COMMENT SOUMETTRE DES COMMUNIQUÉS À MTLCONTREINFO.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 conçu avec un souci de sécurité et qui peut être démarré à partir d'une clé USB ou d'un DVD sur n'importe quel ordinateur. Après avoir éteint Tails et éjecté la clé USB ou le DVD, 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 « proxies » géré par des bénévoles 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 nœuds, pris individuellement, ne sait à la fois qui vous êtes et ce à quoi vous êtes connecté.es. Le troisième nœud décrypte les données et accède au site internet, renvoyant l'information encodée à travers les autres proxies.*

ii. *Une adresse IP (Internet Protocal 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 connexion d'un routeur avec lequel vous avez accédé à internet (disons un wifi public depuis lequel un communiqué a été envoyé), puis comparaient cette adresse avec celle de la carte internet sans-fil de votre ordinateur (disons, confisquée durant une descente), vous seriez connecté.es aux activités que vous avez effectuées 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 MTLCONTREINFO.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 conçu avec un souci de sécurité et qui peut être démarré à partir d'une clé USB ou d'un DVD sur n'importe quel ordinateur. Après avoir éteint Tails et éjecté la clé USB ou le DVD, 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.

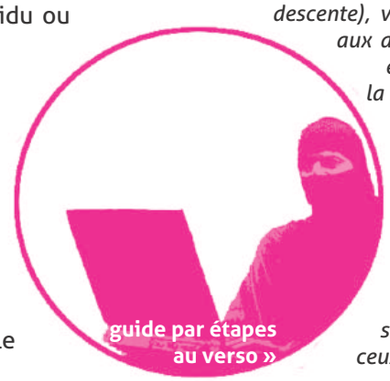
Tous les ordinateurs ont une ***adresse MAC*** [iii], qui peut identifier l'ordinateur spécifique qui s'est connecté à un site internet via l'adresse IP.

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 « proxies » géré par des bénévoles 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 nœuds, pris individuellement, ne sait à la fois qui vous êtes et ce à quoi vous êtes connecté.es. Le troisième nœud décrypte les données et accède au site internet, renvoyant l'information encodée à travers les autres proxies.*

ii. *Une adresse IP (Internet Protocal 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 connexions d'un routeur avec lequel vous avez accédé à internet (disons un wifi public depuis lequel un communiqué a été envoyé), puis comparaient cette adresse avec celle de la carte internet sans-fil de votre ordinateur (disons, confisquée durant une descente), vous seriez connecté.es aux activités que vous avez effectuées 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 *https://tails.boum.org*. Vous pouvez suivre le guide d'installation sur le site pour savoir comment télécharger et vérifier le fichier, l'installer sur une clé USB ou un DVD 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 à gauche). 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.

Fabricant	Touche
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12, F8, F10
Samsung	Esc, F12, F2
Sony	F11, F10
Toshiba	F12

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. Si le wifi a un « portail captif » (comme dans la plupart des chaînes de cafés), vous devrez utiliser le *Unsafe Browser* pour accepter les « termes et conditions » du portail et vous connecter. Un wifi sans portail est préférable.

4 Soumettre un Communiqué

Ouvrez le navigateur TOR et vérifier que Tor est fonctionnel en visitant *https://check.torproject.org*. Allez sur *https://mtlcontreinfo.org/publiez* pour nous envoyer votre communiqué! Si vous souhaitez inclure des images, vidéos, etc., éliminez les informations d'identification (métadonnées) à l'aide de Metadata Anonymization Toolkit (MAT) sur Tails.

Pour approfondir :

- Autoprotection contre la surveillance: astuces, outils et guides pratiques pour des ccommunications en ligne plus sécurisées
- Le zine « Anonymity/Security »
- Le « Surveillance and Counter-surveillance Guide »

1 Télécharger et installer Tails

Tails peut être téléchargé sur *https://tails.boum.org*. Vous pouvez suivre le guide d'installation sur le site pour savoir comment télécharger et vérifier le fichier, l'installer sur une clé USB ou un DVD 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 à gauche). 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.

Fabricant	Touche
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12, F8, F10
Samsung	Esc, F12, F2
Sony	F11, F10
Toshiba	F12

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. Si le wifi a un « portail captif » (comme dans la plupart des chaînes de cafés), vous devrez utiliser le *Unsafe Browser* pour accepter les « termes et conditions » du portail et vous connecter. Un wifi sans portail est préférable.

4 Soumettre un Communiqué

Ouvrez le navigateur TOR et vérifier que Tor est fonctionnel en visitant *https://check.torproject.org*. Allez sur *https://mtlcontreinfo.org/publiez* pour nous envoyer votre communiqué! Si vous souhaitez inclure des images, vidéos, etc., éliminez les informations d'identification (métadonnées) à l'aide de Metadata Anonymization Toolkit (MAT) sur Tails.

Pour approfondir :

- Autoprotection 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 »