Image not found or type unknown

Outils alternatifs : Réseaux et communications [activité tactique]

activ_tact_FR.png
Image not found or type unknown

Ceci est une activité pratique qui vise à guider des personnes ou des groupes dans l’utilisation d’outils alternatifs aux options propriétaires « gratuites ».

Cette activité est beaucoup plus efficace lorsque les participant·e·s font partie d’un même réseau, car iels peuvent déjà commencer à utiliser des nouvelles façons de communiquer ensemble.

Cette activité se concentre sur trois outils de communications couramment utilisés : les courriels, les applications de messagerie/chat et les alternatives à Google docs.

Objectif d’apprentissage

- Élaborer des stratégies pour créer des espaces en ligne sûrs pour elleux-mêmes et leurs réseaux.

À qui s’adresse cette activité ?

Cette activité s’adresse à des participant·e·s ayant différents niveaux d’habiletés avec les outils en ligne.

Temps requis

Vous aurez probablement besoin de 5 heures pour compléter cette activité.

Matériel

- Une connexion internet
- Des ordinateurs portables
- Des téléphones mobiles
- Un projecteur

Mécanique

L’objectif de cette activité est d’encourager vos participant·e·s à être moins dépendant·e·s des options commerciales qui compromettent la vie privée et la sécurité des utilisateurs·trices.

Protonmail (courriel)

Pourquoi Protonmail ?

- Non-commercial
- Hébergé en Suisse où la protection des données est forte
- Fortes politiques de confidentialité des données des utilisateurs·trices
- Offre le chiffrement de bout-en-bout par défaut (tout dépendant de votre groupe, vous aurez peut-être besoin d’expliquer cette notion). Par défaut, Protonmail utilise le chiffrement « au repos ». Les courriels sont stockés et chiffrés sur leurs serveurs – ce qui veut dire que les propriétaires de Protonmail ne peuvent pas lire vos courriels. (Ceci est différent du modèle Google où on utilise seulement le chiffrement « en transit ». Dans ce modèle, les messages sont chiffrés au moment où ils sont envoyés, mais lorsqu’ils arrivent sur leurs serveurs, ils ont les moyens de « dé-bloquer » vos courriels.) Vous aurez peut-être besoin d’expliquer la différence entre HTTPS et GPG.
- Permet aux utilisateurs·trices d’envoyer des courriels protégés par mot de passe entre différents fournisseurs de courriel (c’est-à-dire qu’un·e utilisateur·trice Proton peut envoyer des courriels protégés par mot de passe à un·e utilisateur·trice Gmail, et en utilisant ce même message cela permet de renvoyer un courriel protégé par mot de passe)

- Vous pouvez choisir une option d'autodestruction de vos messages (pour vos communications les plus sensibles)
- Le GPG est intégré à Protonmail, donc si vous cherchez à étendre la formation au chiffrement GPG, c'est un bon outil pour commencer.

Limites de Protonmail

- Les comptes gratuits ont un espace de stockage de 500 Mo. Pour du stockage de 5 Go et plus, les utilisateurs·trices doivent payer : https://proton.me/pricing

Pour se créer un compte gratuitement : https://proton.me/fr

> **Remarques** : Si vous utilisez la même connexion internet (comme c'est le cas dans un atelier de formation), il se peut que Protonmail n'autorise pas la création de plusieurs comptes sur une même adresse IP. Ceci pourrait ralentir votre atelier. Le fait de disposer de plusieurs points d'accès (avec des adresses IP différentes) permettra d'atténuer ce problème.

> **Alerte jargon** : Tout ceci contient beaucoup de jargons. Pour cet atelier, assurez-vous d'établir une façon pour les participant·e·s de vous arrêter quand des concepts sont à clarifier ou incompris. Cela peut être tout simplement de les inviter à lever la main à tout moment s'il y a des choses qu'iels ne comprennent pas. Vous pouvez aussi leur demander directement s'iels connaissent ces termes techniques.

Signal (messagerie)

Pourquoi Signal ?

- Géré et possédé par des militant·e·s geek indépendant·e·s
- Offre le chiffrement de bout-en-bout
- Les protocoles de chiffrement utilisés par Whatsapp sont basés sur ceux de Signal. Contrairement à Whatsapp, Signal n'appartient pas à Facebook alors les communications et les utilisateurs·trices sont plus en sécurité.

- Les messages sur Signal sont seulement stockés sur leurs serveurs jusqu'à ce qu'ils soient reçus par un appareil (mobile ou un ordinateur). Une fois reçu, le message est uniquement stocké sur l'appareil qui l'a envoyé et sur celui qui l'a reçu.

Limites de Signal

- Parfois lent
- L'interface est plutôt de base
- Il faut avoir un numéro de téléphone mobile pour l'utiliser – Ceci peut être un problème dans les contextes où il y a un registre des numéros de téléphone mobile.
- Sur Signal, les messages ne sont pas synchronisés. Ainsi, même si vous utilisez Signal sur votre téléphone et sur votre ordinateur avec le même compte, les messages seront uniquement stockés dans l'appareil qui reçoit le message en premier. Cela fait partie de ce qui rend Signal sécuritaire.

Vous pouvez télécharger Signal sur le Google Play Story ou sur l'App Store.

Tâches pour l'atelier pratique avec Signal

1. Téléchargez l'application.
2. Créez-vous un compte (vous devez avoir un numéro de téléphone mobile).
3. Synchronisez vos contacts.
4. Vous pouvez faire de Signal votre application de messagerie principale, en incluant les SMS. Ceci veut dire que ces messages seront stockés sur votre téléphone qui est chiffré. Signal ne va PAS chiffrer vos envois de SMS.
5. Protégez votre application Signal par mot de passe. Paramètres > Confidentialité > Verrouillage de l'écran.
6. Empêcher les captures d'écran dans l'appli. Paramètres > Confidentialité > Sécurité de l'écran.
7. Vérifiez les identités sur Signal. Tout le monde se partage son numéro Signal dans le groupe. Lorsque vous avez ajouté les autres à vos Contacts, cliquez sur l'un deux et déroulez pour « Voir le numéro de sécurité » et cliquez sur « Vérifier ». Les deux utilisateurs·trices devront scanner des codes QR pour vérifier leurs identités.

    - Cela signifie que si jamais ce contact change de téléphone, vous devrez revérifier son identité sur Signal. Il s'agit d'un niveau de sécurité supplémentaire

pour s’assurer que vous savez à qui vous parlez, et si cette personne n’est plus vérifiée, vous devriez probablement prendre des mesures et être plus prudent·e dans vos messages avec cette personne.

8. Si nécessaire, créez un groupe de discussion Signal.

Riseup Pad / Ethercalc (alternatives à Google Docs)

Pourquoi ?

- Aucune inscription nécessaire pour utiliser ces services.
- Interface simple et légère (utile pour les communautés avec une connexion lente)
- Permet l’anonymat
- Vous contrôlez la durée de stockage du pad ou du tableau

Limites

- Mise en page simple
- On ne peut pas faire de tableaux sur les pads
- L’édition sur Ethercalc n’est pas comme dans Excel

Pour créer un pad : https://pad.riseup.net/

Pour créer une feuille de calcul : https://ethercalc.org

Framapad est une autre option (interface en français) pour créer des pads : https://framapad.org/fr/

Framacalc est aussi une option intéressante pour les feuilles de calcul : https://accueil.framacalc.org/fr/

À prendre en considération pour une utilisation sécuritaire des pads

- Assurez-vous de mettre à jour vos pads puisque certains auront des dates d'expiration et seront supprimés automatiquement s'ils ne sont pas mis à jour.
- Vous pouvez protéger vos pads avec un mot de passe.
- Assurez-vous d'envoyer les liens des pads (et les mots de passe, si c'est le cas) en utilisant des canaux de communication sécurisés.

Jit.si (visioconférence)

Pourquoi Jitsi ?

- Permet de créer des salles de discussion temporaires (aucun compte nécessaire)
- Beaucoup plus difficile de trouver une salle de discussion Jitsi en temps réel (puisqu'elles sont temporaires)
- Aucune application n'est nécessaire sur ordinateur. C'est accessible directement dans le navigateur.
- Le chiffrement de bout-en-bout est assuré.

Limites

- La connexion pour les salles avec plus de 10 personnes est instable et peu fiable

Tâches pour l'atelier pratique avec Jitsi

- Créez une salle sur Jitsi https://meet.jit.si/.
- Partagez le lien avec les participant·e·s.
- Les personnes qui veulent utiliser l'application mobile peuvent la télécharger et y saisir le nom de la salle.
- Tester l'audio, la vidéo et les autres fonctionnalités de l'application.

> **Conseils pour l'animation :** Avant de faire cet atelier, pratiquez-vous à utiliser/installer ces outils, car les étapes peuvent avoir changé.

Ressources supplémentaires

Alternative To est un site qui rassemble des listes et des évaluations d'outils alternatifs (comme des plateformes, des logiciels, des applications). Les outils sont notés et catégorisés en fonction de leurs options de sécurité. C'est une excellente ressource pour trouver des alternatives aux outils populaires.

Pour une ressource en français, vous pouvez utiliser l'annuaire du Libre de Framalibre qui rassemble aussi une liste de logiciels et outils alternatifs : https://framalibre.org/alternatives

Après avoir trouvé un outil alternatif, confirmez ses caractéristiques de sécurité et de vie privée en effectuant une recherche avec les termes suivants :

- Nom du logiciel + enjeux de sécurité
- Nom du logiciel + politique de confidentialité
- Nom du logiciel + vie privée
- Nom du logiciel + évaluation de la sécurité



Revision #4
Created 26 April 2023 00:58:26 by Kira
Updated 28 June 2023 20:22:05 by Kira