Guide pratique pour les rebelles
Protection des données personnelles informatiques

Attention, ce texte vous semblera peut-être complotiste ou alarmiste en première lecture mais il reflète la réalité du monde dans lequel nous vivons. Il est aussi à prendre sous l'angle du Principe de Précaution cher à XR, les risques sont grands donc soyons attentifs et attentives. Les bonnes pratiques identifiées dans ce guide ne sont pas limitées à XR, utilisez les dans votre vie quotidienne même quand vous n'avez "rien à cacher".

Ce document ne doit pas non plus vous faire peur, il s'agit d'être prudent sans sombrer dans la méfiance. Enfin, on sait que la plupart des choses qu'on vous présente dans ce document sont très ennuyantes et alourdissent votre utilisation des outils informatiques. Pour vous soulager, nous avons identifié plusieurs niveaux de sécurité différents, ces niveaux sont relatifs à votre implication et aux informations que vous possédez.

Vous pouvez bien sûr, renforcer votre sécurité au delà de votre niveau d'implication. Par exemple, si vous ne préparez jamais d'action mais que vous êtes à l'aise avec votre ordinateur, n'hésitez pas à utiliser Tor quand même. Bien sûr, ces niveaux sont emboîtés, si vous êtes modérateur (Niveau 4), il faut tenir compte de toutes les pratiques de niveau inférieur. Par exemple, ça ne sert à rien de chiffrer votre disque dur si vous communiquez par Gmail.

Niveaux de sécurité identifiés :
Niveau 0 : Tous niveaux, tout le monde est concerné par ces paragraphes, il s'agit principalement d'une utilisation plus sûre des outils XR.
Niveau 1 : "Membre actif.ve"
Niveau 2 : "Participation"
Niveau 3 : "Organisation"
Niveau 4 : "Modération"

Nous ne savons toujours pas si vous êtes légalement en droit de refuser de donner votre mot de passe de chiffrement, ou même le code PIN de votre téléphone, à la police. Nous essayons de demander à des expert-es en droit informatique et nous vous tiendrons au courant. N'hésitez pas à consulter de temps en temps ce fichier, au cas où on rajouterait de nouvelles bonnes pratiques.

Intro : Pourquoi protéger ses données personnelles et sa présence sur les outils numériques – Tous niveaux

Les activistes écologiques sont bien plus la cible des services de renseignement ou d'attaques internet que les activistes uniquement anti-nucléaire ou pour les droits de l'humain. La principale raison est qu'elles et ils remettent en cause le système dans sa globalité et s'attirent donc l'attention de plus de personnes.

Il y a plusieurs types d'organisations qui peuvent avoir envie de récupérer des informations sur notre mouvement et sur ces membres : les gouvernements via leurs services de renseignement et les entreprises ou lobbys que nous pourrions viser dans certaines de nos actions. Il est important de faire la différence entre les deux, car elles n'ont pas forcément les mêmes moyens, ni la même éthique. Si les services de renseignement peuvent avoir facilement votre adresse personnelle, c'est plus compliqué pour une entreprise privée. Il est donc important de ne pas partager des informations qui nous semblent "de toute façon évidente" ou "trop facile d'accès".

I - Bonnes pratiques sur les outils XR – Tous niveaux

1- Espaces publics / Espaces privés sur la Base et Mattermost

Pour rappel, la base, le rdv, Mattermost, ne sont pas entièrement sécurisés ! N'importe qui peut se créer un compte et avoir accès à toutes les informations partagées dans les espaces publics. Ne jamais discuter d'actions ou échanger des informations personnelles en public.

Les espaces publics concernent tous les fils de discussion de la base et toutes les chaînes publiques de Mattermost (le bloc du haut).

Les espaces privés concernent les conversations en message direct sur la base (icône des 3 barres > icône avec l'enveloppe > vos différentes conversations privées), ainsi que les chaînes privées de Mattermost (le bloc du bas). Vous ne pouvez rejoindre ces conversations que par invitation. Ce sont ces conversations qu'il faut utiliser pour organiser des actions et si vous souhaitez utiliser des informations personnelles.

En pratique :
- ne communiquez jamais votre adresse personnelle
- demandez vous avant toute publication sur des espaces publics si votre publication ne risque pas de vous incriminer ou d'éveiller l'attention des RG ou d'une entreprise sur vous. Par exemple, si une personne demande "qui serait motivé-e pour participer à l'organisation d'une action?", contactez-là en privé plutôt que de répondre "Moi"
- si vous voyez des informations sensibles circuler, signalez les directement avec le bouton prévu à cet effet, en bas à droite (« … » > Drapeau)

2 - Adresse mail

Les adresses mail sont aujourd'hui la principale faille de la sécurité informatique. Deux techniques sont particulièrement communes :

1. Si vous avez une adresse Gmail, les gouvernements (voire mêmes les multinationales) peuvent tout à fait demander à Google l'intégralité de vos échanges. Google est obligé de transmettre toutes vos données aux renseignements américains s'ils le demandent, qui se feront alors un plaisir de transmettre ces informations aux renseignements français dans un élan de solidarité internationale. Google sera aussi très content de vendre ces informations aux multinationales qui voudraient en savoir plus sur vous.

A faire tout de suite :

- Créer une adresse protonmail (sécurisée) : https://protonmail.com/

- Changer votre adresse sur la base :
- **Cliquer sur votre photo en haut à droite**
- **Cliquer sur votre nom**
- **Cliquer sur « Préférences »**
- **Changer l'adresse dans « Courriel »**

- Demander à votre groupe local qu'il enlève vos adresses non protonmail des newsletter

- Supprimer tous les liens avec XR de votre ancienne boîte mail
- **Mails**
- **Balises**

- **Dossier de fichiers**
- **Contacts**
- **Agenda**

2. La méthode la plus répandue aujourd'hui pour piéger une personne par son adresse mail est de lui envoyer un mail qui l'invite à cliquer sur un lien. Par exemple :

"Salut XXX,
C'est YYY, je suis de retour en ville, est-ce que ça te dit qu'on aille boire un verre ?
J'ai retrouvé une photo qu'on a pris ensemble la dernière fois, la voici : *lien de la photo*

A bientôt !
YYY"

Curieuses de l'identité de l'auteur ou l'autrice du message, la plupart des personnes cliquent sur le lien de la photo. **Cela a pour conséquence de télécharger un virus qui peut récupérer les informations de tous vos contacts mails, placer un mouchard virtuel pour enregistrer vos communications futures voire aller fouiller dans tout votre ordinateur, sans que vous ne soyez au courant de rien.** Inutile d'être un as de l'informatique pour le faire, il existe des tutoriels qui vous apprennent à faire ça en libre accès sur Internet.

Pour échapper à ces tentatives d'intrusion, il faut :
- lire attentivement tout le message avant de cliquer sur quoi que ce soit. En particulier,
  - vérifiez l'adresse de l'expéditeur ou l'expéditrice, si elle semble bizarre, supprimez le message
  - si la personne vous invite à cliquer sur un lien, c'est louche, de manière générale ne le faîtes pas

- n'ouvrez pas un lien envoyé par un-e autre rebelle par mail

- si vous voulez envoyer un lien à un-e rebelle, faîtes le par Mattermost ou la Base

II – Je revendique publiquement mon appartenance à XR – Tous niveaux

Nous vous invitons à tout faire pour alerter sur l'urgence et inspirer de la confiance dans XR, c'est à la base du fonctionnement d'XR. Nous ne savons pour l'instant pas, si le relais d'information, ou l'apologie d'XR, peut être un élément à charge dans une condamnation. Nous mettrons cette partie à jour dès qu'un.e spécialiste nous aura répondu.

III - Vous connecter sur la Base ou Mattermost – Niveau 1 "Membre actif.ve"

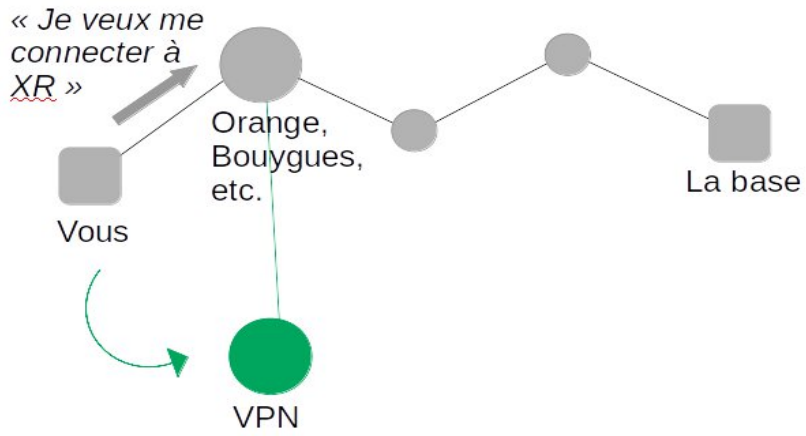
Il faut passer par un petit peu d'architecture web pour bien comprendre ce passage. On a essayé de le simplifier au maximum alors lisez bien tout. Si vous avez la moindre question, n'hésitez pas à nous envoyer un message privé. @greg @leukos @davux

Lorsque vous faites une recherche sur Internet, vous envoyez un message à votre gestionnaire de réseau qui se débrouille ensuite pour chercher l'information que vous voulez. Ainsi à chaque fois que vous vous connectez sur la base, vous envoyez un message à Orange, Bouygues, etc., en disant "je veux me connecter au forum de Extinction Rebellion France". Et tous ces messages sont enregistrés sur votre fichier personnel. Les services de renseignements ont la possibilité de demander à vos gestionnaires de réseau d'avoir accès à vos fichiers de connexion. Ils peuvent donc très facilement voir que vous êtes très proche d'XR. Pour votre propre sécurité, il faut donc passer par un intermédiaire, ce qu'on appelle un « VPN »

PROCEDURES D'INSTALLATION D'UN VPN

Utiliser un VPN

Un VPN crée une interface supplémentaire entre vous et votre fournisseur d'accès Internet. Il devient alors impossible de savoir **qui** cherche à se connecter à la base XR.



Ce VPN est un point de connexion à Internet, les flux de connexion passant par ces points d'accès sont visibles pour des expert-es informatiques. On sait que ce VPN se connecte à XR. Ainsi il faut éviter "d'attirer l'attention", sur ce point de connexion, c'est à dire ne pas trop l'utiliser.

En pratique :
- Utiliser le VPN développé pour XR uniquement pour vous connecter aux outils XR : base, Mattermost, rdv. Ne l'utilisez pas pour écouter de la musique ou des vidéos.

Sur votre ordinateur :

Sur un ordinateur sous Mac :

DETAILLER LA PROCEDURE AVEC DES PHOTOS

Sur un ordinateur sous Linux :

DETAILLER LA PROCEDURE AVEC DES PHOTOS

Sur un ordinateur sous Windows :

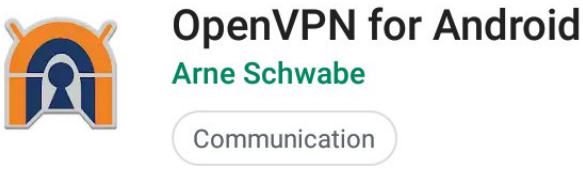
DETAILLER LA PROCEDURE AVEC DES PHOTOS

Sur votre smartphone :

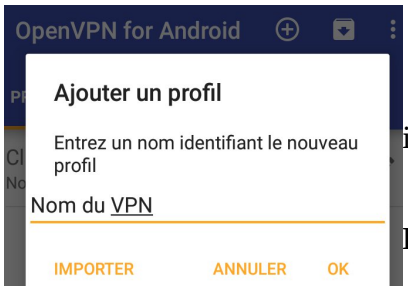
Pour utiliser un VPN sur votre smartphone il faut d'abord télécharger un logiciel spécial.

1. Pour iPhone : téléchargez OpenVPN.
LOGO de l'APPLI + Procédures

1. Pour Android : téléchargez OpenVPN for Android



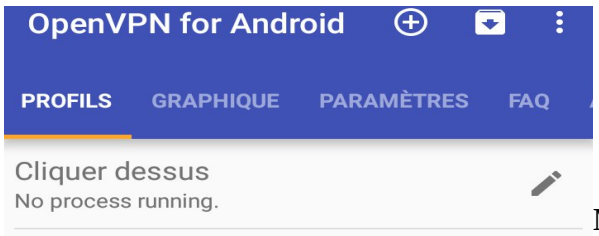
2. Téléchargez le fichier texte qui contient le VPN, il termine par ".ovpn".

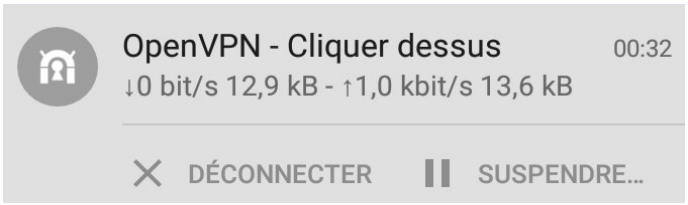


3. Ouvrez l'application OpenVPN.

Cliquez sur le bouton (+), donnez un nom à votre VPN et importez le fichier « .ovpn ».

Une fois que vous avez installé le VPN : i**l faut l'activer ET le désactiver à chaque fois que vous souhaitez vous connecter à "XR"**, que ce soit la base,





Mattermost, le rdv, le compte FB, etc.

IV - Travailler sur le rdv (le cloud) – Niveau 1 "Membre actif"

Tout comme Mattermost ou la base, le rdv est sécurisé des attaques extérieures, mais il est totalement transparent pour n'importe quel.le membre d'XR dont des potentiel.les infiltré.es. Ainsi, **on ne fais pas des fichiers de recensement avec adresses, lieux de travail, personnes à contacter, etc., ouvertement sur la base !**

Comme pour la base, toutes les connexions au rdv sont visibles, en particulier les gros flux de données. Pour ne pas attirer l'attention, **il ne faut pas synchroniser le rdv avec son ordinateur.** Certain-es ont peut-être déjà essayé de le faire en utilisant le logiciel Nextcloud, **il faut totalement arrêter ce genre de pratiques.**

Le rdv n’est pas vraiment fait pour travailler à plusieurs sur un même document. Il faut donc éviter de modifier toutes et tous les fichiers en même temps. Si vous modifier un document seul.e, copiez-collez le sur votre ordinateur, faîtes les modifications nécessaires et re-copiez-collez le sur le rdv, ou modifiez le directement sur le rdv. Si vous voulez contribuer à plusieurs en même temps, créez une conversation Jitsi, désignez une personne pour faire un partage d’écran, pour partager et modifier le document.

Bonnes pratiques :

- Ne pas stocker d‘informations personnelles

- Ne pas synchroniser le rdv sur son ordinateur

- Vous connecter au rdv (cloud) en utilisant un VPN

- Utiliser le rdv comme un espace de stockage, une bibliothèque et peu comme un espace de travail collaboratif

- Eviter de télécharger trop de documents, dans un sens comme dans l’autre, cela attire l’attention sur notre serveur, si le document n’est pas trop compliqué, préférer l’option coller-coller plutôt que télécharger

- Si vous souhaitez modifier un document à plusieurs, le plus simple est de créer une conversation Jitsi (feu de camp ou encore le “Skype XR”), qu’une personne fasse un partage d’écran pour partager le document et que cette personne fasse les modifications demandées par les autres participant-es.

V - Je participe à une action – Niveau 2 “Participation“

1. Je peux me passer de mon téléphone (pas de rôle ni besoin spécifiques)

Passez-vous de votre téléphone.

2. Je ne peux pas me passer de mon téléphone (rôle ou besoin spécifiques)

a) si vous avez un téléphone spécifique à XR (non smartphone), comme celui-ci :

- Supprimez tous les anciens messages

- Supprimez tous les contacts dont vous n’avez pas besoin *(gardez en peu, 10 suffisent en général amplement)*

- Modifier le nom des contacts que vous gardez pour les anonymiser *(cf. Comment bien modifier un nom de contact)*

b) si vous utilisez votre smartphone habituel :

- Supprimez tous les anciens messages

- Supprimez tous les contacts dont vous n'avez pas besoin *(gardez en peu, 10 suffisent en général amplement)*

- Modifier le nom des contacts que vous gardez pour les anonymiser *(cf. Comment bien modifier un nom de contact)*

- Déconnectez-vous de toutes les applications ayant un lien direct ou indirect avec XR : Mattermost, Protonmail

- Nettoyez votre historique de connexion sur tous vos navigateurs internet : Mozilla, Chrome, Safari, etc.

- Vérifiez que votre agenda, vos fichiers de notes, vos documents enregistrés ne contiennent pas de mention d'XR

- *Exemple : "Agenda Dimanche 28/04, réunion action XR"*

- *Exemple : "To-do list, répondre à XXX sur XR"*

- Si vous ne prenez pas de photo, enlevez votre carte SD

- Si vous prenez des photos, videz votre carte SD

- Essayez de vous procurer un téléphone du paragraphe a) pour la prochaine action

Comment bien modifier un nom de contact :

- Ne pas indiquer d'ordre :
A, B, C, D, E, etc ou 1, 2, 3, 4, 5. La police vit dans un univers hiérarchisé. La personne A ou 1, sera considérée comme cheffe par défaut.

- Ne pas utiliser le pseudo XR ou le prénom de la personne :
Imaginez un nom ou un code *(que vous n'oublierez pas!)* assez éloigné de l'identité publique ou XR de vos contacts

- Il est possible d'utiliser les rôles des personnes (Gardien.ne de la paix, Contact police, Contact presse, etc.) lorsque ce sont des rôles publics. **Ne pas utiliser les termes "Organisatrice", "Responsable", "Leader", etc**.

VI – J'organise une action – Niveau 3 "Organisation"

L'organisation d'une action nécessite un degré de sécurité supérieur à la simple participation.

1) En amont de l'action

a) Repérages

Aujourd'hui, les renseignements n'ont pas besoin de mettre un mouchard dans votre téléphone pour savoir où vous allez, votre téléphone le fait tout seul et ils n'ont qu'à demander à votre fournisseur d'accès. Ainsi **ne prenez pas votre téléphone avec vous lorsque vous faîtes des repérages pour planifier vos actions.**

b) Recherches Internet

Vous n'allez jamais sur le site d'H&M, vous y allez tous les jours pendant une semaine, une action XR a lieu devant un H&M et vous ne retournez jamais sur le site ? Ça se voit, et c'est suspect. Ce qui se voit c'est le numéro d'identification de votre fournisseur d'accès, (le premier point sur le schéma du VPN), et c'est donc cela qu'il faut masquer. Vous pourriez utiliser la même méthode

VPN décrite pour accéder aux outils XR, mais nous vous demanderons de faire autrement si possible : **utiliser TOR**.

Pourquoi utiliser TOR ?

TOR est un navigateur internet, comme Mozilla Firefox, Safari ou Google Chrome qui a la particularité de masquer votre identité. Il marche comme plusieurs VPN imbriqués et **changeants**, ce qui fait qu'il est impossible de suivre votre trace **et** en même temps de ne pas montrer le même numéro d'identification. Le fonctionnement de TOR est un petit peu moins rapide que celui des autres navigateurs de recherche mais vous ne devriez pas voir la différence.

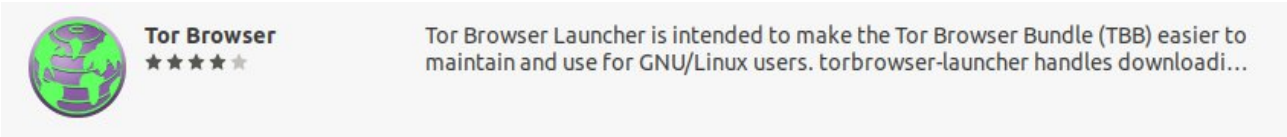
Pourquoi ne pas utiliser le VPN XR ?

Comme surligné en gras dans le paragraphe précédent, le VPN XR masque votre numéro d'identification personnel mais affiche toujours le même au site ciblé. La cible voit donc qu'un nouvel appareil se connecte sur son site régulièrement puis s'arrête brusquement juste après qu'une action XR ait eu lieu. Au bout de trois actions un peu médiatisées, les renseignements et les entreprises connaîtrons le numéro d'identification du VPN XR et sauront lorsque nous préparons une action. TOR permet de modifier régulièrement ce numéro d'identification, c'est la principale raison pour préférer cette solution. Une deuxième est aussi qu'il ne faut pas créer un flux trop important de données à travers le VPN XR, donc ne l'utiliser que pour les outils XR.

Installer TOR sur son ordinateur

- Linux

    - Ouvrir *Logiciels Ubuntu*,
    - Chercher *TOR Browser*,
    - Installer *Tor Browser*



- MAC

PROCEDURES D'INSTALLATION MAC

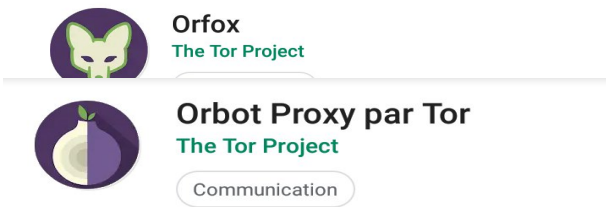
- Windows

PROCEDURES D'INSTALLATION WINDOWS

Installer TOR sur son smartphone

- Android

    - Ouvrir *Play Store*
    - Installer *Orfox*
    - Installer *Orbot*



- Apple

PROCEDURES D'INSTALLATION APPLE

Utiliser TOR

Pour utiliser TOR, il suffit de cliquer sur l'icône logiciel de votre ordinateur ou l'application (Orfox/application Apple) de votre téléphone et de faire vos recherches comme d'habitude.

2) Pendant l'action

- Utilisez un téléphone "sécurisé". Pour cela **des stocks de "téléphones d'action" doivent être rapidement constitués au sein de chaque groupe local.** Ces téléphones rentrent dans le matériel d'action d'XR, **ils doivent donc être pris avant chaque action et restitués à la fin de celle-ci.**

- Prenez les mêmes précautions que les autres participant-es.

VII – Je suis modératrice, modérateur, administratrice, administrateur système – Niveau 4 « Modération »

XR a beau être un mouvement décentralisé, **il existe par-ci par-là, quelques points critiques**, comme par exemple les administrateurs ou administratrices des systèmes informatiques, les modératrices, modérateurs des groupes thématiques ou des groupes locaux. C'est inhérent au modèle holacratique. Nous rappelons ici que **ces points critiques doivent être changés régulièrement**, non seulement pour garantir la démocratie, mais aussi pour assurer la sécurité des membres.

Si vous êtes identifié-e comme tel point critique, nous vous invitons vraiment à protéger plus profondément vos appareils. Si c'était très facile, nous le proposerions à tout le monde, mais c'est un petit peu complexe. Si les informations suivantes ne sont pas claires, n'hésitez surtout pas à nous contacter, nous vous aiderons dans les différentes étapes d'installation. @greg @leukos @davux

Pour être bien clair, vous risquez de voir la police arriver chez vous et perquisitionner votre domicile pour récupérer vos appareils électroniques.

1) Des ordinateurs spécifiques

Lorsque la police perquisitionne votre domicile et saisi votre ordinateur ou votre téléphone, elle est normalement obligée de vous le rendre. Hélas, ça arrive que des choses se perdent…

Il faut donc commencer tout de suite à faire le deuil de vos appareils électroniques. Le mieux est d'avoir un ordinateur dédié à XR, que vous êtes prêt-es à perdre, et que vous pourrez donner à la nouvelle personne qui prendra votre rôle.

Nous allons essayer de nous procurer des ordinateurs de type Thinkpad. **Nous les configurerons et les mettrons à votre disposition.** En attendant, il faut chiffrer vos appareils personnels.

2) Chiffrer son ordinateur

Sur Windows :

Il est possible de chiffrer un disque dur Windows, mais nous vous invitons à plutôt quitter Windows pour Ubuntu. La principale raison est que Windows est très vulnérable aux virus informatiques.

Sur Linux (Ubuntu) :

Le chiffrement de votre disque dur sous Linux se décide au moment de l'installation de Linux. Si vous êtes déjà sous Linus, il faudra le ré-installer. L'installation de Linux nécessite une clé usb vide et c'est un peu technique. **Le mieux serait d'avoir une ou deux personnes dans chaque groupe local chargées de faire l'installation.** Nous allons essayer de monter une équipe pour ça.

a) Copier-coller, l'intégralité de vos documents personnels sur une clé usb ou un disque dur externe.

b) Créer une clé usb exécutable :

- Télécharger le document .iso suivant :

Depuis Windows :

- Télécharger *Rufus*
- Insérer la clé USB vide
- Lancer *Rufus*
- Sélectionner votre clé usb
- Cliquer sur *créer un disque de démarrage*
- Sélectionner le fichier « .iso » que vous venez de télécharger

Depuis Ubuntu :
Dans les versions supérieures à 16.04, un graveur de disque est déjà intégré à Ubuntu, il s'agit de l'application *Créateur de disque*.
- Insérer la clé USB vide
- Lancer *Créateur de disque*
- Sélectionner votre clé usb
- Sélectionner le fichier « .iso » que vous venez de télécharger
- Cliquer sur *créer un disque de démarrage*

c) Installer Ubuntu :
- Éteindre l'ordinateur
- Insérer la clé USB qui contient uniquement le fichier « .iso »
- Allumer l'ordinateur
- Lorsqu'une fenêtre noire s'ouvre pour choisir votre système d'exploitation, choisir Ubuntu
- Suivre les étapes d'installation en faisant bien attention à sélectionner l'option **« Chiffrement du disque »**
- **Vous ne pourrez pas changer le mot de passe maître, donc notez le quelque part et ne l'oubliez pas !**

Sur Mac :

3) Chiffrer son téléphone :

La plupart des smartphones proposent une option de chiffrage du téléphone. Voici son emplacement pour quelques téléphones :

Sony Xperia : « Réglages (ou Paramètres) > Sécurité > Chiffrement »
Samsung Galaxy S7 :
Fairphone :

N'hésitez pas à chiffrer votre carte SD aussi. Par contre, elle sera plus compliquée à ouvrir sur votre ordinateur.

4) Faire des sauvegardes sur des disques durs externes :