

COMMENT SOUMETTRE DES COMMUNIQUÉS À MTLCOUNTER-INFO.ORG DE MANIÈRE SÉCURITAIRE

Nous avons pensé qu'il serait utile de résumer une technique de base pour soumettre des communiqués de manière anonyme, en utilisant le système d'exploitation Tails.

Tails est un système d'exploitation pour ordinateur conçu avec un soucis de sécurité et qui peut être démarré à partir d'une clé USB ou d'un CD sur n'importe quel ordinateur. Après avoir éteint Tails et éjecté la clé USB ou le CD, l'ordinateur peut redémarrer normalement avec son système d'exploitation habituel. Tails est conçu pour ne laisser aucune trace sur l'ordinateur en n'interagissant aucunement avec le disque dur et en utilisant seulement la mémoire vive (qui est automatiquement effacée quand Tails est éteint). De plus, Tails oblige toutes les connexions internet à passer par le **réseau Tor**ⁱ, ce qui est beaucoup plus sécuritaire que d'utiliser simplement le navigateur Tor sur votre système d'exploitation habituel.

Adresse IP et MAC :

Toute connexion internet a une **adresse IP**ⁱⁱ spécifique qui peut être enregistrée par les sites internet qui sont visités et qui révèle la connexion qui a été utilisée. On peut d'ailleurs retracer le lien entre une adresse IP et un.e abonné.e internet, que ce soit un individu ou un commerce comme un café.

Tous les ordinateurs ont une **adresse MAC**ⁱⁱⁱ, qui peut identifier l'ordinateur spécifique qui s'est connecté à un site internet via l'adresse IP.

Tails dissimule automatiquement l'adresse IP en utilisant le réseau TOR et donne automatiquement à chaque utilisateur une fausse adresse MAC dès le départ.

i. TOR est un réseau de de « proxies » géré par des volontaires dans le but explicite d'assurer l'anonymat en ligne. Avec TOR, votre connexion passe à travers trois proxies. Vous vous connectez à TOR et chacun des trois proxies (« noeuds ») auxquels vous accédez encode vos données. Aucun de ces noeuds, pris individuellement, ne sait à la fois qui vous êtes et ce à quoi vous êtes connecté.es. Le troisième noeud décrypte les données et accède au site internet, renvoyant l'information encodée à travers les autres proxies.

ii. Une adresse IP (Internet Protocol address) est une série de chiffres qui vous permet d'envoyer et de récupérer des données à travers une connexion internet (par exemple. 78.125.1.209). Ces chiffres servent à identifier la location physique, le fournisseur de service internet et les détails techniques de votre connexion. C'est comparable à l'adresse d'une maison. Une adresse IP non dissimulée mènera directement des enquêteurs/enquêteuses à votre connexion.

iii. L'adresse MAC (Media Access Controller address) identifie spécifiquement votre ordinateur. Si vous vous connectez à internet, le routeur peut se connecter à votre adresse MAC et conserver ces données. Si des enquêteurs/enquêteuses s'attardaient à lire les données d'un routeur avec lequel vous avez accédé à internet (disons un wifi public depuis lequel un communiqué a été envoyé), puis compareraient cette adresse avec celle de la carte internet sans-fil de votre ordinateur (disons, confisquée durant une descente), vous seriez connectez

aux activités que vous avez effectués en utilisant la connexion de ce routeur. Si l'adresse MAC n'est pas modifiée, il y a une possibilité que vos activités puissent être reliées à vous si les enquêteurs/enquêteuses sont déterminé.es ou suffisamment chanceux.ses.



COMMENT SOUMETTRE DES COMMUNIQUÉS À MTLCOUNTER-INFO.ORG DE MANIÈRE SÉCURITAIRE

Nous avons pensé qu'il serait utile de résumer une technique de base pour soumettre des communiqués de manière anonyme, en utilisant le système d'exploitation Tails.

Tails est un système d'exploitation pour ordinateur conçu avec un soucis de sécurité et qui peut être démarré à partir d'une clé USB ou d'un CD sur n'importe quel ordinateur. Après avoir éteint Tails et éjecté la clé USB ou le CD, l'ordinateur peut redémarrer normalement avec son système d'exploitation habituel. Tails est conçu pour ne laisser aucune trace sur l'ordinateur en n'interagissant aucunement avec le disque dur et en utilisant seulement la mémoire vive (qui est automatiquement effacée quand Tails est éteint). De plus, Tails oblige toutes les connexions internet à passer par le **réseau Tor**ⁱ, ce qui est beaucoup plus sécuritaire que d'utiliser simplement le navigateur Tor sur votre système d'exploitation habituel.

Adresse IP et MAC :

Toute connexion internet a une **adresse IP**ⁱⁱ spécifique qui peut être enregistrée par les sites internet qui sont visités et qui révèle la connexion qui a été utilisée. On peut d'ailleurs retracer le lien entre une adresse IP et un.e abonné.e internet, que ce soit un individu ou un commerce comme un café.

Tous les ordinateurs ont une **adresse MAC**ⁱⁱⁱ, qui peut identifier l'ordinateur spécifique qui s'est connecté à un site internet via l'adresse IP.

Tails dissimule automatiquement l'adresse IP en utilisant le réseau TOR et donne automatiquement à chaque utilisateur une fausse adresse MAC dès le départ.

i. TOR est un réseau de de « proxies » géré par des volontaires dans le but explicite d'assurer l'anonymat en ligne. Avec TOR, votre connexion passe à travers trois proxies. Vous vous connectez à TOR et chacun des trois proxies (« noeuds ») auxquels vous accédez encode vos données. Aucun de ces noeuds, pris individuellement, ne sait à la fois qui vous êtes et ce à quoi vous êtes connecté.es. Le troisième noeud décrypte les données et accède au site internet, renvoyant l'information encodée à travers les autres proxies.

ii. Une adresse IP (Internet Protocol address) est une série de chiffres qui vous permet d'envoyer et de récupérer des données à travers une connexion internet (par exemple. 78.125.1.209). Ces chiffres servent à identifier la location physique, le fournisseur de service internet et les détails techniques de votre connexion. C'est comparable à l'adresse d'une maison. Une adresse IP non dissimulée mènera directement des enquêteurs/enquêteuses à votre connexion.

iii. L'adresse MAC (Media Access Controller address) identifie spécifiquement votre ordinateur. Si vous vous connectez à internet, le routeur peut se connecter à votre adresse MAC et conserver ces données. Si des enquêteurs/enquêteuses s'attardaient à lire les données d'un routeur avec lequel vous avez accédé à internet (disons un wifi public depuis lequel un communiqué a été envoyé), puis compareraient cette adresse avec celle de la carte internet sans-fil de votre ordinateur (disons, confisquée durant une descente), vous seriez connectez

aux activités que vous avez effectués en utilisant la connexion de ce routeur. Si l'adresse MAC n'est pas modifiée, il y a une possibilité que vos activités puissent être reliées à vous si les enquêteurs/enquêteuses sont déterminé.es ou suffisamment chanceux.ses.





1 Télécharger et installer Tails

Tails peut être téléchargé sur tails.boum.org. Vous pouvez aller jeter un coup d'oeil à « l'assistant d'installation Tails » sur le site pour des instructions sur comment télécharger et vérifier le fichier, l'installer sur une clé USB ou un CD et le faire démarrer sur votre ordinateur.

2 Démarrer Tails

Dépendamment d'à quel point vos activités sont risquées, il pourrait être une bonne idée d'utiliser un ordinateur qui n'est pas connecté à votre identité d'aucune manière (au cas où Tails, pour une raison ou une autre, laissait une trace). Ce peut être un ordinateur public hors de la vue des caméras de surveillance, ou un ordinateur utilisé spécifiquement dans ce but.

Si vous démarrez l'ordinateur avec la clé USB branchée et que Tails ne démarre pas automatiquement, il se pourrait que vous ayez besoin d'accéder au « menu de démarrage » de votre ordinateur. Sur la plupart des ordinateurs, vous pouvez appuyer sur une touche du menu pour faire apparaître une liste des différents systèmes sur lesquels il est possible de démarrer (identifier les touches possibles du menu de démarrage pour votre ordinateur selon le fabricant dans la liste ci-bas). Dans ce menu, choisissez votre clé USB. Pour la résolution de problème, référez-vous à « Démarrer Tails » sur tails.boum.org. Vous pourriez avoir besoin de modifier les paramètres du BIOS.

3 Se connecter à internet

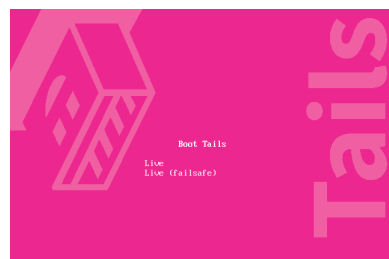
Si vous utilisez un ordinateur portable, vous pouvez accéder à plusieurs réseaux wifi, dont vous connaissez les mots de passe, depuis l'extérieur du bâtiment, et ce même la nuit si le wifi est laissé ouvert. Utilisez un wifi qui n'a pas de « portail captif » (un « portail captif » est un portail qui vous fait accepter des « termes et conditions »).

4 Soumettre un Communiqué

Ouvrez le navigateur TOR et vérifiez que Tor est fonctionnel en visitant check.torproject.org. Allez sur <https://mtlcounter-info.org/add-content/> pour nous envoyer votre communiqué! Si vous souhaitez soumettre des images, vidéos, etc., éliminez les informations d'identification (métadonnées) à l'aide de Metadata Anonymization Toolkit (MAT) sur Tails.



Manufacturer	Key
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12,
Novo,	F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12



Pour approfondir :

- Autoprotection Digitale Contre la Surveillance: Astuces, Outils et Guides Pratiques pour des Communications En Ligne Plus Sécurisées
- Le Zine « Anonymity/Security »
- Le « Surveillance and Counter-surveillance Guide »



1 Télécharger et installer Tails

Tails peut être téléchargé sur tails.boum.org. Vous pouvez aller jeter un coup d'oeil à « l'assistant d'installation Tails » sur le site pour des instructions sur comment télécharger et vérifier le fichier, l'installer sur une clé USB ou un CD et le faire démarrer sur votre ordinateur.

2 Démarrer Tails

Dépendamment d'à quel point vos activités sont risquées, il pourrait être une bonne idée d'utiliser un ordinateur qui n'est pas connecté à votre identité d'aucune manière (au cas où Tails, pour une raison ou une autre, laissait une trace). Ce peut être un ordinateur public hors de la vue des caméras de surveillance, ou un ordinateur utilisé spécifiquement dans ce but.

Si vous démarrez l'ordinateur avec la clé USB branchée et que Tails ne démarre pas automatiquement, il se pourrait que vous ayez besoin d'accéder au « menu de démarrage » de votre ordinateur. Sur la plupart des ordinateurs, vous pouvez appuyer sur une touche du menu pour faire apparaître une liste des différents systèmes sur lesquels il est possible de démarrer (identifier les touches possibles du menu de démarrage pour votre ordinateur selon le fabricant dans la liste ci-bas). Dans ce menu, choisissez votre clé USB. Pour la résolution de problème, référez-vous à « Démarrer Tails » sur tails.boum.org. Vous pourriez avoir besoin de modifier les paramètres du BIOS.

3 Se connecter à internet

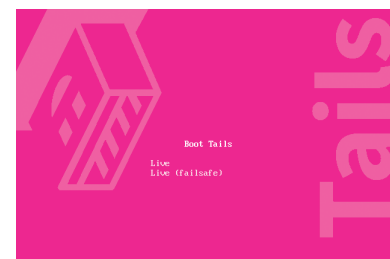
Si vous utilisez un ordinateur portable, vous pouvez accéder à plusieurs réseaux wifi, dont vous connaissez les mots de passe, depuis l'extérieur du bâtiment, et ce même la nuit si le wifi est laissé ouvert. Utilisez un wifi qui n'a pas de « portail captif » (un « portail captif » est un portail qui vous fait accepter des « termes et conditions »).

4 Soumettre un Communiqué

Ouvrez le navigateur TOR et vérifiez que Tor est fonctionnel en visitant check.torproject.org. Allez sur <https://mtlcounter-info.org/add-content/> pour nous envoyer votre communiqué! Si vous souhaitez soumettre des images, vidéos, etc., éliminez les informations d'identification (métadonnées) à l'aide de Metadata Anonymization Toolkit (MAT) sur Tails.



Manufacturer	Key
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12,
Novo,	F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12



Pour approfondir :

- Autoprotection Digitale Contre la Surveillance: Astuces, Outils et Guides Pratiques pour des Communications En Ligne Plus Sécurisées
- Le Zine « Anonymity/Security »
- Le « Surveillance and Counter-surveillance Guide »