T1 P2 - Attention à vos données !

Une autre problématique de la sécurité en ligne en tant que militant.e, est **ce que vous faites de vos données.**

Effet, même avec le meilleurs VPN du monde, faire attention aux données qu'on laisse sur internet est extrêmement important pour protéger votre identité militante.

Le plus primordial est de maintenir une démarcation la plus nette possible entre votre identité militante et votre identité officielle.

Activité sur les réseaux sociaux

Un piège dans lequel peuvent tomber des militant.e.s, se situe au niveau de leur usage des réseaux sociaux.

En effet, si vous utilisez votre compte "officiel", lié à votre identité, sur des réseaux sociaux, dans le but de liker ou de réagir à des posts relatifs au militantisme, ou pire, à des actions auxquelles vous avez participés, vous donnez des élements aux renseignements et aux forces de l'ordre, qui surveillent ces réseaux, pour savoir que vous êtes impliqués dans des actions, ou du moins que vous êtes fortement succeptibles de l'être

Des personnes se sont déjà faites avoir de cette manière, en likant, ou pire, en se faisant prendre en photo sur les réseaux sociaux sur le lieu d'une action, après cette dernière.

En conclusion, ne pas liker ni intéragir avec du contenu militant, depuis un compte associé à votre identité, sur les réseaux sociaux.

Vous pouvez le consulter éventuellement (tant que les réseaux sociaux eux mêmes ne sont pas encore en collaboration avec nos renseignement pour ficher les opinions politiques des internautes, ça ne saurait tarder..) mais pas réagir ni commenter.

Données que vous renseignez sur les sites en tant que militant.es

Lorsque vous créez des comptes sur des sites, dans le cadre de votre activité militante (comme Proton mail), il vous est parfois demandé de renseigner des informations, telle qu'une adresse mail ou un numéro de téléphone de récupération.
Afin de prévenir tout lien possible entre votre identité militante et votre identité officielle, il faut dans ce genre de cas ne pas renseigner d'information faisant le lien entre ces dernieres, ou bien la retirer dès que vous le pouvez

Exemple de Proton mail

Un exemple typique est celui de proton mail.

Proton mail, au moment de créer un compte, vous demande de renseignez une adresse mail et/ou un numéro de téléphone de récupération. Cela n'est initialement pas forcément obligatoire, cependant, il peut arriver que Proton retreigne votre compte et/ou vous demande des données de vérifications (email, num de tel), par exemple pour l'inscription à des services tiers

Vous pouvez pour cela tentez de renseigner une adresse mail anonyme.
Il existe sur internet des services, permettant de créer une adresse mail anonyme et temporaire, dont voici quelques exemples :

- https://yopmail.com/
- https://temp-mail.org
- https://incognitomail.co/

(yopmail semble dorénavent bloqué par proton)
Vous pouvez tapez "anonymous mail inbox service" sur votre moteur de recherche pour en chercher d'autres

Notez que ce qui vaut pour les données de récupérations de compte vaut aussi pour les autres "métadonnées" non chiffrées, comme votre carte bleue (si vous voulez payer une version plus avancées que la version gratuite standard de Proton).

La majorité des données demeure chiffré

Notez que la majorité de vos données, à savoir vos échanges de mails et leurs contenus, reste chiffré (à l'exception de l'objet de l'email).
Les données de récupération ne le sont pas car elles doivent pouvoir être utilisées pour récupérer votre compte.
C'est justement le fait que ces dernières ne soient pas chiffrées, qui les rend de fait accessibles aux forces de l'ordre si ces dernières menaient une enquête à votre encontre, d'où la nécessité de ne

pas y mettre d'information relative à votre identité officielle.

Attention concernant Proton VPN

L'interêt d'un VPN comme Proton VPN est, comme expliqué dans les autres documents, de protéger votre connexion et votre adresse IP.

L'entreprise Proton a déjà accepté de livrer aux forces de l'ordre l'adresse IP de la personne qui se connectait à une adresse mail Proton, permettant à la police de retrouver cette personne.

Si vous utilisez un VPN, y compris lorsque vous vous connectez sur votre compte Proton mail, cela devrait en théorie vous protéger, SAUF si vous utilisez Proton VPN, sur le même compte que votre Proton Mail, dans ce cas, rien n'empêche l'entreprise Proton, de vous retrouver et de donner votre vrai IP aux renseignements, car ils ont à la fois accès aux connexions de la boite mail et aux connexions du VPN.

Pour évitez cela, quand vous vous connectez sur votre Proton mail, utilisez :

- Soit le navigateur Tor
- Soit un VPN autre que Proton VPN
- Soit Proton VPN, mais sur un compte différent de votre boite mail.

Révision #11
Créé 22 février 2025 19:09:25 par mollusque
Mis à jour 15 juillet 2025 18:05:58 par Guest