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

wiggy-cactus-yellow-several.png

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.

wiggy-cactus-blue-several.png
Wiggy not cactus or type several

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 ?

wiggy-cactus-yellow-several.png
Image not found or type unknown

Revision #9
Created 26 April 2023 00:57:37 by Kira

Updated 28 July 2023 15:04:33 by Kira