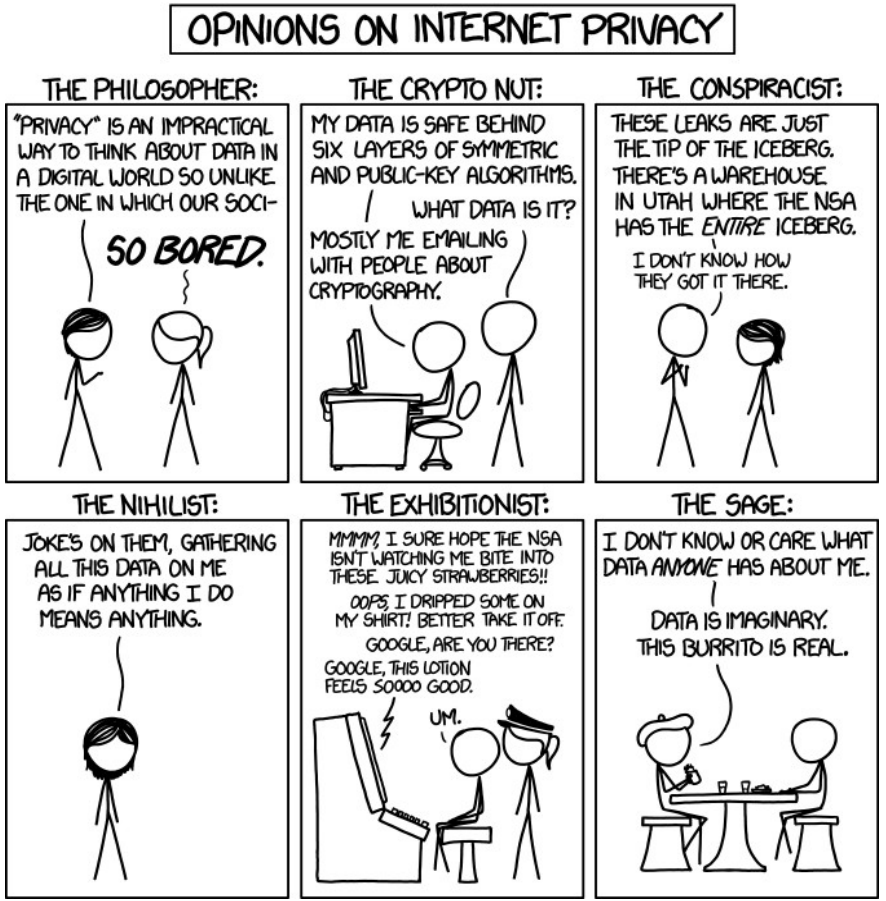
Cybersécurité dans un contexte militant



Source : xkcd

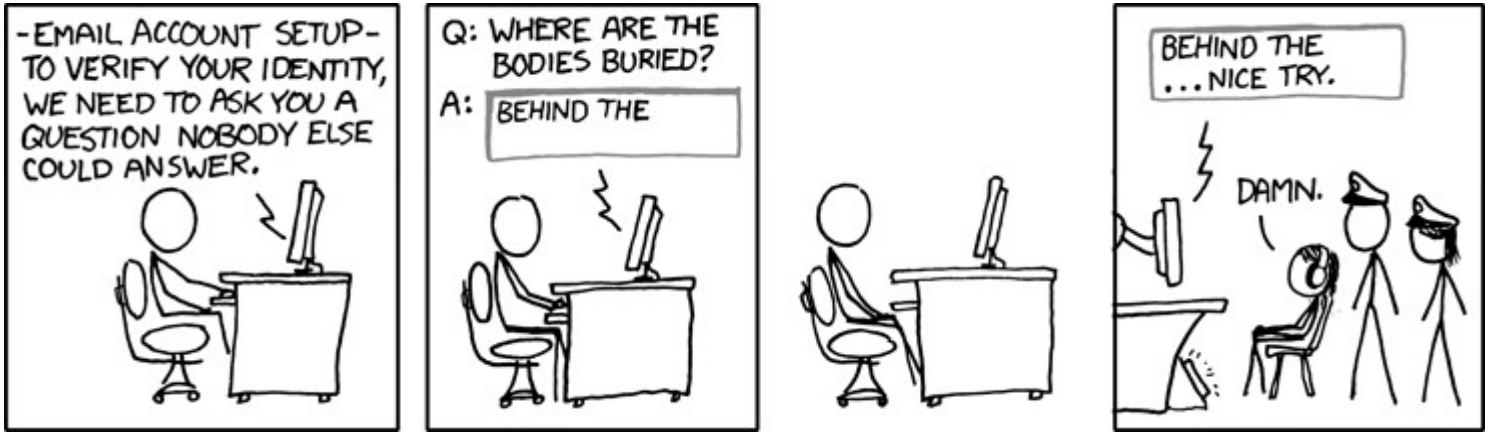
Par Louise
Retouché par Paul

Avertissement

- On n’est pas des expert-e-s en sécurité, ni des avocat-e-s.
- Contenu basé sur notre expérience dans la militance et en informatique.
- Basé sur le document « Surveillance Self-Defense » publié par la EFF : https://ssd.eff.org/

Modèle de risque

- Déterminer un ensemble d’attaques possibles contre lesquelles on souhaite se prémunir. Faire ceci permet d'analyser les risques.
  - Ex.: Je veux transmettre une vidéo à un site Web sans être retracé-e.
  - Ex.: J’habite au Texas et je dois réserver un rendez-vous dans une clinique d’avortement en Arizona sans que ça soit découvert.



Source : xkcd

Modèle de risque

- Cinq questions :
  - **Qu’est-ce que je veux protéger ?**
    - Photos, vidéos, messages …
  - **Contre qui les protéger ?**
    - Contre la police, les fachos, des membres de ma famille …
  - **Quelle est l'ampleur des conséquences si j'échoue ?**
    - L’action de la manif n’aura pas lieu vs. prison
  - **Dans quelle mesure ai-je besoin de les protéger ?**
    - Conversation verbale vs. conversation en ligne
  - **Quelles difficultés suis-je prêt-e à rencontrer pour prévenir ces conséquences ?**
    - Plus de sécurité → plus de travail

Modèle de risque : **Qu’est-ce que je veux protéger**

- Actif : Toute donnée ou tout appareil qui a besoin d'être protégée.
  - Ex. : courriels, listes de contacts, sms, localisation.
- **TODO** : Rédiger une liste des actifs qu'on possède, où ils se trouvent, qui y a accès, et enfin ce qui empêche d'y accéder.
  - Ex.: J’ai parlé de mon avortement par SMS avec mon frère, la vidéo envoyée au site Web est sur mon ordi et dans ma boîte de courriel …
  - La liste devrait être détruite par la suite (c'est un actif aussi !).

Modèle de risque : **Contre qui les protéger**

- Menace : Événement potentiel qui pourrait compromettre vos efforts pour défendre vos données.
  - Menaces intentionnelles : des fachos essaient de vous doxxer.
  - Menaces accidentelles : vous traversez la rue à un feu rouge, la police en profite pour faire une fouille illégale et trouve quelque chose.
- Adversaire : Personne ou organisation qui tente de miner vos objectifs de sécurité.
  - Ex.: Gouvernement, pirate sur un réseau wifi public.
- **TODO**: Rédiger une liste de vos adversaires et de ceux qui pourraient vouloir s'emparer de vos actifs.

Modèle de risque : **Quelle est l'ampleur des conséquences si j'échoue**

- Possibilité d'action : Ce qu'un-e adversaire peut faire pour parvenir ses objectifs.
- Dire qu'un assaillsant a une capacité ne signifie pas nécessairement qu'il l'utilisera. C'est un pensez-y bien.
  - Ex.: La police peut demander à Facebook de leur donner vos messages personnels. Quel impact cela peut avoir ?
  - Ex.: Des fachos peuvent éplucher vos posts sure Twitter. Peuvent-ils découvrir où vous habitez, où vous travaillez ?
- **TODO** : Notez ce que vos adversaires pourrait faire avec vos données personnelles.

Modèle de risque : **Dans quelle mesure ai-je besoin de les protéger**

- Risque = Probabilité * Impact
  - Ex.: La police peut facilement obtenir vos données d'Instagram (probabilité élevée), mais elle n'y trouvera rien parce que vous faites attention à vos publications (impact faible).
  - Ex.: Vous conservez tout ce qui concerne vos pillules hormonales dans une clé encryptée et il est difficile pour un hacker d'y accéder (probabilité faible), ce qui est tant mieux car ces pillules sont illégales où vous habitez (impact élevé).
- **TODO** : Notez les menaces que vous allez prendre au sérieux et celles qui sont trop rares (probabilité faible) ou trop anodines (impact faible).
  - On ne peut pas éliminer tout le risque : il faut accepter un certain niveau de risque.
  - Déterminer ce niveau est quelque chose de personnel et subjectif. Ce n'est pas tout le monde qui ont les mêmes priorités. Parlez à vos camarades.

Modèle de risque : **Quelles difficultés suis-je prêt à rencontrer pour prévenir ces conséquences**

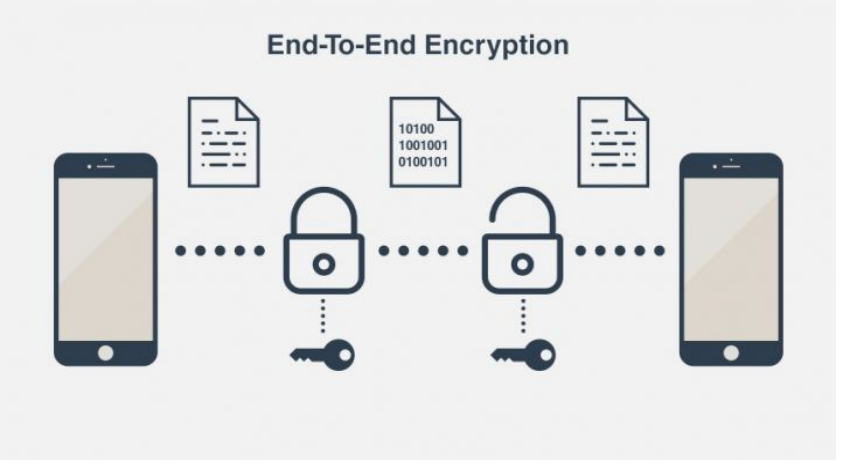
- Trouver un équilibre entre commodité, coût et niveau de risque acceptable.
  - Ex.: Un-e journaliste qui communique avec des militant-e-s devrait utiliser des canaux sécurisés pour éviter que les militant-e-s puissent être retracé-e-s.
  - Ex.: Envoyer des photos de chats à ses ami-e-s peut être non-sécurisé. C'est correct d'avoir une vie publique 😊
- **TODO** : Notez les options qui s'offrent à vous pour vous aider à atténuer vos menaces particulières.
  - Notez aussi si vous avez des contraintes financières, techniques ou sociales.

Modèle de risque : **Conclusion**

- Tous les **TODO**s forment le plan de sécurité.
  - Ce plan doit évoluer selon la situation et ce que vous faites.
    - Ex.: Les attaques contre les personnes LGBTQ+ se multiplient, ça serait bien d'éplucher notre vie en ligne pour éliminer ce qui permet de retracer notre lieu de travail, notre appartement, etc.
    - Ex.: Jusqu'à maintenant, je ne faisais que participer aux manifs, mais maintenant j'en organise.
  - Il est donc important de réviser ce plan fréquemment !

Communiquer avec autrui

- Prioriser les communications en face to face, sans qu'aucune ordinateur et téléphone ne soient impliqués.
- Si l'on communique en ligne, utiliser des moyens de communications avec du chiffrement de bout en bout.
- Traiter les communications numériques comme des conversations publiques.



Communiquer avec autrui (Signal)

- Avantages
  - Facile d'utilisation,
  - Open source et gratuit,
  - End2End Encryption.
- Inconvénients
  - Besoin d'un numéro de téléphone, qui est souvent facile à associer à une personne.
  - Centralisation des serveurs.
- Situation en évolution :
  - Signal est contrôlé en partie par une milliardaire,
  - La firme israélienne Candiru affirme avoir pu briser le logiciel et vend le pouvoir de le faire pour 700k$.
- **Rien n’est mieux que le face-à-face.**

Communiquer avec autrui (courriel Riseup)

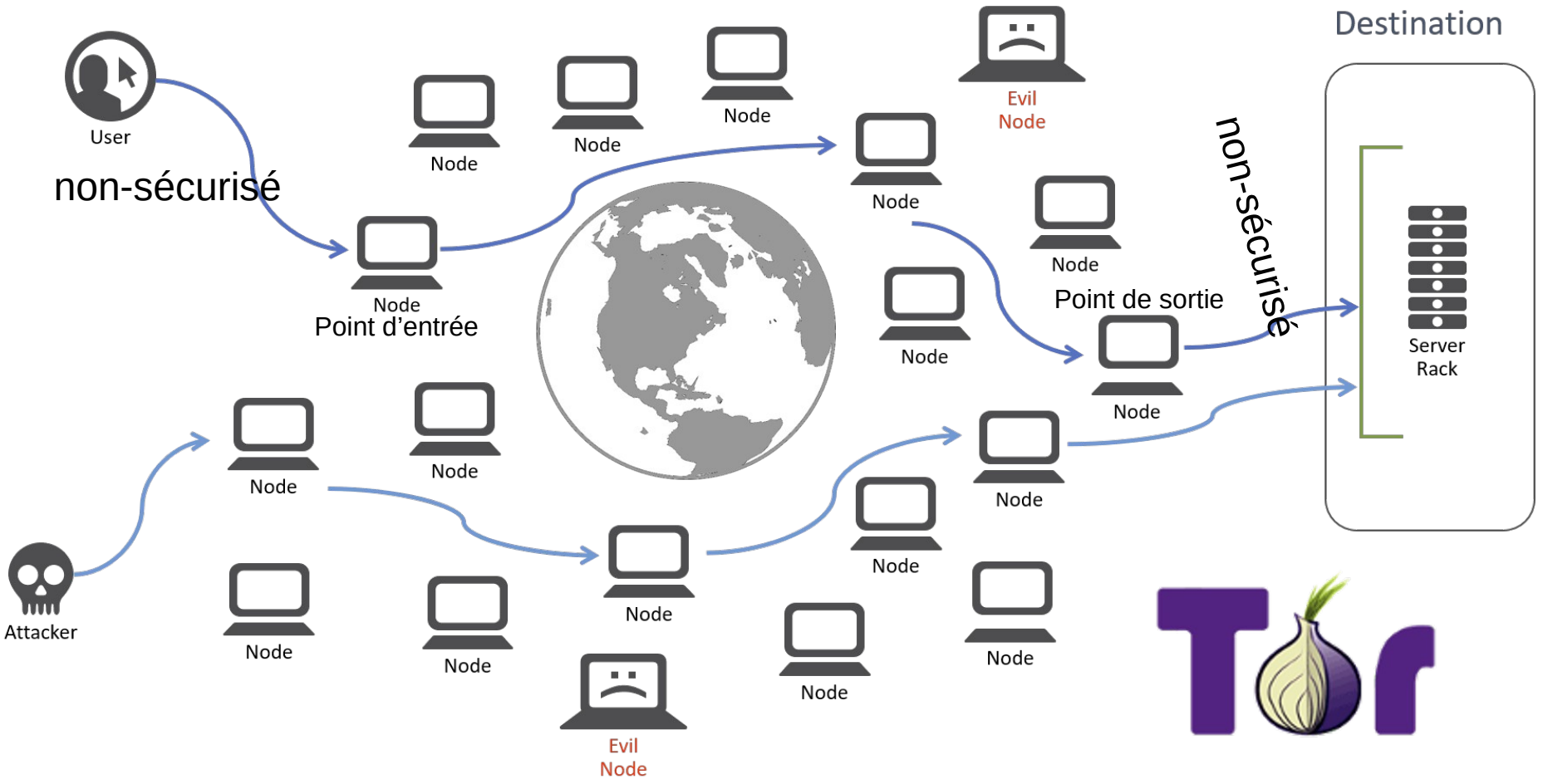
- Avantages :
  - Encryption des serveurs,
  - Fait par des camarades, pour des camarades,
  - Par invitation seulement, ce qui élimine la plupart des fachos.
- Inconvénients :
  - La transmission de messages n'est pas encryptée, il faut utiliser l'encryption PGP (demande plus de compétences techniques),
  - Centralisation des serveurs aux États-Unis, donc vulnérables à plusieurs lois américaines.
- **Rien n’est mieux que le face-à-face.**

Communiquer avec autrui (autres outils)

- Pour le vidéochat : remplacer Zoom, Microsoft Teams par meet.jit.si
- Pour le travail collaboratif : remplacer Google Drive par des sites Web camarades qui offrent Cryptpad, Etherpad, etc.
- Pour le chat : remplacer Facebook Messenger et Signal par Briar ou Cwtch.
  - Briar, Cwtch : pas de serveurs centraux, peut passer par Tor, encrypté de bout en bout, pas besoin d'un numéro de téléphone …
- **Rien n'est mieux que le face-à-face.**

The Onion Router (TOR) Network

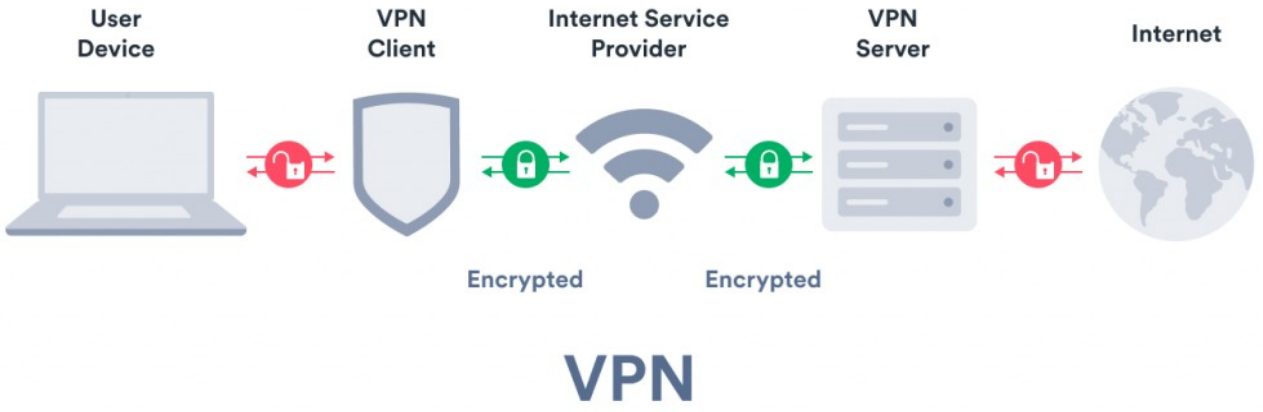
Clinique d'avortement en Arizona



Node qui en fait travaille pour le gouvernement

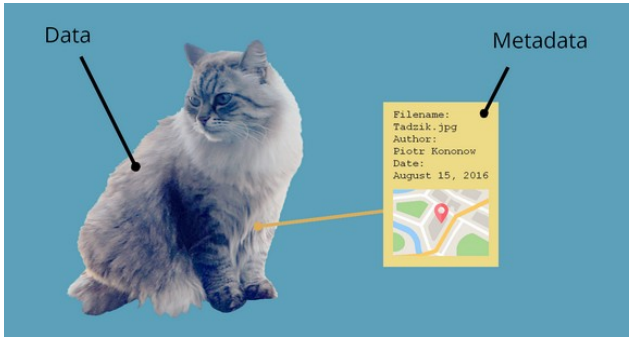
Communiquer avec autrui (VPN)

- Pour les gens qui peuvent se le permettre ($$).
  - Permet de sécuriser ce premier saut crucial vers le réseau Tor.
- Situation en évolution, ça vaut la peine de s'informer :
  - Certain fournisseurs de VPN collaborent avec la police de certains pays.



Ce que l’encryption ne fait pas : Métadonnées

- Beaucoup de fichiers contiennent des métadonnées qui sont utiles dans bien des cas.
  - … sauf quand on veut rester anonymes.
- Exemples :
  - Caméras peuvent ajouter le modèle de la caméra, l’auteur de la photo et parfois même les coordonnées GPS, etc.
  - Documents Word, LibreOffice, PDF contiennent l’auteur, le moment de la dernière modification, etc.
  - Un appel téléphonique va conserver le téléphone source, le téléphone destination, la durée de l’appel, etc.



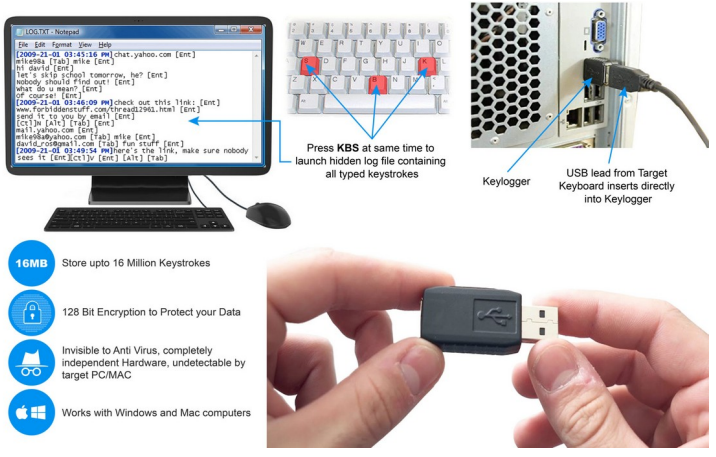
Prenons l’exemple suivant :

- Le médecin d’Alice l’appelle pendant 8 minutes.
- Alice appelle son chum Bob pendant 25 minutes.
- Alice appelle une clinique d’avortement pendant 12 minutes.

Vous n’avez aucune idée des paroles exactes prononcées et pourtant vous savez exactement ce qui s’est passé.

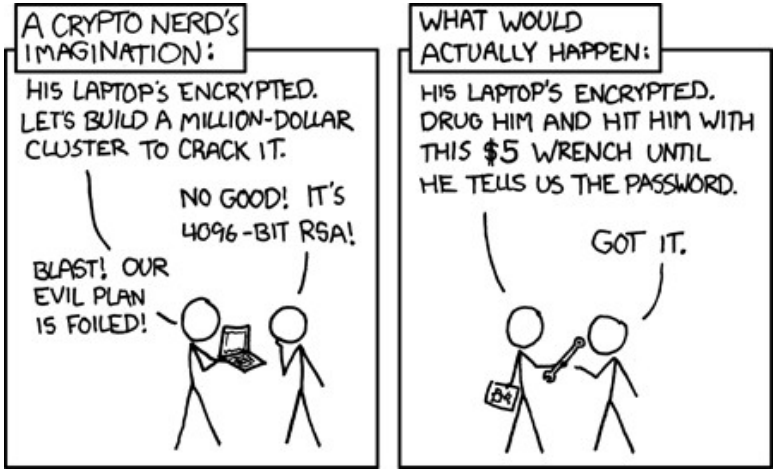
Ce que l’encryption ne fait pas : Keylogging

- Les *keyloggers* sont des logiciels qui enregistrent les touches entrées au clavier.
  - Cela peut être un logiciel installé sur l’ordinateur sans que vous le sachiez, ou une clé physique branchée dans l’ordinateur.
  - Généralement utilisé pour voler des informations bancaires, mais peut être utilisé par des gouvernements.

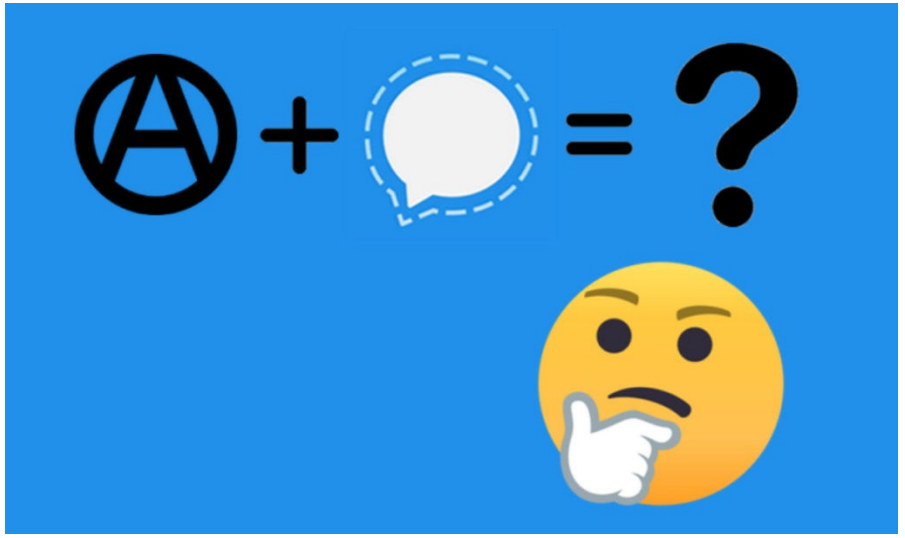


Ce que l’encryption ne fait pas : Rubber Hose Cryptanalysis

- À la blague, l’idée étant que tu tabasses la personne jusqu’à ce qu’iel te donne le mot de passe.
- Sérieusement : les principes de la **culture de sécurité** s’applique.
  - Ne rien dire à une personne qui n’a pas besoin de le savoir.
  - Plus de gens connaissent le secret, plus la probabilité que l’une d’elle craque devant vos ennemis augmente.



Une bonne lecture de chevet : « Signal Fails » et « The P.E.T. Guide »



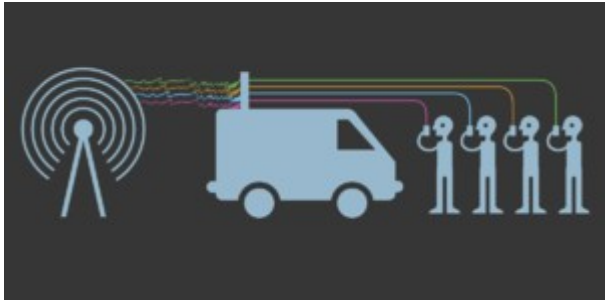
Voir : https://mtlcounterinfo.org/new-communication-infrastructure-for-anarchists/

Assurer la sécurité de vos données

- Encryption de vos appareils
  - Au mieux, utiliser un autre appareil pour vos actions qui doivent être sécurisées.
- Changez votre système d'exploitation
  - Il est facile de débarrer un Windows sans mot de passe.
  - Beaucoup plus difficile pour un Linux avec un disque dur encrypté.
  - Le système d’exploitation Tails (The Amnesic Incognito Live System) peut être installé sur une clé USB.
    - Tails ne conserve aucune donnée une fois fermé.
- Cacher votre adresse IP
  - Différentes approches existent, plusieurs ont été mentionnées ici (VPN, Tor)
- Changer l'adresse MAC de votre appareil (demande plus de compétences techniques)
  - L’adresse MAC est une valeur unique donnée à une carte réseau. Elle permet de vous identifier uniquement sur l’internet.
  - Tails peut cacher l’adresse MAC.

Sécurité numérique en manif

- N’amenez pas votre téléphone !
- N’amenez pas votre téléphone ...
- Si vous devez vraiment l’amener :
  - Fermez votre téléphone, enlever votre carte SIM.
- S’il doit absolument être allumé (ex.: vous êtes photographe) :
  - Ne prenez pas vos camarades en photos,
  - Encryptez votre téléphone et utilisez le NIP (pas de fingerprint ni de Face ID),
  - Désactivez la localisation.



Conclusion

- Remettez fréquemment en question vos pratiques de sécurité numérique.
- **Rien n'est plus efficace que de se parler en personne.**
- **Rien n'est sécuritaire 100%.**
- L'expérience vient... well en expérimentant.
  - Certaines personnes n’aiment pas certains outils (trop difficile à utiliser),
  - Certaines personnes ne peuvent pas utiliser certains outils ($),
  - Les grosses mesures de sécurité ne sont pas pertinentes dans tous les cas …
  - … mais ne pas suivre les mesures appropriées peut coûter cher !
- Ayez ces dicussions de sécurité entre camarades, toutte est subjectif.

Post-conclusion : exemples

- Problème de la chaîne d'infos : Un-e camarade a attiré l'attention de fachos. En épluchant les infos liés à ce nom, les fachos ont trouvé un vieux site Web militant qui a archivé des communications d'une liste de courriel. La/le camarade avait envoyé sur cette liste son téléphone personnel il y a quinze ans. Les fachos ont ainsi pu retracer un appartement lié à ce numéro de téléphone …
- Réseau de connaissance : Les flics ont identifié trois personnes comme suspectes. Toute personne connue par ces trois personnes sera aussi considérée comme suspecte …
  - Nos faiblesses en sécurité ne mettent pas que nous en danger, mais aussi nos camarades.
- Fausse tour cellulaire : Les flics utilisent souvent des fausses tours cellulaires. Cela leur permet d'identifier quel appareil essaie de se connecter à la tour et est donc à proximité.
- Triangulation : Les flics peuvent déterminer la position d'un téléphone cellulaire particulier par triangulation. Un cellulaire essaie de se connecter à plusieurs tour afin de déterminer laquelle est la meilleure : les tours peuvent savoir à quel point le signal est fort en arrivant. On a donc une bonne mesure pour trouver où était le cellulaire.
  - Avec 3G et 4G, cette précision est faible parce qu'il n'y a pas beaucoup de tours. La précision est limitée à genre, un pâté de maison.
  - La 5G demande une très grande quantité de tours. La précision est beaucoup plus grande : les marketers pourront ainsi savoir non seulement dans quel restaurant vous êtes entré-e, mais en plus sur quelle chaise vous vous êtes assis-e.
- Arrêter de tagger les camarades en black bloc sur les photos que vous mettez sur Facebook, yeesh …