رهنمود ارتباطات

برای جامعه مدنی افغانستان

RIGHT TO CONNECT
RTC

2024

رهنمود ارتباطات

برای جامعه مدنی افغانستان

برای تهیه این رهنمود، RTC با نمایندگان مختلف نهاد های جامعه مدنی، در افغانستان و در تبعید، یک سلسله مصاحبه هایی را انجام داده است. بنابراین، این رهنمود در پاسخ به چالش‌های متعددی که نهادهای مدنی، مدافعان حقوق بشر و روزنامه‌نگاران در محیط کاری شان و در تبعید با آن‌ها مواجه هستند، ایجاد شده است. RTCمسئولیت هیچ گونه راهنمایی ارائه شده در اینجا را بر عهده نمی گیرد. اگر در افغانستان کار می کنید، این دستورالعمل ها برای شما موثر واقع میشود و با کاربرد آنها موقعیت خوبی برای درک دقیقتر از افغانستان خواهید داشت.

رهنمود ارتباطات برای جامعه مدنی افغانستان

رفع مسئولیت:

نظرات بیان شده در این رهنمود نظرات نویسنده (های) آن است و لزوماً منعکس کننده نظرات RTC و تمویل کنندگان آن نیست. در حالی که RTC حقوق مالکیت معنوی این رهنمود را حفظ می‌کند، افراد و نهادها حق استفاده، تکثیر و توزیع هر بخشی از این رهنمود را صرفاً برای مقاصد غیرتجاری، آموزشی یا علمی دارند، مشروط بر اینکه استفاده همراه با ذکر نام باشد.

رهنمود ارتباطات برای جامعه مدنی افغانستان

فهرست مطالب

مخففات 1

بخش اول: ارتباطات موسسات غیردولتی 2

ارتباطات موسسات غیردولتی چیست؟ 3

مولفه های ارتباطات موسسات غیردولتی چیست؟ 3

۱. ارتباطات داخلی: 3
۲. ارتباطات خارجی: 4
۳. ارتباطات دادخواهی و کامپاین ها: 4
۴. ارتباطات بحران و اضطرار: 4
۵. مشارکت نهادهای ذینفع: 4
۶. ارتباطات دیجیتال: 5
۷. گزارش دهی و شفافیت: 5

چالش های اصلی موسسات غیردولتی حین برقراری ارتباطات آنلاین در افغانستان چیست؟ 5

۱. سانسور و کنترل رسانه ها: 6
۲. محدودیت های اینترنت و ارتباطات دیجیتال: 6
۴. محدودیت مشارکت عامه: 6
۵. خطر برداشت نادرست از اظهار نظر: 7
۶. مشارکت نهادهای ذینفع: 7

چگونه می توان به چالش های ارتباطی در افغانستان پاسخ داد؟ 7

رهنمود ارتباطات برای جامعه مدنی افغانستان

۱. نحوه رسیدگی به چالش های (۱) سانسور و کنترل رسانه ها (۲) محدودیت های اینترنت و ارتباطات دیجیتال و (۳) امنیت و محرمانه بودن:..... 7
رویکرد اول - استفاده از شبکه های خصوصی مجازی (VPN):.....7
رویکرد دوم - از اپلیکیشن های ارتباطات رمزگذاری شده و خدمات ایمیل امن استفاده کنید: 9
رویکرد سه – جلب توجه نکنید و دور از توجه عامه باشید: 9
رویکرد چهارم - از حساسیت فرهنگی اجتناب کنید: 9
رویکرد پنجم - آموزش منظم به کارمندان در مورد امنیت سایبری: 9
رویکرد ششم - به‌روزرسانی شیوه‌های امنیت دیجیتال را بررسی کنید:.....10
رویکرد هفتم - یک طرح اضطراری برای پاسخ تهدیدات اینترنتی تهیه کنید: 10
رویکرد هشتم – دیتای حساس را رمزگذاری کرده ذخیره کنید:.....10
رویکرد نهم - اسناد و مدارک ارتباطی موجود در دفتر: 10
رویکرد ده – لزوم پالیسی ایجاد رمزهای عبور و کدهای قوی: 10
۲. چگونه به موضوع محدودیت مشارکت عامه پاسخ دهیم؟..... 14
رویکرد اول - دانش و آگاهی از حساسیت ها: 17
رویکرد دوم - استفاده دقیق از زبانهای رسمی: 18
رویکرد سوم - تعامل با رهبران دینی (ملا امام): 18
رویکرد چهارم - ترویج حقوق بشر جهانی در ساختار محلی: 18
رویکرد پنجم - پیام رسانی محلی: 18
رویکرد ششم - تمایز بین ارتباطات خصوصی و عمومی: 18
رویکرد هفتم - نظارت منظم: 19
رویکرد هشتم – کنترل رسانه های اجتماعی:.....19
۴. چگونه می توان با چالش های مشارکت بهره مندان در افغانستان برخورد کرد؟ 19
رویکرد اول - استفاده از فناوری برای ارتباطات امن: 19
رویکرد دوم - از مولتی میدیا هوشیارانه استفاده کنید: 20
رویکرد سوم – تعامل از طریق دنیای مجازی: 20
رویکرد چهارم - شبکه‌های بین المللی و مشارکت با آنها: 20
رویکرد پنجم – استخدام میانجی در خارج از افغانستان:.....20

امن ترین ابزارهای ارتباطی برای موسسات غیردولتی کدام ها اند؟..... 21

امن ترین ارائه دهندگان خدمات ایمیل برای موسسات غیردولتی کدامها اند؟ 24

امن ترین ابزارهای کنفرانس تصویری برای موسسات غیردولتی کدام ها اند؟ 25

موسسات غیردولتی هنگام برقراری ارتباطات از چه اصطلاحاتی باید اجتناب کنند؟ 28

آیا استفاده از پلتفرم های رسانه های اجتماعی برای موسسات غیر دولتی امن است؟ 31

۱. مزایا 31
مزیت اول – دسترسی و تعامل: 31
مزیت دو – دادخواهی و نتورکنگ: 31
مزیت سه – ارتباط مستقیم: 32
مزیت چهار - جذب مساعدت های مالی: 32
مزیت پنج – انتشار مطالب: 32
مزیت شش - به حداکثر رساندن آگاهی و ارتباطات: 32
۲. اضرار 33
ضرر اول - خطرات امنیتی: 33
ضرر دوم - سانسور و نظارت: 33
ضرر سوم - اطلاعات غلط و اطلاعات نارسا: 33
ضرر چهارم - نگرانی های مربوط به حریم خصوصی: 34
ضرر پنجم - خطرات و تعهدات امنیت دیتا: 34
ضرر ششم - پیمایش چالش های امنیتی در قسمت مساعدت های مالی: 34
ضرر هفتم - تقویت اعتماد: 34

موسسات غیردولتی چگونه باید از رسانه های اجتماعی به صورت امن استفاده کنند؟ 35

رویکرد اول - تدابیر حفاظت از دیتا: 35

رویکرد دوم - تنظیمات حریم خصوصی:.....35
رویکرد سوم - آموزش و آگاهی: 35
رویکرد چهارم – طرح نظارت و پاسخ:.....36
رویکرد پنجم – به روزرسانی منظم و وصله‌ها (PATCHES):.....36
رویکرد ششم - تأیید پیوندها و پیام ها: 36

بخش دوم: ارتباطات اجتماعت مسالمت آمیز.....37

ارتباطات اجتماعات صلح آمیز چیست؟.....38

مولفه های ارتباطات اجتماعات صلح آمیز چیست؟.....38

۱. ارتباطات قبل از اجتماع:.....38
۳. ارتباطات پس از اجتماع:.....39
۴. ارتباطات داخلی:.....39
۵. ارتباطات خارجی: 39
۶. ارتباطات اضطراری:.....39
۷. روابط رسانه ای:.....39

چگونه قبل، حین و بعد از یک اجتماع صلح آمیز ارتباطات برقرار کنیم؟ 40

رویکرد اول - رعایت قانون: 40
رویکرد دوم - نظارت بر وضعیت:.....40
رویکرد سوم – تهیه استراتژی ارتباطات داخلی:.....40
رویکرد چهارم – تهیه استراتژی ارتباطات خارجی: 40
رویکرد پنجم – تهیه استراتژی ارتباطباتات اضطراری:.....41
رویکرد ششم – حفظ روابط با رسانه های خارجی و برون مرزی افغان: 41

رویکرد هفتم – ارتباط با شرکت کنندگان: 41
رویکرد هشتم - هماهنگی با موسسات غیردولتی و سازمان های حقوق بشر: 41
رویکرد نهم - کانال های ارتباطات امن را در نظر داشته باشید: 42
رویکرد دهم - تعامل با سازمان ها و رسانه های بین المللی: 42
رویکرد یازدهم - به اجتماعات مجازی روی آورید: 42
رویکرد دوازدهم - نمایش علائم و بنرها: 42
رویکرد سیزدهم – در شعار دادن و انتخاب کلمات دقیق باشید: 42
رویکرد چهاردهم - از گفتگوی صلح آمیز استفاده کنید: 43
رویکرد پانزدهم - از رسانه های اجتماعی استفاده کنید ولی لایف نروید: 43
رویکرد شانزدهم - تماس های اضطراری: 43
رویکرد هفدهم – مدیریت اوضاع تا دور از توجه عامه بمانید: 43
رویکرد هجدهم - ارتباط بین برگذارکنندگان: 43
رویکرد نوزدهم – جلب توجه نکنید: 43
رویکرد بیستم – از وضعیت خود نزدیکان خود را با خبر سازید: 44
رویکرد بیست و یکم – توضیح مختصر: 44
رویکرد بیست و دوم – احتیاط در رسانه های اجتماعی: 44
رویکرد بیست و سوم - نظارت بر وضعیت: 44
رویکرد بیست و چهارم - طرح اضطراری: 44
رویکرد بیست و پنجم - گفتگو پس از اجتماع: 45
رویکرد بیست و ششم - انتشار دقیق اطلاعات: 45
رویکرد بیست و هفتم – پشتیبانی و پیگیری: 45

در جریان یک اجتماع صلح آمیز از چه اصطلاحات باید اجتناب شود؟ 45

امن ترین ابزار و پلتفورم های ارتباطات برای استفاده در افغانستان کدامند؟ 46

مزایا و اضرار استفاده از رسانه های اجتماعی در یک اجتماع صلح آمیز چیست؟ 46

۱. مزایا: 46
مزیت اول – آگاهی و بسیج: 46
مزیت دوم - به اشتراک گذاری اطلاعات: 46
مزیت سوم –ایجاد گردهمایی: 46
مزیت چهارم – توجه جامعه جهانی: 46
مزیت پنجم – دستیابی و تعامل: 47
مزیت ششم – دادخواهی و شبکه سازی: 47
مزیت هفتم - ارتباط مستقیم: 47
مزیت هشتم - نشر اطلاعات: 47
مزیت نهم - به حداکثر رساندن آگاهی و روابط: 48
۲. اضرار: 48
ضرر اول - نظارت و سرکوب توسط مقامات: 48
ضرر دوم - اطلاعات غلط و اطلاعات نارسا: 48
ضرر سوم - تحریک و خشونت: 48
ضرر چهارم – پراکنده شدن: 48
ضرر پنجم - خطرات امنیتی: 49
ضرر ششم - سانسور و نظارت: 49
ضرر هفتم – اطلاعات غلط و اطلاعات نارسا: 49
ضرر هشتم - نگرانی های مربوط به حریم خصوصی: 49

چگونه در رسانه ها و رسانه های اجتماعی در جریان و بعد از یک اجتماع صلح آمیز حاضر شوید؟ 50

رویکرد اول – ابتدا امنیت: 50
رویکرد دوم - گزارش ناشناس: 50
رویکرد سوم - شبکه های امن: 50
رویکرد چهارم - اشتراک گذاری ترجیهی: 50
رویکرد پنجم - نظارت در زمان واقعی: 50
رویکرد ششم – مشارکت با رسانه های داخلی و بین المللی: 51

رویکرد هفتم - شواهد مستند: 51
رویکرد هشتم – اشتراک گذاری کنترل شده: 51
رویکرد نهم - از کانال های استفاده کنید که به پروتکل های محتوای حساس وابسته باشند: 51
رویکرد دهم – حلقه پیشنهادات و انتقادات: 51
رویکرد یازدهم - اقدامات حفاظت از دیتا: 51
رویکرد دوازدهم - تنظیمات حریم خصوصی: 52
رویکرد سیزدهم - آموزش و آگاهی: 52

چگونه می توان گفت و گوی سازنده ای با نمایندگان اداره موقت طالبان ایجاد کرد؟ 52

۱. نتیجه گیری: 53
۲. دستورالعمل ها: 53
۳. تسهیل خروج صلح آمیز: 53
۴. اوضاع را تحت نظر بگیرید: 53
۵. ارتباطات بعد از اجتماع: 54
۶. اجتماع را مستند کنید: 54

منابع 55

رهنمود ارتباطات برای جامعه مدنی افغانستان

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*

بخش اول: ارتباطات موسسات غیردولتی

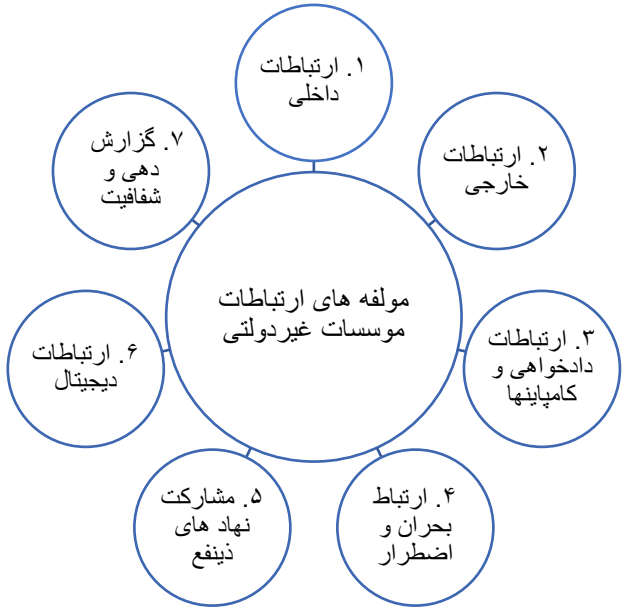
رهنمود ارتباطات برای جامعه مدنی افغانستان

ارتباطات موسسات غیردولتی چیست؟

ارتباطات موسسات غیردولتی به استراتژی‌ها و روش‌هایی اشاره دارد که این موسسات برای به اشتراک گذاشتن اطلاعات، تعامل با نهادهای ذینفع مختلف، پیشبرد اهداف، تطبیق فعالیت‌ها و رسیدن به دستاوردهای شان از آنها استفاده می‌کنند. ارتباطات مؤثر برای موسسات غیردولتی جهت به دست آوردن حمایت، بسیج منابع، تأثیرگذاری بر پالیسی ها و دستیابی به اهداف بسیار مهم است. دامنه ارتباطات موسسات غیردولتی ابعاد داخلی و خارجی را در بر می گیرد و در حال تغییر است چون با رشد رسانه‌ها و فناوری، تحول مقامات، تغییر پالیسی های تمویل کنندگان و رفتارهای مخاطبان تکامل می‌یابد. این امر مستلزم مطابقت، وضاحت و درک عمیق از مقامات، تمویل کنده گان و ارزش‌های مخاطبان است. با تسلط بر این جنبه‌ها، موسسات غیردولتی می‌توانند روابط خود را با بهرمندان تقویت، ایمنی آنها را تضمین کنند، دیدگاه و تأثیرگذاری آن‌ها را افزایش دهند و به وجه احسن به اهداف کاری خود دست یابند.

مولفه های ارتباطات موسسات غیردولتی چیست؟

اینجا چند مؤلفه ارتباطات موسسات غیردولتی را برای شما به معرفی میگیریم، اما نمیتوان مؤلفه ها را به اینها محدود کرد:



۱. ارتباطات داخلی:

موسسات غیردولتی باید مطمئن باشند که اعضا، کارمندان و رضاکاران آنها ایمن، آگاه، با انگیزه، پاسخگو و همسو با اهداف و ماموریت آنها هستند. برای تحقق ارتباطات داخلی، موسسات غیردولتی از ابزارهای مختلفی استفاده می‌کنند، از جمله ایمیل، خبرنامه، جلسات روزمره آنلاین و حضوری، و پلتفرم های جلسات گروهی، مانند Jitsi، Slack یا Microsoft Teams. مؤلفه ارتباطات داخلی موسسات غیردولتی شامل حسابدهی داخلی، به روز رسانی، اجرای برنامه های آموزشی، تغییرات و اصلاحات پالیسی های داخلی، و تسهیل نظرات و بحث های روزانه بین اعضا، کارمندان و رضاکاران میباشد.

شکل ۱: مؤلفه های ارتباطات موسسات غیردولتی

۲. ارتباطات خارجی:

ارتباطات خارجی موسسات غیردولتی هرگونه ارتباطات ممکن و مورد توافق را با تمویل کنندگان، نهادهای ذینفع، مقامات، بهره مندان،رسانه ها و مردم تضمین می‌کند. موسسات غیردولتی از ابزارهای مختلفی برای ارتباطات خارجی استفاده می‌کنند، از جمله وبسایت‌ها، پلتفرم های رسانه های اجتماعی، ابزارهای ارتباطی، بیانیه های مطبوعاتی و موضع‌گیریهای مدنی، ایمیل‌ها، وبلاگ‌ها و رسانه های همگانی. مؤلفه ارتباطات خارجی بر اساس چندین عامل متفاوت است و شامل کمپاین ها جهت افزایش آگاهی در مورد کار موسسات و کسب بودجه، گزارش فعالیت ها و تأثیرات آنها بالای اجتماع، روایت های از تغییر در زندگی بهره مندان، تثبیت موقعیت نهاد، پیام های دادخواهی، و مواد انکشافی میشود.

۳. ارتباطات دادخواهی و کامپاین ها:

موسسات غیردولتی بر افکار عامه، پالیسی ها و قوانین مرتبط با اهداف و مأموریت کاری شان تاثیر گزار اند. آنها از ابزارها و رویکردهای مختلفی استفاده می کنند، از جمله اجتماعات صلح آمیز، لابی گری، برگزاری دادخواست[1]، کمپاین های رسانه های اجتماعی، مشارکت با اینفلوئنسرها اشخاص اثرگذار رسانه های اجتماعی و پخش اطلاعیه های خدمات عامه. موسسات غیردولتی با ایجاد پیام های واضح و قانع‌کننده، شناسایی مخاطبان مورد نظر، و انتخاب ترکیب مناسب کانال‌ها برای رسیدن به حامیان و بسیج آن‌ها، سعی می‌کنند استراتژیک باشند.

۴. ارتباطات بحران و اضطرار:

هدف موسسات غیردولتی مدیریت و کاهش اثرات منفی بحران‌ها بر اهداف و فعالیت‌های روزمره شان است. برای تحقق این امر، آنها از رویکردهای مختلفی از جمله تهیه طرح ارتباطات بحران، ایجاد تیم های واکنش سریع، ایجاد ارتباطات واضح و شفاف در هنگام بحران، ارزیابی و طرح تهیه گزارش پس از بحران استفاده می کنند.

۵. مشارکت نهادهای ذینفع:

[1] Petition drives

موسسات غیردولتی مصمم به ایجاد و حفظ روابط مثبت با افراد و موسساتی اند که در پروژه یا فعایت های عمومی موسسات غیردولتی علاقه دارند یا در آن سهیم هستند. موسسات از روشهای مختلفی استفاده می‌کنند، از جمله به‌روزرسانی‌های منظم، دعوتنامه برای شرکت در برنامه ها یا پروژه ها، نظرسنجی برای جمع آوری اطلاعات، و دریافت حمایت از این نهادها.

۶. ارتباطات دیجیتال:

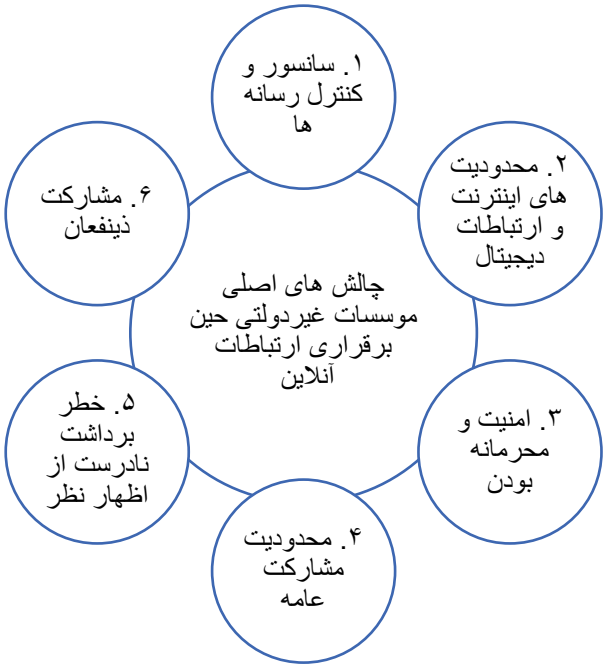
سازمان‌های غیردولتی از ارتباطات دیجیتالی استفاده می‌کنند، زیرا در دنیای امروزی، پلتفرم های دیجیتال برای دستیابی به مخاطبان به صورت وسیع کارآمد و مقرون به صرفه ضروری هستند. آنها از ابزارهای وسیع و استراتژی متعددی استفاده می کنند، از جمله بهینه سازی موتور جستجو SEO (Search Engine Optimization) برای دید بهتر آنلاین، ترویج محتوای کاری شان، بیان روایت های به صورت تصویری، خبرنامه های الکترونیکی، و همچنان تحلیل برای اندازه گیری تعامل و اثرگذاری کاری شان بالای اجتماع.

۷. گزارش دهی و شفافیت:

سازمان‌های غیردولتی با به اشتراک گذاشتن آشکار اطلاعات در مورد فعالیت‌ها، امور مالی و نتایج، از نشان دادن پاسخگویی به تنظیم‌کننده های دولتی، اهداکنندگان، شرکا و ذینفعان اطمینان حاصل می‌کنند. آنها از مکانیسم ها و گزارشهای مختلف پاسخگویی، از جمله گزارشهای نیمه‌سالانه و سالانه، صورت‌های مالی، گزارشهای پروژه، گزارشهای سازمانی، ممیزی‌های مالی و ارزیابی تأثیرات استفاده می‌کنند که اغلب در وبسایت سازمان غیردولتی و در برخی موارد از طریق رسانه‌های اجتماعی به اشتراک گذاشته می‌شوند.

چالش های اصلی موسسات غیردولتی حین برقراری ارتباطات آنلاین در افغانستان چیست؟

ارتباطات موسسات غیردولتی در افغانستان با چالشهای متمایز مواجه است. آنها در یک محیط بسیار محدود و حساس فعالیت می‌کنند که بر نحوه ارتباطات این نهادها در داخل و خارج تأثیر گذاراست. محیط فعالیت موسسات غیردولتی نیازمند یک رویکرد استراتژیک و انعطافپذیر برای ارتباطات، با تاکید بر امنیت شان، سازگاری و حساسیت به بافت پیچیده اجتماعی-سیاسی است. حفظ مؤثریت و تأثیرگذاری در عین حال حصول اطمینان از ایمنی کارمندان و بهره مندان، تعادل ظریفی است که موسسات غیردولتی باید با احتیاط با آن برخورد کنند. در اینجا مروری بر چالش های عمده ای داریم که بر ارتباطات موسسات غیردولتی تأثیرگذار اند:



۱. سانسور و کنترل رسانه ها:

کنترل شدیدی بر آزادی بیان و رسانه های همگانی اعمال شده است که مستقیماً بر نحوه ارتباطات موسسات غیردولتی با مردم تأثیر می گذارد. برای جلوگیری از تحت توجه بودن توسط اداره موقت طالبان به صورت منفی[2]، جو خودسانسوری در میان موسسات غیردولتی به شدت جا افتاده است.

۲. محدودیت های اینترنت و ارتباطات دیجیتال:

دسترسی به اینترنت، استفاده از پلتفرم های دیجیتال و رسانه های اجتماعی همگی تحت نظارت بوده و در برخی موارد محدود شده اند.[3] موسسات غیردولتی باید به دقت از این محدودیت ها عبور کنند تا به فعالیت های خود بدون به خطر انداختن کارمندان و بهره مندان خود ادامه دهند.

۳. امنیت و محرمانه بودن:

ارتباطات فعالیت های موسسات غیردولتی تحت نظارت شدید اداره موقت طالبان است[4]. موسسات غیردولتی باید امنیت و محرمانه بودن ارتباطات خود را برای محافظت از هویت و ایمنی کارمندان خود و افرادی که به آنها خدمت ارایه می کنند، در اولویت قرار دهند. در چنین شرایط، کانال‌های ارتباطات امن و سرویس‌های پیام‌رسانی رمزگذاری‌شده به طور فزاینده‌ای حیاتی می‌باشد.

۴. محدودیت مشارکت عامه:

[2] https://www.hrw.org/news/2021/10/01/afghanistan-taliban-severely-restrict-media
[3] https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf
[4] https://www.csis.org/analysis/talibans-increasing-restrictions-civil-society-and-aid-organizations

دامنه مشارکت عامه و کمپاین های دادخواهی به میزان قابل توجهی در افغانستان کاهش یافته است. موسسات غیردولتی مجبورند ارتباطات عامه خود را محدود کنند و اغلب به فعالیت‌های کم‌رنگ تکیه می‌کنند تا مورد توجه مقامات قرار نگیرند.[5]

۵. خطر برداشت نادرست از اظهار نظر:

ارتباطاتی که حاوی انتقاد از اداره موقت طالبان و یا از حقوق بشر که بر خلاف اصول طالبان و قرائت شان از قوانین شریعت، دفاع می کند، خطرساز هستند. موسسات غیردولتی باید اظهارات خود را با دقت بیان کنند تا اینکه مبادا سهوی کارمندان و فعالیت های خود را به خطر مواجه سازند.

۶. مشارکت نهادهای ذینفع:

تعامل با تمویل کنندگان بین المللی، نهادهای همکار و جامعه جهانی هر روز پیچیده تر می شود.[6] موسسات غیردولتی باید راهی برای انتقال گزارش وقایع از محل، بیان روایت ها، دادخواهی به هدف کسب حمایت از نهادهای بین المللی و نشان دادن تأثیرگذاری شان بالای مردم راه‌های معمول ارتباطات ساده تر و امنی پیدا کنند.

چگونه می توان به چالش های ارتباطی در افغانستان پاسخ داد؟

۱. نحوه رسیدگی به چالش های (۱) سانسور و کنترل رسانه ها (۲) محدودیت های اینترنت و ارتباطات دیجیتال و (۳) امنیت و محرمانه بودن:

رویکرد اول - استفاده از شبکه های خصوصی مجازی (VPN):

استفاده از شبکه های خصوصی مجازی (VPN) برای دسترسی ایمن به اینترنت و دور زدن محدودیت ها و سانسور یکی از روشهای مناسب به شمار میرود. این امر به پنهان کردن ترافیک اینترنت و محافظت از هویت آنلاین شما کمک می کند. به خاطر داشته باشید که به همه کمپنی های ارائه دهندگان خدمات

[5] https://press.un.org/en/2023/sc15222.doc.htm
[6] https://www.rferl.org/a/afghanistan-taliban-ban-swedish-ngo-humanitarian-crisis/32504979.html

VPN اعتماد نکنید. برخی از دولت ها نیز از شرکت های VPN برای دسترسی به داده های مورد نیاز خود استفاده می کنند. در اینجا چند ارائه دهنده خدمات VPN محبوب وجود دارد که می توانید از آنها استفاده کنید:

نام	ارائه دهنده خدمات	مزایا	معایب	کشور میزبان
ProtonVPN	Proton Technologies AG	تعهد قوی به حفظ حریم خصوصی و امنیت، مستقر در سوئیس با قوانین حفظ حریم خصوصی مطلوب، پالیسی عدم ورود به سیستم، ویژگی Secure Core برای امنیت بیشتر.	ممکن است به دلیل رمزگذاری سنگین سرعت کمتری داشته باشد.	Switzerland
	وبسایت	https://protonvpn.com/		
Mullvad	Amagicom AB	متمرکز بر حفظ حریم خصوصی، پالیسی بدون گزارش، پشتیبانی از پرداخت های ناشناس توسط کریدت کارد، پشتیبانی از پروتکل WireGuard، حالت پل مانند برای دور زدن سانسورها.	رابط کاربری ممکن است برای برخی از کاربران کمتر کاربرپسند باشد.	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/		
NordVPN	Tefincom & Co., S.A	شبکه سرور گسترده، رمزگذاری قوی، سرورهای تخصصی برای امنیت بیشتر و مبهم سازی، دو VPN برای محافظت بیشتر.	در سال 2018 یک حادثه امنیتی در یکی از کشورهای (14-Eyes) داشت.	Panama
	وبسایت	https://nordvpn.com/		

Isle of Man	سیاست حفظ حریم خصوصی مانند برخی از ارائه دهندگان دیگر قوی نیست، سرعت متغیر در سرورهای مختلف است.	برنامه های کاربر پسند، رمزگذاری قوی، پشتیبانی از چندین دستگاه، سرورهای اختصاصی برای پخش و تورنت.	Kape Technologies	CyberGhost
	https://www.cyberghostvpn.com/		وبسایت	

شکل ۳: ارائه دهنده خدمات محبوب VPN

رویکرد دوم - از اپلیکیشن های ارتباطات رمزگذاری شده و خدمات ایمیل امن استفاده کنید:
از برنامه های ارتباطی ایمن و رمزگذاری شده و خدمات ایمیل امن برای ارتباطات داخلی و خارجی استفاده کنید. چندین اپلیکیشن ارتباطی امن با قابلیت رمزگذاری و همچنان خدمات ایمیل امن وجود دارد (به شکل های ۸ و ۹ مراجعه کنید).

رویکرد سه – جلب توجه نکنید و دور از توجه عامه باشید:
اگر در افغانستان کار می کنید، رویکردی را استفاده کنید که زیاد مورد توجه عامه نباشید و با حفظ آن در ارتباطات و فعالیت های عمومی تمرکز داشته باشید. از حضور در رسانه های اجتماعی و مصاحبه های تلویزیونی خودداری کنید. این می تواند شما را از نظارت شدید مقامات در امان داشته باشد و اگر چنین نکنید ممکن است اداره موقت طالبان کار شما را حساس یا مشکل ساز بدانند.

رویکرد چهارم - از حساسیت فرهنگی اجتناب کنید:
با مشورت با کارشناسان افغان در طراحی برنامه های تان، اطمینان حاصل کنید که همه ارتباطات و برنامه ها ارتباطی از نظر فرهنگی حساسیت زا نیستند. این امر خطر توجه منفی گروههای حاکم را کاهش می دهد.

رویکرد پنجم - آموزش منظم به کارمندان در مورد امنیت سایبری:
آموزش های منظمی را به کارمندان در مورد امنیت دیجیتال، روشهای ارتباطی امن، و راهنمایی امن در محیط های محدود ارائه دهید. اگر موسسات شما قادر به ارائه چنین آموزشی نیست، با موسسات و

افراد متخصص در امنیت دیجیتال کمک بگیرید. آنها می توانند مشوره های به روز، راه حل های تکنولوژیکی و حمایوی را برای دریافت راه حل به چالش های دیجیتال ارائه دهند. موسسات زیادی وجود دارند که می توانند به شما کمک کنند.

رویکرد ششم - به‌روزرسانی شیوه‌های امنیت دیجیتال را بررسی کنید:

به طور منظم شیوه های امنیت دیجیتال را به روز کنید. فناوری های نظارت دیجیتال به طور مداوم در حال پیشرفت هستند. در نتیجه، به طور منظم اقدامات امنیتی دیجیتال را برای مقابله با تهدیدات جدید و استفاده از فناوری‌های ارتباطی امن در حال ظهور، بررسی و به‌روزرسانی کنید.

رویکرد هفتم - یک طرح اضطراری برای پاسخ تهدیدات اینترنتی تهیه کنید:

یک طرح اضطراری واضح برای اقداماتی که در صورت قطع شدن اینترنت، برخوردهای نظارت دیجیتال یا به خطر افتادن ابزارهای دیجیتال کاربرد داشته باشد تهیه نمایید. وجود چنین طرحها تضمین می کند که کارمندان برای محافظت از اطلاعات شان و اطلاعات افراد دخیل در موسسه، به صورت سریع و امن واکنش نشان دهند.

رویکرد هشتم – دیتای حساس را رمزگذاری کرده ذخیره کنید:

با استفاده از پلتفرم های مناسب، دیتا حساس تان را رمزگذاری کرده ذخیره کنید و همچنان از پلتفرم هایی استفاده کنید که امکانات امنیتی قوی ارائه می دهند. برای اطمینان از یکپارچگی دیتا و و محافظت در برابر دسترسی کسی به آنها یا از دست دادن غیرمجاز این دیتا، از قابلیت های کنترل قابل دسترسی و روشهای امن استفاده کنید.

رویکرد نهم - اسناد و مدارک ارتباطی موجود در دفتر:

علاوه بر امنیت دیجیتال، اطمینان حاصل کنید که اسناد و مدارک موجود در دفتر که حاوی اطلاعات حساس اند امن نگهداری شوند. از اجرای پالیسی های سختگیرانه جهت دسترسی و جابجایی این مدارک استفاده کنید.

رویکرد ده – لزوم پالیسی ایجاد رمزهای عبور وکدهای قوی:

پالیسی هایی را اجرا کنید که مستلزم استفاده از رمزهای عبور قوی و منحصر به فرد برای همه حساب ها و خدمات است. هنگام انتخاب رمز عبور:

- به جای استفاده از یک رمز عبور کوتاه و واضح، یک رمز عبور جدید، پیچیده و قوی بنویسید.

رهنمود ارتباطات برای جامعه مدنی افغانستان

- از نمادها، حروف بزرگ، حروف کوچک، علائم و اعداد در رمز عبور خود استفاده کنید.
- به رمز عبور ویندوز اتکا نکنید. آنها به سرعت شکننده اند.
- از رمز عبور با حداقل هشت کاراکتر استفاده کنید.
- در صورت تغییر دادن، همیشه از یک رمز عبور جدید استفاده کنید.
- از رمز عبور امن استفاده کنید که هیچ ربطی به سرگرمی های شما و یا زندگی شخصی شما ندارد.
- هر یک ماه و یا هر سه ماه، رمز عبور را تغییر دهید.
- کارمندان را تشویق کنید تا از اپلیکیشن های مدیریت رمز عبور برای امن کردن رمز عبور خود استفاده کنند.

در اینجا برخی از امن ترین اپلیکیشن های مدیریت رمز عبور برای موسسات غیر دولتی آورده شده است:

نام	نام ارائه دهنده خدمات	مناسب بودن	کشور میزبان
Bitwarden:	8bit Solutions	اولویت به شفافیت، ایده آل برای کاربران آگاه به امنیت دیجیتال. این اپلیکیشن رمزگذاری منبع باز، سرتاسر و مقرون به صرفه را ارائه می دهد.	ایالات متحده
	وبسایت	https://bitwarden.com/	
LastPass	LogMeIn, Inc	کاربر پسند با احراز هویت چند عاملی و ویژگی های اشتراک گذاری ایمن. مناسب برای کسانی که برای راحتی و همکاری ارزش قائل هستند.	ایالات متحده
	وبسایت	https://www.lastpass.com/	
1Password	AgileBits Inc	دارای ویژگی‌های امنیتی قوی، قابلیت در حال سفر برای محافظت بیشتر، و برج مراقبت برای نظارت بر نقض و تخطی، آن را برای کسانی که به دنبال امنیت جامع هستند ایده‌آل می‌کند.	کانادا
	وبسایت	https://1password.com/	

Dashlane	Dashlane Inc	نظارت بر وب تاریک، VPN و تغییر رمز عبور را ارائه می دهد. برای کاربرانی که به دنبال امنیت بیشتر فراتر از مدیریت رمز عبور اولیه هستند مفید است.	ایالات متحده
	وبسایت	https://www.dashlane.com/	
KeePassXC	KeePassXC Development Team	بهترین برای کاربرانی که کنترل و حریم خصوصی را در اولویت قرار داده و مدیریت رمز عبور محلی رایگان و منبع باز را ارائه می دهند.	آلمان
	وبسایت	https://keepassxc.org/	

شکل ۴: بهترین اپلیکیشن های مدیریت رمز عبور برای سازمان های غیردولتی

رویکرد یازده - از 2FA استفاده کنید:

روش احراز هویت دو مرحله ای (2FA) را در تمام حساب های خود تطبیق کنید. در صورت امکان، احراز هویت دو مرحله‌ای را جهت ایجاد یک لایه امنیتی اضافی در حساب‌ها، به ویژه در حساب هایی که برای فعالیت های موسسه استفاده میکنید، فعال کنید.

رویکرد دوازدهم - ایجاد طرح واکنش به واقعات غیر مترقبه:

برای مقابله با نقض احتمالی امنیتی یا نشت دیتا، یک طرح واکنش روشن و قابل اجرا برای مقابله با واقعات غیر قابل مترقبه ایجاد کنید. این طرح باید شامل مراحل مهار، ارزیابی، اطلاع رسانی و بازیابی باشد. اگر وب سایت شما هک شد یا رمز عبور حساب های شما به خطر افتاد، آماده باشید. شما باید برای همه این سناریوها آمادگی داشته باشید.

رویکرد سیزدهم – استفاده از TOR :

برای موقعیت هایی که نیاز به ناشناس بودن دارید، از ابزارهای طراحی شده برای ارتباطات ناشناس، مانند TOR، برای دسترسی به اینترنت یا انتقال دیتا و اطلاعات حساس استفاده کنید. در اینجا برخی از مناسب ترین TOR ها برای شما به معرفی گرفته شده است:

نام	نام ارائه دهنده خدمات	مناسب بودن	کشور میزبان

Tor Browser	The Tor Project	شناخته شده ترین و پرکاربردترین ابزار برای دسترسی به شبکه TOR. این برای کاربرانی که در هنگام مرور وب نیاز به ناشناس ماندن و محافظت از حریم خصوصی قوی دارند ایده آل است.	جهانی (مرکز آن در ایالات متحده آمریکا)
	وبسایت	https://support.torproject.org/tbb/	
Brave Browser with TOR	Brave Software	همراه با TOR، ویژگی‌های حفظ حریم خصوصی و قابلیت‌های داخلی مسدود کردن تبلیغات را فراهم می‌کند. برای کاربرانی که خواهان یک مرورگر جایگزین با ادغام Tor هستند مناسب است.	ایالات متحده
	وبسایت	https://community.brave.com/	
Whonix	Whonix Project	Whonix یک سیستم عامل متمرکز بر حریم خصوصی است که در داخل یک ماشین مجازی اجرا می شود و تمام ترافیک اینترنت را از طریق شبکه TOR هدایت می کند. برای کسانی که به دنبال راه حل جامع تری برای حفظ حریم خصوصی فراتر از ناشناس بودن مرورگر هستند، مناسب است.	جهانی
	وبسایت	https://www.whonix.org/	
Tails (The Amnesic Incognito Live System)	Tails Project	Tails یک سیستم عامل زنده است که با USB یا DVD طراحی شده و تمام ترافیک اینترنت را از طریق TOR هدایت می کند. این برای کاربرانی که می خواهند ناشناس بمانند و ردپایی از خود در سیستم میزبان بر جای نگذارند مناسب است.	جهانی
	وبسایت	https://tails.net/	
Orbot/Orfox	The Guardian Project	Orbot یک برنامه پروکسی است که تمام ترافیک دستگاه تلفن همراه شما را از طریق شبکه TOR هدایت می کند، در حالی که Orfox مرورگر وب رسمی پروژه TOR برای اندروید است. اینها برای کاربرانی که نیاز به ناشناس بودن TOR در دستگاه های تلفن همراه خود دارند مناسب است.	ایالات متحده

	وبسایت	https://guardianproject.info/apps/info.guardianproject.orfox/	

شکل ۵: برخی از مناسب ترین TOR ها

۲. چگونه به موضوع محدودیت مشارکت عامه پاسخ دهیم؟

پاسخگویی به مشکل مدودیت مشارکت عامه ایجاب می‌کند که موسسات غیردولتی رویکردهای نوآورانه ای را اتخاذ کنند تا به تلاش‌های خود به طور محتاطانه و مؤثر ادامه دهند. با تنظیم استراتژی‌ها برای تمرکز بر ظرافت، امنیت و استفاده از شبکه‌های محلی، موسسات غیردولتی می‌توانند به تعامل با مردم و حمایت از اهداف آنها ادامه دهند. موسسات غیردولتی معمولاً از طریق شوراها، جرگه‌ها و رهبران محلی، با بهره مندان خود تماس می‌گیرند و خدمات خود را ارائه می‌دهند. یک دسته از نهادهای جامعه مدنی در افغانستان به نام شوراها و جرگه ها وجود دارد. آنها شوراهای محلی سنتی هستند که روستاها یا قبایل آنها را ایجاد می کنند، معمولاً برای نشان دادن منافع یک محل به سایر بخش های جامعه. شوراها و جرگه ها نهادهای تصمیم گیری محلی هستند که مسلماً سنتی ترین واحدهای جامعه مدنی در افغانستان به شمار میروند. آنها عموماً از بزرگان روستا تشکیل شده اند و به صورت غیررسمی (یعنی به عنوان گروه های ثبت نشده) فعالیت می کنند.
موسسات غیر دولتی مستقیماً و همچنین از طریق شوراها، جرگه ها و رهبران جامعه با بهره مندان خود ارتباط برقرار می کنند. بهره مندان موسسات غیردولتی اقشار مختلف جامعه هستند، از جمله:

موسسات غیردولتی اغلب بر حقوق زنان، توانمندسازی، آموزش و پرورش، مراقبت های بهداشتی و مقابله با خشونت و تبعیض تمرکز می کنند.	زنان و دختران
موسسات غیردولتی برای بهبود دسترسی به آموزش، مراقبت های بهداشتی، تغذیه و حفاظت از کودکان تلاش می کنند.	اطفال

رهنمود ارتباطات برای جامعه مدنی افغانستان

آوارگان داخلی (IDPs)	موسسات غیردولتی کمک، سرپناه، مراقبت های بهداشتی و حمایت معیشتی را به افراد و خانواده هایی که در داخل به دلیل درگیری ها و حوادث طبیعی آواره شده اند، ارائه می کنند.
پناهندگان	موسسات غیردولتی خدمات و حمایت هایی را برای پناهندگان و عودت کنندگان در افغانستان ارائه می کنند، از جمله کمک در زمینه اسکان مجدد، آموزش، مراقبت های صحی، و فرصت های معیشتی.
جوامع به حاشیه رانده شده	موسسات غیردولتی با برنامه ها و خدمات مختلف، گروه های به حاشیه رانده شده، مانند اقلیت های قومی، افراد دارای معلولیت، و افرادی که در مناطق دورافتاده یا متاثر از درگیری های داخلی زندگی می کنند، هدف قرار می دهند.
قربانیان حوادث طبیعی	موسسات غیردولتی به افراد آسیب دیده از حوادث طبیعی مانند سیل، خشکسالی، زلزله و برف کوچ کمک و حمایت می کنند.
دریافت کنندگان مراقبت های صحی	موسسات غیردولتی از سیستم های مراقبت‌های بهداشتی، ارائه خدمات صحی، ایجاد زیرساخت‌ها، و ترویج آموزش صحی و درمانی و کمپین‌های آگاهی دهی حمایت می‌کنند.

شکل ۶: بهره مندان سازمان های غیردولتی در افغانستان.

برای ارتباط با این بهره مندان، موسسات غیردولتی باید با شوراها و جرگه های محلی و همچنین ملا امامان و رهبران مذهبی، اجتماعی و محلی ارتباط برقرار کنند. این دسته از نهادهای مدنی و افراد می‌توانند نقش مهمی در انتشار اطلاعات و حمایت از تغییر به گونه‌ای موثر ایفا کنند بخصوص اطلاعاتی که از نظر فرهنگی حساس باشد تا کمتر توجه ناخواسته را به خود جلب کند.

پیشوایان دینی (ملا امامان):	این گروه شامل افرادی است که به عنوان امام جماعت مساجد، مربیان دینی در مدارس و مساجد و کارشناسان مذهبی مشغول به کار هستند. ملاها در محلات افراد

	سرشناس و آگاه در ارتباط به ساکنان هستند. آنها بعد سالها خدمت در مسجد ساکنان محل مرتبط به مسجد را می شناسند. اگر موسسات غیردولتی می‌خواهند با بهره مندان واجد شرایط ارتباط برقرار کنند، باید با این رهبران مذهبی رابطه کاری ایجاد کنند.
رهبران محلی (ملک، ارباب):	در قرا و قصبات، ملک ها یا اربابها به‌عنوان نمایندگان محلی عمل نموده و از منافع قریه هم در داخل قریه و هم در خارج از آن نمایندگی می‌کنند. این افراد با همه ساکنان روستای خود ارتباط خوبی دارند و کاردان هستند. موسسات غیردولتی که به دنبال ارائه خدمات به بخشهای خاصی از قریه هستند، متوجه خواهند شد که ملک و ارباب می‌تواند در تسهیل ارتباطات مؤثر باشند.
وکیل گذر:	وکیل گذر نماینده محلات در شهرها است که برای یک دوره خاص توسط مردم محل در یک شهرداری انتخاب می شود. این افراد آگاه نقش کلیدی را در کمک به موسسات غیردولتی از طریق ارتباطات آنها با بهره مندان بازی میکنند.

شکل ۷: افراد کلیدی برای دستیابی به بهره مندان واجد شرایط در افغانستان.

توجه: به خاطر داشته باشید که موثریت این افراد ممکن است بر اساس نگرش فردی آنها متفاوت باشد.

در همین حال سازمان های غیردولتی باید:

• از تعاملات جامعه محور در مقیاس های کوچک با تعداد اندکی از اشتراک کنندگان استفاده کنید. به جای کمپین های عمومی بزرگ، روی برنامه های کوچکتر تمرکز کنید که پر سرو صدا نباشند. کارگاهای آموزشی، گفتگوها و جلسات آموزشی که در محیطهای خصوصی برگزار می‌شوند، می‌توانند بدون جلب توجه، تعامل و آگاهی را تقویت کنند.

• تاکتیک های ارتباطات غیرمستقیم و دادخواهانه را اتخاذ کنید. از داستان سرایی، هنر و رویدادهای فرهنگی به عنوان راه‌های غیرمستقیم برای برقراری ارتباطات پیام‌ها و تقویت بحث‌ها

پیرامون موضوعات مهم استفاده کنید. این روش‌ها می‌توانند کمتر شما را در تقابل قرار دهد و برای مقامات که ساحه کاری شما را محدود میسازند قابل قبول باشند.

• روشهای ارتباطات خصوصی با بهره مندان خود را تقویت کنید و برای تعامل مستقیم با آنها، خطوط ارتباطات قوی و امن را حفظ کنید. برنامه‌های پیام‌رسانی رمزگذاری‌شده و خطوط مستقیم می‌توانند تعاملات خصوصی را تسهیل کنند؛ بعلاوه آنها میتوانند حمایت، اطلاعات و منابع را بدون قرار گرفتن در معرض عمومی برای شما ارائه دهند.

۳. چگونه با خطر برداشت نادرست از اظهار نظر و نشرات مقابله کنیم؟

مقابله با خطر برداشت نادرست از اظهارنظر در افغانستان، به ویژه در مورد ارتباطاتی که به طور بالقوه به عنوان انتقاد از اداره موقت طالبان یا دفاع از حقوق بشر بر خلاف قرائت آنها از شریعت تلقی می شود، نیازمند یک رویکرد استراتژیک و محتاطانه است. موسسات غیردولتی باید از این وضعیت حساس عبور کنند تا بدون به خطر انداختن امنیت و فعالیت های شان به کار خود ادامه دهند. با به کارگیری این رویکردهای استراتژیک، موسسات غیردولتی می توانند محیط پیچیده و خطر ساز فعالیت در افغانستان را کنترل کنند و خطر سوء برداشت نادرست از اظهار نظرات شان و پیامدهای بالقوه را به حداقل برسانند تا برای تحقق اهداف و ارایه خدمت به بهره مندان شان ادامه داده بتوانند.

رویکرد اول - دانش و آگاهی از حساسیت ها:

دانش و آگاهی از حساسیت ها گام های کلیدی در توسعه درک عمیق از موضوعات فرهنگی و سیاسی در افغانستان است. این دانش و آگاهی می تواند ساختار پیام ها را به گونه ای هدایت کند که در محلات طنین اندازی مثبتی داشته باشد و در عین حال اهداف موسسات غیردولتی را ارتقا دهد. تمام فرامین، احکام، متحدالمالها، دستورات و تصمیمات صادر شده توسط اداره موقت طالبان پس از ماه آگست ۲۰۲۱ که مربوط به کار شما هستند را مرور کنید تا از آخرین تحولات و حساسیت ها در افغانستان مطلع شوید. برای اطلاع از فرامین، احکام، متحدالمالها، دستورات و تصمیمات مربوط به کار خود، باید با وزارتخانه ها یا ادارات مربوطه اداره موقت طالبان تماس بگیرید. بنابر ملاحظات که دارند، اداره موقت طالبان هیچ یک از این اسناد را در یک وب سایت مشخص منتشر نکرده است.

رویکرد دوم - استفاده دقیق از زبانهای رسمی:

استفاده دقیق از زبان های رسمی یکی دیگر از عوامل کلیدی در ایجاد ارتباطات بدون تقابل است که بر ارزش ها و اهداف مشترک انسانی مرتبط است. علاوه بر این، موسسات غیردولتی فعال در داخل افغانستان باید از به چالش کشیدن یا انتقاد مستقیم هرگونه تصمیم و سیاست در تریبون های عمومی، رسانه های اجتماعی و رسانه های جمعی خودداری کنند. اگر می خواهید تغییراتی را در کشوری مانند افغانستان ببینید، حرفه ای بودن بسیار امن تر از فعال بودن است. انتقاد از هرگونه تصمیم طالبان در بین مردم، از طریق رسانه‌های اجتماعی و رسانه‌های جمعی، مخالفت با اداره موقت طالبان تلقی می‌شود که طالبان آنرا مخالفت با شریعت میدانند و این امر کار موسسه منتقد را در داخل افغانستان نا ممکن میسازد. به همین دلیل باید استراتژیک برخورد کنید و بیشتر حروفی باشید.

رویکرد سوم - تعامل با رهبران دینی (ملا امام):

تعامل با رهبران مذهبی (ملا امام) نیز در صورتی که دیدگاه مشترکی در مورد مسائل بشردوستانه داشته باشند، گامی مفید است. تأیید یا مشارکت آنها می تواند اعتبار و چارچوب مناسب فرهنگی را به ابتکارات موسسات غیردولتی بدهد و خطر تفسیرهای نامطلوب را کاهش دهد.

رویکرد چهارم - ترویج حقوق بشر جهانی در ساختار محلی:

ترویج حقوق بشر در یک ساختار محلی نیز برای کاهش سطح سوء تعبیر مفید است. موسسات غیردولتی باید بحثهایی را پیرامون حقوق بشر و اهداف انکشافی شان در چارچوب ارزشها و سنتهای محلی تنظیم کنند. نشان دهید که چگونه این ابتکارات با بهبود جامعه مطابقت دارند و به جای تفاوت ها روی ساختار های مشترک تمرکز می کنند.

رویکرد پنجم - پیام رسانی محلی:

پیام های محلی نیز یک عامل کلیدی است. پیام های خود را با روایت ها و دیدگاه های محلی تنظیم کنید. از روایت ها و مثال هایی استفاده کنید که تجربیات و آرمانهای محلی را منعکس می کند، پیام را مرتبط تر می سازد و احتمال سوء تعبیر را کاهش می دهد.

رویکرد ششم - تمایز بین ارتباطات خصوصی و عمومی:

بین ارتباطات عمومی، که ممکن است نیاز به تعمیم و بیان دقیقتر داشته باشد، و ارتباطات خصوصی، که در آن بحثهای مستقیم و خاصتر می‌توانند در گروه‌های امن و بسته انجام شود، تمایز قائل شوید.

رویکرد هفتم - نظارت منظم:
وضعیت ارتباطات خود را در میان اقشار مختلف مردم افغانستان به طور منظم نظارت کنید و استراتژی های خود را بر اساس نظرخواهی تنظیم کنید تا از فهم مورد نظر پیام های تان توسط مردم اطمینان حاصل کنید.

رویکرد هشتم – کنترل رسانه های اجتماعی:
هنگام ارسال هر چیزی در شبکه های اجتماعی، محتاط باشید. تمام ابعاد یک پست در شبکه های اجتماعی را در نظر بگیرید. هرگز اجازه ندهید کارمندان چیزی بدون تایید مافوق خود پست کنند. اگر بودجه شما اجازه می دهد، یک کارشناس ارتباطات و رسانه های اجتماعی استخدام کنید.

توجه: شما درک عمیق تری از فعالیت های تان، پروژه و بهره مندان خود نسبت به ما دارید و در صورت ناکافی بودن این استراتژی ها، می توانید بهترین راه حل ممکن را برای جلوگیری از هرگونه برداشت نادرست از اظهار نظر و نشریات تان بیابید.

۴. چگونه می توان با چالش های مشارکت بهره مندان در افغانستان برخورد کرد؟

پرداختن به پیچیدگی‌های مشارکت بهره مندان در افغانستان، به‌ویژه در شرایطی که موانع وسیعی ارتباطات شما را متاثر میسازد، موسسات غیردولتی نیاز دارند تا رویکردهای بدیع و استراتژیک را اتخاذ کنند. این رویکردهای استراتژیک باید به طور مؤثر واقعیت های عملی را به اشتراک بگذارند، حمایت را جلب کنند و تأثیر کار خود را به تمویل کنندگان بین المللی، شرکا و جامعه جهانی نشان دهند.

رویکرد اول - استفاده از فناوری برای ارتباطات امن:
از ابزارهای ارتباطی امن با قابلیت رمزگذاری برای به اشتراک گذاری، به روز رسانی ها و گزارش ها با شرکای بین المللی استفاده کنید. ابزارهایی مانند سیگنال یا خدمات ایمیل امن می توانند مراسلات محرمانه را تسهیل کنند و اطمینان حاصل شود که اطلاعات حساس به خطر نمی افتد. (لطفاً برای اطلاعات بیشتر در مورد امن ترین ابزارهای ارتباطی و خدمات ایمیل، به شکل های ۸ و ۹ مراجعه کنید.)

رویکرد دوم - از مولتی میدیا هوشیارانه استفاده کنید:

از مولتی میدیا برای مستندسازی فعالیت های تان استفاده کنید، اما اگر احساس نا امنی میکنید آنها را در حساب خود منتشر نکنید. تصاویر و روایت های جذاب می تواند خلاءهای های ارتباطات با جهان را پر کند. اما مراقب باشید؛ ایجاد ویدیوهای تاثیرگذار، مقاله ها، عکس ها و اینفوگرافیک هایی که واقعیت های روزمره زندگی مردم، تلاش های موسسات غیردولتی و روایت های مردم را برجسته می کند، می تواند همه بهره مندان را در معرض خطر بزرگی قرار دهد. حتی اگر آنها از طریق امن ترین ابزارهای ارتباطی با نهادهای بین المللی که ممکن است از آنها برای دادخواهی استفاده کنند، به اشتراک گذاشته شوند.

رویکرد سوم – تعامل از طریق دنیای مجازی:

در حالی که امکان ملاقات حضوری وجود ندارد، از طریق پلتفرم های مجازی با همکاران بین المللی تعامل داشته باشید، اما باید از امن ترین پلتفرم ها استفاده کنید. جلسات مجازی، وبینارها و کنفرانس ها را جهت ارتباط با تمویل کننده گان و همکاران بین المللی راه اندازی کنید. این پلتفرم‌ها همچنین می‌توانند برای میزبانی پانل‌هایی با حضور فعالان، بهره مندان و کارمندان شما مورد استفاده قرار گیرند و نظریات دست اول را در مورد وضعیت افغانستان ارائه دهند. (لطفاً برای اطلاعات بیشتر در مورد امن ترین پلتفرم ها به شکل های ۸ و ۱۰ مراجعه کنید.)

رویکرد چهارم - شبکه‌های بین المللی و مشارکت با آنها:

از شبکه های بین المللی و مشارکت با آنها استفاده کنید، اما رابطه تان با آنها را افشا نکنید چون ممکن برای کارمندان، بهره مندان و مردمی که به آنها خدمات ارایه میدهید خطر ساز باشد. از مشارکت با موسسات غیردولتی بین المللی، گروه های مدافع حقوق بشر، و دفاتر سازمان ملل متحد برای تقویت صدای موسسات غیردولتی استفاده کنید. این همکاری می‌تواند منجر به تلاش‌های مشترک دادخواهانه، و افزایش حامیان در میان طیف وسیعی از مخاطبان بالقوه شود.

رویکرد پنجم – استخدام میانجی در خارج از افغانستان:

افراد میانجی مورد اعتماد را در خارج از افغانستان استخدام کنید. هزاران فعال جامعه مدنی افغانستان و مدافعان حقوق بشر در تبعید وجود دارند که می توانند به شما کمک کنند و به عنوان میانجی در موسسات شما استخدام شوند. از آنهای استفاده کنید که بتوانند آزادانه بین موسسات غیردولتی داخلی افغانستان و موسسات بین‌المللی ارتباط برقرار کنند و بتوانند شما را با تمویل کننده گان بالقوه وصل نمایند. این افراد می توانند به عنوان پیام رسانان شما و مدافعان تان گفتگو های شما را با نهادهای بین المللی تسهیل کنند.

امن ترین ابزارهای ارتباطی برای موسسات غیردولتی کدام ها اند؟

به غیر از چند مورد، هیچ یک از این ابزارهای ارتباطی کاملاً امن نیستند. آنها را بر اساس میزان حساسیت ارتباطات تان انتخاب کنید.

ابزارها	رمزگذاری	حریم خصوصی داده ها	ویژگی های امنیتی
Signal	از رمزگذاری سرتاسر به‌طور پیش فرض برای همه پیام‌ها، تماس‌ها و رسانه‌های مشترک استفاده می‌کند و از پروتکل منبع-باز سیگنال استفاده می‌کند.	حداقل دیتا کاربر را با تمرکز بر حفظ حریم خصوصی کاربر جمع آوری می کند. سیگنال پیام ها را پس از تحویل در سرورهای خود ذخیره نمی کند.	قابلیت محو پیام ها، دارای امنیت صفحه نمایش (جلوگیری از اسکرینشات) و قفل ثبت نام (PIN برای محافظت از حساب) را ارائه می دهد.
Wire	از رمزگذاری سرتاسر به‌طور پیش‌فرض برای همه پیام‌ها، تماس‌ها، پیام های صوتی و تصاویر استفاده می‌کند و از پروتکل منبع-باز سیگنال استفاده برخوردار است.	برخی از اطلاعات کاربر، از جمله نام و مشخصات، شماره تلفن (در صورت ارائه)، و آدرس ایمیل (در صورت ارائه) را برای اهداف مدیریت حساب جمع آوری می کند.	از ویژگی‌هایی مانند حفظ پیام‌ها به یک مدت معین پشتیبانی می‌کند که به‌طور خودکار پس از یک دوره تعیین‌شده حذف می‌شوند و حریم خصوصی را افزایش می‌دهند. علاوه بر این، تأییدیه کاربر را برای جلوگیری از حملات Man-in-the-Middle ارائه می دهد.
Threema	از رمزگذاری سرتاسر برای متن، صدا، ویدئو و فایل‌ها با استفاده از پروتکل Proteus، ساخته	طراحی شده برای حداکثر صرفه جویی در مصرف دیتا، بدون نیاز به ایمیل یا شماره تلفن برای ثبت نام. برای هر کاربر یک Threema	شامل یک ویژگی منحصر به فرد است که به کاربران امکان این را می دهد تا مخاطبین را با کدهای QR تأیید کنند و یک لایه امنیتی اضافی در برابر جعل

	شده بر روی پروتکل سیگنال، استفاده می‌کند. رمزگذاری های سرتاسری را برای همه ارتباطات، از جمله پیام ها، تماس های تلفون و فایل ها فراهم می کند. از رمزنگاری NaCl استفاده می کند و فقط کاربران در حال ارتباط می توانند پیام ها را بخوانند.	ID تصادفی ایجاد می کند و قابلیت ناشناس ماندن را افزایش می دهد. لیست مخاطبین و اطلاعات گروه فقط در دستگاه های کاربر ذخیره می شوند، نه در سرورهای این اپلیکیشن.	هویت احتمالی یا حملات (man in the middle) اضافه می کند. همچنین رمزگذاری را ذخیره میکند و ویژگی نظرسنجی در چت ها را ارائه می دهد که رمزگذاری را حفظ کند.
Session	از رمزگذاری سرتاسر بر اساس پروتکل سیگنال برای پیام ها استفاده می کند. چیزی که Session را متمایز می‌کند، پروتکل TOR آن است که ابر دیتا را پنهان می‌کند و تشخیص اینکه چه کسی با چه کسی در ارتباط است را دشوار می سازد.	پس از ثبت نام، هیچ گونه اطلاعات شخصی (PII) را جمع آوری نمی کند و فقط از معرفه های جلسه برای شناسایی کاربر استفاده می نماید. این رویکرد با مرتبط نکردن حساب‌ها با شماره تلفن یا آدرس ایمیل، حریم خصوصی را به حداکثر می‌رساند. این به گونه ای طراحی شده است که حداقل ردپای دیجیتالی را قابل دریافت میسازد و ناشناس بودن کاربر را به طور قابل توجهی افزایش دهد.	معماری غیرمتمرکز و مسیریابی TOR نه تنها حریم خصوصی قوی دیتا را فراهم می کند، بلکه در برابر نظارت و سانسور شبکه نیز انعطاف پذیر است. عدم وجود سرورهای مرکزی در Session به این معنی است که هیچ نقطه مرکزی وجود ندارد که بتوان اطلاعات کاربر را در آنجا درخواست کرد یا هک نمود.
Viber	رمزگذاری سرتاسری را به طور پیش فرض برای پیام ها و تماس ها فراهم می کند.	دیتای محدودی را در مقایسه با سایرین مانند WhatsApp یا Messenger جمع‌آوری می‌کند و بر حریم خصوصی	قابلیت تخریب پیام ها را به صورت خودکار دارد و برای دسترسی به برنامه در دستگاه جدید به یک پین کد نیاز دارد.

		کاربر تمرکز دارد، به شماره تلفن نیاز دارد.	
WhatsApp	با استفاده از پروتکل سیگنال، رمزگذاری سرتاسر را به طور پیش‌فرض برای پیام‌ها و تماس‌ها فراهم می‌کند.	به‌رغم رمزگذاری، نگرانی‌هایی در مورد اشتراک‌گذاری داده‌ها بین واتس‌اپ و سایر پلتفرم‌های متا ایجاد می‌شود. شماره تلفن لازم است.	تأیید دو مرحله‌ای را ارائه می‌کند، اما روی شیوه‌های مدیریت دیتا متا با خطر تعمق و موشگافی مواجه است.
Telegram	رمزگذاری سرتاسر را فقط در «چت های مخفی» حفظ میکند ولی نه در پیام های معمولی.	دیتا را در سرورهای خود ذخیره می کند تا امکان همگام سازی بین دستگاه ها را فراهم سازد. به ابر دیتا دسترسی دارد. شماره تلفن لازم است.	قابلیت تخریب پیام ها را در چت های مخفی ارائه می دهد و یک API باز برای برنامه های شخص ثالث دارد که ممکن است ملاحظات امنیتی بیشتری ایجاد کند.
IMO	برای تماس‌های صوتی و تصویری قابلیت رمزگذاری راارائه می‌دهد اما در مورد نوع رمزگذاری پیام‌ها شفافیت ندارد.	روش‌های جمع‌آوری دیتا چندان واضح نیستند و نگرانی‌هایی را در مورد حریم خصوصی کاربران ایجاد می‌کند. شماره تلفن لازم است.	کنترل حریم خصوصی کمتری را در مقایسه با رقبای خود ارائه می دهد.
Messenger (Facebook Messenger)	رمز گذاری سرتاسر را فقط در "مکالمات مخفی" ارائه می دهد. پیام‌ها و تماس‌های معمولی رمز گذاری میشوند، اما فیس‌بوک می‌تواند به آنها دسترسی داشته باشد.	بخشی از اکوسیستم فیس بوک است، به اشتراک گذاری دیتا در پلتفرم های تبلیغات هدفمند امکان پذیر است.	مکالمات مخفی اختیاری را ارائه می دهد، اما به طور پیش فرض، مکالمات رمز گذاری نمیشوند.

Delta Chat	از Autocrypt برای رمزگذاری خودکار ایمیل ها هنگام برقراری ارتباط با سایر کاربران دارای قابلیت Autocrypt استفاده می کند.	متکی بر پروتکل های ایمیل است که یک سیستم غیرمتمرکز را ارائه می دهد. پیام ها در سرورهای ایمیل ذخیره می شوند اما رمزگذاری میشوند.	بدون سرور مرکزی، طراحی غیرمتمرکز، عمدتاً بر امنیت ارتباطات ایمیل متمرکز است.
Element (formerly Riot)	از رمزگذاری سرتاسر برای چت ها و تماس ها از طریق پروتکل Matrix استفاده می کند.	شرکت کنندگان می توانند سرورهای خود را میزبانی کنند و کنترل حریم خصوصی را افزایش دهند. با این حال، امنیت شما بستگی به تنظیمات سرور خود شما دارد.	از پیام های گروهی رمزگذاری‌شده، ادغام انواع دیتا و گزینه های سفارشی سازی پشتیبانی می‌کند.

شکل ۸: امن ترین ابزارهای ارتباطی برای موسسات غیردولتی.

امن ترین ارائه دهندگان خدمات ایمیل برای موسسات غیردولتی کدامها اند؟

به غیر از چند مورد، هیچ یک از این ایمیل ها کاملا امن نیستند. آنها را بر اساس حساسیت و اهمیت ارتباطات خود انتخاب کنید.

ابزارها	رمزگذاری	حریم خصوصی داده ها	ویژگی های امنیتی
Riseup	Riseup بر ارائه ابزارهای ارتباطات امن برای فعالان و رهبران جنبش های مدنی با تعهد به ناشناس ماندن این کاربران تمرکز دارد.	Riseup که متعهد به محافظت از ناشناس بودن و حریم خصوصی کاربران است، هیچ گونه اطلاعات شخصی را که به کاربرانش مرتبط شود ذخیره نمی کند و به طور منظم اطلاعات را حذف می کند. این پلتفورم به دلیل موضع قوی خود در عدم به اشتراک گذاشتن دیتا با اشخاص ثالث	ابن پلتفورم شامل خدمات VPN برای محافظت بیشتر از حریم خصوصی کاربران خود به صورت آنلاین است. Riseup همچنین FA2 را در خدمات خود اضافه میکند تا یک لایه امنیتی اضافی برای دسترسی به حساب وجود داشته باشد.

		شناخته شده است، مگر اینکه از بر اساس حکم قانون مجبور شود.	
	وبسایت	https://riseup.net/en/email	
Autistici/Inventati (A/I)	استفاده از PGP را برای ارتباطات ایمیل رمزگذاری شده توصیه می کند. خدمات آنها، شامل ایمیل و میزبانی وب، از رمزگذاری SSL/TLS برای دیتای در حال انتقال است.	متعهد به حفظ حریم خصوصی کاربران است، نه آنها ردیابی و نه هم در معرض دید قرار میدهد. این پلتفورم خدماتی را با هدف حفظ حداقل دیتا و تضمین ناشناس ماندن کاربر ارائه می دهد.	خدمات آن برای فعالان و کسانی که نگران حریم خصوصی هستند طراحی شده است و خدمات ناشناس را از طریق یکپارچه سازی VPN و TOR ارائه می دهد.
	وبسایت	https://www.autistici.org	
ProtonMail:	رمزگذاری سرتاسر را برای ایمیل‌ها ارائه می‌دهد و اطمینان می‌دهد که فقط فرستنده و گیرنده می‌توانند محتوا را بخوانند.	از رمزگذاری دسترسی صفر استفاده می کند، به این معنی که حتی خود ProtonMail هم نمی تواند به محتوای ایمیل های شما دسترسی داشته باشد.	سرورهای ProtonMail که تحت قوانین حفظ حریم خصوصی سوئیس کار می کنند، در سوئیس واقع شده اند که به دلیل حفاظت از حریم خصوصی قوی خود شناخته شده میباشند.
	وبسایت	https://proton.me/mail	
Tutanota	ایمیل ها و ضمیمه ها را به صورت خودکار رمزگذاری می کند و ارتباطات را امن می سازد.	حداقل اطلاعات شخصی را جمع آوری می کند و گزینه های پرداخت ناشناس را برای ویژگی های برتر ارائه می دهد.	این پلتفورم مستقر در آلمان است، و مشمول مقررات سختگیرانه GDPR اروپا می باشد که بر حریم خصوصی کاربران تأکید دارد.
	وبسایت	https://tuta.com	
Disroot	یک پلتفرم متمرکز بر حریم خصوصی که ایمیل، فضای ذخیره‌سازی و سایر خدمات را برای فعالان و موسسات غیر دولتی ارائه می دهد.	بر روی رمزگذاری و اقدامات امنیتی برای محافظت از دیتای کاربر و ارتباطات در برابر نظارت تأکید می کند.	به عنوان یک پلتفورم جامعه محور، Disroot برای شفافیت، حریم خصوصی و آزادی بیان ارزش قائل است و نیازهای فعالان را برآورده می نماید.
	وبسایت	https://disroot.org/en	

شکل ۹: امن ترین ارائه دهندگان خدمات ایمیل برای موسسات غیردولتی.

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

به غیر از چند مورد، هیچ یک از این ابزارهای ویدئو کنفرانس کاملا امن نیستند. آنها را بر اساس حساسیت ارتباطی خود انتخاب کنید.

ابزارها	ویژگی های امنیتی	حریم خصوصی داده ها	رمزگذاری
Jitsi Meet	رمزگذاری سرتاسری را برای کنفرانس های ویدئویی فراهم می کند و کانال های ارتباطی امن را تضمین می نماید.	با قابلیت پلتفورم منبع باز بدون پرداخت است. کاربران می توانند سرورها را برای حفظ حریم خصوصی بیشتر میزبانی کنند.	اتاق‌های محافظت‌شده با رمز عبور را ارایه میکند، با کنترل دید شرکت‌کنندگان در این اتاق ها، و کاربران نیاز به رمز عبور دارند تا وارد جلسات شوند.
	وبسایت	https://meet.jit.si	
BigBlueButton	از ورود رمزگذاری شده پشتیبانی می کند و شامل ویژگی های امنیتی برای حفظ حریم خصوصی و محرمانه بودن جلسات است.	این پلتفورم برای زمینه های آموزشی طراحی شده، و همچنان دسترسی کنترل شده به ضبط صدا و ویژگی های خاصی را فراهم می کند.	این پلتفورم قابلیتهای دسترسی و اجازه ورود به جلسات را به صورت انتخابی ارایه میکند، کنترل جلسات بدست تسهیل کننده است، و ابزارهای کمکی برای نوشتن روی تخته مجازی را نیز برای تسهیل کننده فراهم می نماید.
	وبسایت	https://demo.bigbluebutton.org	
Whereby	رمزگذاری سرتاسری را برای تماس ها و جلساتی که در پلتفرم انجام می شود ارائه می دهد.	امکان تنظیم رمز عبور برای جلسات و کنترل دسترسی به آنها را فراهم می کند.	اتاق‌های جلسه مجازی و ویژگی‌های اتاق انتظار به صورت امن و محافظت‌شده با رمز عبور پردازش داده شده اند.
	وبسایت	https://whereby.com	
Blue Jeans	رمزگذاری را در وقفه بین جلسات و حین تسهیل برای امن سازی دیتای کاربر در طول تماس ها و کنفرانس فراهم می کند.	ویژگی حفظ حریم خصوصی مانند پوشش دیتا و اشتراک کنترل‌شده شرکت‌کننده گان جلسه را ارائه می نماید.	ویژگی اشتراک، کنترل حریم خصوصی، و کنترل نظارت امنیت جلسات را فر اهم میکند.
	وبسایت	https://www.bluejeans.com	
GoToMeeting	از پروتکل های رمزگذاری قوی برای امن سازی دیتا در طول تماس و کنفرانس استفاده می کند.	مقررات حفاظت از دیتا را راعایت میکند، اما دیتای کاربر ممکن است برای بهبود خدمات جمع آوری شود.	دارای ویژگی قفل کردن جلسات است، محدودیت‌های اشتراک‌گذاری در صفحهات را ارایه میکند، و برای شما حق این را میدهد تا کسی بدون اجازه وارد جلسات نشود.
	وبسایت	https://www.goto.com/meeting	

رهنمود ارتباطات برای جامعه مدنی افغانستان

Facetime/i Message (Apple)	دارای قابلیت رمزگذاری سرتاسر برای پیامها، تماس های صوتی و تصویری در اکوسیستم اپل.	مجهز با قابلیت حفاظت از حریم خصوصی قوی به دلیل معیارهای رمزگذاری اپل و تعهد به حریم خصوصی کاربر.	دارای قابلیت مسدود کردن مخاطبان، احراز هویت Face ID/Touch ID برای برنامه‌ها، و اتمام iMessages به صورت خودکار
	وبسایت	https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web	
Google Meet	ارایه کنفرانس تصویری امن با رمزگذاری سرتاسر برای همه کاربران G Suite .	معیارهای امنیتی Google حفاظت از دیتا را تضمین می‌کند، اما حریم خصوصی کاربر ممکن است تحت تأثیر جمع‌آوری دیتا برای تبلیغات تجارتی قرار گیرد.	دارای قابلیت قفل جلسات، کنترل حریم خصوصی، و اقداماتی برای جلوگیری از دسترسی غیرمجاز.
	وبسایت	https://meet.google.com	
Duo (Google)	از رمزگذاری سرتاسر برای تماس‌ها و چت‌های ویدیویی استفاده می‌کند و ارتباطات را از دسترسی شخص ثالث ایمن نگاه میدارد.	جمع آوری دیتای کاربر برای بهبود خدمات را اجرای میکند البته با رعایت استانداردهای امنیتی Google بر حریم خصوصی.	تماس‌های ویدیویی رمزگذاری میشود تا از رهگیری ارتباطات جلوگیری شود، و دارای قابلیت Face Match برای احراز هویت دو مرحله ای است.
	وبسایت	https://meet.google.com/calling/	
Microsoft Teams	دارای قابلیت انتقال و ذخیره امن دیتا با پروتکل های رمزگذاری جامع.	دارای مقررات سختگیرانه حریم خصوصی دیتا با تنظیمات و کنترل پیشرفته حریم خصوصی برای کاربران.	دارای قابلیت رمزگذاری ارتباطات و جلسات، احراز هویت دو مرحه ای، کانال های امن و استانداردهای قابل تطبیق.
	وبسایت	https://www.microsoft.com/en-ca/microsoft-teams/log-in	
Xspace	Xspace رمزگذاری سرتاسری برای تماس‌های ویدیویی را فراهم می‌کند و انتقال امن دیتا را در طول جلسات و ارتباطات فضای خصوصی تضمین می‌کند.	حفاظت از دیتای کاربر را اولویت می دهد و مطابقت با قوانین حریم خصوصی دیتا را تضمین می کند.	اتاق‌های جلسات با رمز عبور محافظت میشود، برای دسترسی به جلسات تسهیل کننده تسلط مطلق دارد، و دارای ویژگی امن برای اشتراک گذاری اسناد دارد.
	وبسایت	https://twitter.com/	
Clubhouse	Clubhouse به دلیل عدم رمزگذاری انتها به انتها با انتقاداتی مواجه شد که منجر به نگرانی‌های مربوط به حریم خصوصی در مورد امنیت چت‌های صوتی روی پلتفورم شد است.	کاربران به دلیل شیوه‌های حفظ دیتا و حوادث امنیتی قبلی که شامل اشتراک افراد د ر جلسات به صورت ناخوانده می‌شوند و دسترسی به مکالمات خصوصی میداشته باشند، نگرانی‌های مربوط به حریم خصوصی را مطرح کرده‌اند.	دارای ابزارهای محدود برای تسهیل و کنترل مکالمات در مقایسه با سیستم های عامل کنفرانسها، که می تواند بر امنیت کاربران تأثیر بگذارد.
	وبسایت	https://www.clubhouse.com/	

Zoom	در اوایل با انتقاداتی در ارتباط به رمزگذاری اولیه روبرو شد، اما از آن زمان به بعد پروتکل‌های امنیتی خود را برای ارائه رمزگذاری سرتاسری همه جلسات و پیام‌رسانی ها ارتقا داد.	بهبود شیوه های حفظ حریم خصوصی دیتا و شفافیت پس از بررسی دقیق در این پلتفورم، ارائه گزینه ها برای کاربران جهت کنترل اشتراک گذاری دیتا و تنظیمات امنیتی. ارایه طیف وسیعی از ویژگی‌های امنیتی مانند حفاظت از رمز عبور، اتاق‌های انتظار، کنترل تسهیل کننده و رمزگذاری سرتاسر برای محافظت از ارتباطات کاربر.
	وبسایت	https://zoom.us/

شکل ۱۰: امن ترین ابزار کنفرانس تصویری برای موسسات غیردولتی.

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

هنگامی که موسسات غیردولتی ارتباط برقرار می‌کنند، به‌ویژه در محیطی که نظارت بر محتوای مطالب رایج است، اجتناب از برخی اصطلاحات می‌تواند به حداقل رساندن خطر و نظارت بر ارتباطات آنها کمک کند. کشورهای وجود دارد که از تکنالوژی پیشرفته ای برای ارتقای قابلیت های نظارتی شان استفاده میکنند. از سال ۲۰۱۴، این موضوع با پیشرفت تکنالوژی گسترش یافته است و امکان استفاده از روش های نظارتی فراگیر و پیچیده تر را فراهم کرده است. در حال حاضر، قابل ذکر است که استفاده از هوش مصنوعی در نظارت بر فعالیت‌های آنلاین نگرانی‌های جدیدی را در مورد حفظ حریم خصوصی ایجاد کرده است.

روش‌های نظارت از ساحه کاری ماموران استخبارات به سیستم‌های سخت‌افزاری و نرم‌افزاری تجاری و دولتی انتقال پیدا کرده است. پیش از این، از افرادی نظارت صورت میگرفت که به عنوان خطرات امنیت ملی تلقی می شدند. اکنون، به دلیل سیستم‌های نظارت و فیلترینگ بر روی اینترنت که توسط دولت اجرا می‌شود، همه ما به عنوان مظنونین بالقوه مطرح هستیم.

تکنالوژی به کار گرفته شده بین کاربران متمایز نیست و با همه به یک شکل برخورد میشود. ایمیل ها، پیام ها و مرورگرهای وبسایت ما را برای کلمات کلیدی خاصی اسکن می کنند. با شناسایی موارد مشکوک، یا به تیم های نظارتی هشدار می دهند یا ارتباطات ما را قطع می کنند. رمزگذاری (encryption) به عنوان یکی از آخرین سنگرهای حریم خصوصی آنلاین است که ما را قادر می سازد ارتباطات خود را امن کنیم تا فقط دریافت کننده گان مورد نظر بتوانند آنها را رمزگشایی کنند و بخوانند.

موسسات غیردولتی در سرتاسر جهان با خطرات قابل توجهی مواجه هستند، از جمله نظارت و محدودیت های مختلف که ارتباطات آنها را محدود می کند و اغلب منجر به عواقب سختی برای ادامه حمایت از آنها می شود. علاوه بر این، امنیت ابزارهای دیجیتال آنها به طور فزاینده ای به خطر مواجه است. ایمیل ها به مقصد نمیرسد؛ حساب های رسانه های اجتماعی به خطرات قابل توجهی مواجه اند و هک میشوند؛ اتصالات اینترنتی آنها غیر قابل اعتماد هستند؛ ارتباطات آنها به دقت رصد می شوند؛ دستگاه های کامپیوتر و تلفون های هوشمند آنها توقیف می شوند؛ و بدافزار های انترنتی دیتای مهم آنها را از بین می برند.

این چالش‌ها، از جمله بررسی شدید مقامات بر محتوای آنلاین و انتقام‌جویی سریع از ارتباطات «نامطلوب» توسط موسسات غیردولتی، مسائلی کاملاً مستند هستند. موسسات غیردولتی دائماً در بسترهای دیجیتالی مانند سایت‌های خبری، رسانه‌های اجتماعی و وبلاگ‌ها نظارت می‌شوند. آنها با موانع متعددی مانند شکاف دیجیتال، سرکوبی که توسط ابزارهای دیجیتالی فعال می‌شود، نقض حقوق به بهانه امنیت ملی، آسیب‌پذیری‌های سایبری گسترده و به صورت کلی نا امنی های دیجیتالی عمومی روبرو هستند. با کسب مهارت در استفاده از رایانه، تلفن های هوشمند و درک اینترنت، موسسات، فعالان و مدافعان حقوق بشر می توانند بهتر از ابتکارات خود محافظت کنند و به طور مؤثر از حقوق خود و افرادی که قصد حمایت از آنها را دارند دفاع کنند.

یکی از مثالهای نظارت شدید دولتها "سپر طلایی" چین است که به عنوان یک تکنالوژی پیشرفته عمل می کند و بر روی یک زیرساخت اینترنتی ملی جدا از وب جهانی کاربرد دارد تا امنیت ملی را از طریق پایگاه های دیتای متمرکز کاربران و نظارت جامع افزایش دهد. هیچ دیتا از بدون فلتر عبور نمیکند. سپر طلایی با ادغام قابلیت‌های نظارت گسترده در شبکه، فیلتر محتوا را به دستگاه‌های اطلاعات عمومی و خصوصی مختلف گسترش می‌دهد و از تکنالوژی پیچیده

بر اساس گزارش نظارت بر رسانه‌های اجتماعی (Freedom House)، دولت‌ها در سراسر جهان، از رژیم‌های استبدادی گرفته تا دولت‌های کوچکتر، به طور فزاینده‌ای در حال سرمایه‌گذاری در تکنالوژی پیشرفته برای نظارت جمعی از شهروندان در رسانه‌های اجتماعی هستند. این عمل که فراتر از قابلیت‌های جاسوس‌افزارهای (Spyware) سنتی گسترش می‌یابد، شامل

جمع آوری دستا به صورت خودکار، سازماندهی و تجزیه و تحلیل حجم وسیعی از دیتا از بسترهای ارتباطی دیجیتال است. با توجه به استفاده گسترده از این پلتفرم ها برای اهدف شخصی و سیاسی، مردم نظارت بر رسانه های اجتماعی را تهاجمی می دانند. در کشورهایی مانند ایران و چین، مقامات هزاران نفر را برای نظارت بر فعالیت‌های آنلاین مردم و گزارش مخالفان نظام استخدام و بسیج کرده اند. علاوه بر این، پیشرفت‌های هوش مصنوعی (AI) توانایی این سیستم های نظارتی را برای تجزیه و تحلیل روابط، احساسات و حتی پیش‌بینی مکان‌های کاربران افزایش داده و الگوها و اطلاعاتی را فراتر از قابلیت‌های تشخیص انسان آشکار می‌کند.[7]

در افغانستان، اداره موقت طالبان در کنترل ارتباطات افغانها به خارج با موانعی مواجه است، کاری که بدون حمایت کشورهای خارجی مثل چین و ایران و پیشرفت در عرصه تکنالوژی زمان گیر و چالش برانگیز خواهد بود. نظارت بر رسانه های اجتماعی، مثل اقدامات در ایران، چین و روسیه، به ابزاری استراتژیک برای اداره موقت طالبان در اعمال کنترل و نظارت بر صداهای مخالف آنها تبدیل شده است. در حال حاضر، اداره موقت طالبان از استراتژی های خاص خود استفاده نموده و از نظارت رسانه های اجتماعی برای تقویت قدرت خود و پذیرش تاکتیک های مشابه با استفاده از هنجارهای منطقه ای استفاده می کند. به قول نمایندگان موسسات غیردولتی و فعالانی که در این زمینه با آنها مصاحبه صورت گرفت، اداره موقت طالبان همان استراتژی ایران و چین را با استخدام صدها نفر برای نظارت بر دارندگان حساب‌های شبکه های اجتماعی افغان در افغانستان و خارج از کشور دنبال می‌کند. به عنوان یک موسسه غیردولتی که در این شرایط فعالیت می‌کند، افزایش فعالیت رسانه های اجتماعی در مورد موضوعات جامعه مدنی می‌تواند شما را هدف نظارت اداره موقت طالبان تبدیل کند. سخنرانی در اجتماعات عمومی یا رسانه ها، دفاع از حقوق بشر، یا مبارزه با فساد اداری، احتمال بررسی را افزایش می دهد. نکته مهم این است که نظارت هدفمند نیازی به فعالیت مجرمانه ندارد، زیرا دولت‌ها در سراسر جهان از الگوریتم های سایبری پیچیده برای نظارت بر متخصصان از جمله فعالان، روزنامه‌نگاران و موسسات غیردولتی استفاده می‌کنند. دولت ها از دیتای به دست آمده از نظارت برای تحقیر فعالان، دخالت دادن آنها در اتهامات ساختگی و سازماندهی دستگیری آنها استفاده کرده اند و همچنان این دیتا بدست آمده تهدید فراگیر و مداخله غیرقابل توجیه توسط دولتها را در برنامه های مشروع نهادهای جامعه مدنی برجسته می کند. بنابراین، هنگام برقراری ارتباط در افغانستان، موسسات غیردولتی باید به استفاده از اصطلاحاتی که ممکن است ناخواسته باعث توهین یا تفسیر نادرست شود، توجه داشته باشند. به خاطر داشته باشید که اگر میخواهید تغییرات مثبت درافغانستان ایجاد کنید، اتخاذ یک رویکرد حرفه ای امن تر از یک رویکرد فعالانه یا فعال محور است.

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

آیا استفاده از پلتفرم های رسانه های اجتماعی برای موسسات غیر دولتی امن است؟

استفاده از پلتفرم های رسانه های اجتماعی می تواند برای موسسات غیردولتی فعال در افغانستان هم سودمند و هم چالش برانگیز باشد. برای کاهش خطرات و به حداکثر رساندن مزایای استفاده از رسانه‌های اجتماعی، موسسات غیردولتی باید پالیسی های شفاف برای رسانه‌های اجتماعی را ایجاد کنند، پروتکل‌های امنیتی برای رسانه های اجتماعی داشته باشند، کارکنان را در زمینه امنیت دیجیتال آموزش دهند، و در این پلتفورم ها به‌طور عاقلانه و مسئولانه با مردم در تماس باشند. در اینجا چند مورد از مزایا و معایب استفاده از رسانه های اجتماعی را برای نهادهای مدنی به معرفی میگیریم.

۱. مزایا

مزیت اول – دسترسی و تعامل:

پلتفورم‌های رسانه‌های اجتماعی به موسسات غیردولتی ابزاری ارزشمند برای گسترش دامنه دسترسی، و تعامل مستقیم با مردم جهان و افزایش آگاهی در مورد اهداف آنها ارائه می‌دهند. با استفاده از دسترسی گسترده و ماهیت تعاملی رسانه‌های اجتماعی، موسسات غیردولتی می‌توانند به طور مؤثری با کارمندان خود ارتباط برقرار کنند، روایتهای تأثیرگذار را به اشتراک بگذارند، و از میان مخاطبان مختلف برای خود حمایت کسب کنند. این رویکرد دیجیتالی نه تنها پیام آنها را تقویت می‌کند، بلکه حس ارتباط و مشارکت را در میان حامیان آنها رشد میدهد و تعامل بلادرنگ را ممکن می‌سازد. در نتیجه، رسانه های اجتماعی نقش یک کاتالیزور پویا را برای موسسات غیردولتی ایفا می کند که به دنبال ایجاد تغییر و جلب توجه گسترده برای ابتکارات خود هستند.

مزیت دو – دادخواهی و نتورکنگ:

پلتفورم‌های رسانه‌های اجتماعی به سازمان‌های غیردولتی مجموعه‌ای از ابزارهای چند بعدی را برای حمایت از تحولات اجتماعی، حمایت از اهداف آنها و ایجاد ارتباط با موسسات همفکر، و تمویل کنندگان ارائه می‌دهند. با استفاده از قدرت ارتباطات رسانه‌های اجتماعی، موسسات غیردولتی می‌توانند به طور موثر آگاهی مردم را در مورد مسائل مهم افزایش دهند، حمایت مردم از کمپین‌ها را تقویت کنند، و راه های مشارکت را ایجاد کنند که تأثیر فعالیت های آنها را تقویت نماید.

این چشم انداز دیجیتال نه تنها به عنوان یک پلتفورم برای پخش پیام ها عمل می کند، بلکه یک اجتماع شبکه ای را شکل میدهد که به ایجاد تغییرات مثبت و پیشبرد اهداف جمعی در هر حوزه تأثیر اجتماعی خاص خود را دارد.

مزیت سه – ارتباط مستقیم:

ارتباط مستقیم با مخاطبان نقش مهمی در دستیابی به اهداف موسسات غیر دولتی دارد. برخلاف وبسایت‌ها که اغلب با بازدیدکنندگان ارتباط برقرار می‌کنند، رسانه‌های اجتماعی تعامل دو طرفه با حامیان و تمویل کنندگان را تسهیل می‌کنند و اجازه می‌دهند تا ارتباط فوری و فعالانه برقرار شود. مجهز به اطلاعات سفارشی شده، این ابزارهای ارتباطی به صورت مستقیم می توانند به طور موثر روند کار موسسات را از افزایش آگاهی تا رسیدن به فعالیت مطلوب تسریع کنند.

مزیت چهار - جذب مساعدت های مالی:

رسانه‌های اجتماعی به‌عنوان یک ابزار حیاتی برای تسهیل طرح‌های جذب مساعدت های مالی، مشارکت تمویل کنندگان، و هماهنگی کمپاین‌های تامین مالی جمعی برای تقویت پروژه‌های موسسات غیردولتی در افغانستان به شمار میروند. استفاده از این پلتفورم‌ها به موسسات غیردولتی این فرصت را میدهد تا از دسترسی گسترده به امکانات تعاملی ارتباطات، و قابلیت ارایه روایت های خود برای جلب توجه حامیان بالقوه، ایجاد روابط با تمویل کننده گان و بسیج منابع مالی برای برنامه های بشردوستانه خود استفاده کنند.

مزیت پنج – انتشار مطالب:

گنجاندن رسانه‌های اجتماعی در استراتژی اطلاع‌رسانی، موسسات غیردولتی را قادر می‌سازد تا موضوعات حساس را در زمان معین، منابع ارزشمند و مفید، موضوعات آموزشی و اعلامیه های اضطراری را به طور مؤثر به عموم مردم منتشر کنند. با استفاده از پلتفورم‌های رسانه های اجتاعی موسسات غیردولتی می‌توانند به سرعت اطلاعات مهمی را پخش کنند، با مخاطبان خود ارتباط داشته باشند و به رویدادهای در حال اتفاق پاسخ مؤثری بدهند و اطمینان حاصل کنند که ارتباطات آنها نه تنها به موقع، بلکه تأثیرگذار و گسترده است.

مزیت شش - به حداکثر رساندن آگاهی و ارتباطات:

رسانه‌های اجتماعی به‌عنوان ابزار قوی برای برقراری ارتباطات عمل می‌کنند و به‌عنوان پلتفورم های مؤثر برای افزایش آگاهی نقش موثری دارند. این ابزار موسسات غیر دولتی را قادر می‌سازد تا با میلیون‌ها شخصی که به دنبال ارتباطات با افراد دیگر، نهادها و اهدافی هستند که با علایقشان

مطابقت دارند، ارتباط برقرار کنند. رسانه های اجتماعی با به اشتراک گذاری اطلاعات و تصاویر، نظریات شان را در مورد نهادهای دیگر ارائه می دهند و پیام هایی را که با دقت حمل میکنند از طریق همین ابزار ها به نمایش میگذارند.

۲. اضرار

ضرر اول - خطرات امنیتی:

اجرای استراتژی رسانه های اجتماعی در مناطق درگیر جنگ مانند افغانستان می تواند چالش های امنیتی را ایجاد کند که شامل خطراتی برای رفاه کارمندان، بهره مندان و دارایی های متعلق به موسسات فعال در این مناطق است. با استفاده از پلتفورم های رسانه های اجتماعی، موسسات غیردولتی باید نگرانی های مربوط به پخش اطلاعات حساس، هدف قرار گرفتن کارمندان یا بهره مندان، و حفاظت از منابع مهم در محیط مملو از بی ثباتی و خطرات امنیتی را بررسی کنند.

ضرر دوم - سانسور و نظارت:

موسسات غیردولتی فعال در بسیاری از کشورها به شمول افغانستان هنگام استفاده از کانال‌های رسانه‌های اجتماعی ممکن با موانعی در ارتباط با سانسور اینترنتی، اقدامات نظارتی و محدودیت‌های آزادی بیان مواجه می‌شوند. تکثیر این موانع شامل کنترل‌های سختگیرانه بر روی محتوای آنلاین، اقدامات نظارتی بیشتر است که حریم خصوصی و امنیت افراد را تهدید می‌کند، و محدودیت‌هایی را ارتباط به آزادی برقراری ارتباطات آشکار در پلتفرم‌های دیجیتال به همراه دارد. این چالشها چشم انداز پیچیده ای را ایجاد میکند که موسسات غیردولتی باید در هنگام استفاده از رسانه‌های اجتماعی در افغانستان در نظر بگیرند، و نیاز خود را به بررسی دقیق و انطباق پذیر برای تضمین استراتژی‌های ارتباطات مؤثر و ایمن فراهم نمایند.

ضرر سوم - اطلاعات غلط و اطلاعات نارسا:

پلتفورم‌های رسانه‌های اجتماعی به‌عنوان مجرای انتشار اطلاعات غلط، تبلیغات و روایت‌های نادرست عمل می‌کنند و اعتبار و جایگاه موسسات غیردولتی را به خطر می‌اندازند. گسترش محتوای گمراه‌کننده از طریق این کانال‌ها می‌تواند اعتبار موسسات غیردولتی را خدشه‌دار کند، اعتماد مردم را تضعیف کند و تصویر دقیق مأموریت و فعالیت‌های آنها را مخدوش کند. در نتیجه، موسسات غیردولتی باید مراقب چشم انداز رسانه‌های اجتماعی برای مبارزه موثر با اطلاعات نادرست و حفظ یکپارچگی دیجیتالی خود باشند.

ضرر چهارم - نگرانی های مربوط به حریم خصوصی:
موسسات غیردولتی باید در ارتباط به حریم خصوصی دیتا، آسیب پذیری‌های سایبری و تهدیدات امنیت اطلاعات در هنگام نشر دیتای حساس در پلتفورم های رسانه‌های اجتماعی احتیاط کنند. به اشتراک گذاری چنین اطلاعاتی خطرات بالقوه مربوط به نقض دیتا، دسترسی غیرمجاز و بهره برداری توسط عوامل مخرب را باز می کند و بر اهمیت اجرای پروتکل های قوی برای محافظت از اطلاعات حساس و حفظ یکپارچگی عملکرد آنها در قلمرو دیجیتال تأکید می کند.

ضرر پنجم - خطرات و تعهدات امنیت دیتا:
هنگام استفاده از خدمات رسانه های اجتماعی، کنترل مدیریت دیتا و امنیت آن از اداره موسسه شما خارج می شود و آن به عنوان ملکیت معنوی پلتفورم به حساب میاید. این پلتفورم ها به دیتای داخلی شما و اطلاعات جمع آوری شده از منابع خارج از حساب کاربری مانند تصاویر به اشتراک گذاشته شده در پلتفورم هایی مانند فیس بوک و همچنان به جزئیات شخصی و مالی شما دسترسی دارند. برای این پلتفورم ها و موسسات بسیار مهم است که پایبند به قوانین و مقررات جهانی در مورد مدیریت دیتای خود شان، شرکا و بهره مندان شان باشند. با دسترسی به یک سایت رسانه اجتماعی، موسسات قسمتی از کنترل دیتای خود را از دست میدهند و باید هوشیارانه از این پلتفورمها استفاده نمایند و امنیت دیتای خود را به حد اکثر برسانند.

ضرر ششم - پیمایش چالش های امنیتی در قسمت مساعدت های مالی:
معاملات مالی در پلتفورم های رسانه های اجتماعی چالش های امنیتی را برای موسسات حین جمع آوری مساعدت مالی ایجاد می کنند. در حالی که پلتفورم هایی مانند فیس بوک ابزارهای مساعدت مالی را ارائه می دهند، ولی نیاز به دیتای حساس مالی شما دارند، همچنان حدودی برای پرداخت مساعدت ها دارند و به اعتماد کاربران در امنیت پلتفورم متکی هستند. در مقابل، وبسایت های دارای مجوز SSL، محیط امن‌تر و قابل کنترل‌تری را برای تمویل کنندگان ارائه می‌دهند و از حفاظت دیتا و مدیریت بهتر وجوه مالی در نسخه‌های دسکتاپ و موبایل تضمین میکند.

ضرر هفتم - تقویت اعتماد:
پلتفورم‌های رسانه‌های اجتماعی اعتماد ذاتی را به اندازه افزونه های دامنه وبسایت ارائه نمی دهند. یکی از مزایای کلیدی داشتن یک وبسایت در ارتباط با افزونه های دامنه قابل اعتماد، مانند .org است، که به طور گسترده برای گرد هم آوردن موسسات با علایق یا دلایل مشترک، و تقویت تلاش ها برای اعمال تغییرات مثبت شناخته شده است. این سطح از اعتماد و آگاهی، که برای درک

نهاد بسیار مهم است، چیزی است که کانال های رسانه های اجتماعی به سادگی نمی توانند با آن کنار بیایند.

موسسات غیردولتی چگونه باید از رسانه های اجتماعی به صورت امن استفاده کنند؟

موسسات غیردولتی می‌توانند از رسانه‌های اجتماعی به طور امن و مؤثر با اجرای برخی از کار شیوه های موثر برای مهار خطرات از ناحیه رسانه‌های اجتماعی و در عین حال محافظت از دیتا و حضور آنلاین خود و به حداقل رساندن این خطرات احتمالی مرتبط با تعاملات آنلاین استفاده کنند.

رویکرد اول - تدابیر حفاظت از دیتا:
موسسات غیردولتی باید امنیت اطلاعات حساس خود را که در رسانه های اجتماعی به اشتراک می گذارند در اولویت قرار دهند. با به کارگیری اقدامات موثر مانند ایجاد رمزهای عبور قوی و منحصربه‌فرد، فعال کردن احراز هویت دو مرحله ای (2FA)برای حفاظت بیشتر، و محدود کردن دسترسی به حساب‌های رسمی نهاد به طور انحصاری برای پرسنل قابل اعتماد و مسلکی، موسسات غیردولتی می‌توانند به طور موثر خطر دسترسی غیرمجاز، نقض دیتا و سوء استفاده احتمالی از اطلاعات محرمانه را کاهش دهند.

رویکرد دوم - تنظیمات حریم خصوصی:
استفاده از تنظیمات حریم خصوصی ارائه شده توسط پلتفورم های رسانه های اجتماعی برای موسسات غیردولتی جهت کنترل حضور آنلاین بسیار مهم است. با ترتیب دقیق این تنظیمات برای مدیریت نمایان شدن پستها، پیام ها و جزئیات نمایه، موسسات غیردولتی می‌توانند از اطلاعات حساس و مکالمات در دسترس عموم محافظت کنند. این رویکرد فعال به موسسات غیردولتی کمک می‌کند حریم خصوصی خود را حفظ نموده، از دیتای حساس محافظت کنند و از یکپارچگی کانال‌های ارتباطی خود در پلتفورم های رسانه‌های اجتماعی حمایت نمایند.

رویکرد سوم - آموزش و آگاهی:
تجهیز کارمندان به آموزش گسترده در مورد امنیت دیتا، پروتکل‌های حریم خصوصی و دستورالعمل‌های رسانه‌های اجتماعی برای موسسات غیردولتی ضروری است تا به طور موثر خطرات را در تعاملات و ارتباطات آنلاین خود کاهش دهند. موسسات غیردولتی با آموزش کارمندان در مورد شناسایی و پاسخ به تهدیدات احتمالی، سیستم دفاعی خود را در برابر نقض امنیت سایبری، نقض حریم خصوصی و انتشار اطلاعات نادرست تقویت می‌کنند. این اقدام پیشگیرانه تضمین می کند که کارمندان به خوبی آماده

هستند تا به طور امن در سیستم های عامل دیجیتال حرکت کرده، از دیتای حساس محافظت نموده، و اعتبار موسسه را در حوزه آنلاین حفظ کنند.

رویکرد چهارم – طرح نظارت و پاسخ:

ایجاد پروتکل‌های نظارتی دقیق برای حساب‌های رسانه‌های اجتماعی موسسات غیردولتی حیاتی است تا به سرعت دسترسی‌های غیرمجاز را شناسایی، فعالیت‌های مشکوک را رصد نموده و محتوای نامناسب را بررسی کنند. با انجام ارزیابی منظم و واکنش سریع به حوادث یا نقض امنیتی، موسسات غیردولتی می‌توانند به طور موثر از حضور آنلاین خود محافظت نموده، یکپارچگی کانال‌های ارتباطی خود را حفظ کنند و اعتماد مخاطبان خود را با خود داشته باشند. داشتن یک برنامه پاسخگو و به خوبی تعریف شده تضمین می کند که موسسات غیردولتی می توانند خطرات ناشی از حضور در رسانه های اجتماعی را کاهش دهند، آسیب های احتمالی را محدود کنند و از یک محیط دیجیتالی امن و معتبر برای بهره مندان خود حمایت نمایند.

رویکرد پنجم – به روزرسانی منظم و وصله‌ها (Patches):

حفظ حساب‌های رسانه‌های اجتماعی با آخرین وصله‌های امنیتی و به‌روزرسانی نرم‌افزاری برای موسسات غیردولتی حیاتی است تا از آسیب‌پذیری احتمالی و سوء استفاده مهاجمان سایبری جلوگیری کنند. موسسات غیردولتی با حفظ تنظیمات امنیتی و اجرای سریع به‌روزرسانی، می‌توانند امنیت دارایی‌های دیجیتالی خود را تقویت کنند، خطر نقض امنیت را کاهش دهند و حفاظت از دیتای حساس خود را که به اشتراک گذاشته شده افزایش دهند.

رویکرد ششم - تأیید پیوندها و پیام ها:

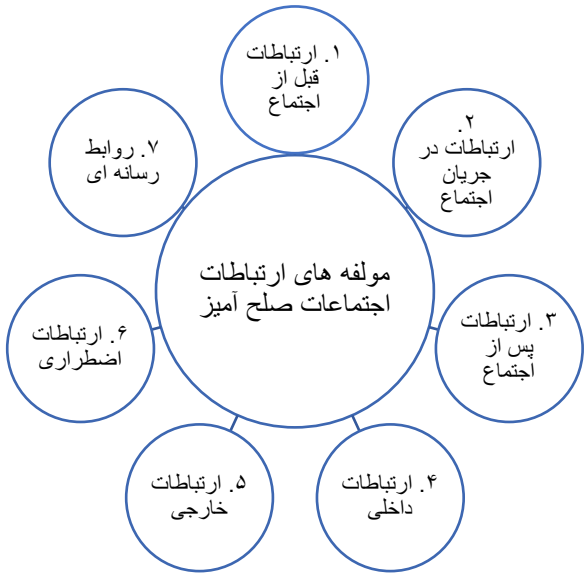
موسسات غیردولتی باید تأیید مشروعیت پیوندها، پیام‌ها و درخواست‌های دریافتی از طریق کانال‌های رسانه‌های اجتماعی را در اولویت قرار دهند تا خطر کلاهبرداری‌های فیشینگ (phishing)یا فعالیت‌های متقلبانه را کاهش دهند. با ترویج ترفند احتیاط در میان کارمندان، تأکید بر اهمیت بررسی پیوندهای ناشناخته، و خودداری از به اشتراک گذاری اطلاعات شخصی و نهاد، موسسات غیردولتی می توانند دفاع خود را در برابر تهدیدات سایبری و نقض احتمالی دیتا افزایش دهند. این رویکرد فعال تضمین می‌کند که موسسات غیردولتی از دقت در امنیت سایبری حمایت میکنند، از اطلاعات حساس محافظت نموده و تأثیر تلاش‌های مخرب برای به خطر انداختن امنیت دیجیتال خود را کاهش می‌دهند.

بخش دوم: ارتباطات اجتماعت مسالمت آمیز

ارتباطات اجتماعات صلح آمیز چیست؟

ارتباطات اجتماعات صلح آمیز به روش هایی اشاره دارد که توسط برگذارکنندگان، رضاکاران و شرکت کنندگان این اجتماعات جهت به اشتراک گذاشتن اخبار و اطلاعات، برنامه ریزی و تدارکات اجتماع و پیام های مرتبط در جریان یک اجتماع صلح آمیز، مانند اعتراضات، تظاهرات، گردهمایی ها و غیره استفاده می شود. چنین ارتباطات برای هماهنگی مؤثر فعالیت‌های صلح‌آمیز، امن نگه‌داشتن شرکت‌کنندگان و با خبر نگه داشتن آنها از وقایع در جریان یک اجتماع ضروری است. در این قسمت ارتباطات، ارتباطات شامل برنامه ریزی قبل از اجتماع، حین اجتماع و پس از اجتماع است.

مولفه های ارتباطات اجتماعات صلح آمیز چیست؟



۱. *ارتباطات قبل از اجتماع:*

استفاده از پلتفورم های دیجیتال مانند رسانه های اجتماعی، ایمیل و وبسایت جهت گسترش آگاهی، جلب حمایت و به اشتراکگذاری جزئیات مربوط به زمان، مکان و اهداف اجتماع.

۲. *ارتباطات در جریان اجتماع:*

استفاده از وسایل مختلف مانند بلندگو، علائم و وسایل شخصی برای انتقال پیام به شرکت کنندگان و هدایت موثر اجتماع. برنامه های پیام‌رسان گروهی یا رسانه های اجتماعی نیز می‌توانند به‌روزرسانی‌های فوری را برای مدیریت لوجستیک و پاسخگویی به شرایط پیش‌بینی نشده تسهیل کنند.

شکل ۱۱: مولفه های ارتباطات اجتماعات صلح آمیز.

۳. ارتباطات پس از اجتماع:

برای حفظ تعامل با اشتراک کنندگان و شتاب در اسرع وقت از طریق اطلاعیه ها، پیامها، توضیحات، یا نشراتی که نتایج اجتماع را خلاصه می کند، از شرکت کنندگان ابراز قدردانی کرده و مراحل بعدی یا اقدامات بعدی را مشخص ساخت.

۴. ارتباطات داخلی:

مؤلفه ارتباطات داخلی یک اجتماع صلح آمیز شامل همه راهبردها و ابزارهای مورد استفاده جهت هماهنگی ارتباطات بین برگذارکنندگان، رضاکاران و اشتراک کنندگان است که مستقیماً در برگذاری اجتماع دخیل اند. ارتباطات داخلی موثر برای حفظ موثریت اجتماع، تضمین امنیت و انطباق با تغییرات موقعیتی در جریان اجتماع بسیار مهم است.

۵. ارتباطات خارجی:

تعامل با رسانه ها و سایر نهادهای خارجی برای پخش گسترده تر پیام اجتماع و به تصویر کشیدن دقیق و مطلوب آن است.

۶. ارتباطات اضطراری:

ارتباطات اضطراری در جریان اجتماعات صلح آمیز به استراتژی های پیش تعریف شده ای اشاره دارد که برای انتقال سریع اطلاعات و پیام ها در مورد موضوعات فوری و همچنین هماهنگ کردن واکنش بین برگذار کنندگان، پرسنل امنیتی، رضاکاران و شرکت کنندگان استفاده می شود. این شکل از ارتباطات برای مدیریت بحران های احتمالی و تضمین امنیت همه افراد دخیل و حاضر ضروری است.

۷. روابط رسانه ای:

مدیریت ارتباطات با رسانه ها برای اطمینان از اینکه اهداف و روایت های اجتماع به درستی درک و گزارش شده است یک امر مهم تلقی میشود. روابط با رسانه ها ارتباطات را تضمین میکند که بیانیه های مطبوعاتی، مصاحبه توسط سخنگویان از پیش تعیین شده و جلسات توجیهی در رسانه ها قبل و بعد از اجتماع به درستی انجام شود.

چگونه قبل، حین و بعد از یک اجتماع صلح آمیز ارتباطات برقرار کنیم؟

برقراری ارتباطات موثر در جریان یک گردهمایی مسالمت آمیز در افغانستان مستلزم ملاحظات ویژه برای اطمینان از امنیت و رعایت قوانین محلی و هنجارهای فرهنگی است. در اینجا چند روش خاص برای برقراری ارتباطات قبل، حین و بعد از اجتماع به معرفی گرفته شده است:

رویکرد اول - رعایت قانون:
مقررات اداره موقت طالبان برگذاری یک اجتماع صلح آمیز بدون مجوز از وزارت امور داخله را ممنوع کرده است. اخذ مجوز از وزارت داخله این اداره بسیار چالش برانگیز است و در حدی است دریافت آن امکان ندارد مگر اینکه اجتماع به نفع خود این اداره باشد. شما نباید ریسک کنید یا هیچ تلاشی برای بدست آوردن آن به خرچ ندهید. بعید است که تلاش برای برقراری گفتگوی سازنده با نمایندگان اداره موقت طالبان برای تأیید یک اجتماع صلح آمیز نتایج مثبتی به همراه داشته باشد. بنابراین، خود و افراد دخیل در این اجتماعات را در همان لحظه اول به خطر مواجه نسازید.

رویکرد دوم - نظارت بر وضعیت:
اطمینان حاصل کنید که اطلاعات قابل اعتمادی در مورد برگذاری اجتماعات صلح آمیز جمع آوری کرده اید. منابع خبری و گزارش های نهاد های حقوق بشر را برای تازه ترین جزئیات بررسی کنید.

رویکرد سوم – تهیه استراتژی ارتباطات داخلی:
تهیه یک استراتژی داخلی برای شناسایی ابزارهای ارتباطی مورد استفاده و امن جهت هماهنگی و ارتباطات بین برگذار کنندگان، رضاکاران و هر فرد ذینفع کلیدی که مستقیماً در برگذاری اجتماع دخیل است، یک نیاز مبرم است. ارتباطات داخلی موثر برای حفظ موثریت اجتماع، تضمین امنیت دست اندرکاران و انطباق با تغییر مواضع در جریان یک اجتماع بسیار مهم است. لطفاً برای یافتن امن‌ترین و بهترین ابزارها و پلتفرم‌های برای برقراری ارتباطات داخلی به شکل‌های ۸، ۹ و ۱۰ مراجعه کنید.

رویکرد چهارم – تهیه استراتژی ارتباطات خارجی:
تهیه استراتژی ارتباطات خارجی برای رسیدگی به نحوه تعامل با رسانه ها و سایر نهادهای خارجی برای پخش گسترده تر پیام اجتماع و به تصویر کشیدن آن به طور دقیق و مطلوب همچنان نیاز مبرم

است. لطفاً برای یافتن امن‌ترین و بهترین ابزارها و پلتفرم‌ها برای برقراری ارتباطات خارجی به شکل‌های ۸، ۹ و ۱۰ مراجعه کنید.

رویکرد پنجم – تهیه استراتژی ارتباطباتات اضطراری:

تهیه استراتژی ارتباطات اضطراری قبل از برگذاری یک اجتماع صلح آمیز برای انتقال سریع اطلاعات در مواردا‌ضطراری و هماهنگ کردن واکنش ها بین برگذارکنندگان، پرسنل امنیتی، رضاکاران و شرکت کنندگان یک امر حتمی است. این استراتژی برای مدیریت بحران های احتمالی و تضمین امنیت همه افراد حاضر ضروری است.

رویکرد ششم – حفظ روابط با رسانه های خارجی و برون مرزی افغان:

رسانه‌های محلی به دلیل حفظ امنیت خبرنگاران و رسانه‌های خود هرگز اجتماع صلح آمیز شما را پوشش خبری نمی‌دهند، زیرا آنها از پوشش هر گونه اجتماع توسط اداره موقت طالبان منع شده اند. ارتباط خود را با رسانه های خارجی و رسانه های برون مرزی حفظ کنید تا مطمئن شوید که اهداف و روایت های اجتماع صلح آمیز به درستی انعکاس یافته و گزارش شده است. در این نوع ارتباطات شما متوانید از بیانیه های مطبوعاتی، مصاحبه توسط سخنگویان تعیین شده و جلسات مختصر رسانه ها بعد از اجتماع استفاده کنید. برای اقدامات امنیتی، لطفاً از رهنمواجتماعات صلح آمیز ما برای جامعه مدنی افغانستان که قبلا چاپ شده استفاده کنید.

رویکرد هفتم – ارتباط با شرکت کنندگان:

اطمینان حاصل کنید که همه شرکت کنندگان در اجتماع از دستورالعمل های امنیتی آگاه هستند. بسیار مهم است که بر اهمیت حفظ رفتار مناسب، پاسخگویی به اقدامات و پایبندی به کدهای رفتاری توافق شده تاکید شود. علاوه بر این، همه را تشویق کنید که مراقب باشند و هر گونه فعالیتی را که ممکن است در جریان اجتماع با آن مواجه شوند گزارش دهند. برای اقدامات امنیتی، لطفاً به رهنمود اجتماعات صلح آمیز برای جامعه مدنی افغانستان که قبلا به چاپ رسیده مراجعه نمایید.

رویکرد هشتم - هماهنگی با موسسات غیردولتی و سازمان های حقوق بشر:

در صورت امکان، با موسسات غیردولتی بین‌المللی و سازمان‌های حقوق بشر تماس بگیرید تا از نظریات آنها را در مورد شرایط کنونی در افغانستان اطلاع حاصل کنید. آنها دارای تجربه و دانش دقیق در مورد وقایع و اقدامات احتیاطی امنیتی لازم هستند.

رویکرد نهم - کانال های ارتباطات امن را در نظر داشته باشید:

اگر قصد دارید در یک اجتماع شرکت کنید یا آن را سازماندهی نمایید، به روشهای امن برای برقراری ارتباطات فکر کنید. سرویس‌های پیام‌رسانی رمزگذاری‌شده می‌توانند حریم خصوصی و امنیت بیشتری را برای برگذارکنندگان و شرکت‌کنندگان ارائه دهند. هرگز از شماره تلفن محلی خود هنگام شرکت در اجتماعات استفاده نکنید. لطفاً برای یافتن امن‌ترین ابزارهای ارتباطی به شکل‌های ۸، ۹ و ۱۰ مراجعه کنید.

رویکرد دهم - تعامل با سازمان ها و رسانه های بین المللی:

اطمینان حاصل کنید که سازمان های بین المللی حقوق بشر و رسانه ها از برگذاری اجتماع آگاه هستند. گاهی اوقات، در کشورهای نا امن، نهادهای بین المللی می توانند تا حدی شما را از خطرات حفظ کنند. لطفاً برای یافتن امن‌ترین و بهترین ابزارها و پلتفرم‌ها برای برقراری ارتباطات با نهادهای خارجی به شکل‌های ۸، ۹ و ۱۰ مراجعه کنید.

رویکرد یازدهم - به اجتماعات مجازی روی آورید:

ارزیابی کنید که اگر یک اجتماع صلح آمیز حضوری امکان پذیر نیست و شما را به خطر مواجه میسازد به یک اجتماع مجازی از طریق پلتفرم های آنلاین که می تواند بدون خطر شما را به اهداف تان برساند روی آورید. لطفاً برای یافتن امن‌ترین و بهترین ابزارها و پلتفورم‌ها برای برگذاری یک اجتماع مجازی به شکل‌های ۸ و ۱۰ مراجعه کنید.

رویکرد دوازدهم - نمایش علائم و بنرها:

استفاده از وسایلی مانند علائم، بنرها یا نمادها را برای بیان پیام خود در نظر بگیرید. این ابزارها می توانند در انتقال اهداف یا خواسته های شما به ناظران، رسانه ها و مقامات نقش داشته باشند ولی در تهیه آنها در حدی افراط نکنید که شما را به خطر بیندازد.

رویکرد سیزدهم – در شعار دادن و انتخاب کلمات دقیق باشید:

در شعارهایی که هدف اجتماع را منعکس می کند، همصدا باشید. این باعث ایجاد احساس با هم بودن را برای شما میدهد. تأثیرات پیام خود را افزایش دهید، اما از هرگونه واژه های خطر ساز و حساس که اداره موقت طالبان به آنها واکنش تند نشان میدهند اجتناب کنید. همچنین، درصد بالایی از کلمات زمانی که در شعار ها استفاده میشوند ممکن غلط برداشت شوند و شما را به خطرات جدی روبرو سازند،مواظب باشید.

رویکرد چهاردهم - از گفتگوی صلح آمیز استفاده کنید:
اگر با مقامات اداره موقت طالبان و مخالفان معترض به صورت ناخواسته مواجه شدید، سعی کنید با آنها گفتگوهای صلح آمیز داشته باشید و از هرگونه خشونت خودداری کنید و راهی پیدا کنید که فوراً منطقه را ترک کنید.

رویکرد پانزدهم - از رسانه های اجتماعی استفاده کنید ولی لایف نروید:
در جریان اجتماع، تویت زنده یا به‌روزرسانی‌ها را در پلتفرم های رسانه‌های اجتماعی به اشتراک نگذارید یا به اصطلاح رسانه های اجتماعی لایف نروید. ارسال عکس‌ها، فیلم ها و بیانیه‌های از جریان اجتماعات به جذب مخاطب و افزایش آگاهی در مورد اهداف شما کمک می‌کند، اما همه را در معرض خطر قرار می‌دهد. اگر می خواهید چیزی را به اشتراک بگذارید، آن را بعد از رویداد انجام دهید. در همین حال، هنگام ارسال فیلم و عکس در شبکه های اجتماعی مراقب باشید. استفاده از یک حساب کاربری ناشناس، محو کردن چهره های شرکت کنندگان و استفاده از VPN و TOR به شدت توصیه می شود. لطفاً برای یافتن بهترین VPN و TOR به شکل های ۳ و ۵ مراجعه کنید.

رویکرد شانزدهم - تماس های اضطراری:
مطمئن شوید که شماره های تماس اضطراری را در تلفن خود ذخیره کرده اید یا آنها را یادداشت نموده و نزد خود نگه دارید. در همین حال، داشتن یک تماس اضطراری در تلفن و یا در یک کاغذ همراه می تواند عزیزان شما را در صورت تشنج در معرض خطر قرار دهد.

رویکرد هفدهم – مدیریت اوضاع تا دور از توجه عامه بمانید:
برای جلوگیری از جلب توجه ناخواسته، در جریان اجتماع صلح آمیز زیاد جلب توجه نکنید. از اعلامیه های افراط آمیز، بلندگوهای زیاد و بنرهای با دید بالا خودداری کنید.

رویکرد هجدهم - ارتباط بین برگذارکنندگان:
یک خط ارتباطی محتاطانه بین برگذارکنندگان در جریان اجتماع برای هماهنگی اقدامات و پاسخگویی به شرایط پیش‌بینی نشده حفظ کنید. اگر کسی ارتباطات الکترونیکی را زیر نظر دارد، از سیگنال های ظریف استفاده کنید.

رویکرد نوزدهم – جلب توجه نکنید:
پس از اختتام اجتماع، مطمئن شوید که دیگر با لباسی که در هنگام اجتماع به تن داشتید، ظاهر نشوید و هیچ گونه علایم یا اشیای مرتبط و قابل توجه از محل تجمع با خود حمل نکنید.

رویکرد بیستم – از وضعیت خود نزدیکان خود را با خبر سازید:
از طریق یک ابزار ارتباطی امن در رسانه های اجتماعی که خدمات رمزگذاری سرتاسری را ارائه می دهد، با خانواده یا دوستان خود تماس بگیرید. به آنها اطلاع دهید که در امن هستید. اگر فکر می کنید ایمن نیستید، مکان خود را به اشتراک نگذارید.

رویکرد بیست و یکم – توضیح مختصر:
با شرکت کنندگان در یک مکان برای گفتگو در مورد اجتماع جمع نشوید. در حالی که در امنیت هستید، هر گونه اقدام لازم را برای پیشبرد اجتماع برنامه ریزی کنید. برای هر هماهنگی از یک ابزار ارتباطی رسانه های اجتماعی مانند سیگنال استفاده کنید که رمزگذاری ۱۰۰٪ سرتاسر را ارائه می دهد. با شماره تلفن صحبت نکنید.

رویکرد بیست و دوم – احتیاط در رسانه های اجتماعی:
مهم است که مراقب آنچه در رسانه های اجتماعی به اشتراک می گذارید باشید. گاهی اوقات اطلاعاتی که پست می کنیم می تواند خطرات بالقوه ای برای خود یا اطرافیانمان ایجاد کند. اگر باید چیزی را در رسانه های اجتماعی به اشتراک بگذارید، از یک حساب کاربری ناشناس و یک VPN استفاده کنید.

رویکرد بیست و سوم - نظارت بر وضعیت:
پس از اتمام اجتماع، حتما از طریق منابع خبری از اتفاقات منطقه خود مطلع شوید. این به شما کمک می کند تا در مورد عواقب اجتماع و هرگونه تغییری که ممکن است بر امنیت شما تأثیر بگذارد مطلع باشید.

رویکرد بیست و چهارم - طرح اضطراری:
مطمئن باشید که برنامه ای را در صورتی که اجتماع صلح آمیز به هرج و مرج کشانده میشود یا توسط نیروهای امنیتی پراکنده میشود، طرح ریزی کرده و پیش بینی نموده اید. بهتر است در محل خود نمانید و از سفر خودداری کنید مگر در موارد ضروری. جایی برای ماندن پیدا کنید. فقط در صورتی مکان خود را فاش کنید که مطمئن باشید کسی شما را به اداره موقت طالبان تحویل نخواهد داد. در یک جای امن بمانید و هیچ تلفون و دستگاه تلفون با خود حمل نکنید.

رویکرد بیست و پنجم - گفتگو پس از اجتماع:
برای بحث در مورد نتایج اجتماع و تجارب بدست آمده، یک جلسه مختصر ساده با برگذارکنندگان کلیدی دایر کنید. اطمینان حاصل کنید که این کار را به صورت امن و خصوصی انجام دهید. به جای تجمع حضوری، با استفاده از امن ترین ابزار ارتباطی رسانه های اجتماعی که خدمات پیام رسانی رمزگذاری شده را ارائه می دهد، یک جلسه مجازی را سازماندهی کنید. لطفاً برای یافتن امن ترین ابزار برای ارتباط خود به شکل های ۸، ۹ و ۱۰ مراجعه کنید.

رویکرد بیست و ششم - انتشار دقیق اطلاعات:
اگر اطلاعات مربوط به اجتماع را به صورت عمومی به اشتراک می گذارید (به عنوان مثال، از طریق رسانه های اجتماعی یا مطبوعات)، در مورد آنچه به اشتراک گذاشته می شود بسیار محتاط باشید تا از عواقب احتمالی جلوگیری کنید. تصاویر باید بر جنبه های صلح آمیز بودن اجتماع، بدون تحریک مقامات متمرکز باشد. در همین حال، همه صورت اشتراک کنندگان باید مخدوش باشد تا شناسایی نشوند. در غیر این صورت، چهره تمام شرکت کنندگانی که در یک ویدیو یا عکسی که قرار است منتشر شود، آنها را به خطر میندازد.

رویکرد بیست و هفتم – پشتیبانی و پیگیری:
در صورت وجود هرگونه عواقب و اقدامات از سوی مقامات، از شرکت کنندگان حمایت کنید. با سازمان های داخلی و بین المللی حقوق بشر خواستار همکاری شوید.

در جریان یک اجتماع صلح آمیز از چه اصطلاحات باید اجتناب شود؟

قبل، در حین و بعد از یک گردهمایی در افغانستان، مهم است که از برخی اصطلاحات که ممکن است حساس یا نامناسب تلقی شوند، اجتناب شود. معرفی این اصطلاحات خاص کمی دشوار است، اما هر چیزی که مربوط به موضوعاتی باشد که با ایدئولوژی اداره موقت طالبان در تضاد باشد مورد استقبال قرار نمی گیرد. هنگام برقراری ارتباطات در چنین محیطی، توجه به آداب و رسوم محلی، هنجارهای فرهنگی و محیط سیاسی بسیار مهم است. برای جزئیات بیشتر در مورد نحوه نظارت اداره موقت طالبان بر استفاده از این اصطلاحات، لطفاً به بخش *موسسات غیردولتی هنگام برقراری ارتباطات از چه اصطلاحاتی باید اجتناب کنند؟*، که ما اطلاعات بیشتری در مورد استفاده از اصطلاحات حساس در این بخش ارائه نموده ایم.

امن ترین ابزار و پلتفورم های ارتباطات برای استفاده در افغانستان کدامند؟

لطفاً به شکل‌های ۸، ۹ و ۱۰ برای امن‌ترین ابزارها و پلتفورم های ارتباطات مراجعه نمایید.

مزایا و اضرار استفاده از رسانه های اجتماعی در یک اجتماع صلح آمیز چیست؟

۱. مزایا:

مزیت اول – آگاهی و بسیج:
پلتفرم های رسانه های اجتماعی می توانند ابزار قدرتمندی برای افزایش آگاهی و بسیج سریع و موثر شرکت کنندگان باشند. اطلاعات مربوط به زمان، مکان و هدف اجتماع می تواند در مدت زمان کوتاهی به مخاطبان گسترده ای برسد.

مزیت دوم - به اشتراک گذاری اطلاعات:
رسانه های اجتماعی امکان رساندن تازه ترین اخبار و اطلاعات را برای همه فراهم می کنند، که ممکن برای هماهنگی فعالیت ها و پاسخ به هرگونه تغییر یا شرایط اضطراری در جریان اجتماع بسیار مهم باشد.

مزیت سوم –ایجاد گردهمایی:
این پلتفرم‌ها می‌توانند به ایجاد گردهمایی های افراد همفکر که از یک هدف حمایت می‌کنند، کمک کند و حس همبستگی را در میان شرکت‌کنندگان تقویت نماید.

مزیت چهارم – توجه جامعه جهانی:
از طریق رسانه های اجتماعی، موضوعاتی که در عمق اجتماع قرار دارند می توانند توجه جامعه جهانی را به خود جلب کنند، که به طور بالقوه منجر به حمایت و فشار جامعه جهانی بر گروه مستقر در افغانستان می شود که ممکن است نتایج مثبتی را در پی داشته باشد.

مزیت پنجم – دستیابی و تعامل:

پلتفرم های رسانه های اجتماعی به برگذارکنندگان یک منبع ضروری برای گسترش نفوذ آنها، ارتباط مستقیم با جامعه جهانی و افزایش دید برای اهدافشان را میباشد. با استفاده از دسترسی گسترده و قابلیت‌های تعاملی رسانه های اجتماعی، برگذارکنندگان می‌توانند به وضوح اهداف خود را منتقل سازند، روایت‌های قویی را منتشر نمایند و از مخاطبان مختلف حمایت کنند. این استراتژی دیجیتال نه تنها پیام آنها را تقویت می کند، بلکه احساس مشارکت را در بین حامیان ایجاد می نماید و امکان تعامل و نتیجه گیری فوری را فراهم می کند.

مزیت ششم – دادخواهی و شبکه سازی:

پلتفرم های رسانه های اجتماعی مجموعه ای از ابزارهای همه‌کاره را برای تقویت تحولات اجتماعی، جلب حمایت از ابتکارات آن‌ها و ایجاد روابط با همفکران و تمویل کنندگان ارائه می‌کنند. با استفاده از قابلیت‌های ارتباطات رسانه های اجتماعی، برگذارکنندگان می‌توانند به طور موثر موضوعات مهم را برجسته سازند، حمایت مردم را برای تلاش‌های خود انرژی بخشند، و همکاری‌هایی را انکشاف دهند که نفوذ آنها را افزایش دهد. این محیط دیجیتال نه تنها به عنوان رسانه ای برای انتشار پیام ها عمل می کند، بلکه به ایجاد یک جامعه متصل متعهد به ایجاد تحولات مثبت اجتماعی و دستیابی به اهداف مشترک در قسمت تأثیرات اجتماعی کمک می کند.

مزیت هفتم - ارتباط مستقیم:

تعامل مستقیم با مخاطبان برای رسیدن به اهداف ضروری است. رسانه های اجتماعی ارتباط تعاملی با حامیان شما را امکان پذیر می کند و امکان تبادل نظریات فوری را به صورت فعالانه فراهم می کند. این کانال های ارتباطات مستقیم، که با اطلاعات مناسب تقویت شده اند، می توانند به طور موثر آگاهی را افزایش دهند و انجام اقدامات مورد نظر را سرعت بخشند.

مزیت هشتم - نشر اطلاعات:

گنجاندن رسانه های اجتماعی در استراتژی اطلاع‌رسانی برگذارکنندگان را قادر می‌سازد تا به‌روزرسانی‌های حساس به زمان، منابع ارزشمند، محتویات آموزشی و اعلامیه های اضطراری را به طور مؤثر به عموم مردم منتشر کنند. برگذارکنندگان می‌توانند با بهره‌گیری از فوریت و دسترسی گسترده پلتفورم های رسانه های اجتماعی، به سرعت اطلاعات حیاتی را پخش کنند، با مخاطبان در ارتباط شوند و به وقایع در حال آشکار شدن پاسخ مؤثری بدهند و اطمینان حاصل کنند که ارتباطات آنها نه تنها به موقع، بلکه تأثیرگذار و گسترده است.

مزیت نهم - به حداکثر رساندن آگاهی و روابط:
رسانه های اجتماعی به عنوان یک ابزار قدرتمند به هدف اتصال عمل می کنند و به عنوان یک پلتفورم پویا برای افزایش آگاهی نقش مهمی دارند. این به برگذارکنندگان توان این را می دهد تا با مخاطبان زیادی که به دنبال ارتباط با افراد همفکر و اهداف همسو هستند و به آنها اهمیت می دهند، درگیر شوند. رسانه‌های اجتماعی از طریق اشتراکگذاری فوری اطلاعات و تصاویر، پنجره‌ای را به یک مجموعه عظیمی از افراد ارائه می‌کنند و پیام‌های به‌خوبی ساخته‌شده‌ای را که هدف آن را منعکس می‌کنند، تقویت می نمایند.

۲. اضرار:

ضرر اول - نظارت و سرکوب توسط مقامات:
خطر نظارت بر رسانه های اجتماعی در افغانستان زیاد است. استفاده از این پلتفرم‌ها می‌تواند برگذارکنندگان و شرکتکنندگان را در معرض خطراتی از جمله دستگیری یا بدتر از آن، در صورتی که به عنوان مخالفان سیاسی تلقی شوند، قرار دهد.

ضرر دوم - اطلاعات غلط و اطلاعات نارسا:
انتشار اطلاعات غلط و اطلاعات نارسا می تواند به سرعت در رسانه های اجتماعی شیوع شود و به طور بالقوه منجر به سردرگمی، انتشار شایعات و تضعیف اهداف اجتماع شود.

ضرر سوم - تحریک و خشونت:
پستهای رسانه‌های اجتماعی را می‌توان خارج از چارچوب مفاهیم اصلی یا برای تحریک خشونت یا اقدامات تهاجمی دستکاری کرد که ممکن صلح آمیز بودن و قانونی بودن اجتماعات را به خطر بیندازد.

ضرر چهارم – پراکنده شدن:
در حالی که رسانه های اجتماعی می توانند که سبب متحد شدن یک اجتماع شوند، آنها نیز می توانند گروه ها را پراکنده کنند. تفاوت در نظرات و رویکردها می تواند آشکارتر شود و منجر به انشعاب گروه ها و تضعیف قدرت جمعی شرکت کنندگان در اجتماعات شود.

ضرر پنجم - خطرات امنیتی:

ادغام استراتژی های رسانه های اجتماعی در مناطق متشنج مانند افغانستان می تواند موانع امنیتی ایجاد کند که شامل تهدیدات بالقوه برای امنیت برگذارکنندگان، پرسنل امنیتی و رضاکاران می شود. هنگام استفاده از پلتفورم های رسانه های اجتماعی، برگذارکنندگان باید به نگرانی‌های مربوط به افشای اطلاعات حساس، هدف قرار دادن احتمالی شرکتکنندگان یا رضاکاران، و حفاظت از منابع ضروری در مناطقی که با بی‌ثباتی و چالش‌های امنیتی روبرو اند، رسیدگی کنند.

ضرر ششم - سانسور و نظارت:

برگذارکنندگان اجتماعات مسالمت آمیز در افغانستان با چالش های مرتبط با سانسور اینترنتی، تاکتیک های نظارت و محدودیت های آزادی بیان در هنگام استفاده از پلتفورم های رسانه های اجتماعی مواجه هستند. برای غلبه بر این موانع، باید قوانین سختگیرانه محتوای دیجیتال، نظارت بیشتر که خطراتی برای حریم خصوصی و امنیتی ایجاد می‌کند و محدودیت‌هایی در ارتباطات آزاد از طریق کانال‌های آنلاین دنبال کرد. این موانع محیط پیچیده ای را که برگذارکنندگان باید در آن هنگام استفاده از رسانه‌های اجتماعی در افغانستان کار کنند، برجسته می‌کند، و بر نیاز به مشورت و تعدیل سنجیده برای تضمین رویکردهای ارتباطی کارآمد و امن تأکید می‌نماید.

ضرر هفتم – اطلاعات غلط و اطلاعات نارسا:

پلتفورم های رسانه های اجتماعی به‌عنوان کانال‌هایی برای انتشار اطلاعات غلط، تبلیغات و روایت های نارسا عمل می‌کنند که خطری برای شهرت و اعتبار برگذارکنندگان اجتماعات صلح‌آمیز ایجاد می نماید. انتشار اطلاعات غلط از طریق این پلتفورم‌ها می‌تواند چهره یک اجتماع صلح آمیز را مخدوش کند، اعتماد عمومی را از بین ببرد و چهره واقعی اهداف و مقاصد آنها را لکه دار سازد.
بنابراین، برگذار کندگان باید هنگام استفاده از رسانه‌های اجتماعی برای مقابله موفقیت‌آمیز با اطلاعات غلط و اطلاعات نارسا و محافظت از یکپارچگی خود در حوزه دیجیتال هوشیار باشند.

ضرر هشتم - نگرانی های مربوط به حریم خصوصی:

برگذارکنندگان اجتماعات صلح‌آمیز باید در هنگام به اشتراک گذاری دیتای حساس در کانال‌های رسانه‌های اجتماعی، در قسمت حریم خصوصی دیتا، خطرات سایبری و تهدیدات امنیت اطلاعات احتیاط کنند. تصمیم برای افشای چنین اطلاعاتی، آسیب‌پذیری را در معرض نقض احتمالی دیتا، دسترسی غیرقانونی و سوء استفاده توسط نهادهای مخرب قرار می‌دهد و اهمیت ایجاد حفاظت و روش قوی برای حفاظت از دیتای حساس و حفظ اعتبار فعالیت‌های آنها در حوزه آنلاین را برجسته می‌کند.

چگونه در رسانه ها و رسانه های اجتماعی در جریان و بعد از یک اجتماع صلح آمیز حاضر شوید؟

در افغانستان، استفاده از رسانه‌ها و رسانه‌های اجتماعی برای پوشش یک اجتماع صلح‌آمیز به دلیل محیط بسیار محدود و تحت نظارت، نیازمند برنامه‌ریزی استراتژیک دقیق است. در اینجا برخی از دستورالعمل ها و اقدامات احتیاطی وجود دارد که هنگام استفاده از رسانه ها و بسترهای اجتماعی در جریان و بعد از یک اجتماع باید در نظر بگیرید:

رویکرد اول – ابتدا امنیت:
همیشه امنیت شرکت کنندگان را در اولویت قرار دهید. اگر افشای اطلاعات به احتمال زیاد منجر به اقدامات تنبیهی علیه اشتراک کنندگان شود، لازم است آن اطلاعات پنهان بماند.

رویکرد دوم - گزارش ناشناس:
از ناشناس ماندن گزارش دهندگان برای محافظت از هویت آنها اطمینان حاصل کنید. از روش هایی مانند اعوجاج صدا و مخدوش کردن چهره در فیلم ها و عکس ها برای محافظت از شرکت کنندگان در برابر احتمال اقدامات تنبیهی استفاده کنید.

رویکرد سوم - شبکه های امن:
از ابزارهای ارتباطی امن و رمزگذاری شده برای انتشار اطلاعات استفاده کنید. این امر خطر نظارت و رهگیری توسط مقامات را کاهش می دهد. لطفاً به شکل های ۸، ۹ و ۱۱ مراجعه کنید.

رویکرد چهارم - اشتراک گذاری ترجیهی:
انتخابی باشید که چه چیزی را در چه زمان و با کی به اشتراک بگذارید. از پخش مکان‌های استراتژیک و محلات وقوع اجتماع و یا حرکاتی که می‌تواند توسط مخالفان علیه شرکت‌کنندگان استفاده شود، خودداری کنید.

رویکرد پنجم - نظارت در زمان واقعی:
برای رفع هرگونه سوءتعبیر یا سوء استفاده از اطلاعات به اشتراک گذاشته شده، وضعیت را به طور مستمر رصد کنید. برای جلوگیری از تشدید ممکن است شفاف سازی یا حذف سریع پست ها ضروری باشد.

رویکرد ششم – مشارکت با رسانه های داخلی و بین المللی:
با رسانه های محلی و بین المللی قابل اعتمادی که ممکن است وقایع را به طور گسترده تری پوشش دهند، تعامل داشته باشید، و برای تعامل با آنها، یک لایه حفاظتی اضافی را نیز فراهم کنید تا در امن باشید چون ممکن ارتباطات شما توسط مقامات رهگیری شود.

رویکرد هفتم - شواهد مستند:
شواهد مستند تویری و متنی از اجتماع را گردآوری و بایگانی کنید تا مطمئن شوید که به طور امن ذخیره می شود و می توان برای حمایت های بعدی بدون به خطر انداختن امنیت افراد درگیر به آن دسترسی داشته باشید. اما مراقب باشید که مدارک مستند به بیرون درز نکند.

رویکرد هشتم – اشتراک گذاری کنترل شده:
روایت ها را با انتشار اطلاعات در مراحل مختلف کنترل کنید تا موضوع حین گفتمان عمومی سلسله ارتباط خود را از دست ندهد و ضمنا ریسک های ناشی از این گفتمان کانترول شود.

رویکرد نهم - از کانال های استفاده کنید که به پروتکل های محتوای حساس وابسته باشند:
از کانال‌ها و پلتفرم‌هایی استفاده کنید که پروتکل‌هایی را برای محتوای حساس ایجاد کرده‌اند و از عواقب مضر جلوگیری میکنند.

رویکرد دهم – حلقه پیشنهادات و انتقادات:
یک حلقه پیشنهادات و انتقادات با شرکت کنندگان و حامیان تان ایجاد کنید تا موثریت استراتژی رسانه را ارزیابی کنید و برای فعالیت های آتی در آینده اصلاحاتی داشته باشید.

رویکرد یازدهم - اقدامات حفاظت از دیتا:
امن سازی اطلاعات حساس در رسانه های اجتماعی برای اجتماعات بسیار مهم است. برگذارکنندگان می‌توانند با اجرای روشهای امنیتی سختگیرانه از این اطلاعات محافظت کنند، مانند ایجاد رمزهای عبور قوی و منحصربه‌فرد، فعال کردن احراز هویت دو مرحله ای برای امنیت بیشتر، و محدود کردن دسترسی فقط به این دیتا به استثنای خود شان. اتخاذ این اقدامات به جلوگیری از دسترسی غیرمجاز، نقض دیتا و سوء استفاده از اطلاعات محرمانه کمک می کند و در نتیجه از حضور دیجیتال آنها محافظت می کند و اعتماد مخاطبان خود را حفظ می کند.

رویکرد دوازدهم - تنظیمات حریم خصوصی:
برگذارکنندگان یک اجتماع صلح آمیز باید از تنظیمات حریم خصوصی ارائه شده توسط پلتفورم های رسانه های اجتماعی برای مدیریت موثر حضور آنلاین خود استفاده کنند. تنظیم دقیق این تنظیمات برای کنترل افرادی که می‌توانند پست‌ها، پیام‌ها و اطلاعات نمایه‌شان را ببینند، به اجازه می‌دهد برگذارکنندگان از دیتای حساس و مکالمات خصوصی در برابر قرار گرفتن در معرض عموم محافظت کنند. این استراتژی عمدی به حفظ محرمانه بودن، امن سازی اطلاعات مهم و حفظ یکپارچگی کانال های ارتباطی آنها در پلتفرم های مختلف رسانه های اجتماعی کمک می کند.

رویکرد سیزدهم - آموزش و آگاهی:
برای برگذارکنندگان ضروری است که به پرسنل امنیتی و رضاکاران آموزش کامل در زمینه امنیت دیتا، شیوه‌های حفظ حریم خصوصی، و دستورالعمل‌های رسانه‌های اجتماعی ارائه دهند تا به طور موثر خطرات را در طول تعاملات و ارتباطات آنلاین به حداقل برسانند. آموزش این افراد برای شناسایی و رسیدگی به تهدیدات احتمالی، توانایی آنها را برای مبارزه با نقض امنیت سایبری، نقض حریم خصوصی و انتشار اطلاعات نادرست تقویت می کند. با برداشتن این گام های پیشگیرانه، پرسنل امنیتی و رضاکاران برای پیمایش امن در پلتفورم‌های دیجیتال، محافظت از اطلاعات حساس و حفظ یکپارچگی شهرت آنلاین اجتماع تجهیز می شوند.

چگونه می توان گفت و گوی سازنده ای با نمایندگان اداره موقت طالبان ایجاد کرد؟

مقررات اداره موقت طالبان صراحتاً انجام یک اجتماع صلح آمیز بدون مجوز قبلی از وزارت امور داخله را ممنوع می کند. کسب مجوز از وزارت داخله بسیار چالش برانگیز و غیرممکن است. ما اکیداً توصیه می‌کنیم از ریسک کردن و وقت گذاشتن در این مورد بیهوده است و با درخواست چنین مجوز خود را به خطر میندازید. احتمال موفقیت در یک گفتگوی سازنده با نمایندگان اداره موقت طالبان برای کسب مجوز برای برگذاری یک اجتماع صلح آمیز نا ممکن است.

همچنین ممکن است برگذاری یک اجتماع صلح آمیز و رویارو شدم با نمایندگان اداره موقت طالبان در جریان چنین اجتماع بدون مجوز منجر به عواقب نامطلوب شود. توصیه می کنیم بلافاصله محل را ترک کنید و پس از اجتماع به منطقه برنگردید. برای جزئیات بیشتر، لطفاً به رهنمود اجتماعات صلح آمیز برای جامعه مدنی افغانستان مراجعه کنید.

در پایان یک اجتماع صلح آمیز چه اقداماتی باید صورت پذیرد؟

۱. نتیجه گیری:

اختتام اجتماع صلح آمیز را اعلان کنید. به طور معمول، این اعلامیه باید با تحویل پیام مطابقت داشته باشد. در برخی مواقع، به علت نگرانی‌های امنیتی ممکن است نیاز به انجام یک اجتماع صلح آمیز زودتر از موعد مقرر باشد. در چنین حالات از یک کانال امن و مناسب برای اطلاع رسانی همه شرکت کنندگان در مورد نتیجه گیری از اجتماع استفاده کنید. قبل از بسیج، بسیار مهم است که زمان پایان اجتماع و چگونگی پایان دادن به آنرا اعلام کنید.

۲. دستورالعمل ها:

به شرکت کنندگان در مورد نحوه پراکنده شدن از اجتماع دستورالعمل روشن ارائه کنید. آنها را تشویق کنید که منطقه را به صورت صلح آمیز ترک کنند و از هرگونه درگیری با مقامات یا مخالفان معترض خودداری کنند. توصیه می شود شرکت کنندگان مسیرهای متفاوت و امنی را برای خروج از ساحه اجتماع انتخاب کنند.

۳. تسهیل خروج صلح آمیز:

برای خروج امن و اضطراری، تعیین راهها و مسیرهای امن و ابلاغ آنها برای شرکت کنندگان بسیار مهم است. مطمئن شوید که این مسیرها را به وضوح شناسایی کنید.

۴. اوضاع را تحت نظر بگیرید:

به عنوان یک برگذار کننده، مراقب نشانه های تنش یا درگیری های احتمالی باشید تا بتوانید به طور موثر با شرکت کنندگان و رضاکاران ارتباط برقرار کنید. باخبر بودن شما ضروری است و به سرعت با هر مشکلی که پیش می آید مقابله کنید و راه حلی برای آن جستجو کنید. رفتار مسالمت آمیز را ترویج دهید و در صورت لزوم برای حل هر گونه اختلاف یا درگیری مداخله کنید.

۵. ارتباطات بعد از اجتماع:

هنگام به اشتراک گذاشتن اطلاعات با شرکت کنندگان بعد از پایان اجتماع بسیاراحتیاط کنید. این اطلاعات ممکن است شامل تازه ترین اخبار در مورد اجتماع یا رویدادهای بعدی مرتبط با اهداف تان، روشهای حفظ امنیت دست اندرکاران، یا عدم مشارکت آنها به علت نگرانی‌های امنیتی باشد. یک روش تماس امن برای مشارکتکنندگان ارائه دهید تا همچنان با هم در تماس باشند، تازه ترین اخبار را دریافت کنند، یا به دلایل امنیتی قطع رابطه کنند. حفظ ارتباطات و مشارکت مداوم با همه شرکت کنندگان ضروری است.

۶. اجتماع را مستند کنید:

مطمئن شوید که شخصی برای مستندسازی اجتماع و وقایع مربوط به آن با گرفتن عکس و فیلم تعیین شده است، و البته در صورتی که انجام این کار امن تلقی شود. این اسناد به عنوان مدرکی بر ماهیت اجتماع شما عمل می کند و می تواند در مقابله با هر گونه روایت یا ادعای نادرستی که ممکن است متعاقباً ظاهر شود، مفید باشد. به‌علاوه، ارزیابی موثر اجتماع، مشخص کردن هر گونه چالشی که با آن مواجه می‌شوید، و برجسته کردن زمینه‌هایی برای بهبود در رویدادهای آینده بسیار مهم است. از به اشتراک گذاری تصاویر و فیلم ها با افراد مختلف خودداری کنید. اگر می خواهید آنها را در رسانه های اجتماعی پست کنید، از یک حساب ناشناس، VPN یا TOR برای حفظ حریم خصوصی و مخدوش کردن چهره همه شرکت کنندگان استفاده کنید.

منابع

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

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