La cybersécurité pour militant-e-s

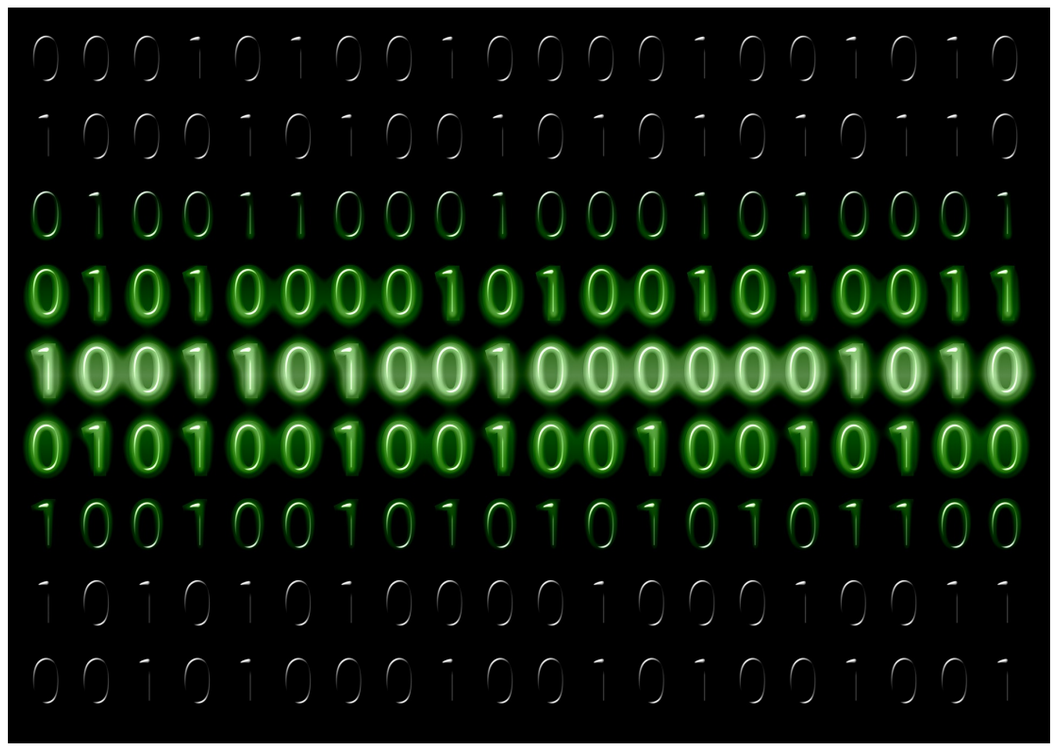
(et pas que!)

?

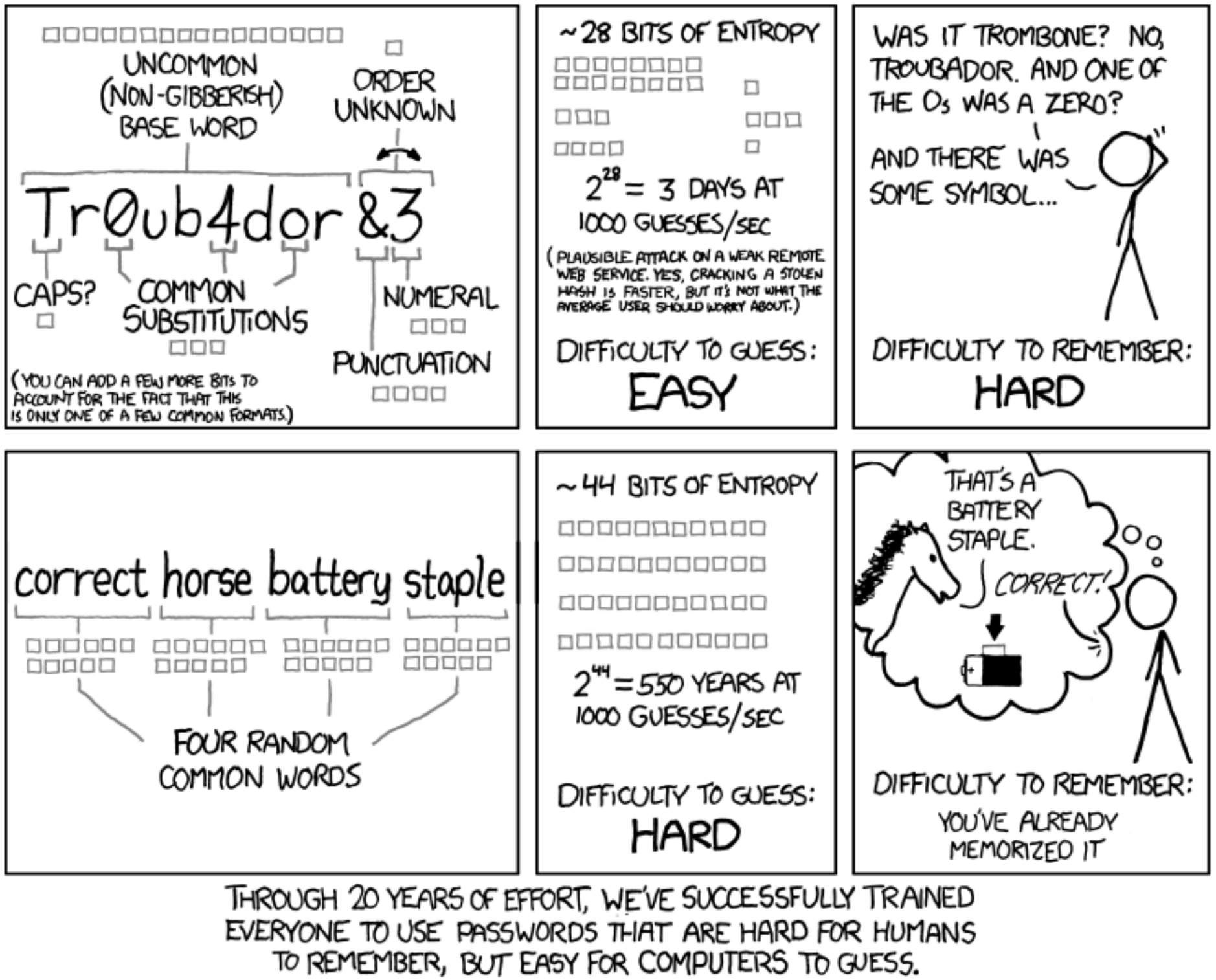
Hygiène Numérique

Plus c'est long plus c'est bon! Plus on en a mieux c'est.
Une forte entropie c'est le minimum!

Je suis ....?



L'entropie d'un mot de passe



Source https://xkcd.com/936/

Hygiène Numérique

- Comment générer un mot de passe fort?
  -> Maximiser l'entropie + longueur
  Ex: Diceware (Méthode des dès), Générateur.

- Mots de passe sur Firefox / Chrome sont en clair!

- KeePassX / Gestionnaire de mots de passe
  (iOS / Android / macOS / Windows / Linux)

- Double Authentification / 2-Step Factor
  (Facebook, Google, Twitter, LinkedIn, Paypal...)

Hygiène Numérique

On me vole mon PC / Téléphone

Qu'est-ce que je perd?

Qu'est-ce qu'on y trouve?

Hygiène Numérique

Un disque dur est très peu couteux!
CAD $79 - 1TB

SAUVEGARDEZ!
(+ Chiffrement pour confidentialité)

Pour se protéger du vol, saisie ou gros dégâts, mettre le disque à l'abri chez un proche.

macOS: Carbon Copy Cloner, ...
Windows: CloneZila, ...

Hygiène Numérique

Le chiffrement de disque c'est simple aujourd'hui!

CHIFFREZ!

macOS: FileVault (en 1 clic!)
Windows: BitLocker *(seulement version Pro)*

Hygiène Numérique

Mettre à jour, c'est se protéger!

Mise à jour du système

Mise à jour des applications

Mise à jour de l'antivirus

La navigation en mode privée...

Ne rend pas anonyme et laisse des traces!

Je n'ai rien à cacher?

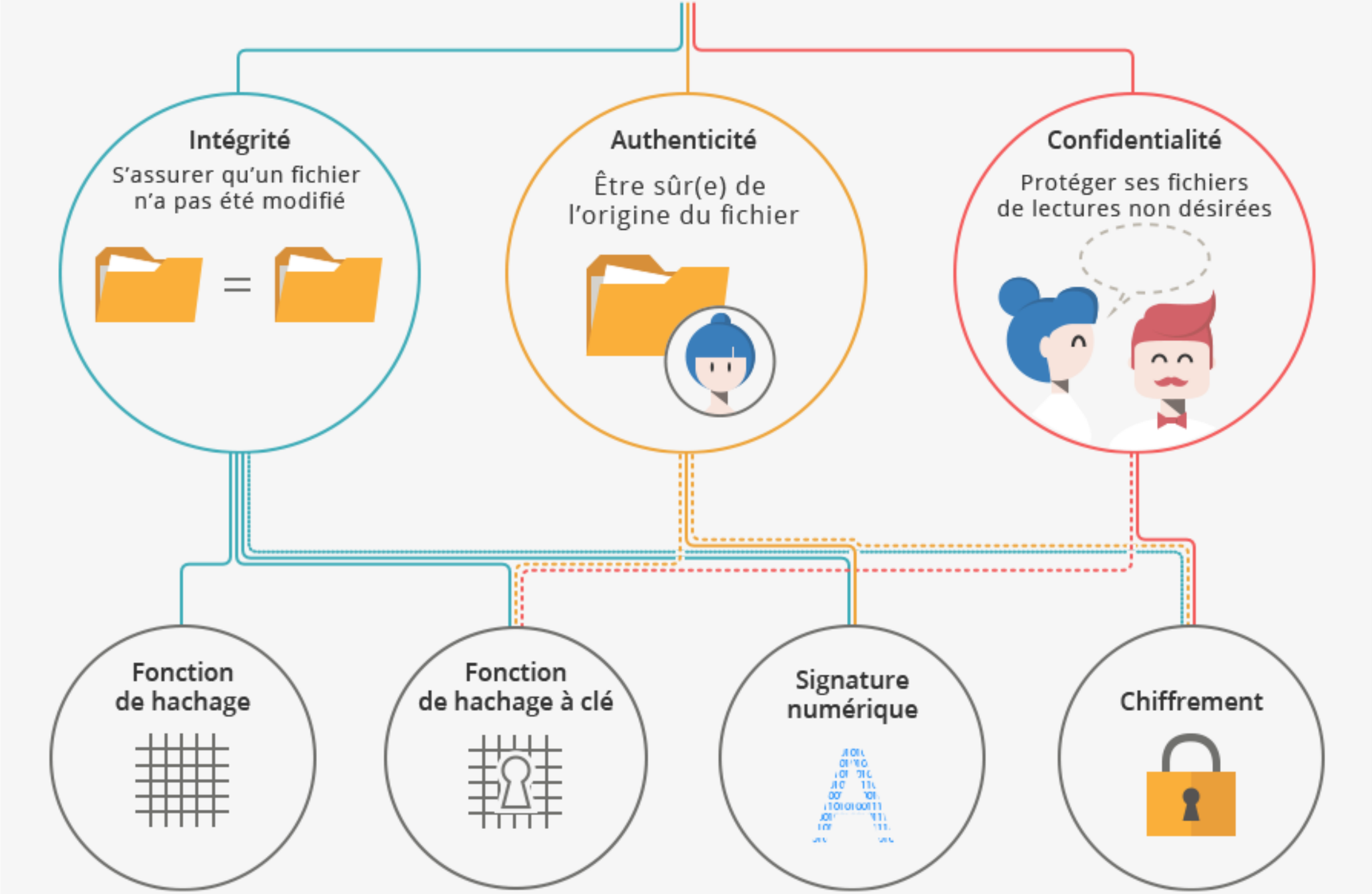
http://jenairienacacher.fr/

Franchissement de frontière

- Backup en lieu sûr.
- Supprimer le plus de données: Données sensibles et Dropbox, Google Drive, historique, mots de passe enregistrés.
- Se déconnecter de tous les sites (effacement de cookies) et emails
- Désactiver la biométrie
- Éteindre PC et téléphone chiffrés

Si problème transmettre tout ce qui s'est passé en anglais à borders@eff.org
+ d'infos: Digital Privacy at the U.S. Border: Protecting the Data On Your Devices and In the Cloud (disponible en PDF)
https://www.eff.org/wp/digital-privacy-us-border-2017
https://www.eff.org/issues/know-your-rights

La cryptographie



Metadata / Métadonnées

Une métadonnée est une donnée servant à décrire une autre donnée.

Ex pour un texte/sms : la donnée = le contenu ; la métadonnée = l'expéditeur, la localisation, l'heure, la date, etc.

Les métadonnées ne sont pas considérées comme des données personnelles à proprement parler, elles sont donc collectées plus facilement. Le problème est qu'elles en disent beaucoup sur nous tout de même !

Le modèle de menace

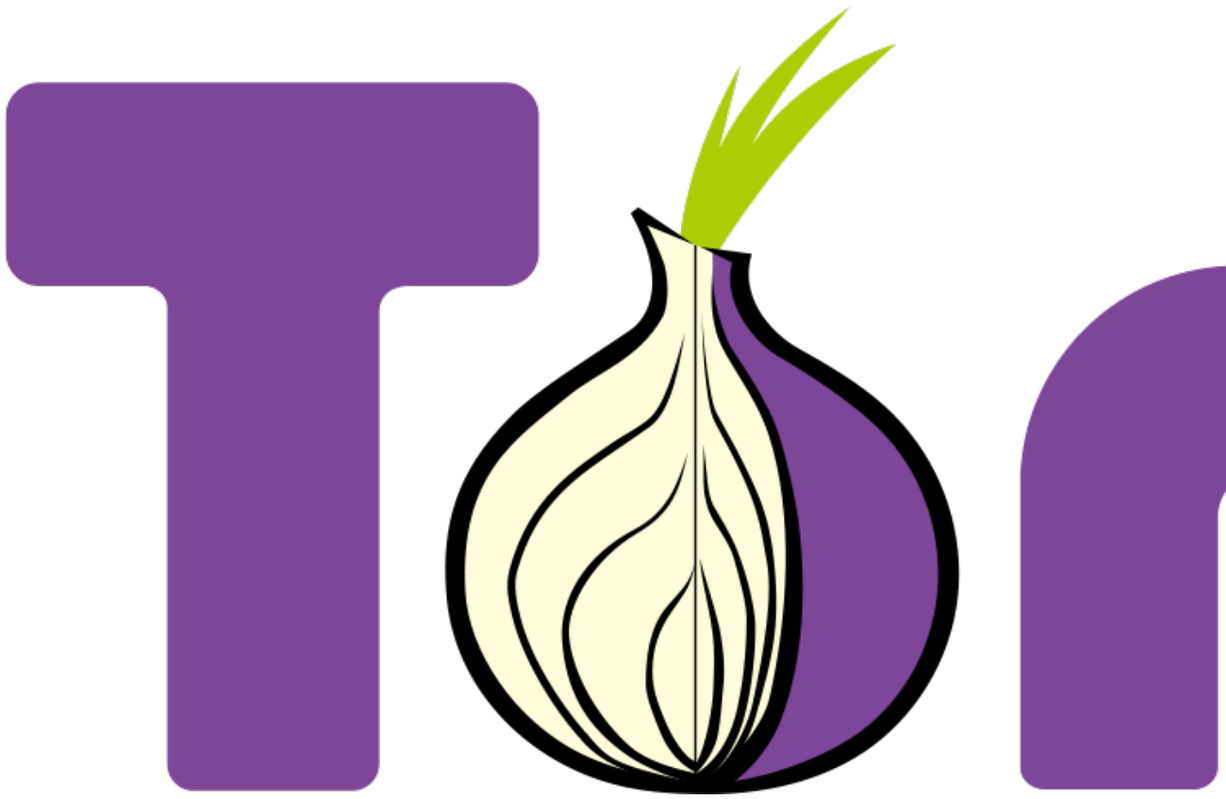
Voici les cinq questions à vous poser pour évaluer votre modèle de menace:

1. Que souhaitez-vous protéger ?
2. Contre qui souhaitez-vous le protéger ?
3. Quelle est la probabilité que vous ayez besoin de le protéger ?
4. Quelles seraient les conséquences si vous échouiez ?
5. Quels désagréments êtes-vous disposé à affronter afin de vous en prémunir ?

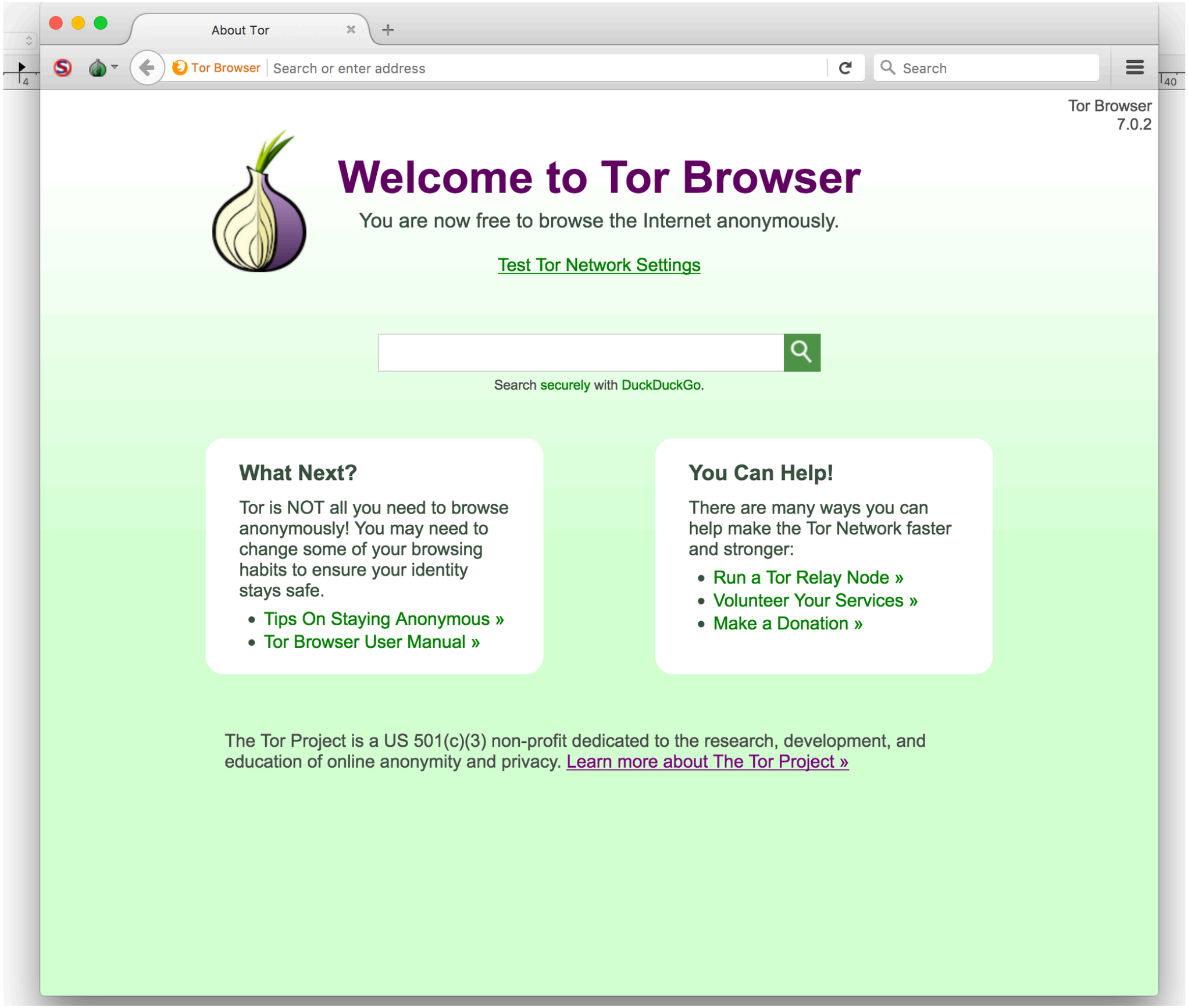
Source: https://ssd.eff.org/fr/module/une-introduction-au-mod%C3%A8le-de-menace

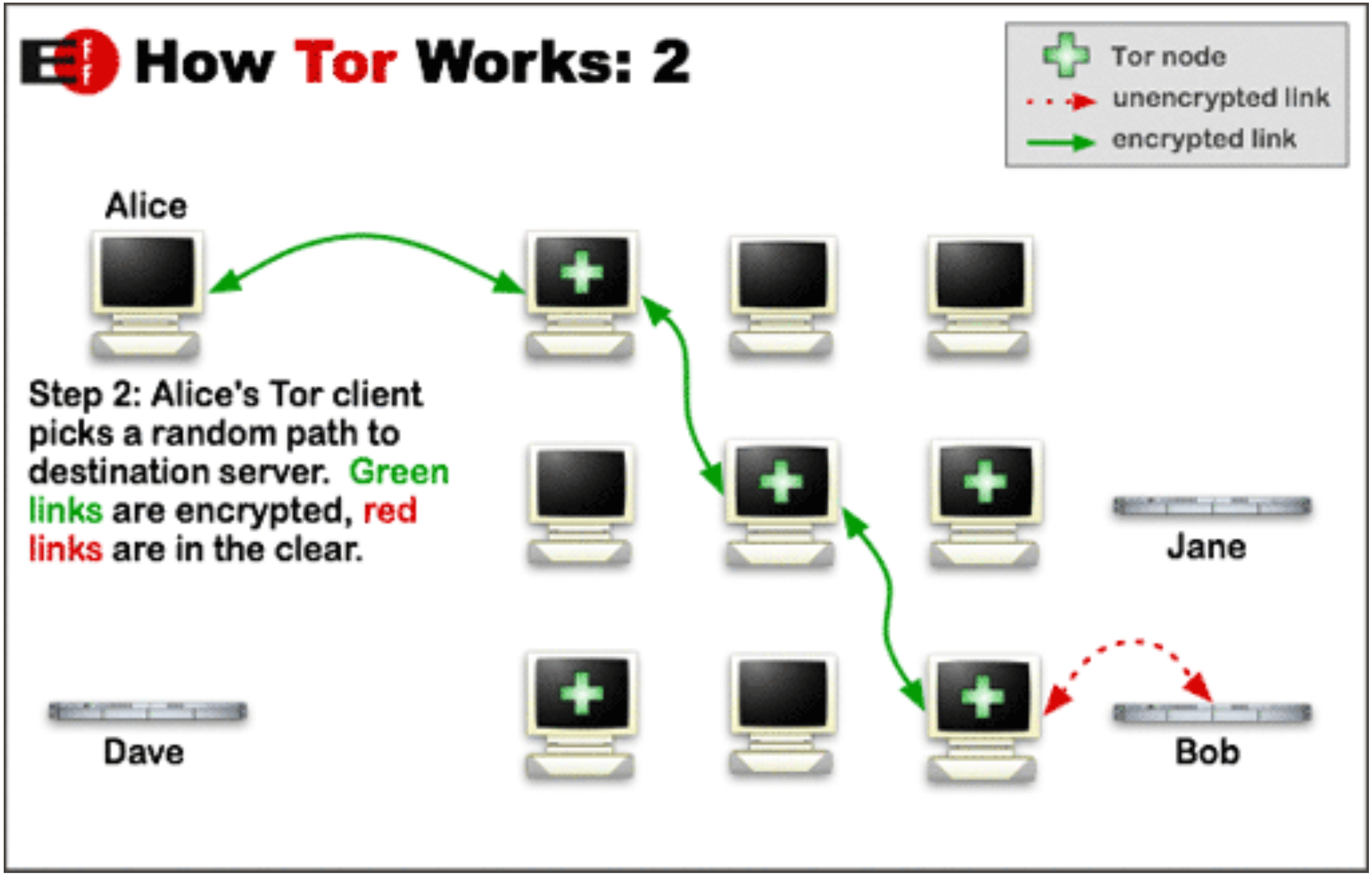
- Dois-je verrouiller ma porte ?
- Dans quelle sorte de verrou ou verrous dois-je investir ?
- Ai-je besoin d’un système de sécurité plus avancé ?
- Quels sont les actifs dans ce scénario ?
    - L’intimité de ma maison
    - Les éléments à l’intérieur de ma maison
- Quelle est la menace ?
    - Quelqu’un peut entrer par effraction.
- Quel est le risque réel de voir quelqu’un entrer par effraction ? Est-il probable ?

Source: https://ssd.eff.org/fr/module/une-introduction-au-mod%C3%A8le-de-menace



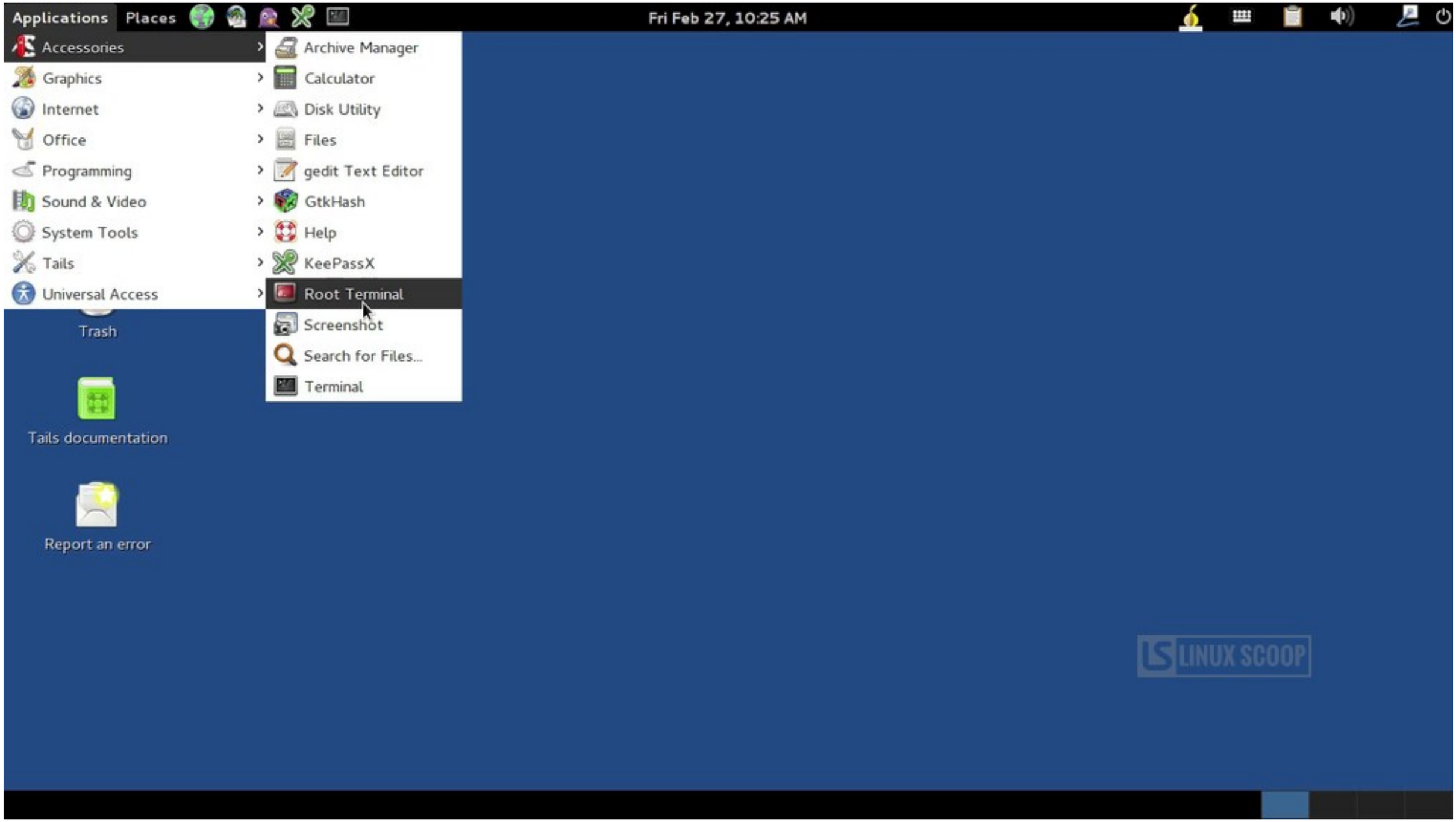
https://www.torproject.org/


About Tor
Tor Browser
Search or enter address
Search
Tor Browser
7.0.2
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with DuckDuckGo.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
Tor Browser User Manual »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »



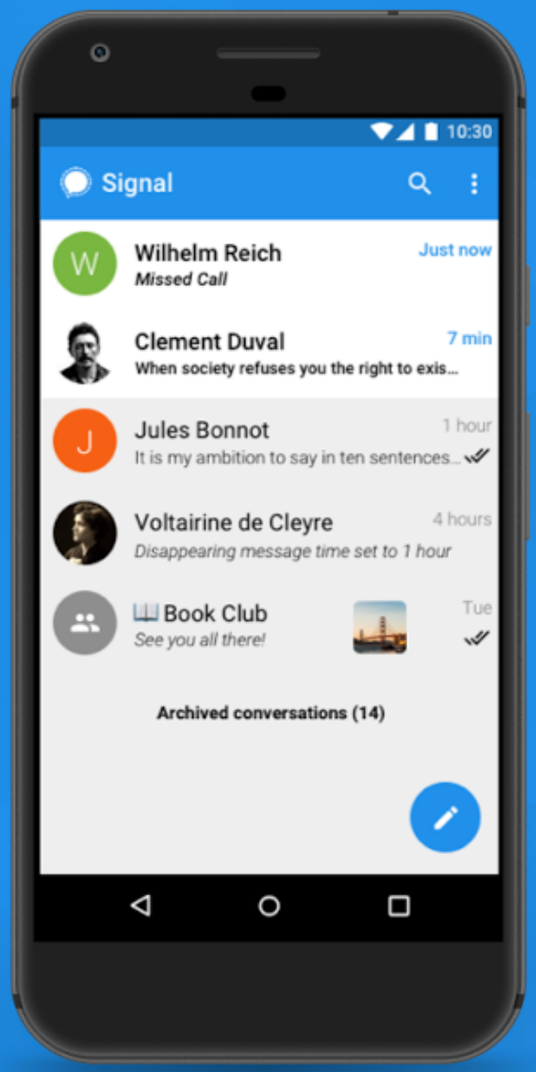
Source: https://www.torproject.org/about/overview.html.en

https://tails.boum.org/index.fr.html


Applications
Places
Fri Feb 27, 10:25 AM
Accessories
Graphics
Internet
Office
Programming
Sound & Video
System Tools
Tails
Universal Access
Archive Manager
Calculator
Disk Utility
Files
gedit Text Editor
GtkHash
Help
KeePassX
Root Terminal
Screenshot
Search for Files...
Terminal
Trash
Tails documentation
Report an error
LINUX SCOOP

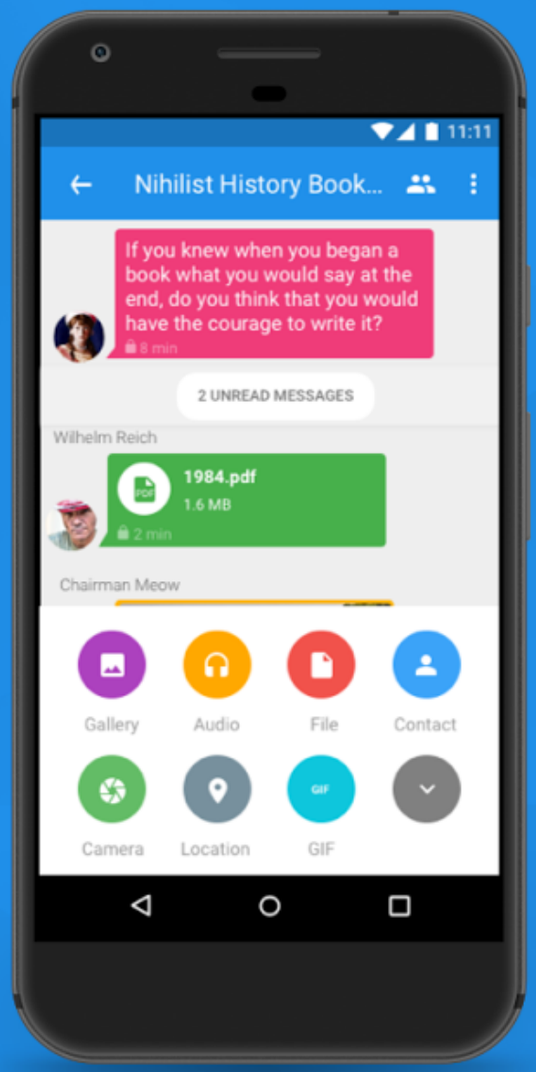
Signal (iOS / Android)

Stay Private



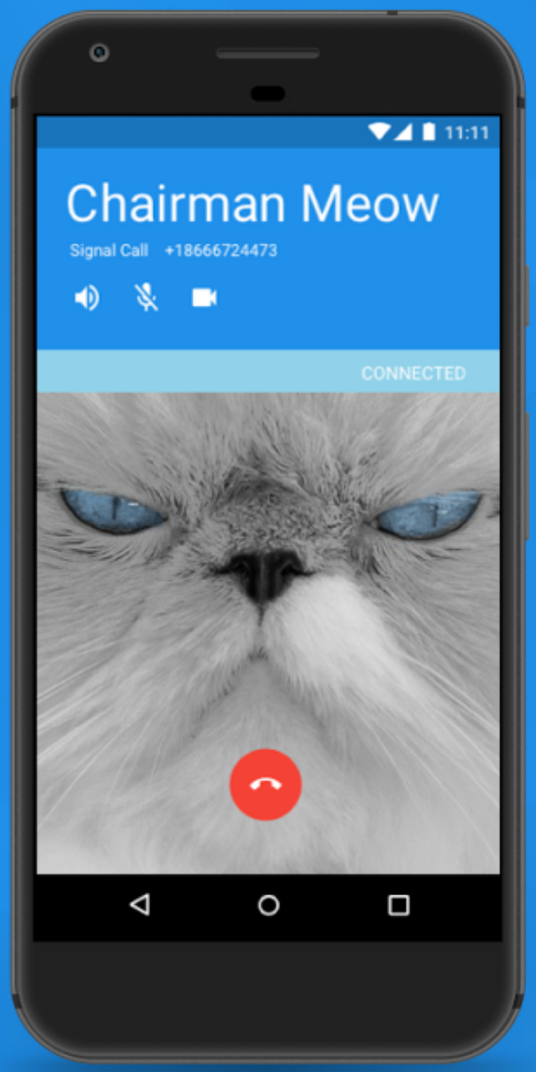
Everything is always end-to-end encrypted

Send Anything



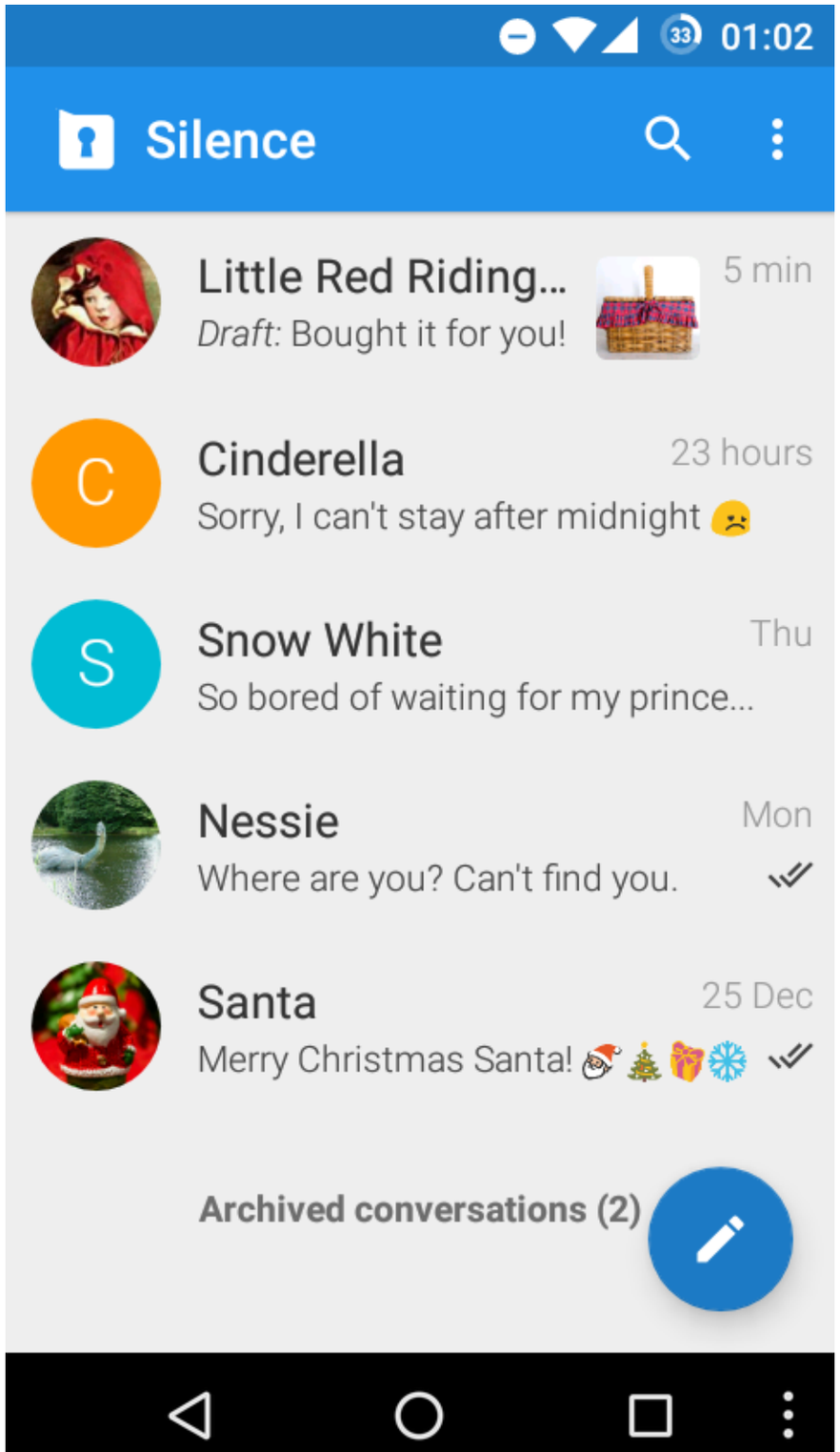
Message with text, gifs, audio, or any file type

Voice or Video Calls



Make crystal-clear voice or video calls from anywhere

Silence (iOS / Android)



ProtonMail.com (iOS / Android / Web)

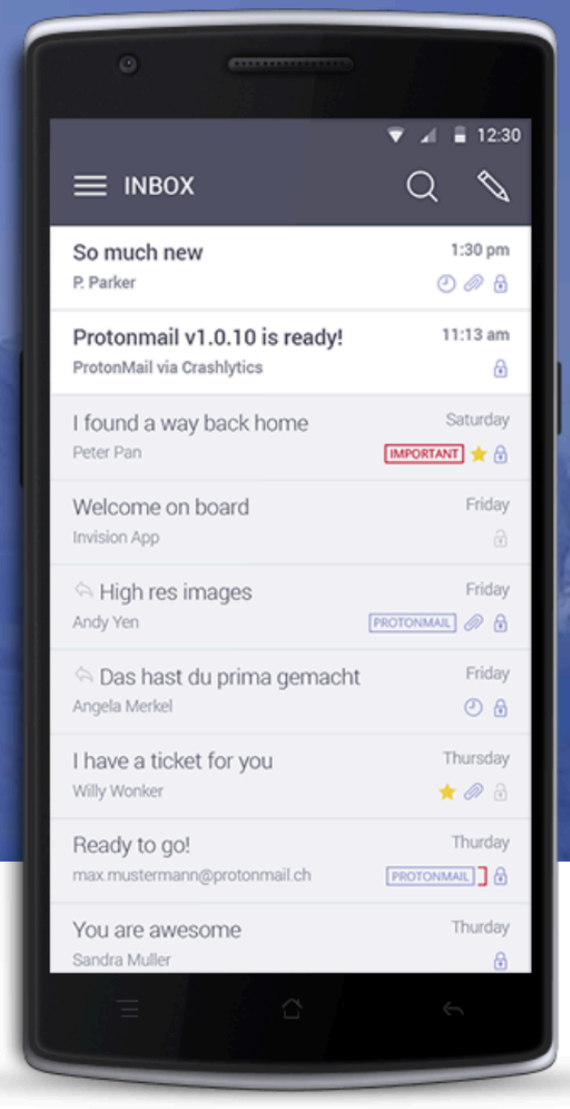
ProtonMail

About Security Blog Careers Support Donate LOG IN SIGN UP

Secure Email Based in Switzerland

Secure Your Communications with ProtonMail

GET YOUR ENCRYPTED EMAIL ACCOUNT



The ProtonMail mobile apps are now available worldwide.

Introducing Encrypted Email for Your Mobile Device

Get the Android App | Get the iOS App | Use the Web Version

Je suis, je chiffre!

Il est nécessaire de chiffrer le plus possible les communications indépendamment de l'importance de son contenu.

Ex:
Message avec la liste de course
Message avec information importante

Cela permet de ne pas dévoiler que la communication comporte un caractère important.

Ressources

- Surveillance Self-Defense by the EFF
  https://ssd.eff.org/

- Security in a Box (Multi-langue)
  https://securityinabox.org/fr/

- A DIY Guide to Feminist Cybersecurity
  https://hackblossom.org/cybersecurity/

- Securing Your Digital Life Like a Normal Person
  https://medium.com/@mshelton/securing-your-digital-life-like-a-normal-person-a-hasty-and-incomplete-guide-56437f127425

- Current Digital Security Resources (Très bonne liste à jour!)
  https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c

Ressources

- Zen and the art of making tech work for you
  https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

- The Digital First Aid Kit
  https://www.digitaldefenders.org/digitalfirstaid/

- Getting Started with Digital Security For Activists
  https://blog.witness.org/2016/11/getting-started-digital-security/
  https://witness.org/resources/

- Guide d’autodéfense numérique
  https://guide.boum.org/

- CryptoParty
  https://www.cryptoparty.in/

- Le Guide de survie Tails
  https://chouettecouetteblog.wordpress.com/

Crypto.Québec est un média numérique à but non-lucratif fondé en juillet 2015 à Montréal par Jean-Philippe Décarie-Mathieu, Luc Lefebvre, et Steven Lachance.

https://crypto.quebec/
equipe@crypto.quebec
facebook.com/crypto.quebec
twitter.com/cryptoqc

ESN514

L’école de sécurité numérique est un projet chapeauté par Alternatives en partenariat avec la Chaire de recherche du Canada en éducation aux médias et droits humains et le CIRA.

https://www.esn514.net/
esn514@riseup.net
facebook.com/esn514/
twitter.com/esn514

Questions?

À faire cette semaine!

- Activer la double authentification / 2-Step Factor (Facebook, Google, Twitter, LinkedIn, Paypal...)

- Installer Signal, Silence sur son téléphone et l'utiliser

- Faire ses mise à jour, backups de son ordinateur

- Chiffrer le disque de son ordinateur

- Utiliser un gestionnaire de mot de passe (KeePassX, 1Password, LastPass) et changer ses mots de passe.