زموږ د خپرو شویو معلوماتو او مطالبو څخه ګټه پورته کړئ.

په افغانستان کې د اړیکو لپاره خوندي وسیلې او پلاټفورمونه کوم یو دي؟

مهرباني وکړئ، د اړیکو په برخه کې د خوندي وسیلو او پلاټفورمونو لپاره ۸ م، ۹ م او ۱۰ م شکلونه وګورئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

په یوه سوله ییزه غونډه کې د ټولنیزو رسنیو ګټې او زیانونه څه شی دي؟

ا . ګټې:

لومړۍ ګټه - پوهاوی او راټولېدنه:
د ټولنیزو رسنیو پلاټفورمونه کولای شي د ګډونوالو د پوهاوی لوړولو، پراخې راټولېدنې او اغېزمن ګډون لپاره د یوې قوي وسیلې په توګه کار وکړي. او د غونډې د موخې، وخت او ځای اړوند معلومات په کمه موده کې خپلو ډېرو مخاطبینو ته ورورسوي.

دویمه ګټه - د معلوماتو شریکول:
ټولنیزې رسنۍ ټولو ته د تازه او نویو خبرونو او معلوماتو وررسولو امکان برابروي، چې د غونډې په بهیر کې د بېړنیو شرایطو، هر ډول تغیر ته ځواب ورکولو او فعالیتونو په همغږي کولو کې ضرور او خپله برخه پراخه ونډه لري.

دریيمه ګټه - راټولېدنې رامنځ ته کول:
دا پلاټفورمونه کولای شي د هغو همفکرو افرادو تر منځ چې له یوې موخې ملاتړ کوي، همغږي رامنځ ته او مرسته ورسره وکړي او د ګډونوالو تر منځ د پیوستون احساس پیاوړی کړي.

څلورمه ګټه - د نړېوالې ټولنې پام:
د ټولنیزو رسنیو له لارې، هغه موضوعات چې د ټولنې په ژورو کې شتون لري، کولای شي د نړېوالې ټولنې پام ځان ته راواړوي او په بالقوه توګه په افغانستان کې پر مېشتو ډلو، د نړېوالې ټولنې د ملاتړ له امله پر دغو ډلو د فشار راوستو لامل کېږي او ښايي ډېرې مثبتې پايلې له ځانه سره ولري.

پنځمه ګټه - لاسرسی / ترلاسه کول او تعامل:
د ټولنیزو رسنیو پلاټفورمونه د تنظیم کوونکیو لپاره اړینه سرچینه ده چې خپل نفوذ پراخ کړي، په مستقیمه توګه له نړېوالې ټولنې سره اړيکې پيدا او د دوی د موخو په برخه کې یې پام راواړوي. ټولنیزو رسنیو ته د پراخه لاسرسی او د دغه رسنیو د تعاملی ورتیاوو له لارې، تنظیم کوونکي کولای شي په روښانه توګه خپلې موخې بیان کړي، قوي روایتونه او کیسې وړاندې کړي او له مختلفو مخاطبینو نه ملاتړ وکړي. دغه ډیجټلی ستراتېژي نه یوازې دا چې د دوی پیغام قوي کوي، بلکه د ملاتړو تر منځ د ګډون او یووالې احساس رامنځ ته کوي او د تعامل سمدستي یا زر تر زره پایلې ته زمینه برابروي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

شپږمه ګټه - عدالت غوښتنه او شبکه جوړول:

د ټولنیزو رسنیو پلاټفورمونه د ټولنیز بدلون د هڅو لپاره د خو اړخیزه وسیلو ټولګه ده چې د نوښتونو په برخه کې ملاتړ تر لاسه کوي او د ورته او همغږي فکرونو لرونکیو ادرسونو او تمویلوونکیو تر منځ د اړیکو رامنځ ته کولو زمینه مساعدوي. د ټولنیزو رسنیو د اړیکو د وړتیاوو په کارولو سره، تنظیموونکي کولای شي په اغېزناکه توګه مهم مسایل روښانه کړي، د خپلو هڅو لپاره د خلکو ملاتړ څواکمن کړي او د خپل نفوذ او پېژندنې لپاره خپلو همکاریو ته پرمختګ ورکړي. د ډیجیټال دغه چاپېریال نه یوازې دا چې د یوه رسنیز پیغام په خپرولو کې عمل ترسره کوي، بلکه د یوې ژمنې او وصل شوې ټولنې په رامنځ ته کولو کې مرسته کوي چې د مثبتو ټولنیزو بدلونونو په رامنځ ته کولو او د ټولنیزو اغېزو په برخه کې ګډو موخو رسېدو ته ژمن وي.

اوومه ګټه - مخامخ یا مستقیمه اړیکه:

موخو ته د رسېدو لپاره، له مخاطبینو سره مستقیم تعامل ته اړتیا ده. ټولنیزې رسنۍ ستاسې له ملاتړو سره د تعاملي اړیکو او په فعاله توګه او چټکې سره د نظریاتو د تبادلې امکان برابروي. د مستقیمو اړیکو دغه چینلونه، چې په مناسبو اطلاعاتو پیاوړي شوي دي، کولای شي په اغېزناکه توګه پوهاوی ته پراختیا او د موخې وړ اقداماتو ترسره کولو ته چټکتیا ورکړي.

اتمه ګټه - د اطلاعاتو خپرول:

د اطلاع رسونې په ستراتېژۍ کې د ټولنیزو رسنیو شاملول تنظیم کوونکیو ته دا توان ورکوي چې په اغېزناکه توګه د وخت تازه او حساس معلومات، ارزښتناکه سرچینې، تعلیمي او روزنیزه منځپانګې او بېړني اعلامیې او خبرتیاوې خلکو ته خپاره کړي. تنظیموونکي کولای شي د ټولنیزو رسنیو او پراخو پلاټفورمونو نه ګټه پورته او په چټکې سره حیاتي معلومات خپاره کړي، له ګټه اخیستونکیو سره په اړیکه کې شي، راځرګندېدونکیو پېښو ته اغېزناک ځواب ورکړي او ډاډ تر لاسه کړي چې معلومات یې نه یوازې دا چې په مناسب وخت شریک کړي، بلکه اغېزناک او پراخه معلومات هم دي.

نهمه ګټه - د اړیکو او پوهاوي پراخول:

ټولنیزې رسنۍ د اړیکو جوړولو په برخه کې د یوې پیاوړې وسیلې او د پوهاوي لوړولو په برخه کې د یوه متحرک پلاټفورم په توګه کار کوي. دا تنظیموونکیو ته دا توان او وړتیا ورکوي چې هغو ډېرو مخاطبینو سره چې د ګډو موخو او همغږیو په لټه کې دي او دوی ته د ارزښت وړ دي، سره یو ځای شي. د معلوماتو او انځورونو د سمدستي شریکولو له لارې، ټولنیزې رسنۍ د خلکو یوې سترې ډلې ته کړکۍ پرانیزي او په سمه توګه چمتو شوی پیغامونه چې مطلوبه موخې منعکسوي، پیاوړي کوي.

۲ . زیانونه:

لومړی زیان - د چارواکیو له لوري څارنه او ځپل:

په افغانستان کې پر ټولنیزو رسنیو د څار خطر ډېر دی. د تنظیموونکیو او کډونوالو لخوا د دغه پلاټفورمونو نه ګټه پورته کول شاید دوی له خطر او ګواښونو سره مخ کړي، او یا له دې پورته د سیاسی مخالفینو په ډله کې حساب او بندي کړل شي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

دویم زیان - ناسم او نیمګړي معلومات:

د ناسمو او نیمګړیو معلوماتو خپرول کولای شي په ټولنیزو رسنیو کې په چټکۍ سره خپاره شي او په بالقوه یا احتمالي توګه د ګډوډۍ لامل شي، اوازې خپرې کړي او د غونډې د موخې په کمزوره کولو تمامه شي.

درېیم زیان .تاوتریخوالی او هڅونه:

په ټولنیزو رسنیو کې لیکل یا پوستونه د اصلي موخو او مفاهیمو له شرایطو بهر هم کارول کېدای شي او یا هم د تاوتریخوالي یا تېري کوونکو هڅو لپاره ترې ګټه پورته شی چې ښایي د سوله ییزې غونډې قانوني والی او مشروعیت له ګواښ سره مخ کړي.

څلورم زیان – خوربدل /خواره کېدل:

که څه هم ټولنیزې رسنۍ کولای شي د یوې غونډې د یووالي سبب شي، خو کولای شي غونډه ګډه وډه او ګډونوال خواره واره کړي. د نظرونو او چلندونو توپېر کولای شي ډېر راڅرګند او د ډلو د خواره واره کېدو او په غونډه کې د ګډونوالو د ډله ییز ځواک د کمزورۍ لامل شي.

پنځم زیان .امنیتي ګواښونه:

د افغانستان په څېر ناکراره سیمو کې د ټولنیزو رسنیو د ستراتیژۍ ادغام او شاملول کولای شي امنیتي خنډونه او ګواښونه رامنځ ته کړي او د دې ډېر احتمال شته چې د تنظیوونکیو، امنیتي پرسونل او رضاکارانو لپاره ګواښوونکي تمامه شي. د ټولنیزو رسنیو له پلاټفورمونو نه د ګټې اخیستنې پر مهال، تنظیموونکي باید د حساسو معلوماتو له افشا کولو ډډه کولو مخنیوي، د ګډونوالو او رضاکارانو د احتمالي په نښه کولو مخنیوي او په هغو سیمو کې چې پې ثباتي موجوده او د امنیتي ننګونو سره د مخامخ کېدو چانس ډېر وي او د اړینو سرچینو خوندي کېدو تدابیرو ته وار له مخه پام کړی او چمتو والی ولري.

شپږم زیان - سانسور او څارنه:

په افغانستان کې د سوله ییزې غونډې تنظیموونکي د ټولنیزو رسنیو کارولو پر مهال د انټرنیټ د سانسور، د څارنې تاکتیکونو او د بیان پر ازادۍ پورې تړلیو محدودیتونو او ننګونو سره مخ دي. د دې ډول خنډونو لرې کولو او برلاسي ترلاسه کولو ته باید د ډیجټل منځپانګې لرونکي سخت قوانین، د څارنې او ځیرتیا زیاتوالی چې د محرمیت او امنیتي ګواښونه رامنځ ته نشي او د انلاین چینلونو له لارې د ازادو اړیکو محدودیتونه باید تعقیب شي. دا خنډونه هغه پېچلی چاپېریال په ګوته کوي، چېرته چې تنظیموونکي د افغانستان په څېر چاپېریال کې د ټولنیزو رسنیو کارولو پر وخت کار کوي، او د اغېزناکو، خوندي او ګټورو اړیکو د لارو چارو د باوري کولو او سمون لپاره یې خوندیتوب اړین دی.

اووم زیان - ناسم معلومات او نیمګړي معلومات:

د ټولنیزو رسنیو پلاټفورمونه د ناسمو معلوماتو، پروپاګند او نیمګړو کیسو او روایتونو خپرولو لپاره د چینلونو په توګه کار کوي چې د دوی دا عمل کولای شي د سوله ییزې غونډې تنظیموونکیو نېک شهرت او اعتبار ته زیان ورواړوي. د دغو پلاټفورمونو له لارې د ناسمو معلوماتو خپرول کولای شي د یوې سوله ییزې غونډې انځور پیکه او بدرنګه کړي، عمومي باور ټپي یا له منځه یوسي او غونډې د موخو او مقصدونو رښتینې څېره یا انځور داغداره کړي. له دې امله، تنظیموونکي باید د ټولنیزو رسنیو د کارونې پر وخت له ډېر احتیاطه کار واخلي او په بریالیتوب د ناسمو او نیمګړیو معلوماتو پر وړاندې خپل دریځ قوي او مبارزه وکړي او په ډیجیټل ساحه کې خپل یووالی او ځواک بشپړ او خوندي وساتي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

اتم زیان - د خصوصي حریم اړوند اندېښنې:
د سوله ییزو غونډو تنظیمونکي باید د ټولنیزو رسنیو په چینلونو کې د حساسې ډیټا او معلوماتو خپرولو پر مهال، د ډیټا د خصوصي حریم ، سایبري خطرونو او امنیتي ګواښونو له کبله، له احتیاطه کار واخلي. د دغه ډول معلوماتو د افشا کولو پرېکړه، د ډیټا د احتمالي سرغړونې زیان رسونه او په ناقانونه توګه د مخربو ادارو لخوا لاسرسی او ناوړه ګټه اخیستل اسانه کوي او د حساسو معلوماتو خوندوي کولو او د دوی انلاین فعالیتونو اعتبار ساتلو لپاره د قوي خوندیتوب او میتودونو رامنځ ته کولو اهمیت په ګوته کوي.

د یوې سوله ییزې غونډې په بهیر کې او وروسته رسنیو او ټولنیزو رسنیو ته باید په څه ډول راڅرګند شئ؟

په افغانستان کې، د یوې سوله ییزې غونډې د پوښښ لپاره د رسنیو او ټولنیزو رسنیو کارول د خورا محدود او کنټرول شوي چاپېریال له امله یوه دقیق او محتاط ستراتېژیک پلان ته اړتیا لري. دلته ځینې لارښوونې او احتیاطي تدابیر دي چې باید په پام کې ونیول شي چې په څه ډول د غونډې پر مهال او له غونډې وروسته رسنیو ته راڅرګند او د ټولنیزو رسنیو پلاټفورمونه وکارول شي.

لومړۍ لاره - لومړی امنیت:
د ګډونوالو خوندیتوب او امنیت ته مو تل لومړیتوب ورکړئ. که چېرې د معلوماتو افشا کول د ګډونوالو پر مجازاتو تمامېږي، پکار ده چې دغه معلومات پټ پاتې شي.

دویمه لاره - ناپېژانده ګزارش:
د ګزارش ورکوونکیو د هویت د خوندیتوب لپاره د دوی د ناپېژانده پاتې کېدو داډ تر لاسه کړئ. په ویډیوګانو او انځورونو کې د غړ تحریف او د مخ تت کولو او مسخ کولو له میتودونو کار واخلئ تر څو ګډونوال له احتمالي او پېښېدونکیو مجازاتو نه خوندي پاتې شي.

دریمه لاره - خوندي شبکې:
د معلوماتو د خپرولو لپاره له خوندي او کوډ شویو وسیلو نه کار واخلئ. دا کار د چارواکیو له لورې د ځارنې او مداخلې خطر کموي. مهرباني وکړئ، ۸ م، ۹ م، او ۱۰ م شکل ته مراجعه وکړئ.

څلورمه لاره - په غوره توګه شریکول:
ټاکونکي اوسئ چې څه، په کوم وخت کې، او له چا سره شریکوئ. په ستراتېژیکو ځایونو کې له خپرولو او د راغونډېدو ځایونو یا حرکتونو کې چې کېدای شي د مخالفینو لخوا د ګډونوالو پر وړاندې وکارول شي، ډډه وکړئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

پنځمه لاره - د مناسب وخت ځارنه:
د شریک کړل شویو معلوماتو د ناسم تعبیر یا ناسمې ګټې اخیستنې مخنیوي ته، وضعیت په پرلپسې ډول وڅارئ. کېدای شي د کړکېچ د مخنیوي لپاره د پستونو زر تر زره پاکولو اړتیا پېښه شي.

شپږمه لاره - له کورنیو او بهرنیو رسنیو سره ګډون:
له سیمه ییزو او نړیوالو باوري رسنیو سره ګډون چې کېدای شي پېښې په پراخه کچه تر پوښښ لاندې راولي، تعامل ولرئ. او له دوی سره د تعامل لپاره د یوې بلې خوندې وسیلې په لټه کې هم شئ تر څو خوندي پاتې شئ، کېدای شي ستاسې اړیکه د چارواکیو مداخلې ته زمینه مساعده نه کړي.

اوومه لاره - مستند شواهد:
د غونډې انځوریز او لیکل شوي مستند شواهد راټول او ارشیف کړئ تر څو ډاډ تر لاسه کړئ چې په خوندي توګه ساتل کېږي او د راتلونکي وخت د ملاتړ لپاره، بې له دې چې د افرادو امنیت ته ګواښ ور پېښ شي، دغه شواهدو ته لاسرسی شونی وي.

اتمه لاره .کنترول شوي خپرېدنې:
په مختلفو مرحلو کې د معلوماتو په خپرولو سره روایتونه کنټرول کړئ تر څو موضوع د عامه خبرو اترو په بهیر کې خپل تړاو له لاسه ور نه کړي او په ورته وخت کې د دې خبرو اترو نه رامنځ ته شوې خطرونه مهار کړل شي.

نهمه لاره - له هغو چینلونو ګټه واخلئ چې د حساسي منځپانګې له پروتوکولونو سره تړلې وي:
له هغو چینلونو او پلاتفورمونو نه ګټه واخلئ چې د حساسې منځپانګې لپاره یې پروتوکولونه رامنځ ته کړي او د ناوړو پایلو مخنیوی کوي.

لسمه لاره - د ورانديزونو او نیوکو حلقه:
له خپلو ګډونوالو او ملاتړو د نیوکو او وړاندیزونو یوه حلقه رامنځ ته کړئ چې رسنیزه ستراتېژي وارزوئ او د راتلوونکیو فعالیتونو لپاره اصلاحات پکې راولئ.

یوولسمه لاره - د ډیټا یا معلوماتو د ساتنې تدابیر:
د غونډو لپاره په ټولنیزو رسنیو کې د حساسو معلوماتو خوندیتوب ډېر مهم دی. تنظیمونکې کولای شي اد معلومات د سختو امنیتي کړنو په پلي کولو سره خوندي کړي، لکه د قوي او ځانګړیو پاسورډونو رامنځ ته کول، د لا ښه او خوندي امنیت لپاره د هویت د تصدیق لپاره دوه مرحله یي فاکتور فعالول او معلوماتو ته لاسرسی تر ځان پورې محدودل. د دغه ډول اقداماتو پلي کول د غیر مجاز یا ناقانونه لاسرسي، د ډیټا د سرغړونو او محرمو معلوماتو نه د ناوړه ګټې اخیستنې په مخنیوي کې ډېره مرسته کوي او په پایله کې به د دوی د ډیجیټل شتون خوندي او د لیدونکو باور پر ځای وساتي.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

دولسمه لاره - د خصوصي حريم ترتيبول:

د یوې سوله ییزې غونډې تنظیمونکې باید په اغېزناکه توګه د خپل انلاین شتون د اداره کولو لپاره، د ټولنیزو رسنیو لخوا چمتو شویو پلاټفورمونو د محرمیت ترتیبات وکاروي. د دې ترتیباتو ښه تنظیمول د دې کنټرول لپاره چې څوک کولای شي د دوی پوسټونه، پیغامونه او د پروفایل معلومات وګوري، کوربه ته د دې وړتیا او اجازه ورکوي چې حساسه ډیټا او شخصي خبرې اترې د عامه افشا کېدو څخه خوندي کړي. دغه قصدي یا عمدي ستراتېژي د محرمیت ساتلو، مهمو معلوماتو خوندي کولو او د ټولنیزو رسنیو په مختلفو پلاټفورمونو کې د دوی د اړیکو د چینلونو بشپړتیا ساتلو په برخه کې مرسته کوي.

دیارلسمه لاره - روزنه او پوهاوی:

د تنظیموونکیو لپاره دا اړینه ده چې خپل امنیتي پرسونل او رضاکارانو ته د ډیټا د امنیت او خوندیتوب، د خصوصي حریم د خوندیتوب په لارو چارو، او د ټولنیزو رسنیو د لارښودونو په اړه بشپړه روزنه ورکړي چې د انلاین اړیکو او تعاملاتو په بهیر کې د خطر کچه تر ممکنه حده راټیټه کړي. د احتمالي ګواښونو پېژندلو او په ګوته کولو کې به د دې اشخاصو روزنه وشي کولای چې د سایبري امنیت د سرغړونو، د خصوصي امنیت د سرغړونو او ناسمو معلوماتو خپرېدو سره د مبارزې په برخه کې د دوی وړتیا پیاوړې او خطرونه راکم کړي. د دغه ډول فعالو ګامونو په اخیستو سره، امنیتي پرسونل او رضاکاران د ډیجیټل پلاټفورمونو په خوندي توګه لټون او د حساسو معلوماتو په ساتنه او د غونډې د انلاین شهرت، ښه نوم او بشپړتیا ساتلو په برخه کې مرستندوی تمامېږي.

څنګه کولای شو د طالبانو د موقتي اداري له استازو سره رغنده خبرې اترې رامنځ ته کړو؟

د طالبانو موقتي اداري مقررات په صراحت سره د یوې داسې غونډې ترسره کول چې وار له مخې یې د کورنیو چارو له وزارته اجازه نه وي اخیستې، منع اعلان کړي دي. له کورنیو چارو وزارت څخه د دغه ډول اجازې ترلاسه کول ناممکن او ننګوونې چاره ده. موږ سپارښتنه کوو چې په دې برخه کې ځان له خطر سره مخامخول او خپل وخت بې ځایه لګول دي او د دغه ډول غوښتنې په کولو سره ځان له خطر سره مه مخامخ کوئ. د یوې سوله ییزې غونډې ترسره کولو اجازې تر لاسه کولو لپاره، د طالبانو له موقتي اداري سره د رغندو خبرو اترو د بریا احتمال امکان نه لري.

همدارنګه دا هم امکان لري چې له اجازې پرته د یوې سوله ییزې غونډې ترسره کولو کې د طالبانو د موقتي اداري له استازو سره مخامخ کېدل ښايي په ناوړو پایلو تمام شي. سپارښتنه کوو چې بې له ځنډه سیمه پرېږدئ او له غونډې وروسته سیمې ته مه ورګرځئ. د بشپړو معلوماتو لپاره، مهرباني وکړئ، په افغانستان کې د مدني ټولنو لپاره د سوله ییزو غونډو لارښود ته مراجعه وکړئ.

د یوې سوله ییزې غونډې په پای کې کوم اقدامات باید ترسره شي؟

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

۱ . پايله يا نتيجه ګيري:

د سوله ييزې غونډې پای اعلان کړئ. له معمول سره سم، دغه اعلاميه بايد د پيغام سره ورته والی ولري. په بعضې حالاتو کې، د امنيتي اندېښنو له امله ښايي د يوې غونډې د ترسره کولو موده له ټاکل شوې وخته لنډه او زر تمامه شي. په دغه ډول حالاتو کې ټولو ګډونوالو ته د غونډې پای ته رسېدو د اطلاع ورکولو په موخه، له يوه خوندي او مناسب چينل څخه کار واخلئ او ټول ګډونوال خبر کړئ. مخکې له راټولېدو څخه، دا ډېره مهمه ده چې د غونډې د پای وخت او د پای ته رسولو څرنګوالی يې وار له مخه اعلان کړئ.

۲ . لارښوونې:

ګډونوالو ته روښانه او واضح لارښوونې وکړئ چې څنګه او په څه ډول له ګڼې ګوڼې ووځي، هغوی وهڅوئ چې په سوله ييزه بڼه سيمه پرېږدي او له مخالفو اعتراض کوونکيو او چارواکيو سره له هر ډول شخړې نه ډډه وکړي. سپارښتنه کېږي چې ګډونوال دې د غونډې له سيمې د وتو لپاره مختلفې او خوندي لارې وټاکي.

۳ . د سوله ييزه وتو اسانتيا:

د بېړني او خوندی وتو لپاره، د خوندي لارو ګودرو ټاکل او ګډونوالو ته يې ابلاغول ډېر ضرور دي. ډاډه شئ چې دغه لارې په روښانه او اسانه توګه پېژندل شوې وي.

۴ . وضعيت وڅارئ:

د يوه تنظيموونکي په توګه، د احتمالي تاوتريخوالي يا شخړې نخښې وګورئ او وڅارئ، تر څو وشئ کولای په اغېزناکه توګه له ګډونکوونکيو او رضاکارانو سره اړيکه ټينګه وساتئ. ستاسې خبرېده ضرور دي چې وشئ کولای په چټکۍ سره د هرې پېښې شوې ستونزې پر وړاندې مقابله وکړئ او حللاره ورته پيدا کړئ. سوله ييز رفتار دود کړئ او د اړتيا په صورت کې د هر ډول اختلاف يا شخړې د حل لپاره، مداخله وکړئ.

۵ . له غونډې وروسته اړيکې:

له غونډې وروسته د ګډونوالو سره د معلوماتو شريکولو پر مهال له ډېر پام او احتياطه کار واخلئ. په دې معلوماتو کې ښايي د غونډې وروستي خبرونه او موضوعات يا ستاسې په موخو پورې اړوند راتلونکې پېښې، د ګډونوالو خوندي ساتلو لارې چارې يا د امنيتي اندېښنو له امله د دوی د نه ګډون موضوعات شامل وي. د ګډونوالو سره په اړيکه کې د پاټې کېدو، د وروستيو خبرونو تر لاسه کولو يا د امنيتي دلايلو له امله د غونډې د منحل کېدو لپاره د اړيکو خوندي ميتود برابر کړئ تر څو په اړيکه کې پاتې شئ، ځکه چې د ټولو ګډونوالو سره يووالی او د پرلپسې اړيکې ساتل اړين دي.

۶ . غونډه مستنده کړئ:

ډاډه شئ چې يو څوک د غونډې په بهير کې د غونډې او د غونډې اړوند پېښو د مستند کولو په موخه، د انځورونو اخيستو او فيلم جوړولو لپاره ټاکل شوی دی، خو په هغه صورت کې چې د دې کار ترسره کول خوندي وګڼل شي. دغه اسناد ستاسې د غونډې د ماهيت د ثبوت په توګه کار کوي او کولای شي د وروسته راڅرګندېدونکيو ناسمو رواياتو يا ادعاګانو پر وړاندې تاسې سره د کره ثبوت او دليل په توګه مرسته وکړي. سربېره پر دی، د غونډې اغېزمنه ارزونه وکړئ، کومو ننګونو سره چې مخ ياست، هغه په ګوته کړئ او په راتلونکې کې، په پېښو کې د پرمختګ او برلاسي لپاره ساحې روښانه کړئ. له مختلفو خلکو سره د انځورونو يا فلمونو له شريکولو څخه ډډه وکړئ. که غواړئ چې په ټولنيزو رسنيو کې يې خپاره کړئ، د ټولو ګډونوالو د څېرو د خرابولو او د خصوصي حريم د خونديتوب لپاره له يوه ناپېژانده حساب يا نه ګټه ادرس يا TOR يا VPNواخلئ.

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

سرچينې

1. https://www.hrw.org/news/2021/10/01/afghanistan-taliban-severely-restrict-media
2. https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf
3. https://www.csis.org/analysis/talibans-increasing-restrictions-civil-society-and-aid-organizations
4. https://press.un.org/en/2023/sc15222.doc.htm
5. https://www.rferl.org/a/afghanistan-taliban-ban-swedish-ngo-humanitarian-crisis/32504979.html
6. https://protonvpn.com/
7. https://mullvad.net/en
8. https://www.expressvpn.com/
9. https://nordvpn.com/
10. https://www.cyberghostvpn.com/
11. https://righttoconnect.org/online-resources/
12. https://bitwarden.com/
13. https://www.lastpass.com/
14. https://1password.com/
15. https://www.dashlane.com/
16. https://keepassxc.org/
17. https://support.torproject.org/tbb/
18. https://community.brave.com/
19. https://www.whonix.org/
20. https://tails.net/
21. https://guardianproject.info/apps/info.guardianproject.orfox/
22. https://riseup.net/en/email
23. https://www.autistici.org
24. https://proton.me/mail
25. https://tuta.com
26. https://disroot.org/en
27. https://meet.jit.si

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.

28. https://demo.bigbluebutton.org
29. https://whereby.com
30. https://www.bluejeans.com
31. https://www.goto.com/meeting
32. https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web
33. https://meet.google.com
34. https://meet.google.com/calling/
35. https://www.microsoft.com/en-ca/microsoft-teams/log-in
36. https://twitter.com/
37. https://www.clubhouse.com/
38. https://zoom.us/
39. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

Copyright © 2024 RIGHT TO CONNECT (RTC). All rights reserved.