Comment envoyer un communiqué anonyme sans se faire prendre

Comment envoyer un communiqué anonyme sans se faire prendre

Texte d'origine en anglais
How to submit an anonymous communiqué and get away with it
Anonymous contribution to the No Trace Project
2024

Traduction et mise en page
No Trace Project
notrace.how/resources/fr/#comment-envoyer

Un communiqué de revendication est un message à propos d'actions directes (généralement) illégales, partagé via des sites web de contre-information ou des publications imprimées. Les médias *mainstream* peuvent censurer certaines tactiques ou les raisons derrière le choix d'une cible peuvent ne pas être claires : envoyer un communiqué est un moyen de directement partager des informations, tactiques, et motivations politiques.

Ce guide explique comment envoyer un communiqué anonyme en ligne en toute sécurité. Il est destiné aux anarchistes, mais pourrait aussi bénéficier d'autres publics comme les journalistes ou les groupes dissidents qui partagent des informations tout en gardant leurs identités secrètes. Bien que certains communiqués soient signés par les groupes ou individus qui les publient, ce guide se concentre sur les communiqués anonymes.

Rien de ce qu'on fait sur les ordinateurs ou Internet n'est jamais entièrement sécurisé, mais on peut réduire la plupart des risques liés à la technologie en appliquant quelques principes simples. Il existe de nombreuses méthodes au-delà de celles que nous partageons ici, mais on espère que les instructions qui suivent vous seront utiles.

Sommaire

Termes clés

Communiqué : Un message à propos d'actions directes (généralement) illégales, partagé via des sites web de contre-information ou des publications imprimées.

Modèle de menace : Une analyse des risques qui peuvent compromettre notre sécurité, de la probabilité que ces risques surviennent, et de comment les atténuer.

Tor : Abbréviation de « The Onion Router. » Tor est un puissant système d'anonymisation qui fait passer vos connexions Internet par une série de serveurs (appelés « noeuds ») contrôlés par des bénévoles et répartis sur toute la planète. Vous pouvez en apprendre plus et télécharger le navigateur Tor sur torproject.org/fr.

Navigateur : Le logiciel qui vous permet d'accéder à Internet. En dehors du navigateur Tor, il y a aussi par exemple Firefox, Edge, Brave et Chrome.

Système d'exploitation : Ensemble de logiciels qui disent au matériel d'un ordinateur comment fonctionner. Il y a par exemple Windows, Mac, Linux, et Tails.

Tails : Un système d'exploitation qui fonctionne depuis une clé USB et laisse très peu de traces numériques sur votre ordinateur. Tails anonymise votre navigation web de manière très efficace, en la faisant entièrement passer par Tor. Vous pouvez en apprendre plus et installer Tails sur tails.net/index.fr.html.

Stylométrie : Une technique de la police scientifique qui analyse le vocabulaire et le style d'un texte pour identifier ses auteurs et deviner leurs caractéristiques : dialecte, niveau d'éducation, vocabulaire/formulations/fautes d'orthographe.

Métadonnées : Données à propos de données. En ce qui concerne les fichiers numériques, ce sont des données contenues dans un fichier photo ou vidéo comme le modèle d'appareil photo ou la date et l'heure où la photo a été prise. Le terme peut aussi désigner des données en lien avec vos schémas typiques d'utilisation d'Internet, ou la date et heure à laquelle un compte a été créé.

Email jetable : Un compte email anonyme temporaire ou à usage unique, typiquement sans identifiants de connexion.

Chiffrement : Une méthode pour rendre inintelligible le contenu d'un message pour qu'il ne soit lisible que par son destinataire.

Le guide

1. Obtenir une clé Tails et choisir quel ordinateur utiliser

Créez ou empruntez une clé Tails, c'est-à-dire une clé qui contient les fichiers nécessaires au fonctionnement du système d'exploitation amnésique Tails. Vous pouvez l'installer depuis tails.net/index.fr.html ou demander à un·e ami·e qui s'y connait en informatique de vous aider. Pour créer votre clé Tails, utilisez le navigateur Tor et laissez un peu de temps entre la création de la clé et l'envoi du communiqué, pour que les deux évènements ne puissent pas être facilement corrélés. Il est recommandé de créer sa propre clé Tails plutôt que d'en emprunter une pour dissimuler vos habitudes et pratiques numériques et pour que ce soit plus difficile de compromettre la sécurité de plusieurs personnes en infectant une seule clé.

La recommandation générale pour la plupart des gens est d'utiliser un ordinateur personnel que vous utilisez uniquement avec Tails, sur un Wi-Fi public. Les risques liés à l'utilisation de Tails sur un ordinateur personnel que vous utilisez aussi pour d'autres choses sont assez faibles, mais pas inexistants. Évitez de vous asseoir là où votre écran ou clavier seraient visibles par des caméras de surveillance. (Si vous êtes rapides, ça peut être pratique de vous mettre dans des toilettes publiques avec un seul cabinet ou des cabinets qui ferment bien.)

Selon votre modèle de menace, d'autres choix en terme d'ordinateur et de réseau peuvent être plus adaptés à vos besoins. Utiliser un Wi-Fi public ou un ordinateur public (par exemple dans une bibliothèque ou un cybercafé) peut révéler des informations sur vos mouvements, surtout si vous êtes déjà sous filature. Les ordinateurs publics eux-même peuvent être compromis au niveau matériel ou via une collaboration volontaire de leurs propriétaires/gestionnaires avec la police, et ça peut être quasiment impossible à

détecter. Utiliser un ordinateur chez vous, sur votre Wi-Fi personnel, peut vous rendre plus vulnérables à des menaces comme des caméras cachées ou des attaques par corrélation sophistiquées sur le réseau Tor. Et, bien sûr, si vous stockez votre ordinateur dans un endroit pas sécurisé, il pourrait être compromis par une modification matérielle (comme un enregistreur de frappe, ou *keylogger*) ou un logiciel malveillant (ce risque-là est plus faible quand on utilise Tails). Pour plus d'infos sur comment établir le modèle de menace propre à votre situation et vous renseigner sur comment ces attaques ont été utilisées contre d'autres militants, visitez le No Trace Project (notrace.how/fr) ou AnarSec (anarsec.guide, en anglais).

2. Démarrer Tails

Insérez la clé Tails dans l'ordinateur lorsqu'il est éteint. Allumez l'ordinateur et appuyez sur des touches particulières pour accéder au menu de boot. Référez-vous au tableau ci-après (copié depuis tails.net, où on peut aussi trouver des instructions plus détaillées) pour savoir quelles touches sont nécessaires pour votre ordinateur. Si vous devez cherchez l'info sur Internet, utilisez le navigateur Tor et laissez pas mal de temps entre cette recherche et l'envoi du communiqué.

Manufacturer	Key
Acer	F12, F9, F2, Esc
Apple	Option
Asus	Esc
Clevo	F7
Dell	F12
Fujitsu	F12, Esc
HP	F9
Huawei	F12
Intel	F10
Lenovo	F12, Novo
MSI	F11
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12
Others...	F12, Esc

Au démarrage, vous allez sans doute voir des messages comme « Press [key] to access boot menu » (« Appuyez sur [une touche] pour accéder au menu de boot ») ou « Press [key] to access BIOS options » (« Appuyez sur [une touche] pour accéder aux options du BIOS »). Certains ordinateurs vont vous dire « Press [key] to interrupt normal startup » (« Appuyez sur [une touche] pour interrompre le démarrage normal »), ce qui vous amène au menu de boot. Ensuite, sélectionnez votre clé USB dans la liste et votre ordinateur va démarrer sur Tails.

Dans l'écran de bienvenue de Tails, quand on vous propose de déverrouiller le Stockage persistant (si vous l'avez créé), ne le faites pas. N'importe quoi de sauvegardé dans le Stockage persistant serait impossible à réellement supprimer, à moins de reformatter et détruire la clé Tails. Si vous devez conserver des données entre plusieurs sessions Tails, utilisez une deuxième clé USB chiffrée que vous pouvez détruire après coup. Pour savoir comment créer une clé USB chiffrée depuis Tails, lisez « Tails for Anarchists » (« Tails pour les anarchistes ») sur anarsec.guide[1].

Tails vient avec de nombreux logiciels utiles pré-installés, dont le navigateur Tor (pour naviguer sur Internet), Nettoyeur de métadonnées (pour supprimer les métadonnées des fichiers, dont des photos et vidéos), GIMP (pour faire de la retouche photo), LibreOffice (des versions open source de Microsoft Word/PowerPoint/Excel), et plus encore.

3. Démarrer le navigateur Tor et choisir des sites où envoyer le communiqué

Connectez-vous à Internet et utilisez le navigateur Tor pour sélectionner des sites web de contre-information que votre communiqué pourrait intéresser. Vous trouverez ci-après quelques sites pertinents, classés par zone géographique.

Amérique du Nord :

- unravel.noblogs.org
- scenes.noblogs.org

[1] *Note du No Trace Project (NdNTP) :* En français, le TuTORiel Tails[2] explique également comment créer une clé USB chiffrée depuis Tails.

[2] https://notrace.how/resources/fr/#tutoriel-tails

- animalliberationpressoffice.com
- unsalted.noblogs.org (Michigan/Midwest US)
- phlanticap.noblogs.org (Philadelphie)
- tailsrosecitycounterinfo.noblogs.org (Portland)
- indybay.org (Californie)
- mtlcontreinfo.org (Montréal)

Europe :

- Allemagne :
  - de.indymedia.org
  - chronik.blackblogs.org
- Italie :
  - ilrovescio.info
  - lanemesi.noblogs.org
- France :
  - attaque.noblogs.org
  - sansnom.noblogs.org
  - lille.indymedia.org

Amérique centrale et Amérique du Sud :

- informativoanarquista.noblogs.org

International :

- unoffensiveanimal.is
- actforfree.noblogs.org
- anarquia.info
- abolitionmedia.noblogs.org

Ces sites ont généralement une page « contact » ou « contributions » qui explique comment envoyer les informations que vous voulez publier. Ça peut être une adresse email ou un formulaire intégré au site. Certains offrent les deux options (voir les étapes 5–7).

4. Écrire votre communiqué

(Si votre action a déjà été couverte par les médias *mainstream*, réfléchissez à si publier un communiqué vaut le coup. Demandez-vous : Est-ce qu'il apporte des informations pertinentes particulières qui vont encourager d'autres personnes à agir ? Est-ce que les personnes que vous voulez toucher vont voir la couverture médiatique existante ? Est-ce que la cible de l'action comprend les raisons derrière l'action, si jamais c'est important qu'elle les comprenne ? Parfois ça peut être mieux d'envoyer un article d'un média *mainstream* aux sites de contre-information, plutôt que d'écrire un communiqué original.)

Si vous décidez que rédiger une contribution vaut le coup, tapez votre communiqué dans un éditeur de texte comme LibreOffice Writer ou l'Éditeur de texte, PAS dans le navigateur. Le rythme auquel vous tapez au clavier est très unique, particulièrement pour des textes longs, et par défaut peut être analysé sur de nombreux sites web. N'enregistrez pas le document.

Incluez uniquement des informations que la police a déjà. N'ajoutez pas des détails du genre combien vous étiez, votre histoire ou vos identités, où vous avez obtenu le matériel, vos itinéraires d'arrivée ou de fuite, ou encore un discours politique long et stylistiquement unique. Tout ça pourrait sans le vouloir faciliter une enquête contre vous.

Pour éviter qu'une analyse par stylométrie puisse vous identifier ou regrouper ensemble plusieurs de vos contributions, faites court—moins de 300 mots si possible. Si vous écrivez avec un·e ami·e, travaillez le texte ensemble pour dissimuler vos styles respectifs. LibreOffice Writer peut identifier les fautes d'orthographe et les erreurs de ponctuation. Des formulations inhabituelles ou particulières peuvent aider des enquêteurs à relier un communiqué à d'autres écrits. Tout écrire en minuscules ou en majuscules peut dissimuler certains styles, mais peut être en soit un style remarquable. Certaines personnes recommandent de faire passer le texte dans Google Translate ou des logiciels similaires pour dissimuler certains choix de vocabulaire et de formulation. Ça peut être particulièrement efficace si on traduit entre plusieurs langues qui sont peu utilisées sur Internet ou qu'on utilise plusieurs logiciels de traduction automatique. Une

traduction française du texte « Qui a écrit ça ? »[3] de Zündlumpen #76 aborde ce sujet de manière poussée.

5. Compresser puis supprimer les métadonnées des photos et vidéos

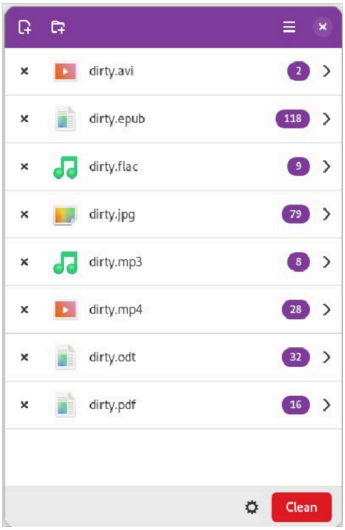
D'abord, réfléchissez sérieusement à si poster des visuels de votre action clandestine, particulièrement des vidéos, vaut le coup. Des visuels peuvent fournir aux enquêteurs plein d'informations qu'iels n'ont peut-être pas encore. Renseignez-vous sur les techniques d'*open-source intelligence* (OSINT) et d'analyse vidéo. Des détails comme les visages, la peau, les tatouages, les cicatrices, la taille, la posture, ou des vêtements ou accessoires uniques peuvent mener à des identifications. Dans le cas des vidéos, des trucs aussi basiques que le grésillement des fils électriques dans vos murs, les bruits de circulation, ou une simple feuille d'arbre peuvent fournir des informations dévastatrices à la police, ou à n'importe quel internaute avec du temps à perdre (oui, vraiment n'importe qui). Et bien sûr, le son de votre voix ou du moteur de votre voiture peut être accablant. Le mieux est d'utiliser un appareil photo ou une caméra jetables (obtenus pour l'occasion, puis jetés) pour éviter que des photos et vidéos d'actions différentes soient reliées via le « bruit » propre au capteur de chaque appareil.

Si vous décidez qu'envoyer des photos ou vidéos vaut le coup, compressez-les pour supprimer des détails superflus en réduisant le nombre de pixels. Des visuels de basse résolution peuvent appuyer votre message sans accidentellement fournir des preuves comme des reflets détaillés ou des traces de pneus. En bonus, cela réduit la taille des fichiers qui sont alors plus faciles à uploader et partager. Pour les images, ouvrez-les dans GIMP puis sélectionnez « Fichier > Exporter sous ». Cliquez sur « Sélectionner le type de fichier » et choisissez « Image JPEG » dans la liste. Utilisez le curseur « Qualité » pour réduire la qualité de l'image, en cliquant sur « Afficher l'aperçu dans la fenêtre d'image » pour vérifier que l'image ne se dégrade pas trop.

[3] https://notrace.how/resources/#wer-schreibt-denn-da

Compresser des vidéos est plus compliqué ; consultez la documentation de Tails sur le son et la vidéo pour des suggestions de logiciels et comment les installer. Il y a des sites web qui compressent des vidéos pour vous, mais l'option la plus sécurisée est toujours quelque chose hors ligne. Si vous uploadez une version haute qualité sur un site, ce site pourrait conserver une copie et/ou fournir des informations à la police. Si vous n'êtes pas sûr·e·s des preuves que votre vidéo peut contenir, ou que vous n'êtes pas sûr·e·s de comment en retirer des informations potentiellement compromettantes, c'est peut-être mieux de simplement ne pas l'inclure dans votre contribution.

Une fois vos fichiers compressés, la dernière étape est de supprimer les métadonnées, ces informations numériques qui ne sont pas visibles dans le visuel mais sont visibles dans les propriétés du fichier. Démarrez Nettoyeur de métadonnées, cliquez sur « Ajouter des fichiers » en haut à gauche, et sélectionnez vos fichiers. Cliquez sur « Nettoyer » en bas à droite pour retirer les métadonnées et écraser les fichiers d'origine.



6. Accéder au formulaire de contribution du site (si il y en a un)

Comme mentionné à l'étape 3, certains sites de contre-information ont des formulaires intégrés. Souvent c'est un moyen facile et sécurisé d'envoyer un communiqué, surtout si vous envoyez seulement du texte. Chaque site est un peu différent, donc cherchez la page « contact » ou « contributions » des sites auxquels vous voulez envoyer votre communiqué.

Certains sites acceptent les photos et vidéos via leur formulaire en ligne, d'autres proposent d'utiliser des sites de partage de fichiers particuliers. Si les fichiers ne peuvent pas être uploadés directement, une solution est de les uploader sur file.espiv.net pour pouvoir copier-coller l'URL dans le formulaire. Notez que certains sites de contre-information peuvent ne pas accepter les fichiers envoyés de cette manière, car cela implique des risques pour les administrateur·ice·s du site. Vérifiez les règles relatives aux contributions et les sites de partage de fichiers proposés, le cas échéant.

Copiez-collez votre communiqué dans le champ principal du formulaire, entrez de fausses informations non-identifiantes dans les autres champs, uploadez les photos et vidéos nettoyées le cas échéant, et envoyez ! Si tout ça fonctionne, passez directement à l'étape 9.

Si le site auquel vous voulez envoyer le communiqué a seulement une adresse email ou que vous avez des difficultés techniques dans l'utilisation de leur formulaire de contribution (par exemple si le communiqué n'est pas reçu, ce que vous pourriez ne remarquer que plusieurs jours plus tard en constatant que celui-ci n'a pas été posté), ça peut être mieux d'envoyer votre communiqué par email, comme détaillé dans les étapes 7–8.

7. Créer un compte Protonmail, ou autre compte email jetable

Si vous n'utilisez pas de formulaire de contribution, vous pouvez envoyer un email depuis un compte créé pour l'occasion. Une option est Protonmail (proton.me)—de nombreux sites de contre-information utilisent aussi Protonmail, ce qui rend votre email chiffré de bout-en-bout par défaut. Notez que ce chiffrement n'est pas aussi sûr que d'utiliser PGP avec un fournisseur d'emails de confiance et que Protonmail en tant qu'entreprise n'est pas notre alliée (ils ont déjà collaboré avec les flics et menti à propos de cette collaboration). Ceci dit, le contenu de votre message a pour but d'être posté publiquement. L'intention n'est pas ici de garder le contenu de votre message totalement secret, mais de minimiser les métadonnées ou informations identifiantes que vous pourriez accidentellement envoyer avec le message. N'envoyez JAMAIS d'informations identifiantes en même temps qu'un communiqué.

Pour le nom d'utilisateur, choisissez 2–3 mots aléatoires. Le site web randomwordgenerator.com peut aider pour l'aléatoire. Utilisez d'autres mots aléatoires pour le mot de passe (idéalement plus de 6 pour un mot de passe sécurisé). Ne conservez ces identifiants nulle part.

Comme vous utilisez Tor, Protonmail va vous demander une méthode de vérification secondaire. Entrez une adresse email jetable créée sur guerrillamail.com, yopmail.com, tempr.email, ou un autre site d'emails jetables pour pouvoir recevoir le code de confirmation.

Si vous ne voulez pas utiliser Protonmail, vous pouvez essayer d'envoyer votre communiqué directement depuis un site d'emails jetables. Cependant, la plupart de ces sites permettent seulement de recevoir des emails et ceux qui permettent d'en envoyer (tempr.email) sont parfois moins fiables, notamment avec les pièces jointes.

Envisagez d'essayer plusieurs méthodes, ou variez les méthodes d'un communiqué à l'autre, afin d'éviter de créer des métadonnées relatives à vos habitudes de contribution.

8. Créer et envoyer l'email

Copiez-collez votre communiqué dans le contenu de l'email. Si vous envoyez votre email entre deux comptes Protonmail (ou autre service qui propose un chiffrement de bout-en-bout entre les comptes du service), le contenu de votre email va être chiffré. Le sujet, en revanche, n'est jamais chiffré—pour votre sécurité et celle du destinataire, mettez quelque chose de vague comme sujet ou laissez le sujet vide.

Les photos peuvent généralement être directement ajoutées en pièce jointe à l'email. Les vidéos ou autres fichiers volumineux peuvent être uploadés sur Proton Drive (même compte que pour l'email) ou file.espiv.net et envoyés sous forme de lien. Notez que certains sites de contre-information peuvent ne pas accepter les fichiers envoyés de cette manière, car cela implique des risques pour les administrateur·ice·s du site. Vérifiez les règles relatives aux contributions et les sites de partage de fichiers proposés, le cas échéant.

Relisez tout une dernière fois pour être sûr·e·s qu'il n'y a pas d'erreurs et que vous avez mis en pièce jointe tout ce que vous vouliez. Et puis envoyez l'email !

9. Terminer, ranger

Fermez les logiciels ouverts, ne conservez aucun identifiant, et n'utilisez pas le compte email (si vous en avez créé un) pour autre chose. Éteignez l'ordinateur et retirez votre clé Tails. Celle-ci peut être réutilisée de manière sûre, sans être reliée à la session précédente, sur le même ordinateur ou un autre.

Le cas échéant, supprimez les photos et vidéos puis détruisez et jetez tout appareil photo, caméra, ou carte SD utilisés pour l'action. Le mieux est de briser les appareils en petits morceaux (la NSA[4] recommande des bouts de moins de 2 mm), ce qui est faisable avec un mixeur puissant. C'est aussi

[4] *NdNTP :* National Security Agency, une agence de renseignements des États-Unis.

possible d'utiliser un marteau, un chalumeau, ou un acide puissant. Évitez d'inhaler les fumées produites par la combustion, la fonte, ou autres réactions chimiques de métaux ou plastiques.

Envisagez de vous débarrasser de cette brochure si vous utilisez une version imprimée, en la détruisant ou en l'offrant à un·e ami·e de confiance. Elle ne prouve pas que vous avez commis des crimes, mais ferait un peu tâche devant un tribunal, comme preuve corroborante.

Conclusion

Ça y est ! Ça peut paraître beaucoup d'étapes au début, mais ce n'est pas si dur et c'est de plus en plus facile chaque fois que vous le faites.

Restez *safe*, soyez dangereux, ne vous faites pas prendre.

Sites web pertinents :

- tails.net/index.fr.html
- torproject.org/fr
- notrace.how/fr
- anarsec.guide
- file.espiv.net
- randomwordgenerator.com
- proton.me
- guerrillamail.com
- yopmail.com
- tempr.email

Un communiqué de revendication est un message à propos d'actions directes (généralement) illégales, partagé via des sites web de contre-information ou des publications imprimées. Les médias *mainstream* peuvent censurer certaines tactiques ou les raisons derrière le choix d'une cible peuvent ne pas être claires : envoyer un communiqué est un moyen de directement partager des informations, tactiques, et motivations politiques. Ce guide explique comment envoyer un communiqué anonyme en ligne en toute sécurité.

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable—faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.