Créer des espaces sûrs en ligne

Pour favoriser l’apprentissage et renforcer les capacités en matière de création d’espaces sûrs en ligne, en particulier pour les groupes et les personnes à risque.

Introduction et objectifs d'apprentissage

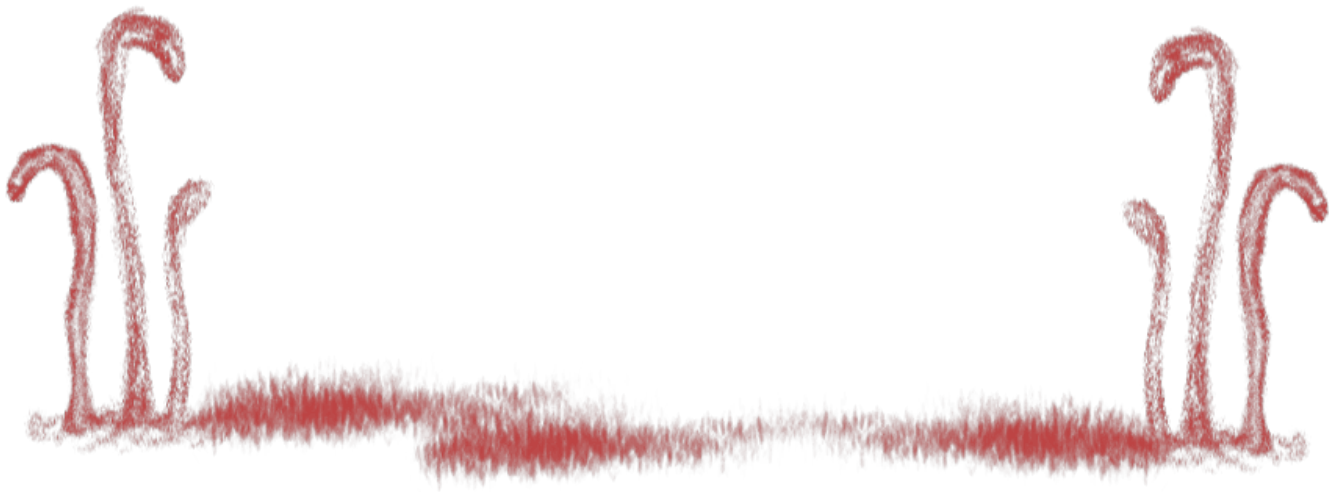
espaces-surs_FR.png
Image not found or type unknown

Ce module vise à faciliter l’apprentissage et à renforcer les capacités en matière de création d’espaces sûrs en ligne, en particulier pour les groupes et les personnes à risque. Grâce à ce module, vous pouvez explorer, par le biais d’activités et de discussions, les facteurs qui exercent une influence sur la capacité de créer des espaces où les militant·e·s des droits sexuels, les militant·e·s féministes et leurs communautés peuvent se sentir en sécurité. Notre tâche est d’explorer la signification de tels espaces pour les militant·e·s féministes et militant·e·s des droits sexuels.

Objectifs d’apprentissage

À la fin de ce module, les participant·e·s pourront :

- Définir ce qu'iels entendent par espace en ligne sûr / privé.
- Élaborer des stratégies pour créer des espaces en ligne sûrs pour elleux-mêmes et leurs réseaux.
- Développer leurs connaissances des questions de confidentialité et de la manière dont celle-ci touche les femmes et leur vie.
- Comprendre les limites de la plupart des réseaux sociaux en matière de confidentialité.



Activités et parcours d'apprentissage

> **Cette page est essentielle** à la bonne utilisation et compréhension de ce module. En suivant les parcours d'apprentissage, cela permet aux participant·e·s de mieux appréhender les sujets étudiés.

Parcours d'apprentissage

Nous vous suggérons de commencer ce module par l'une de ces activités d'introduction : Espace « sûr/safe » : Exercice d'analyse et visualisation, La bulle, ou Imagine ton espace rêvé sur Internet **pour permettre aux participant·e·s de commencer à explorer les concepts.** Si vous voulez être plus spécifique, il existe des activités d'introduction sur le consentement et la confidentialité (Réseau social de partage de photos), le stockage en nuage et la confidentialité des données (Le nuage), et sur le consentement et les autorisations sur nos appareils (Visualisation + discussion : Paramètres et autorisations). Selon les objectifs de votre groupe, celles-ci pourront aider votre groupe à **se familiariser avec les concepts de sécurité et de confidentialité.**

Vous pouvez utiliser Imagine ton espace rêvé sur Internet pour travailler avec un groupe qui a besoin de redéfinir les paramètres de sécurité et de confidentialité d'un espace en ligne existant ou en concevoir un nouveau en prenant en compte ces paramètres.

Travaillez ensuite avec le groupe la compréhension des concepts en passant aux **activités d'approfondissement.**

- L'activité "Règles" de sécurité en ligne explique aux participant·e·s comment protéger leurs espaces en ligne, et elle permet également de clarifier les principes de base de la sécurité en ligne.
- Confidentialité, consentement et sécurité est une activité plutôt de type exposé participatif permettant de clarifier et d'approfondir les concepts.

Les activités tactiques sont des séances pratiques.

- Rendre les espaces en ligne plus sûrs est une activité visant à faire des espaces rêvés une réalité, notamment en relevant les défis actuels de conception de politique des espaces

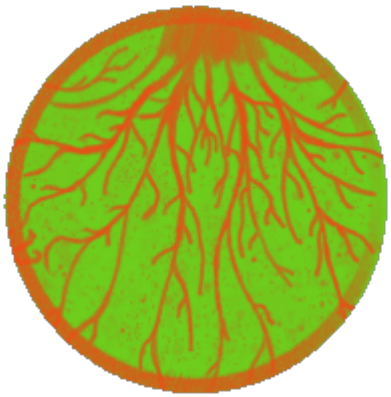
en ligne se trouvant en contradiction avec la vision des espaces rêvés. Si vous souhaitez familiariser les participant·e·s aux services en ligne, cette activité est utile pour analyser les paramètres, les règles et les normes des espaces. Il ne s’agit pas d’un guide étape par étape visant à ajuster les paramètres car ceux-ci changent trop souvent.

- L’activité Outils alternatifs : Réseaux et communications est pertinente pour les participant·e·s qui souhaitent commencer à s'éloigner des plateformes et des outils propriétaires, commerciaux et moins sûrs.

Activités d’introduction

- Espace « sûr/safe » : Exercice d’analyse et visualisation
- La bulle - exercice de visualisation
- Imagine ton espace rêvé sur Internet
- Réseau social de partage de photos
- Le nuage
- Visualisation + discussion : Paramètres et autorisations

Activités d'approfondissement



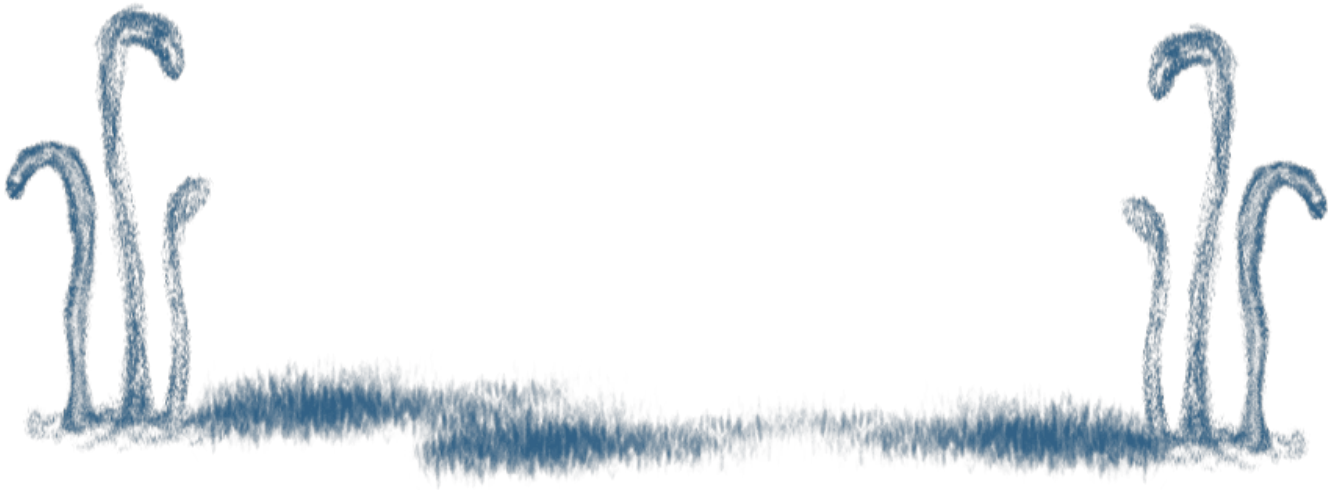
- Information + activité : Confidentialité, consentement et sécurité
- Information + activité : "Règles" de sécurité en ligne

Activités tactiques

- Rendre les espaces en ligne plus sûrs
- Outils alternatifs : Réseaux et communications

Ressources | Liens | Lectures

- Présentation de Jac sur les médias sociaux (anglais seulement)



Espace « sûr/safe » : Exercice d’analyse et visualisation [activité d'introduction]

Le but principal de cet exercice de visualisation est de permettre aux participant·e·s d'exprimer leurs propres définitions et de rechercher une compréhension commune de ce que serait un espace « sûr » ou un « safe space ».

ativ-intro_FR.png
Image not found or type unknown

Il s'agit d'un exercice de visualisation. Le but principal de l'exercice est de permettre aux participant·e·s d'exprimer leurs propres définitions et de rechercher une compréhension commune de ce que serait un espace « sûr » ou un « safe space ». Ce premier exercice pourra aider un groupe de personnes à concevoir ensemble de nouveaux espaces sûrs en ligne ou à redessiner un espace existant sur la base de valeurs communes en la matière.

Cette activité peut aussi nous aider à briser la glace et à fonder nos idées concernant la sécurité des espaces en ligne sur notre expérience vécue des espaces physiques dits « sûrs » ou « sécuritaires ».

Cette activité comporte trois étapes :

- Visualisation individuelle de la ligne du temps, en mots ou en dessin
- Discussion en petits groupes autour du terme « Sûr/Safe »
- Réflexion collective exhaustive visant à identifier et débattre des définitions communes et divergentes au sein du groupe concernant la notion d’espace « Sûr/Safe »

Suite à cette activité, il est fortement conseillé de faire celle-ci : Information + activité : Confidentialité, consentement et sécurité.

Objectifs d'apprentissage

- Définir ce que les participant·e·s entendent par espace en ligne sûr/privé.

À qui s'adresse cette activité ?

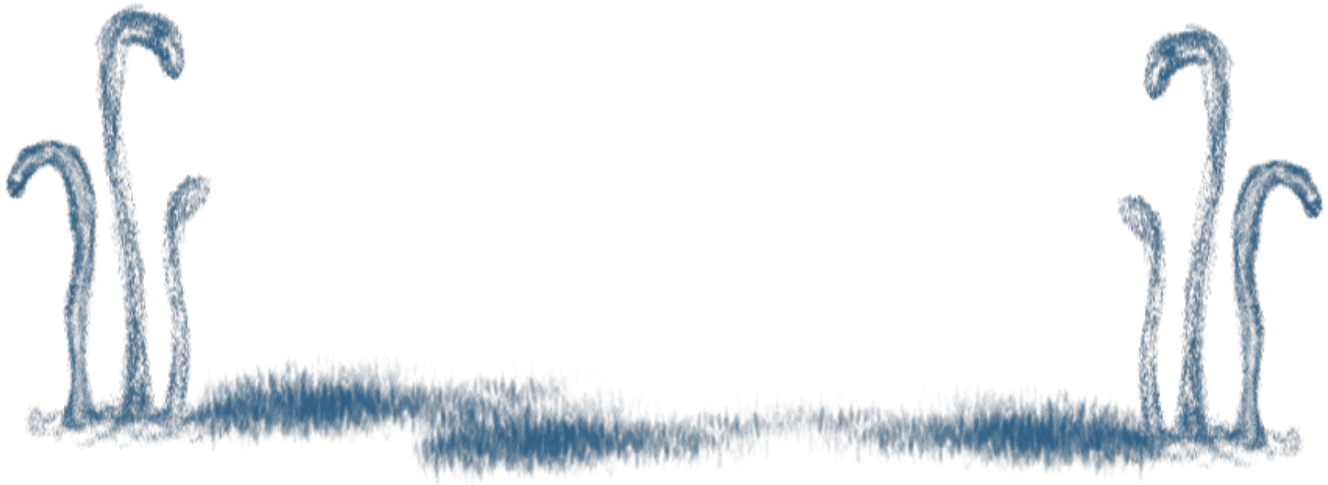
Cette activité peut être menée auprès de participant·e·s possédant différents niveaux d'expérience concernant à la fois les espaces en ligne et l’aménagement/la création d'espaces dits « sûrs ».

Temps requis

Cette activité prendra environ **40 minutes.**

Matériel

- Tableau à feuilles mobiles
- Marqueurs
- Papier à dessin



Mécanique

Visualisation individuelle - 10 minutes

Demandez aux participant·e·s de fermer les yeux et de retrouver une circonstance, un lieu ou un moment précis où iels se sont senti·e·s le plus en sécurité ou le plus « Safe ». Encouragez-les à être précis·e·s dans leur visualisation - non pas en termes de lieu/date/circonstance, mais en ce qui concerne les facteurs qui ont joué sur leur sentiment de sécurité. Le lieu, moment ou circonstance

peuvent être imaginaires.

Option: Dessin

Vous pouvez également demander aux participant·e·s de visualiser et de dessiner le lieu, le moment et la circonstance dans lesquels iels se sont senti·e·s le plus « Safe », en représentant également les éléments et facteurs qui leur ont inspiré ce sentiment.

Discussion en petits groupes - 15 minutes

En petits groupes de trois à cinq personnes, demandez aux participant·e·s d'échanger autour de ce qu'iels ont visualisé.

> **Observation :** si l'atelier ne réunit que six participant·e·s ou moins, vous pouvez animer les deux étapes de discussion avec l'ensemble du groupe. Le recours aux petits groupes a pour but de s'assurer que chaque participant·e aura le temps d'exposer sa propre visualisation.

Groupe complet - 15 minutes

Pour traiter la question, écrivez « SÛR » ou « SAFE » au centre d'une feuille de papier et faites une « carte conceptuelle » des réponses à la question suivante : « Qu'est-ce qui, dans ce lieu, moment ou circonstance, vous a donné un sentiment de sécurité ? ».

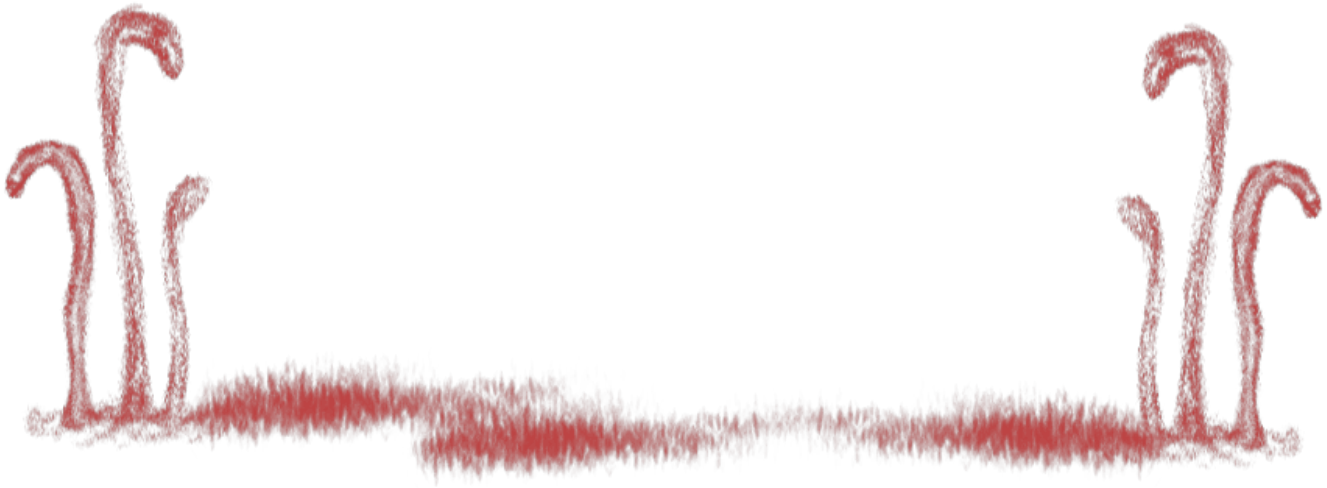
À la fin de l'exercice, vous aurez dressé une liste de mots, de phrases et de concepts associés à la notion de « sécurité ».

Conseils pour l'animation de l'atelier

- Relever les points communs et interroger les divergences surgies des réponses
- Relever et mettre l'accent sur les facteurs susceptibles de s'appliquer aux espaces virtuels, ou en rapport avec les notions élémentaires susmentionnées
- Faire systématiquement la synthèse des principaux enseignements tirés de l'activité pour renforcer les concepts

Suggestion

- En plus du tableau à feuilles mobiles, vous pouvez, pour dresser la carte conceptuelle du mot « SÛR » ou « SAFE », demander à un·e co-animateur/animatrice de noter les mots et les concepts évoqués par les participant·e·s dans un document .txt ou .docx afin de créer, à la fin du débat, un nuage de mots à l'aide d'un générateur de nuage de mots qui permettra aux participant·e·s de visualiser graphiquement les mots associés à « SÛR » ou « SAFE ».



La bulle - exercice de visualisation [activité d'introduction]

activ-intro_FR.png
Image not found or type unknown

Le but de cet exercice de visualisation est de susciter une discussion à propos de la vie privée. L'exercice permet également à la personne formatrice et aux participant·e·s de comprendre les différentes inquiétudes au sein du groupe concernant la vie privée.

Cette activité ne vise pas à approfondir les connaissances sur la vie privée, mais plutôt à amener les participant·e·s à réfléchir sur leurs conceptions personnelles de la vie privée.

Cette activité devrait être jumelée avec Rendre les espaces en ligne plus sûrs ou Information + activité : Confidentialité, consentement et sécurité.

Objectif d'apprentissage

- Développer une compréhension des enjeux de vie privée et de la manière dont celle-ci touche les femmes et leur vie.

À qui s'adresse cette activité ?

Cette activité peut être faite avec des participant·e·s ayant un niveau varié d'expérience quant aux enjeux de vie privée en ligne et hors ligne.

Temps requis

Vous aurez besoin d'**environ 40 minutes** pour cette activité.

Matériel

- Tableau à feuilles mobiles
- Marqueurs/feutres
- Des petits post-it

Mécanique

Pour cet exercice de visualisation, les participant·e·s auront des grandes feuilles de papier (du tableau à feuilles mobiles) et des marqueurs pour dessiner.

Visualisation individuelle - 30 minutes

Si vous êtes à l'aise de le faire, fermez vos yeux. Imaginez un point brillant. Est-ce qu'il est immobile ? Est-ce qu'il bouge ? Comment bouge votre point brillant ?

Maintenant, imaginez un cercle autour du point. Et maintenant, imaginez qu'ils bougent ensemble. Le point reste toujours au centre du cercle. Vous êtes ces deux choses : le point étant vous-même, et le cercle étant vos limites. Comment vous sentez-vous dans ce cercle ? Ceci est une visualisation de vous-même entouré·e de vos limites qui vous font sentir en sécurité.

Maintenant, demandez aux participant·e·s de dessiner un avatar d'elleux-mêmes dans un cercle au centre de leur feuille. Le cercle représente leur bulle personnelle de vie privée.

Il y a des choses à l'intérieur et à l'extérieur de cette bulle.

Invitez ensuite les participant·e·s à écrire sur des post-it (un élément par post-it) les choses les plus privées pour elleux ainsi que les personnes avec qui iels partagent ces éléments personnels. Ces post-it sont placés dans la bulle. Puis, invitez-les à placer les éléments publics en dehors de leur bulle.

Voici des exemples de ces choses :

- les gens avec qui iels partagent des choses
- leurs informations personnelles
- leurs sentiments et émotions
- leurs activités

Voici un exemple de ce à quoi cela pourrait ressembler :

LaBulle-Exemple1.png
Image not found or type unknown

Après avoir fait leur premier cercle, demandez-leur d'en dessiner un deuxième et de ré-organiser leurs post-it en fonction des niveaux de partage d'informations qu'iels souhaitent avoir avec ces différentes personnes.

Cela pourrait ressembler à ceci :

LaBulle-Exemple2.png
Image not found or type unknown

Puis, demandez-leur de dessiner un nouveau cercle, plus près de leur avatar et d'y mettre les choses qu'iels ne partageraient avec personne.

LaBulle-Exemple3.png
Image not found or type unknown

Débriefing en grand groupe - 25 minutes

Pour faire un retour sur l'activité, questionnez les participant·e·s sur les réflexions/observations qu'iels ont eu en dessinant leur bulle.

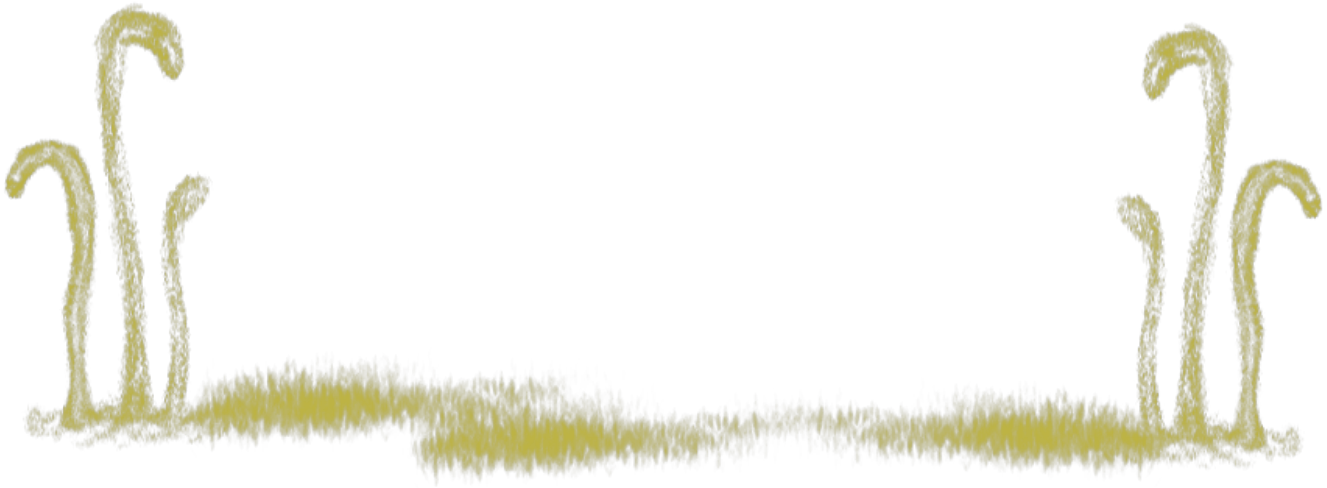
Demandez-leur comment iels ont décidé de mettre certaines choses à l'intérieur ou à l'extérieur de la bulle. Questionnez-les aussi sur la proximité qu'iels partagent avec les choses en dehors de leurs bulles.

Amenez-les à réfléchir sur la façon dont leurs bulles représentent la création d'espaces sûrs (en ligne et hors ligne) pour elleux-mêmes.

Voici quelques questions-guides pour ce retour en groupe :

- Comment avez-vous regroupé les personnes et les choses à l'intérieur et à l'extérieur de votre bulle ?
- Avez-vous senti le besoin d'avoir plus que 3 bulles ? Pourquoi ?
- Quelles ont été vos réflexions entourant vos responsabilités, vos émotions/sentiments, et les choses que vous voulez exprimer ? Y avait-il une différence entre ces éléments ? Est-ce qu'on peut voir cette différence dans vos dessins de bulles ?
- Est-ce que vous avez déjà été forcé·e de sortir une personne/une émotion/un problème de votre bulle ? Comment cela s'est-il produit ? Comment avez-vous fait face à cette situation ? Avez-vous été capables de remettre ces choses dans votre bulle ?
- Dans votre dessin de bulles, quelles sont les choses sur lesquelles vous communiquez en ligne ? Et avec quelles personnes communiquez-vous dans les espaces en ligne ? Discutez.

> **Conseil d'animation:** Ne faites pas de commentaires sur les bulles des participant·e·s ni sur la disposition des informations/sentiments/pensées dans leur dessin. Encouragez les autres participant·e·s à faire de même. Des petites choses comme exprimer de la surprise, hausser les sourcils ou rire lorsqu'une personne présente sa bulle minent la création d'un environnement sûr pour les participant·e·s.



Imagine ton espace rêvé sur internet [activité d'introduction]

À l’occasion de cette activité, les participant·e·s examineront les éléments caractéristiques d’un espace en ligne favorable à l’épanouissement de leur communauté. Selon les objectifs du groupe et de l'atelier, les animateurs/animatrices peuvent inviter les participant·e·s à examiner les façons d'exister et d’agir en ligne.

ativ-intro_FR.png
Image not found or type unknown

À l’occasion de cette activité, les participant·e·s examineront les éléments caractéristiques d’un espace en ligne favorable à l’épanouissement de leur communauté. Selon les objectifs du groupe et de l'atelier, les animateurs/animatrices peuvent inviter les participant·e·s à examiner les façons d'exister et d’agir en ligne.

Cet exercice de visualisation peut déboucher sur un débat autour des espaces en ligne fréquentés par les participant·e·s ainsi que sur les possibilités et les limites de ces plateformes par rapport à l’espace idéal qu’iels imaginent.

Objectif d'apprentissage

- Élaborer des stratégies pour créer des espaces en ligne sûrs pour les participant·e·s et leurs réseaux.

À qui s'adresse cette activité ?

Cette activité s'adresse aux personnes qui fréquentent les espaces en ligne. Elle peut aider des groupes à réaménager des espaces en ligne qui, en l’état actuel, ne les desservent pas, ou à en créer de nouveaux.

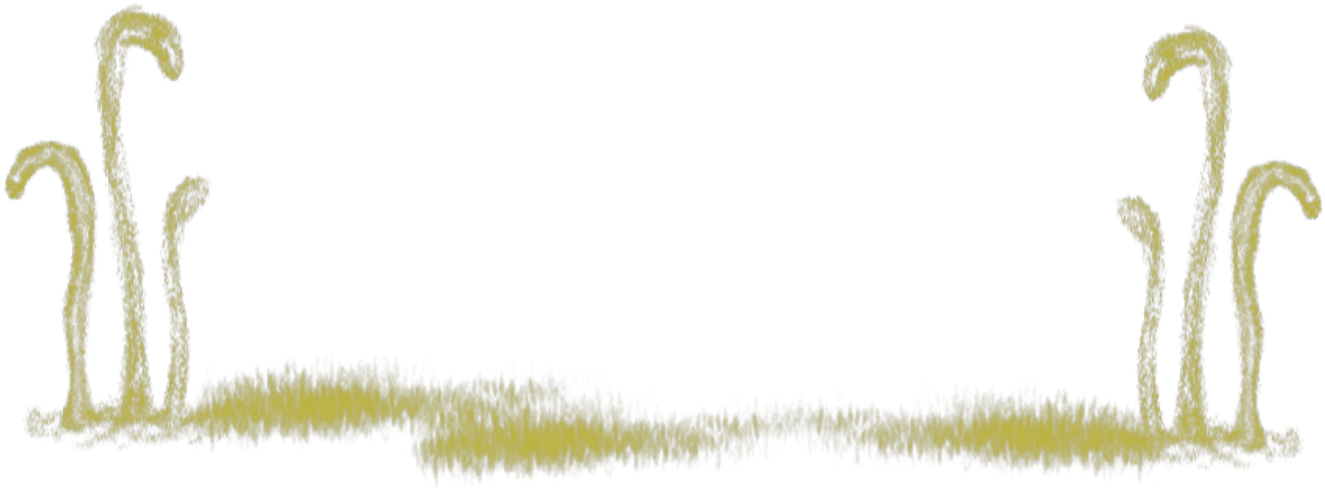
Temps requis

Durée totale suggérée pour un atelier standard de 12 à 15 participant·e·s : **2.5 heures**

- Débat autour des questions suivantes : « Pourquoi sommes-nous présent·e·s en ligne ? » « Pourquoi est-ce important pour nous ? » : 30 minutes
- Travail de groupe : 45 minutes
- Présentations (4-5 groupes de 5-6 minutes chacun) : 30 minutes
- Débriefing et débat en plénière : 45 minutes

Matériel

- Tableau à feuilles mobiles
- Marqueurs



Mécanique

Discussion : Pourquoi sommes-nous présent·e·s en ligne ? Pourquoi est-ce important pour nous ?

Comme il s’agit d’examiner les nombreuses raisons pour lesquelles Internet peut menacer notre sécurité ou notre vie privée, il est nécessaire de situer le débat autour de ce qui motive les participant·e·s à être présent·e·s en ligne. Si vous connaissez déjà le groupe, vous pouvez partir de ses propres activités en ligne. Si vous le connaissez moins bien, demandez aux participant·e·s de

donner des exemples de ce qu'iels font en ligne et qu’iels considèrent important.

Ouvrez un espace de discussion concernant les différentes facettes de la vie des gens.

Quelques questions qui permettront d’orienter les discussions :

- Quels espaces fréquentez-vous en ligne ? Pour y faire quoi ?
- Quelles sont les limites des espaces que vous fréquentez ? Examinez le cas de chaque plateforme concernée.
- Des incidents vous ont-ils donné un sentiment d’insécurité dans les espaces que vous fréquentez ? Encore une fois, abordez cette question par plateforme/outil.
- Associez-vous des espaces en ligne distincts aux différentes facettes de votre vie ? Expliquez. Comment choisissez-vous d’associer tel ou tel espace à tel ou tel aspect de votre vie ?

> **Conseil pour l’animation de l’atelier :** Rappelez que l’espace de leurs rêves sur Internet est destiné au travail personnel, politique/militant. Ainsi, selon les réponses des participant·e·s aux questions ci-dessus, mettez-les au défi de réfléchir à leur propre travail personnel et militant ainsi qu’à leur utilisation d’Internet.

Prenez en note les points importants soulevés lors du débat.

Activité en petit groupe

Tout en gardant les résultats du débat à l'esprit, formez des petits groupes (de 3 à 5 participant·e·s) et demandez-leur de développer leur espace rêvé sur Internet.

Profitez des discussions en petits groupes pour demander aux participant·e·s de réfléchir et répondre aux questions suivantes :

- Comment s’appelle cet espace en ligne de vos rêves ?
- Pourquoi cet espace est-il important ?
- À qui s’adresse-t-il ? À qui est-il fermé ? Comment s’en assurer ?
- Que font les gens dans cet espace ?
- Quelles en sont les règles ?
- Qui peut y venir (ou pas) ?
- À quoi ressemblera cet espace ?
- Comment les personnes se retrouveront-elles dans cet espace ?
- De quels sujets pourra-t-on y parler (ou pas) ?
- Qui est responsable de l’administration de cet espace ?

Demandez aux groupes de dessiner cet espace de la façon la plus imaginative possible et demandez-leur de préparer une présentation créative à l’intention de l’ensemble des participant·e·s.

Échanges autour des présentations

Pour l’analyse des présentations, encouragez les autres participant·e·s à demander des éclaircissements et à dresser une liste des questions les plus stratégiques/éthiques/significatives et de les garder à l’esprit jusqu'à ce que chaque groupe ait présenté ses idées.

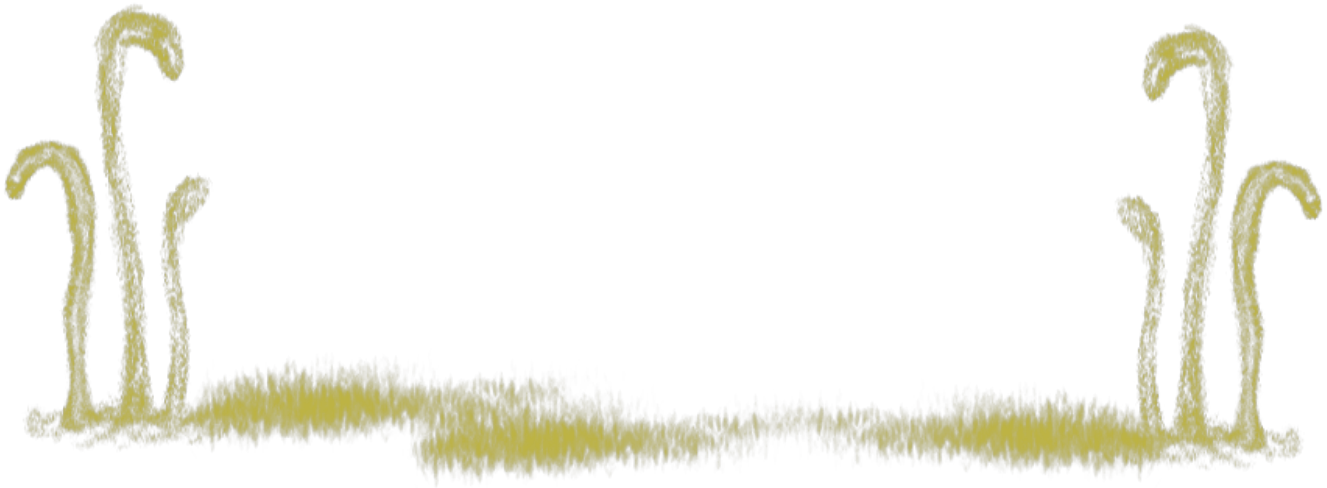
Débriefing

En conclusion de cette activité, discutez de ce qui suit :

- Quels sont les éléments essentiels à prendre en compte lors de la conception d'espaces « sûrs » ? (reprenez les idées échangées à l’étape précédente)
- « Sûrs », oui, mais pour qui ? Nous-mêmes, mais nous faisons aussi partie d’autres groupes. Quels sont potentiellement les moments où nous devons veiller à notre propre sécurité et à celle des autres et inversement ? (référence : Information + Activité : "Règles" de sécurité en ligne).
- Quelles sont les limites de cet espace en ligne ? Un espace peut-il être totalement « sûr » ? Qu'est-ce qui pourrait fragiliser cette sécurité ?
- Après avoir compris le point 3, réfléchir aux questions suivantes : qui contrôle et façonne les espaces en ligne ? Comment ces espaces fonctionnent-ils, comment s’intègrent-ils à d’autres espaces (continuité des espaces en ligne et hors ligne) ? Si ces espaces sont importants pour nous, comment pouvons-nous les utiliser stratégiquement et les concevoir de façon plus consciente au service de notre activisme ?

Conseils d’animation

1. Posez des questions sur d'autres aspects de l’aménagement d’espaces en ligne « sûrs » :
    1. Qui menace la sécurité de cet espace ? La menace est-elle interne et/ou externe ? Comment protéger cet espace ?
    2. Où sont hébergés les espaces ? (Les lois et règlements nationaux peuvent avoir un impact sur l’existence même de ces espaces et les suites éventuelles en cas d'utilisation abusive.)
    3. Faut-il tenir compte de certaines considérations juridiques pour créer un espace de cette nature pour le groupe cible ?
    4. Quelles sont les responsabilités et les obligations des plateformes et réseaux sociaux lorsque les choses tournent mal ? Que sont réellement ces plateformes ? Que devraient-elles être ? Consulter les Principes de Manille sur la responsabilité des intermédiaires.
    5. Quelles sont les règles internationales et nationales en matière de respect de la vie privée ? Quelles sont les considérations juridiques en matière de protection de la vie privée ?
2. Ces questions pourront mener directement à un exposé sur les principes de la sécurité en ligne ou à une conférence sur la protection de la vie privée sur les réseaux sociaux.



Réseau social de partage de photos [activité d'introduction]

activ-intro_FR.png
Image not found or type unknown

Cet exercice de visualisation a pour but d’amener les participant·e·s à penser aux notions de consentement en ligne, de confidentialité des données en passant par les autorisations et conditions générales d’utilisation des applications qu’iels utilisent.

Objectifs d’apprentissage

- Envisager une perspective féministe de l’espace numérique sur
  - le consentement valable et éclairé
  - le contrôle total des données et informations personnelles en ligne

À qui s’adresse cette activité ?

Cette activité peut être utilisée avec des participant·e·s ayant différents niveaux d’expérience en matière de consentement et de vie privée en ligne et hors ligne. Idéalement, les participant·e·s devraient avoir en main l’appareil qu’iels utilisent pour se connecter sur internet.

Temps requis

45 minutes

Matériel

- Tableau à feuilles mobiles avec le scénario écrit ou imprimé dessus
- Post-it
- Marqueurs/feutres

Mécanique

Dans cet exercice de visualisation, les participant·e·s auront besoin des post-it et marqueurs pour écrire.

Visualisation individuelle - 15 minutes

D’abord, lisez ce scénario écrit sur votre tableau à feuilles mobiles :

« Imaginons que vous ayez inventé ou que vous possédez un réseau social de partage de photos (comme Instagram). Vous faites de l’argent en offrant aux utilisateurs·trices de publiciser leurs contenus à des populations ciblées en fonction de l’âge, la localisation et les intérêts. Pour ce faire, vous devez avoir accès aux galeries photos des utilisateurs·trices. Quelles autorisations demanderiez-vous ? Et quelles seraient les informations que vous fourniriez dans les conditions générales d’utilisation ? »

Vous pourriez demander aux participant·e·s de réfléchir aux aspects suivants :

- Propriété et archivage des photos téléchargées
- Accès à la galerie photos des utilisateurs·trices
- Utilisation des données des utilisateurs·trices à des fins publicitaires

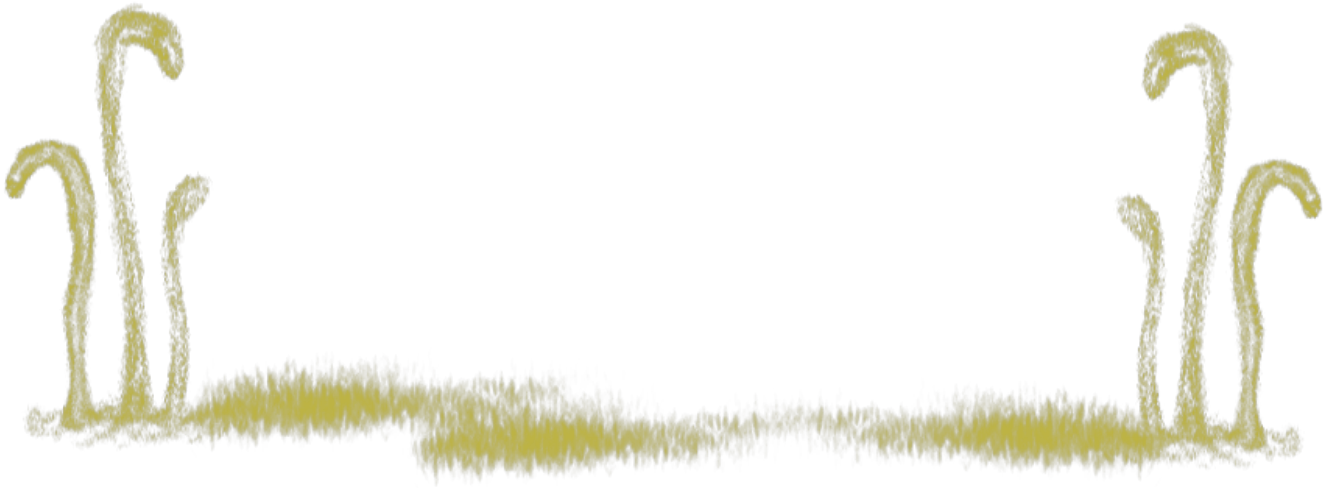
Débriefing en grand groupe - 25 minutes

Pour faire un retour sur l’activité, questionnez les participant·e·s sur les réflexions/observations qu’iels ont eu en écrivant leurs réponses.

Voici quelques questions-guides pour le débriefing :

- Quelles seraient les autorisations que vous demanderiez ?
- Avez-vous des idées de conditions générales d’utilisation que vous donneriez aux utilisateurs·trices ?
- Qui serait propriétaire des photos publiées ?
- Où les photos seraient-elles stockées ?
- Comment demanderiez-vous le consentement pour accéder à la galerie photos des utilisateurs·trices ?
- Comment utiliseriez-vous ces données à des fins publicitaires ?
- Pensez-vous qu’il y a un lien entre le fonctionnement du consentement en ligne et le consentement hors ligne ?

Vous pouvez ensuite revenir sur leurs réponses et en discuter avec le groupe.



Le nuage [activité d'introduction]

ativ-intro_FR.png
Image not found or type unknown

L’objectif de cet exercice de visualisation est de susciter une discussion entourant le stockage en nuage (sur le Cloud) et la confidentialité des données. Cette activité ne vise pas à approfondir les connaissances sur la vie privée, mais plutôt à amener les participant·e·s à réfléchir sur leurs conceptions personnelles de la vie privée sur le nuage/Cloud.

Objectifs d’apprentissage

- Envisager une perspective féministe de l’espace numérique sur le contrôle total des données et informations personnelles en ligne

À qui s’adresse cette activité ?

Cette activité peut être faite avec des participant·e·s ayant différents niveaux d’expérience quant aux enjeux de vie privée liés au nuage/Cloud.

Temps requis

45 minutes

Matériel

- Feuilles A4 pour dessiner
- Marqueurs/feutres

Mécanique

C’est un exercice de visualisation pour comprendre comment fonctionne le nuage. Donnez du papier et des marqueurs pour que les participant·e·s puissent dessiner.

Visualisation individuelle - 15 minutes

Demandez aux participant·e·s de visualiser le nuage en tant qu'espace physique et de le dessiner sur leur feuille. Vous pouvez les inviter à réfléchir aux questions suivantes :

- À quoi ressemble l'espace ?
- Qui contrôle l'espace ?
- Pouvez-vous voir ce qui se passe à l'intérieur ?
- Est-ce que vous (et votre communauté) pouvez vérifier/tester l'espace ?

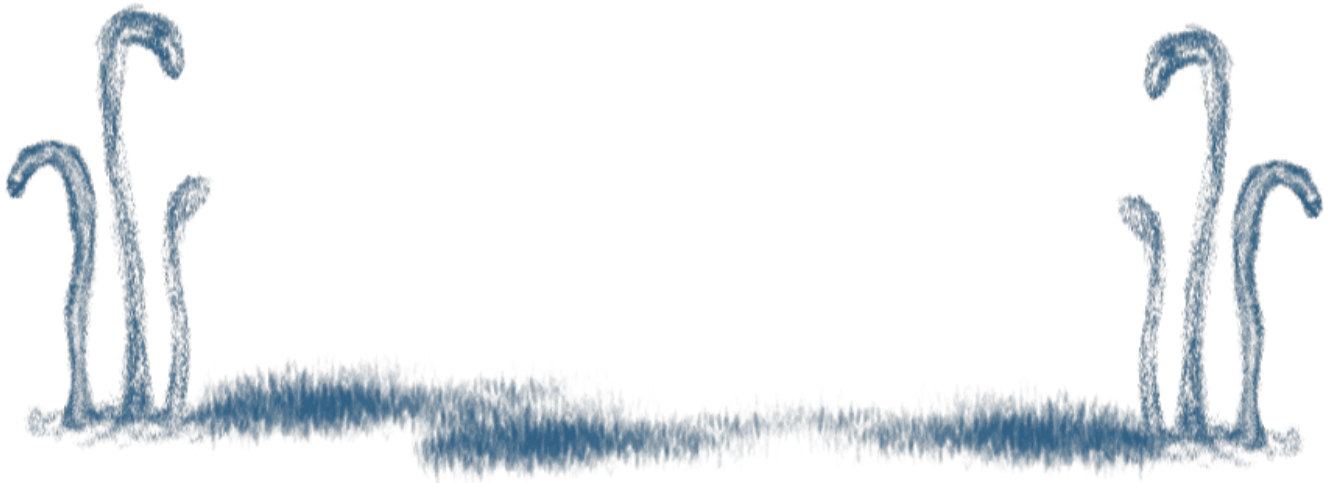
Débriefing en grand groupe - 25 minutes

Pour faire un retour sur l'activité, demandez aux participant·e·s quelles étaient leurs réflexions/observations au moment de dessiner leur nuage.

Voici quelques questions-guides pour le débriefing :

- Comment avez-vous imaginé et visualisé votre nuage ?
- Qui contrôlait l'entrée dans votre espace ?
- Est-ce que votre nuage est de type propriétaire ou open-source (à code source ouvert) ? Demandez-vous quelle proportion de l'espace vous est accessible.
- Quelle est la différence entre un espace de stockage en nuage propriétaire et open-source ?
- Qu'est-ce que vous préférez comme type de stockage en ligne ? Pourquoi ?

Vous pouvez ensuite revenir sur leurs réponses et en discuter avec le groupe.



Visualisation + discussion : Paramètres et autorisations [activité d'introduction]

Le but de cet exercice est de faciliter la discussion sur le consentement en ligne, les paramètres des appareils et les autorisations.

ativ_intro_FR.png
Image not found or type unknown

Il s'agit d'un exercice de visualisation et de discussion. Le but de cet exercice est de faciliter la discussion sur le consentement en ligne, les paramètres des appareils et les autorisations. Il peut également aider les participant·e·s à comprendre les différentes préoccupations concernant le consentement sur leurs appareils personnels.

Objectifs d'apprentissage

- Envisager une perspective féministe de l'espace numérique sur
  - le consentement valable / éclairé,
  - le contrôle total des données et informations personnelles en ligne,
- Apprendre des pratiques permettant de contrôler son avatar numérique.

À qui s'adresse cette activité ?

Cette activité peut être utilisée avec des participant·e·s ayant différents niveaux d'expérience en matière de consentement et de confidentialité en ligne et hors ligne, de préférence avec l’appareil qu’iels utilisent pour se connecter à Internet.

Temps requis

Cette activité prend environ 1h30.

Matériel

- Post-it pour écrire
- Feuilles de papier A4 vierges pour dessiner
- Marqueurs pour écrire et dessiner

Mécanique

Il s'agit d'un exercice de visualisation et de discussion. On distribue aux participant·e·s des post-it et des marqueurs pour écrire et dessiner.

Visualisation individuelle - 30 minutes

Tout d'abord, demandez aux participant·e·s quel appareil iels utilisent pour accéder à Internet (téléphones portables, tablettes, ordinateurs personnels, ordinateur de bureau au travail / à la maison / dans d'autres espaces publics, etc.). Demandez-leur ensuite de réfléchir et d'écrire sur les post-it les trois premières activités auxquelles iels ont consenti sur leur portable, quelles que soient les applications.

Ensuite, sur des feuilles de papier vierge, demandez-leur de dessiner leur portable. Demandez-leur ensuite d'identifier le système d'exploitation utilisé par leur appareil. Enfin, demandez-leur d'écrire (dans le dessin du portable) les 5 applications qu'iels utilisent le plus, de vérifier les autorisations accordées à ces applications et de les noter à côté de chacune des applications.

Discussion avec tout le groupe - 1 heure

Une fois que tous les participant·e·s ont visualisé ces détails, demandez-leur de parler ce qu'iels ont visualisé. Certaines applications (telles que WhatsApp, Facebook, Twitter, Google Maps, etc.) sont couramment utilisées par de nombreuses personnes, vous pouvez donc identifier des points

communs dans les réponses. Recherchez leurs points communs et questionnez leurs différences.

> **Remarque :** S'il y a plus de 6 participant·e·s, vous pouvez éventuellement créer de plus petits groupes de 6 chacun pour vous assurer que chaque participant·e a bien le temps de parler de ce qu'iel a visualisé.

Vous pouvez ensuite animer le débat avec quelques questions telles que :

- Quel appareil avez-vous dessiné ?
- Votre appareil se connecte-t-il à Internet ?
- Si votre appareil est un téléphone, s'agit-il d'un portable basique ou d'un smartphone ?
- Quel système d'exploitation votre appareil utilise-t-il ? (Exemple : Android, iOS, Windows, etc.)
- Votre système d'exploitation est-il open source ou à source fermée ?
- Quel est le fabricant de votre appareil ?

Avant de passer aux questions sur les paramètres et les autorisations, vous pouvez expliquer que :

> *« Comme les téléphones intelligents offrent encore plus de fonctionnalités et d'options que les téléphones à fonctions, la quantité d'informations qui peuvent être observées et enregistrées est bien plus importante. De plus, les utilisatrices·teurs de smartphones partagent ces informations d'identification très détaillées sur elleux-mêmes et leur utilisation avec beaucoup plus d'entreprises que leur opérateur de réseau mobile. Chaque application que vous choisissez d'installer peut également envoyer des données sélectionnées sur votre utilisation, les heures d'appel, les contacts et l'utilisation des données à la personne qui a fait cette application.*
>
> *Ce qu'une application peut voir et enregistrer est souvent défini par les personnes qui conçoivent l'application, mais il y a très peu de lois et de règlements qui limitent cela. De même, le système d'exploitation et le fabricant d'un smartphone ont un impact sur la destination de vos données et sur les personnes qui peuvent les voir en dehors de votre opérateur de réseau mobile. »*
>
> *Traduction libre* - Source

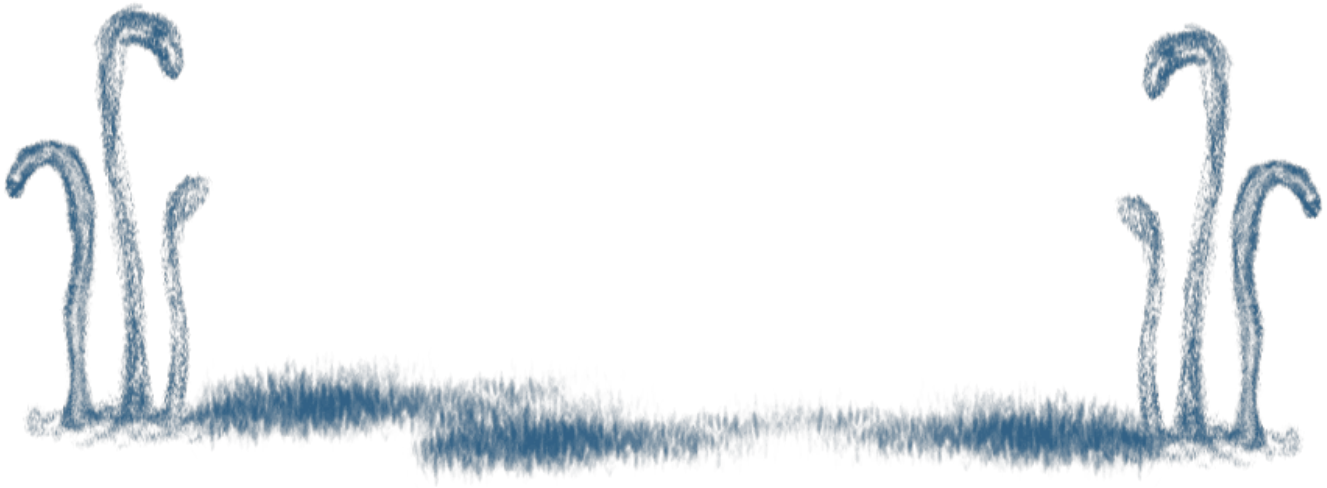
Une fois cette compréhension de base établie, vous pouvez pousser la discussion plus dans le détail des paramètres et des autorisations de leurs appareils. Voici quelques questions permettant d'orienter les débats :

- Quelles sont les fonctionnalités de votre téléphone auxquelles vos applications peuvent accéder ? (Exemple : caméra, microphone, emplacement, etc.)
- Pourquoi pensez-vous que ces applications aient besoin de ces informations ?
- Avez-vous consenti à ce que ces informations soient partagées ?

- Pensez-vous qu'il existe un lien entre le consentement hors ligne et un tel consentement en ligne ?
- Selon vous, où ces informations finissent-elles ?
- Pensez-vous que ces informations sont protégées ?

Vous pouvez consulter les informations suivantes pour orienter les débats :

> *« Les appareils Android partagent une quantité massive de données avec Google, puisque leur système d'exploitation est profondément lié au compte Google de l'utilisatrice·teur. Si vous utilisez les services et les applications de Google ainsi qu'un smartphone fonctionnant sous Android, Google connaît une énorme quantité d'informations sur vous - peut-être plus que vous ne le pensez, puisqu'il enregistre et analyse ces données.*
>
> *De même, les iPhones (utilisant iOS comme système d'exploitation) fournissent une quantité similaire d'informations sur les utilisatrices·teurs à Apple, qui peut être combinée plus de données d'une utilisatrice·teur s'iel utilise d'autres produits et services Apple. De plus, l'iPhone et Apple sont des logiciels/matériels hautement propriétaires et la source du code est fermée. Cela inclut l'iPhone lui-même, ainsi que les applications Apple; en comparaison, Android est un logiciel libre, ce qui permet à chacun de revoir son code et de savoir ce que fait Android.*
>
> *Les smartphones sont capables d'utiliser les satellites GPS (Global Positioning System) en plus de la triangulation de la position approximative que les tours de réseau mobile peuvent fournir. Cela donne des données de localisation beaucoup plus détaillées aux opérateurs et à toutes les applications qui ont accès à ces informations. Cette localisation plus précise peut être jointe, avec la date et d'autres informations, à toutes les données que le téléphone recueille pour les afficher en ligne ou les stocker dans sa mémoire. »* Traduction libre - Source



Information + activité : Confidentialité, consentement et sécurité [activité d'approfondissement]

Cette activité d'apprentissage consiste à donner des informations et à animer une discussion sur les questions relatives à la confidentialité, au consentement et à la sécurité.

ativ_aprof_FR.png
Image not found or type unknown

Cette activité d'apprentissage consiste à donner des informations et à animer une discussion sur les questions relatives à la confidentialité, au consentement et à la sécurité.

> Nous vous suggérons d'utiliser cette activité pour approfondir les notions abordées dans d'autres activités d'apprentissage telles que : Espace « sûr/safe » : Exercice d’analyse et visualisation ou La bulle.

Objectif d'apprentissage

- Mieux comprendre les problèmes de confidentialité, et comment la confidentialité affecte les femmes et leur vie.

À qui s'adresse cette activité ?

Cette activité peut être destinée à des participant·e·s ayant différents niveaux d'expérience dans le domaine des espaces en ligne et la création d'espaces sûrs. Si les participant·e·s n'ont qu'une

compréhension très basique des concepts féministes tels que l'agentivité et le consentement, il faudra clarifier ces termes avant de débuter cette activité de discussion.

Temps requis

Minimum de 40 minutes.

Matériel

- Tableau à feuilles mobiles ou tableau blanc
- Marqueurs

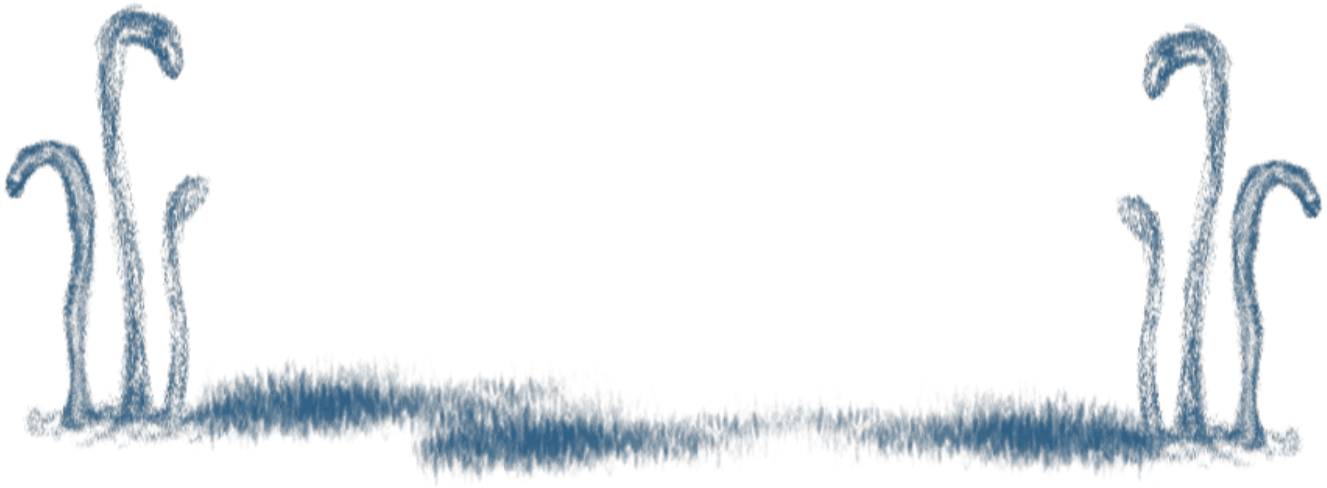
Vous pouvez également avoir recours à une présentation visuelle pour cette activité.

Mécanique

Si les activités Espace « sûr/safe » : Exercice d’analyse et visualisation ou La bulle ont déjà été réalisées, utilisez les retours de ces activités pour amorcer la définition de la confidentialité. De manière plus spécifique :

- Appuyez-vous sur les définitions de sécurité / sûreté évoquées lors des activités liées aux questions de confidentialité et de consentement.
- Reprenez et clarifiez les concepts clés soulevés au cours de l'activité d'apprentissage préalable (c'est l'occasion de clarifier des notions / idées contraires aux valeurs féministes concernant la confidentialité, le consentement et la sécurité).
- Appuyez-vous sur les expériences partagées dans l'activité précédente qui mettent en évidence les liens entre la confidentialité, le consentement et la sécurité.

Points clés à soulever au cours de cette activité d'information et de discussion.



Parler consentement et confidentialité

Parler du « consentement »

Nous avons tendance à considérer le consentement comme quelque chose de ponctuel (un peu comme signer un document une fois et puis c'est réglé). Cependant, par expérience, nous savons que le consentement est à la fois simple et complexe. Simple dans son principe mais complexe dans ses implications. Voici quelques points à discuter :

- Durée du consentement.
- Possibilité de retirer son consentement, ce que cela signifie pour un·e utilisatrice·teur de retirer son consentement et de ne plus utiliser la plateforme ou l'outil.
- Les données / informations concernant les utilisatrices·teurs qu'iels cèdent lorsqu'iels accordent leur consentement à des services.
- Comment ces données sont utilisées.
- Conditions de consentement : ne pouvoir consentir que dans certaines circonstances et pas dans d'autres.

Présentez la vidéo Thé et consentement.

Présentez cette bande dessinée (en anglais) ou toute autre ressource pertinente sur le consentement :


Wanna watch Pulp Fiction?
Sure!
1/2 hour later...
Eh, I'm not really liking this, let's do something else.
No! You said you'd watch the movie so you're staying until it's done.
Thanks for letting me borrow your car.
No problem!
The next week...
What are you doing?
Borrowing your car! You said I could.
You can't take my car whenever you want it!
That's bullshit! You said I could have it once so I should be able to have it all the time.
I really like The Fluffy Bunnys' new song.
The middle of the night...
Augh! What the hell?
You said you liked this song!
Yeah, but I don't want to listen to it while I'm sleeping!
So that's the design I want, someday. Right here.
While he's unconscious...
Bzzzzzz
You tattooed me while I was passed out? What is wrong with you?!
You said you wanted it!
But I didn't want it when I was unconscious and didn't know what was happening!
Thanks for making breakfast, Sweetie.
You're welcome!
The next morning...
Where's breakfast?
I didn't feel like cooking. Have some cereal.
You are my wife and it is your duty to cook for me! Now make me some eggs or there will be hell to pay!

La personne animatrice peut présenter certains scénarios pour mettre en évidence les points suivants :

- Accepter les conditions d'utilisation des plateformes commerciales propriétaires pour pouvoir utiliser ces plateformes.
- Scénarios d'urgence où nous consentons à permettre à d'autres de contrôler nos espaces / appareils pour pouvoir les préserver. Comment s'assurer que ce consentement conditionnel soit bien temporaire ? Vous pourriez utiliser en exemple l’option des « contacts de confiance » sur Facebook pour illustrer ce point.
- Événements qui demandent aux participant·e·s de se connecter à l'entrée. Quelles sont les implications en termes de consentement ?
- Partager un mot de passe à un·e proche comme un acte d'intimité et de confiance. Quelles sont les conséquences de cela ?
- Demandez aux participant·e·s des exemples de situations où iels ont donné leur consentement à différentes plateformes ou services.

Parler de « confidentialité »

Les points clés à transmettre peuvent inclure l**es différentes dimensions de la confidentialité :**

Territoriale / spatiale

- Pourquoi fermons-nous nos portes ? Quelles sont les portes que nous fermons ou verrouillons ?
- Comment protégeons-nous nos espaces et pourquoi ?
- Pourquoi fermons-nous la porte quand nous faisons pipi ? Quand tout le monde le fait ?

Relationnelle

- Protégeons-nous la vie privée des personnes que nous connaissons ? Qui parmi elles ?
- Violons-nous la vie privée de nos parents, ami·e·s, collègues lorsque nous parlons d'eux et elles ?

Incarnée / corporelle (incarnation et identité numérique)

- Quelles parties de votre corps choisissez-vous de révéler ? Quels vêtements choisissez-vous de porter et en fonction de qui (le regard comme violation de la vie privée) ?
- Incarnation en ligne. Autoreprésentation en ligne. Des choses simples comme les photos de profil, aux identités soigneusement conçues, à d'autres types d'informations qui révèlent des choses sur notre corps (santé / médecine / sexualité / genre). Et comment cela traduit également le corps en données.

Confidentialité des données

- Quelles données cédons-nous volontiers à propos de nous-mêmes et des autres ?
- Sommes-nous en mesure de consentir à la collecte, au stockage et à l'agrégation de nos données ?
- Qu'en est-il des données nous concernant qui sont collectées, stockées et agrégées sans notre consentement ?

Définir la confidentialité

- Définir la vie privée comme un droit humain fondamental et pourquoi c'est essentiel pour les femmes.
- Comment la vie privée a été définie dans la politique (nationale, régionale et internationale), et ce que cela signifie pour les individus, les défenseuses des droits humains et les femmes.
- Comment la vie privée se déroule sur Internet : comment les réseaux sociaux semblent redéfinir la vie privée à la fois dans la pratique individuelle et dans l'utilisation par la plateforme des données des utilisatrices·teurs.
- Comment Internet (dans la manière dont il est utilisé et développé) remet en question la façon dont nous pratiquons la confidentialité.
- La relation entre la vie privée et le consentement.

Questions favorisant la discussion

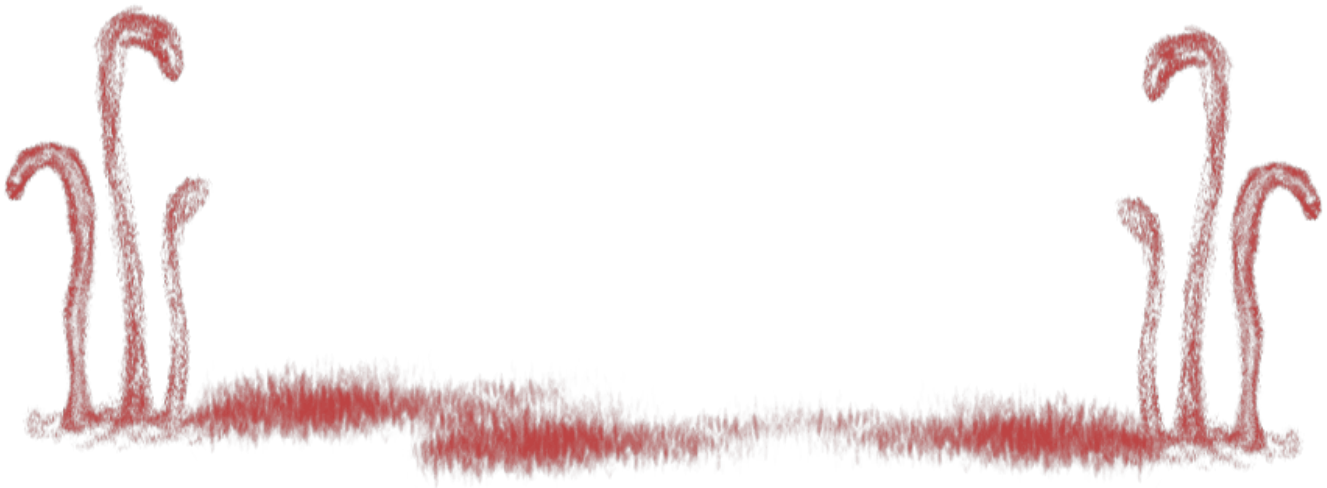
- Quand perdons-nous notre droit à la vie privée ? Par exemple : l'anonymat facilite-t-il le harcèlement en ligne et la VBG ?
- Quelle est l'importance de la relation entre l'anonymat et la confidentialité et la sécurité ?
- À l'ère des selfies et des gens cédant volontiers leurs informations personnelles et celles des autres, la vie privée est-elle morte ?
- Techniquement, comment fonctionnerait la confidentialité par défaut sur Internet ? Quel genre de changements les plateformes comme Facebook devraient-elles faire pour parvenir à une confidentialité par défaut ? (Nous pourrions développer une activité autour de cela à l'avenir.)

Conseils pour la préparation de l’atelier

Cette activité d'apprentissage donne en grande partie la parole à la personne animatrice, il est toutefois important de retrouver l'espace sûr, ouvert et interactif qui caractérise tous les ateliers FTX. Cela peut être fait en rappelant aux participant·e·s qu’iels peuvent lever la main pour intervenir, pour des questions ou pour débattre d’un point, le clarifier ou renchérir. L'autre façon d'encourager l'interaction pendant une activité de style présentation est d’amener les sujets en mode « pop corn » : Posez une question au groupe pour aborder un sujet, puis utilisez leurs réponses pour lancer une présentation ou apporter des informations.

Pour préparer cette activité d'apprentissage, la personne animatrice devra s’informer au préalable sur les éléments suivants :

- L'état d'avancement des questions de confidentialité (politiques, tendances, cas récents).
- Comprendre la confidentialité dans son contexte : lois en vigueur là où se déroule l'atelier ou en fonction du contexte des participant·e·s, cas récents pertinents pour les participant·e·s.
- Principes féministes de l'Internet (en anglais) ou la version PDF en français.



Ressources supplémentaires

En anglais

- Feminist Principles of the Internet
- "Neutral" definition of Consent (Merriam-Webster)
- "Neutral" definition of Consent (Wikipedia)
- "Neutral" definition of privacy (Merriam-Webster)
- "Neutral" definition of privacy (Wikipedia)
- Privacy and EDRI
- Three key issues for a feminist internet: Access, agency and movements
- A feminist internet and its reflection on privacy, security, policy and violence against Women
- GISWatch 2015: Sexual rights and the internet & Full report
- GISWatch 2013: Women’s rights, gender and ICTs & Report
- How much control do we have over our data?
- Establishing a baseline of privacy and security knowledge

- What privacy & anonymity have to do with tech-related VAW
- Invasion of Privacy & The Murder of Qandeel Baloch - By Digital Rights Foundation
- Peeping Tom Porn and Privacy - By Rohini Lakshané
- Mapping and privacy: Interview with Privacy International's Gus Hosein
- The ability to say NO on the Internet

Information + activité : "Règles" de sécurité en ligne [activité d'approfondissement]

Cette activité d'apprentissage consiste à partager les principes de base de la sécurité en ligne et à demander aux participant·e·s d'articuler des politiques personnelles ou organisationnelles visant à protéger leur sécurité en ligne.

ativ_aprof_FR.png
Image not found or type unknown

Cette activité d'apprentissage consiste à partager les principes de base de la sécurité en ligne et à demander aux participant·e·s d'articuler des politiques personnelles ou organisationnelles visant à protéger leur sécurité en ligne.

> Cette activité peut être effectuée après Information + activité : Confidentialité, consentement et sécurité ou Imagine ton espace rêvé sur Internet, et servir de base pour Rendre les espaces en ligne plus sûrs.

Cette activité d'apprentissage comprend trois parties principales :

- Information concernant les principes de base de la sécurité en ligne
- Réflexion sur les pratiques de communication
- Articuler des « règles de sécurité en ligne ».

Objectif d'apprentissage

- Développer des stratégies pour créer des espaces en ligne sûrs pour les participant·e·s et leurs réseaux.

À qui s'adresse cette activité ?

À des participant·e·s ayant différents niveaux d'expérience. Notez toutefois que les participant·e·s les plus expérimenté·e·s dans le domaine de la sécurité numérique pourraient trouver cette activité trop basique.

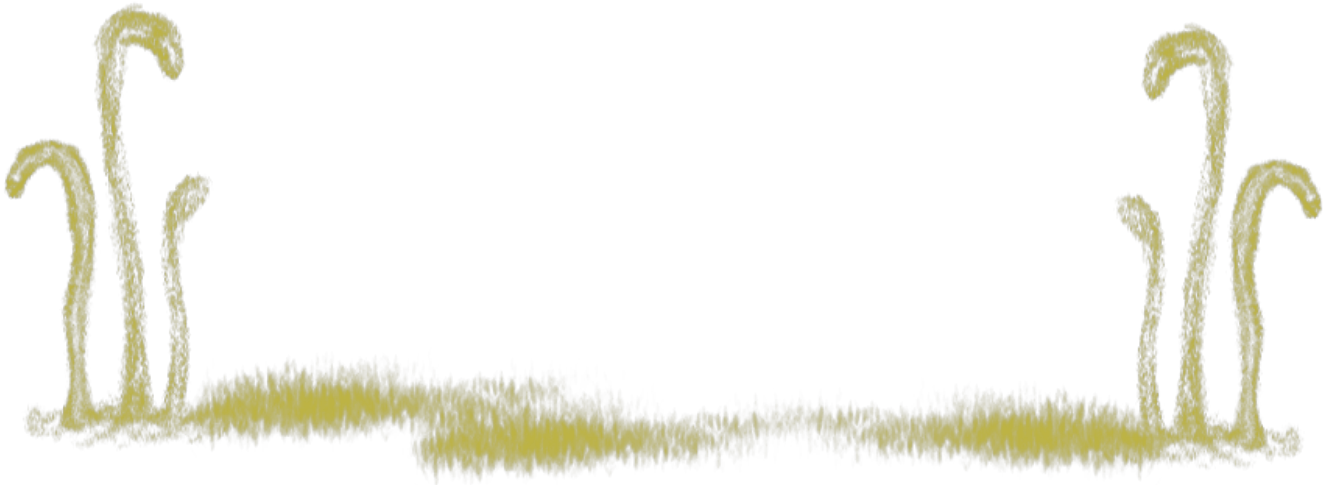
Temps requis

105 minutes au total (1h45minutes):

- Information concernant les principes de base de la sécurité en ligne (15 minutes)
- Activité sur les pratiques de communication (30 minutes)
- Information concernant les points à considérer pour la sécurité en ligne (20 minutes)
- Activité sur l'articulation des « Règles de sécurité en ligne » (30 minutes)
- Débriefing / synthèse (10 minutes)

Matériel

- Tableau à feuilles mobiles/tableau blanc
- Marqueurs
- Papier d'imprimante



Mécanique

Commencez par énumérer les **Principes de base de la sécurité en ligne** (voir Ressources supplémentaires)

> **Remarque :** Lorsque vous exposez les principes, essayez de vous référer à des exemples qui ont été partagés lors des activités d'apprentissage précédentes.

Demandez ensuite aux participant·e·s de réfléchir à leurs pratiques de communication en les faisant remplir individuellement ce formulaire (remplissez-en un qui vous servira d'exemple). Pour contextualiser et éviter les confusions, demandez aux participant·e·s de réfléchir aux dernières 24 heures et avec qui iels ont communiqué et ce sur quoi iels ont communiqué.

Avec qui communiquez-vous ?	**Quels sujets communiquez-vous ?**	**La communication est-elle privée ?**	**Canaux de communication**
Mère	Mon voyage actuel	Oui	Facebook Messenger
Kartika	Détails des travaux en cours	Oui	Courriel, Telegram, Facebook messenger
Lisa	Événement avec iel le mois prochain	Oui	Email
Marina	Dîner avec lui la semaine prochaine	Oui	SMS
	Pourquoi Trump est nul	Non	Groupe Facebook
	Principes féministes de la technologie	Non	Blog personnel

> **Remarque sur l'intersectionnalité :** Les noms sur le tableau sont des noms suggérés. Vous pouvez modifier ces noms pour qu'ils correspondent à des noms plus courants dans votre pays ou votre contexte.

Vous pouvez partir des personnes avec lesquelles les participant·e·s ont communiqué ou les sujets sur lesquels iels ont communiqué au cours des dernières 24 heures.

Après avoir demandé aux participant·e·s de remplir leurs formulaires individuels, demandez-leur de réfléchir aux questions suivantes :

- Selon elleux, parmi leurs communications faites au cours des dernières 24 heures, lesquelles devraient être le plus sécurisées ?
- Parmi leurs communications faites au cours des dernières 24 heures, laquelle cause le plus de stress ? Pourquoi ?

Passez ensuite à la présentation des **Enjeux à prendre en compte pour la sécurité en ligne** (voir Ressources supplémentaires).

Ensuite, demandez aux participant·e·s de réfléchir aux domaines à prendre en compte et d'écrire leurs « Règles de sécurité en ligne » personnelles sur la base de ce modèle :

- Parmi les sujets sur lesquels vous communiquez, quels sont ceux qui sont privés et quels sont ceux qui sont publics ?
- Avec qui communiquez-vous et sur quoi ?
- À qui permettez-vous l’accès à vos canaux de communication ?
- À quel canal ou appareil de communication limitez-vous l'accès des autres ?

> **Remarque :** Ces règles sont des projets de règles et sont propres à chaque personne. Il est important de travailler cette activité de cette façon et de continuer à réitérer les Principes de base de la sécurité en ligne.

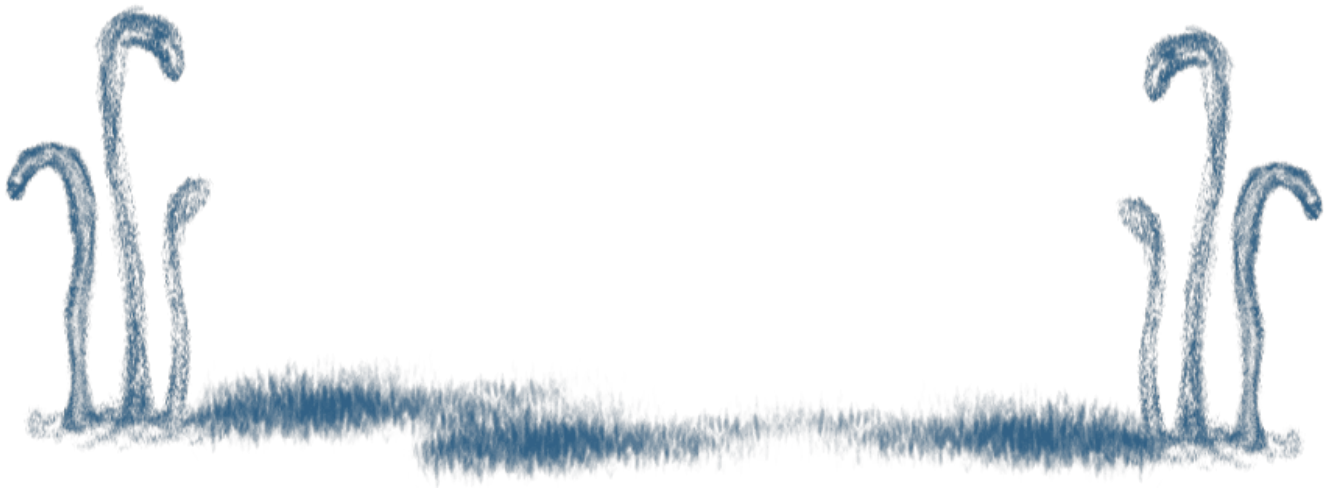
Après que les participant·e·s ont écrit leurs « Règles de sécurité en ligne », débriefez l'activité :

- Réflexions concernant vos pratiques de communication ?
- Cette activité a-t-elle permis d’identifier des inquiétudes ?
- Que faut-il clarifier d'autre ?

Il est suggéré de passer ensuite à l’activité Rendre les espaces en ligne plus sûrs.

Conseils pour la préparation de l’atelier

Vous pouvez lire cet article (en anglais) de Level Up : Rôles et responsabilités d'un·e formatrice·teur en sécurité numérique pour vous préparer mentalement à cette activité.



Ressources supplémentaires

Principes de base de la sécurité en ligne

- L'idée d'une sécurité en ligne parfaite est fausse. Le scénario de sécurité et de sûreté est contextuel : il change avec le temps. Ce qui est sûr aujourd'hui ne le sera peut-être pas demain.
- La sécurité en ligne doit toujours avoir lieu d’un bout à l’autre. Vos précautions de sécurité sont limitées par la personne la moins sécurisée avec laquelle vous communiquez ou la plateforme la moins sécurisée que vous utilisez.
- La sécurité en ligne impliquera toujours une combinaison de stratégies, de comportements et d'outils. Le simple fait d'installer des applications de sécurité n'est pas synonyme de sécurité en ligne, surtout si vous avez des pratiques et un comportement de communication non sécurisés.

> **Conseil d’animation :** Ces principes peuvent sembler moralisateurs et peuvent amener les participant·e·s à développer une certaine paranoïa quant à leur sécurité. Une façon de procéder, en tant que formatrice·teur féministe, est de donner des exemples personnels relatifs à votre expérience. De cette façon, les participant·e·s ne vous verront pas comme quelqu'un qui les jugera pour leurs choix de communication et de sécurité numérique.

Enjeux à prendre en compte pour la sécurité en ligne

Ce sont des enjeux que les participant·e·s doivent considérer lorsqu'iels envisagent leur sécurité en ligne.

Avec qui communiquez-vous et sur quoi communiquez-vous avec ces personnes

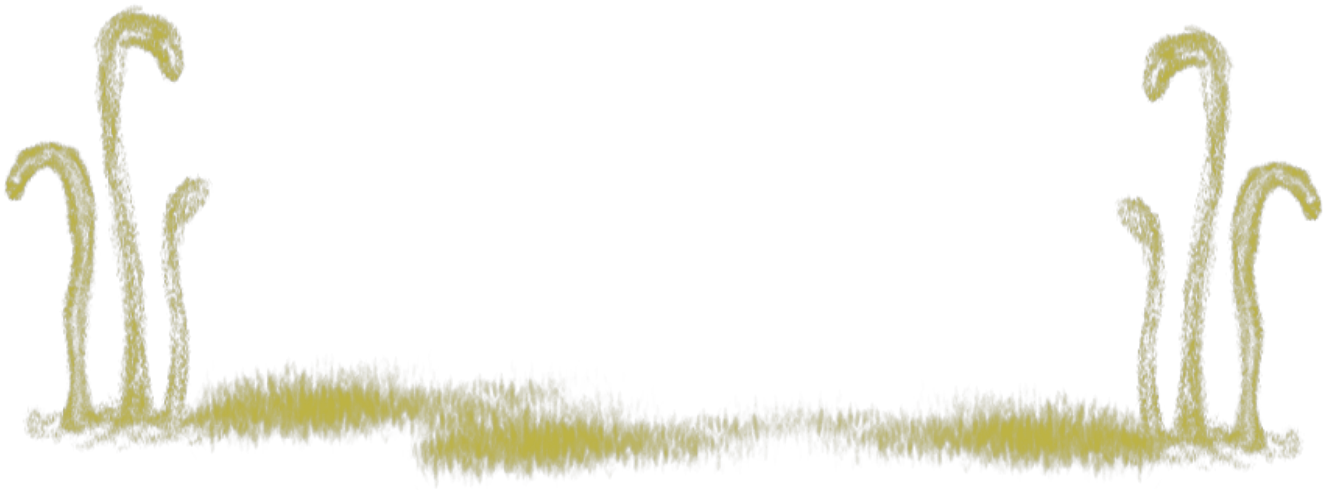
- Quels sujets abordez-vous avec les différentes personnes avec qui vous communiquez ?
- Certains des sujets que vous communiquez sont-ils sensibles ? De quelle manière ? De quoi s’agit-il ?
- Les personnes avec lesquelles vous communiquez se trouvent-elles dans une situation à risque ? Ont-elles fait l'objet de surveillance ? Le travail qu'iels font constitue-t-il une menace pour quelqu'un qui a du pouvoir ?
- Vous trouvez-vous dans une situation à risque ? Avez-vous vous-même fait l'objet de surveillance ?

Ce que vous utilisez pour communiquer

- Quelles plateformes utilisez-vous ? Savez-vous où elles sont hébergées ?
- De quels appareils disposez-vous ?
- Utilisez-vous différents appareils pour différentes personnes ? Différenciez-vous les appareils en fonction de la nature publique ou privée de vos communications ?
- Qui a accès à ces canaux de communication ? Sont-ils partagés ?

Vos contextes, capacités et risques spécifiques

- Existe-t-il des lois dans votre pays qui menacent votre sécurité en ligne en tant qu'individu ? Lesquelles et comment fonctionnent-elles ?
- Y a-t-il eu des exemples de cas où des personnes dans votre contexte (définissez le comme vous le souhaitez) ont vu leur sécurité en ligne compromise ? Comment ?
- Avez-vous déjà fait l'objet de surveillance ? Par qui ?
- Faites le bilan de votre situation. Y a-t-il des informations que vous ne souhaitez pas divulguer au public ? Pourquoi ?
- Comment protégez-vous vos canaux de communication ? Disposez-vous des mots de passe pour chaque appareil et canal de communication ?



Rendre les espaces en ligne plus sûrs [activité tactique]

Le but de cette activité est de passer en revue les options de confidentialité des plateformes de réseaux sociaux (comptes et groupes), en se concentrant sur celles utilisées par les participant·e·s.

activ_tact_FR.png
Image not found or type unknown

Le but de cette activité est de passer en revue les options de confidentialité des plateformes de réseaux sociaux (comptes et groupes), en se concentrant sur celles utilisées par les participant·e·s.

Pour les groupes qui ont suivi l'exercice Imagine ton espace rêvé sur Internet, il s’agit d’une activité visant à rendre réels nos espaces de rêve, en abordant notamment les enjeux actuels de conception et les politiques des espaces en ligne qui se trouvent en contradiction avec nos visions d’un espace rêvé. Les groupes qui possèdent déjà des espaces en ligne, et qui souhaitent les modifier pour se sentir plus en sécurité, peuvent également utiliser cette activité.

Si vous souhaitez vous familiariser avec les services en ligne, cette activité vous donne des conseils pour analyser les paramètres, les politiques et les normes des espaces en ligne. Il ne s’agit cependant pas d’un guide étape par étape pour ajuster les paramètres, car ceux-ci changent trop fréquemment.

Objectifs d’apprentissage

- Développer des stratégies pour créer des espaces en ligne sûrs pour les participant·e·s et leurs réseaux.
- Comprendre les limites des options de confidentialité des différents médias sociaux.

À qui s'adresse cette activité ?

Cette activité peut être destinée à des participant·e·s ayant différents niveaux d'expérience dans le domaine des espaces en ligne et la création d'espaces sûrs (safe). Les participant·e·s devront explorer et ajuster les options de confidentialité sur les plateformes qu’iels utilisent.

Temps requis

Environ **3 heures.**

Matériel

- Une copie électronique des tableaux de planification (voir plus bas)
- Ordinateurs pour que les participant·e·s puissent travailler sur leurs tableaux
- Tableau à feuilles mobiles
- Marqueurs

Mécanique

1. Cartographie de votre espace

Développez des nouveaux espaces : Si vous avez fait l'activité Imagine ton espace rêvé sur Internet, vous pouvez utiliser les espaces que vous y avez créés comme point de départ.

Modifiez des espaces existants : Il est possible que votre groupe préfère modifier ou remodeler un espace en ligne déjà existant. Identifiez un espace que les participant·e·s utilisent déjà ou bien demandez-leur de former des petits groupes en fonction des espaces en ligne qu'iels fréquentent.

Invitez les groupes à répondre aux questions suivantes (utilisées dans Imagine ton espace rêvé sur Internet) :

- Comment s'appelle cet espace en ligne ?
- Pourquoi cet espace est-il important ?
- À qui s'adresse-t-il ? À qui est-il fermé ? Comment s'en assurer ?

- Que font les gens dans cet espace ?
- Quelles en sont les règles ?
- Qui peut y venir (ou pas) ?
- À quoi ressemblera cet espace ?
- Comment les personnes se retrouveront-elles dans cet espace ?
- De quels sujets pourra-t-on y parler (ou pas) ?
- Qui est responsable de l'administration de cet espace ?

Demandez aux groupes de dessiner cet espace de la façon la plus imaginative possible et demandez-leur de préparer une présentation créative à l'intention de l'ensemble des participant·e·s.

2. Choisir des espaces qui fonctionnent et vérifier la sécurité

Si vous avez déjà fait Information + activité : "Règles" de sécurité en ligne, vous avez donc probablement déjà eu une discussion sur le choix des espaces et sur l'évaluation des risques par rapport aux communications en ligne.

Choisir les espaces pour leur fonctionnalité

Comment choisissez-vous les plateformes et comment évaluez-vous les risques présents pour vous sur ces plateformes ? Choisissez des espaces qui vous aideront à atteindre vos objectifs de communication et essayez de participer à ces espaces en évitant de vous exposer à des risques que vous ne souhaitez pas prendre.

Regardez la carte de l'espace que vous avez faite. Êtes-vous en mesure d'identifier une plateforme qui vous permette de créer l'espace que vous avez cartographié ? Dans votre espace, quelles composantes seront les plus faciles à créer ? Les plus difficiles ? Existe-t-il des espaces alternatifs qui seront plus favorables ou défavorables à ces composantes ?

Choix stratégique des espaces

L'espace que vous avez choisi correspond-il à votre stratégie ? Est-ce un bon espace pour : organiser, mobiliser, faire des annonces, exercer une influence sur le discours ?

Note à l'animation : Présentez comment ces différentes activités entraînent différents niveaux de risque.

Questions suggérées :

- Quels risques comportent les différents types de communication ?
- Avec qui communiquez-vous dans le cadre de ces activités ?

- Avec qui ne communiquez-vous pas ?
- Quelles seraient les conséquences si quelqu'un à qui un message n'était pas destiné y accédait ?
- Comment choisir le degré d'ouverture au public ?
- À quels risques les personnes peuvent-elles faire face si elles sont reconnues en tant que créatrices ou destinataires des messages de cette communication ?

Cette discussion mène à la discussion suivante qui examine les risques qui préoccupent le plus les gens.

> **Conseil d'animation :** Cette section peut aller très vite si tout le monde s'accorde à n'utiliser qu'une seule plateforme, par exemple Facebook. Il est également possible de parler de plusieurs outils et plateformes.

Discussion OU information

Évaluation des dimensions liées à la sécurité et à Internet : quels sont les problèmes actuels ?

Demandez au groupe : Quels sont les risques liés à la sécurité qui vous préoccupent dans les espaces en ligne ? Animez cette discussion pour inclure les préoccupations concernant les actions que les individus peuvent entreprendre dans ces espaces ainsi que les actions entreprises par les éditeurs des logiciels propriétaires des espaces.

> Si vous avez déjà fait l'activité Information + activité : "Règles" de sécurité en ligne, vous pouvez y faire référence et abréger cette section.

Dans le cas contraire, animez la discussion sur les risques liés à la sécurité dans les espaces en ligne. Appuyez-vous sur les expériences des participant·e·s, mais préparez également quelques exemples d'histoires de violation de la vie privée dans des espaces en ligne qui ont eu un impact sur des personnes.

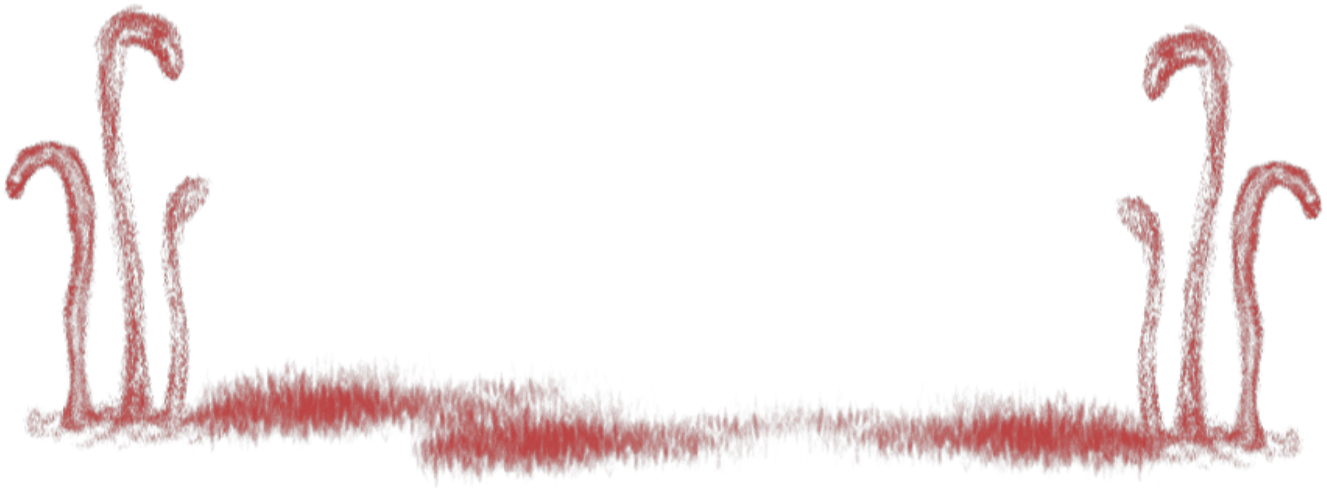
Discussion: Demandez aux participant·e·s quelles sont leurs préoccupations en matière de sécurité dans les espaces en ligne. Y a-t-il des incidents ou des risques spécifiques inquiétants qu'iels souhaitent aborder dans leur espace de rêve ou dans leur espace repensé ?

Information: Nous vous suggérons de vous familiariser avec quelques études de cas et d'en parler ici. Pour aller le plus vite possible, faites en plutôt une présentation. Si vous avez plus de temps ou si vous souhaitez en discuter de manière plus approfondie, utilisez des articles, de courtes vidéos, des interviews ou autres concernant ces cas et partagez-les avec le groupe. Demandez aux membres du groupe d'en discuter à deux ou par petits groupes.

- Politiques du nom réel et leurs implications pour l'organisation et l'expression en ligne.

- Le mythe selon lequel être en ligne c'est être anonyme et donc en sécurité, à contraster avec les lois et des politiques qui ne permettent pas cet anonymat.
- L'expérience des femmes sur Internet (harcèlement, attaques, etc.)
- La valeur d'Internet : Pourquoi les gens sont attaché·e·s aux espaces en ligne ? En quoi est-ce utile pour nous et notre communauté ?
- Diversité d'accès et niveau de confort des espaces en ligne que nous choisissons. Avoir choisi une plateforme spécifique constitue-t-il un obstacle empêchant les personnes de nos communautés d'y participer ?
- L'espace que vous avez choisi d'utiliser représente t-il un coût financier pour les personnes de votre communauté ?

> **Note à l'animation :** Demandez aux participant·e·s de réfléchir aux raisons pour lesquelles les plateformes que nous utilisons ne sont pas plus sûres de par leur conception.



3. Faites un plan : Abordez les risques propres aux espaces que vous utilisez

En utilisant les espaces de rêve ou les espaces repensés comme exemples, demandez aux participant·e·s de planifier la mise en œuvre de cet espace en ligne.

Cette activité est plus pertinente s'iels ont déjà des espaces actifs qu'iels veulent sécuriser et préserver.

Questions à considérer ici :

- Paramètres de confidentialité sur les réseaux sociaux. Est-ce suffisant ? En quoi les paramètres disponibles sont limités ?

- Vous envisagez de passer à des espaces non commerciaux. Quels sont les obstacles ?
- Options plus sûres pour les communications en ligne, les outils qui offrent le chiffrement par défaut.

À prendre en considération	Plateforme ou espace	Comment y remédier
Qui peut voir quoi ?	Twitter (par exemple)	Passer en revue mes paramètres de confidentialité ; prendre en compte le contenu que je publie, auquel je réponds, ainsi que les paramètres de confidentialité par défaut sur différents types de contenu ; réduire le nombre de personnes avec qui je suis lié·e ; désactiver l'option où les autres peuvent m'identifier
Connaissez-vous toutes les personnes à qui vous êtes lié·e ?		Vérifier à qui je suis connecté·e ; supprimer les liens avec les personnes que je ne connais pas ;
Souhaitez-vous utiliser votre vrai nom ; la complexité de la question de l'anonymat		Utiliser un pseudonyme ; empêcher les autres de me nommer par mon vrai nom
Souhaitez-vous partager votre localisation ?		Non, je ne souhaite pas partager automatiquement ma localisation ; désactiver les services de localisation ; limiter les publications de photos montrant ma localisation

Autorisation

À prendre en considération	Plateforme ou espace	Comment y remédier
M'assurer de bien m'être déconnecté.e	f-book	Ne pas sauvegarder le mot de passe dans le navigateur ; revoir les paramètres sur f-book concernant la déconnexion automatique
Identification à deux facteurs sur les comptes et les appareils		Configurer l'identification à deux facteurs pour être plus sûr.e qu'il n'y a que moi qui puisse me connecter
Comptes partagés		Vérifier qui a accès aux comptes partagés ; examiner les politiques de mot de passe sur ces comptes

Appareils

À prendre en considération	Plateforme ou espace	Comment y remédier
Sécurité au niveau de l'appareil	Twitter ou autre	Ne pas se connecter automatiquement à des applications ou via des navigateurs

Est-il souhaitable que des notifications s'affichent sur mes appareils ?		Désactivez les notifications audio et visuelles

Administration des groupes

Si vous travaillez avec un groupe pour mettre en place un espace en ligne, utilisez le tableau de questions suivant et parcourez les réponses afin de trouver les bons paramètres sur la plateforme que vous utilisez pour mettre en place les préférences du groupe.

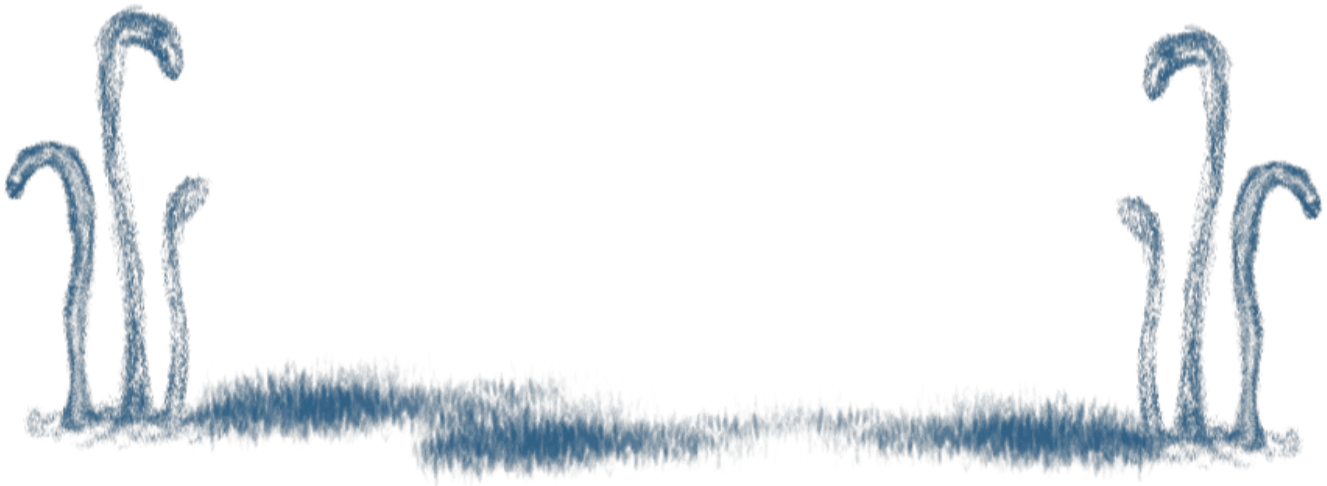
Exemple de tableau de conception / mise en œuvre :

Lien vers un groupe ou une page personnelle	https://www.facebook.com/APCNews	**Que faire pour le mettre en œuvre ?**
Qui peut voir cet espace ?	N'importe qui sur Internet	La page de notre groupe est publique sur Facebook et accessible aux moteurs de recherche
À qui est destiné cet espace ?	Aux membres d'APC, à la communauté et aux membres potentiels d'APC	Nous invitons le personnel d'APC et les membres du réseau à se joindre à ce groupe. Nous les mentionnons dans les publications et les invitons aux événements publiés sur cette page
À qui cet espace ne s’adresse-t-il pas ?	Aux membres d'APC, à la communauté et aux membres potentiels d'APC	fermé / public. Nous limitons qui peut publier, mais rendons la page consultable sur Facebook et accessible aux moteurs de recherche
Que font les gens dans cet espace ?	Recevoir ds notifications sur le travail APC et des liens vers le contenu du réseau APC publiés ailleurs	
Qui peut créer du contenu dans cet espace ? Quel genre de contenu ?	Personnel et membres	-
Comment souhaitez-vous communiquer les règles qui encadrent cet espace ?	En utilisant la page « À propos » de notre groupe	Nous allons définir nos règles en nous basant sur ce tableau de questions et réponses, puis nous le publierons sur notre page « à propos »

Conseil *care* et bien-être : Évoquer des questions liées au risque et à la technologie peut être source de stress pour les participant·e·s. Prenez-en bien compte. Consacrez une pause à un exercice de respiration ou laissez les participant·e·s se promener sur place pour qu’iels décompressent quand iels en ont besoin.

Ressources supplémentaires

- Consultez les guides de sécurité de l'Asso Échap : https://echap.eu.org/ressources/
- Pour plus d'outils et ressources, consultez ce site web : https://myshadow.org/fr
- How to Increase Your Privacy on Twitter (en anglais)
- Security in a Box: Social networking
- Security in a Box: Keep your online communication private
- Create and maintain secure passwords



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