Renforcer la sécurité des responsables de la mise en œuvre des services VIH travaillant avec des populations clés

Formation virtuelle pour une direction organisationnelle

avril 2021

PEPFAR USAID FROM THE AMERICAN PEOPLE EpiC LINKAGES

Bienvenue, introductions et contexte

Objectif de la session

- Accueillir tous les participants et les présenter les uns aux autres.
- Parvenez à une compréhension commune du contenu et des objectifs de la formation ainsi que de la participation de chacun à la formation.
- Identifiez la sécurité des exécutants comme un domaine important et nouveau dans la programmation du VIH.

Activité A. Introductions

- Nom et titre
- Expériences en matière de formation à la sécurité
- Un espoir/une attente de cette formation

Groupe	Personne 1	Personne 2
A		
B		
C		
D		
E		
F		
G		
H		
I		

Activité B. Normes du groupe

- Ces sessions seront enregistrées.
- Ne communiquez pas d'informations permettant d'identifier d'autres personnes lorsque vous racontez des incidents de sécurité.
- Participez pleinement.
- Arrivez à l'heure et restez pendant toute la durée de chaque session.
- Ne partagez pas ce que vous entendez dans ce webinaire en dehors de cet espace.

Revoir l'ordre du jour et les attentes

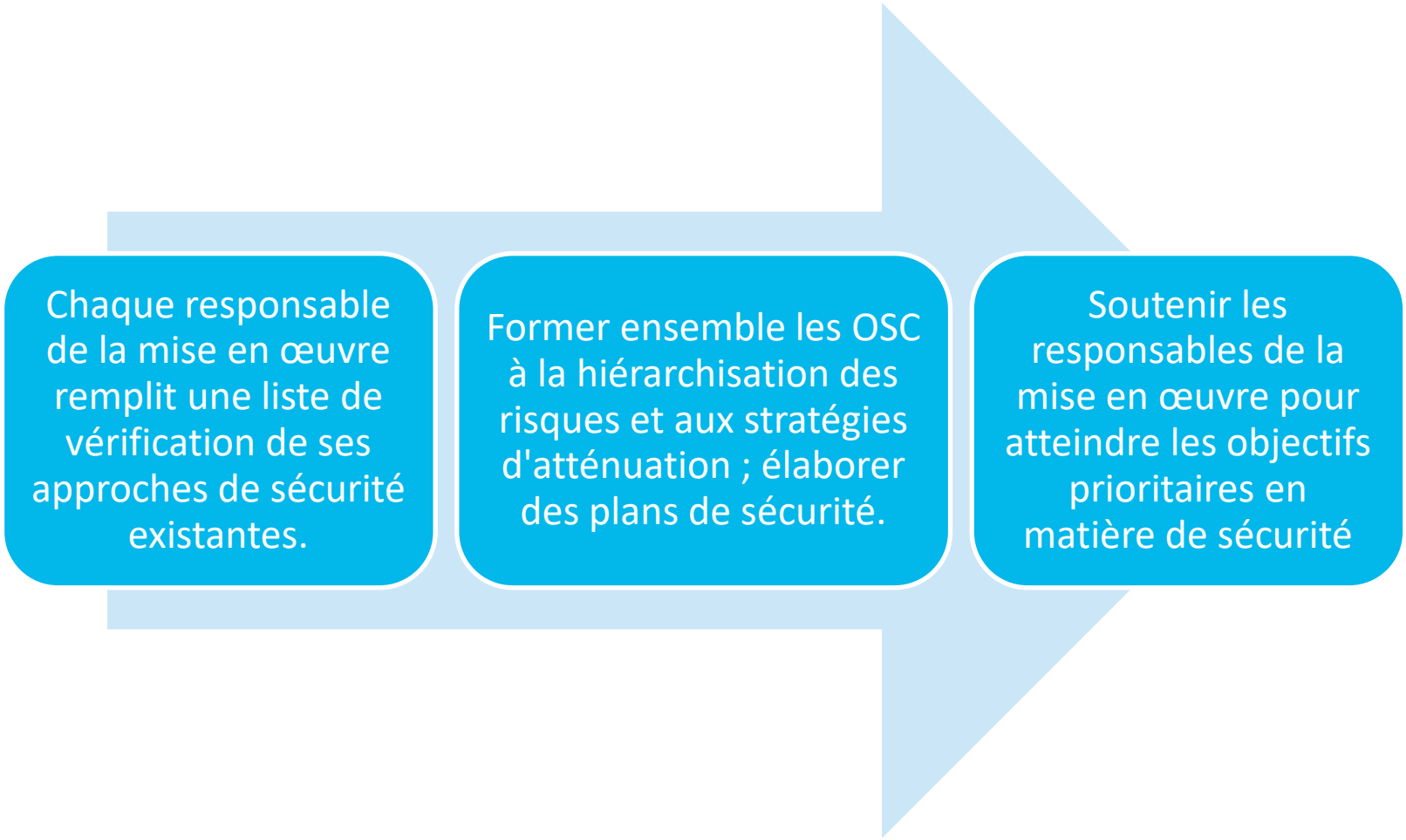
Pour recevoir un certificat attestant que vous avez suivi cette formation :

- Les participants participeront et contribueront à chaque session (au moins deux fois verbalement et 5 fois par chat).
- Les participants effectueront tous les devoirs à la maison.
- Les participants doivent remplir le post-test et obtenir un score d'au moins 85 %.

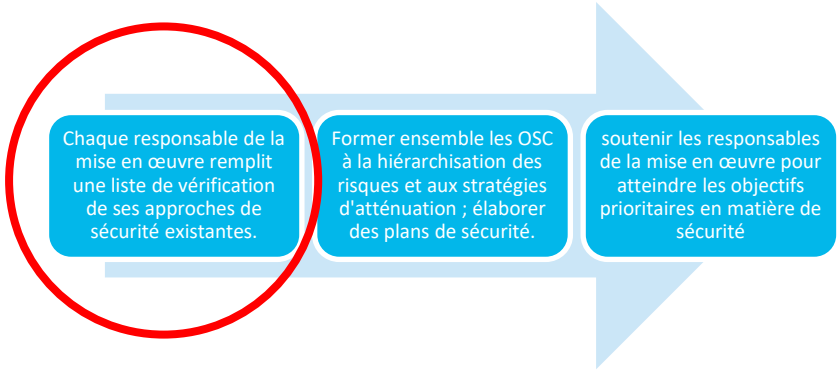
Dates de la formation :

Heure	Session
JOUR 1	
8:00	Bienvenue, introductions et contexte
8:45	Termes clés et recommandations majeures
9:15	Identification et évaluation de la menace
9:55	Clôture du Jour 1
JOUR 2	
8:00	Récapitulatif du Jour 1 et Devoir #1
8:25	Limiter la capacité de nuire d'un agresseur
9:00	Sécurité numérique
9:40	Revoir nos capacités et plan de partage de compétences
9:55	Clôture du Jour 2
JOUR 3 - Session spéciale, Présentations du groupe	
	Présentations du groupe
JOUR 4	
8:00	Jour 2 récapitulatif et réflexions sur la session spéciale
8:10	Utiliser ce que vous avez appris : défi sécuritaire Etudes de cas
8:45	Formule d'évaluation des risques
9:05	Plan de sécurité
9:35	Prochaines étapes
9:50	Réflexions et clôture

Aperçu du processus

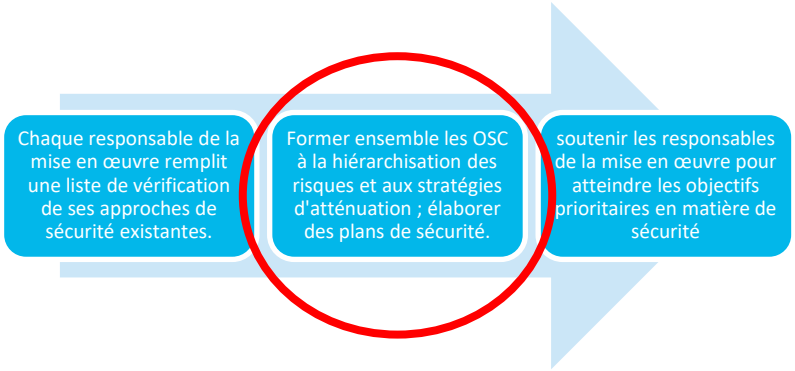


Etape 1



- Cultiver et sensibiliser les alliés externes
- Influencer la perception publique du projet ou de l'organisation
- Documenter les préjudices pour le suivi et le plaidoyer
- Protection des bureaux, des centres d'accueil et d'autres lieux physiques
- Assurer la sécurité des travailleurs lors des actions de sensibilisation physiques et numériques
- Développer des protocoles de sécurité fonctionnels et institutionnalisés, y compris pour les urgences.
- Assurer la sécurité des données et des communications
- Questions transversales : préparation aux situations d'urgence, sécurité numérique, COVID-19

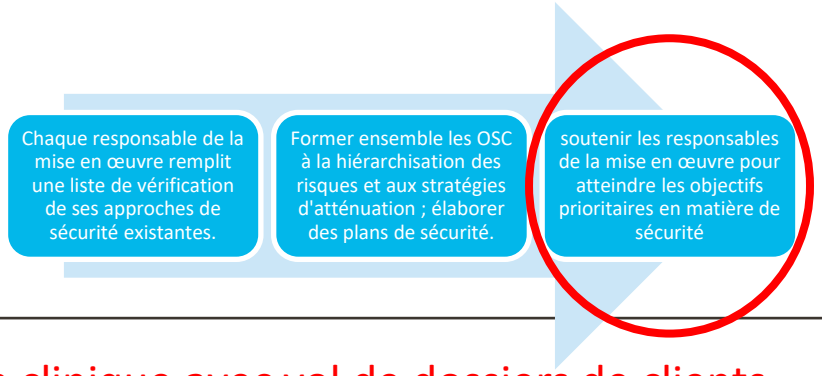
Etape 2



Objectifs de l'atelier

- Identifier les points forts et les lacunes en matière de sécurité et partager les points forts entre les responsables de la mise en œuvre.
- Classer par ordre de priorité les risques de sécurité auxquels le programme est confronté et déterminer les lacunes les plus importantes à combler pour chaque OSC.
- Rédiger des plans de sécurité spécifiques aux OSC qui traitent des risques prioritaires et de la manière dont les compétences seront développées pour gérer ces risques.

Etape 3



Risque (de quelque chose): Un cambriolage à la clinique avec vol de dossiers de clients.

Menaces	Vulnérabilités	Capacité existante	Capacité requise
Elevé • Des travailleurs de proximité ont été suivis jusqu'à la clinique par des groupes de hurleurs qui disent que nous encourageons l'homosexualité. • Des messages menaçants ont été graffités sur la clinique.	• Nous sommes dans un quartier où il y a peu de circulation le soir. • Nous n'avons pas d'agents de sécurité à la clinique après 17 heures. • Nous n'avons pas de moyen de contrôler les visiteurs pendant la journée. • Le personnel ne verrouille pas toujours les dossiers des patients. • Les fenêtres et les portes n'ont pas de barreaux ; elles peuvent être brisées avec des pierres.	• Nous disposons d'un agent de sécurité pendant les heures d'ouvertures de la clinique (de 9 h à 17 h). • Nous avons le logo de l'USAID et du MS sur notre panneau. • Nous nous sommes présentés et avons expliqué notre travail aux officiers de police travaillant dans le district. • Nous avons des armoires fermées à clé pour stocker tous les dossiers papier des clients. • Nous utilisons des UIC et conservons principalement des informations électroniques cryptées.	• Journaux de bord des visiteurs • Formation de tout le personnel sur le stockage sécurisé des documents (politique de bureau propre). • Discuter avec le propriétaire de la nature de notre travail. • Installer des mesures de sécurité physique pour les fenêtres et les portes. • Créer un journal des incidents de sécurité pour suivre les tendances ; envisager d'utiliser ce journal pour plaider auprès du donateur en faveur de fonds pour une présence de sécurité accrue.

La sécurité des exécutants dans les programmes de lutte contre le VIH : Une histoire incomplète

- Une plus longue histoire de violence/réponse à la crise pour les bénéficiaires des programmes VIH pour les PC (par exemple, Avahan, début des années 2000) et les organisations axées sur les droits des LGBT (par exemple, le consortium Dignité pour tous, 2012).
- Les programmes des PC ont constaté et de plus en plus documenté l'insécurité des exécutants.
- Arrestations et détentions
- Perquisitions et cambriolages de bureaux
- Attaques contre le personnel (physiques, sexuelles, économiques et émotionnelles).
- LINKAGES et Frontline AIDS développent une boîte à outils ; LINKAGES et Synergia développent des supports de formation destinés aux responsables de la mise en œuvre des programmes VIH des PC (2018).
- Efforts pour améliorer spécifiquement la sécurité des données (2019)
- LINKAGES/EpiC étendent le travail de sécurité à l'ensemble du projet, à la sécurité numérique et aux tests d'indexation, et à de nouvelles régions (MENA, 2019-21).

Quoi, qui, pourquoi ?

Dans votre contexte :

- A **quoi** ressemblent les incidents de sécurité affectant les exécutants ?
- **Qui** commet des abus contre les exécutants du programme des PC ?
- **Pourquoi** les attaques contre les exécutants se produisent-elles ?

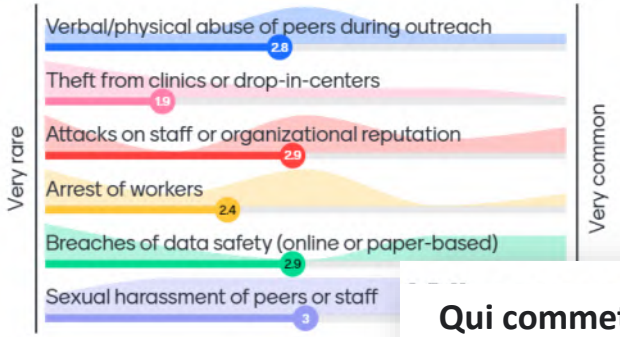
Les exécutants du programme PC peuvent inclure :

- Travailleurs de proximité/mobilisateurs communautaires
- Pairs éducateurs/navigateurs
- Agents de santé communautaire
- Membres de la communauté
- Directeurs et responsables de programmes
- Agents de programme - Travailleurs des centres d'accueil
- Cliniciens (par exemple, médecins, infirmières)
- Conseillers et prestataires de soutien psychosocial
- Personnel de bureau (par exemple, réceptionnistes)
- Personnel de soutien (par exemple, chauffeurs, gardiens)
- Activistes, défenseurs et militants communautaires - Avocats et assistants juridiques
- Alliés et champions

Activité C. Quoi, qui, pourquoi ?

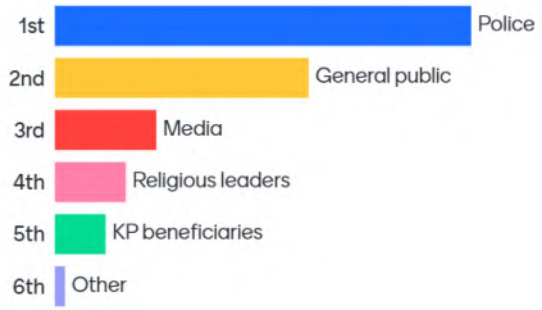
Go to www.menti.com and use the code 98 42 23 8

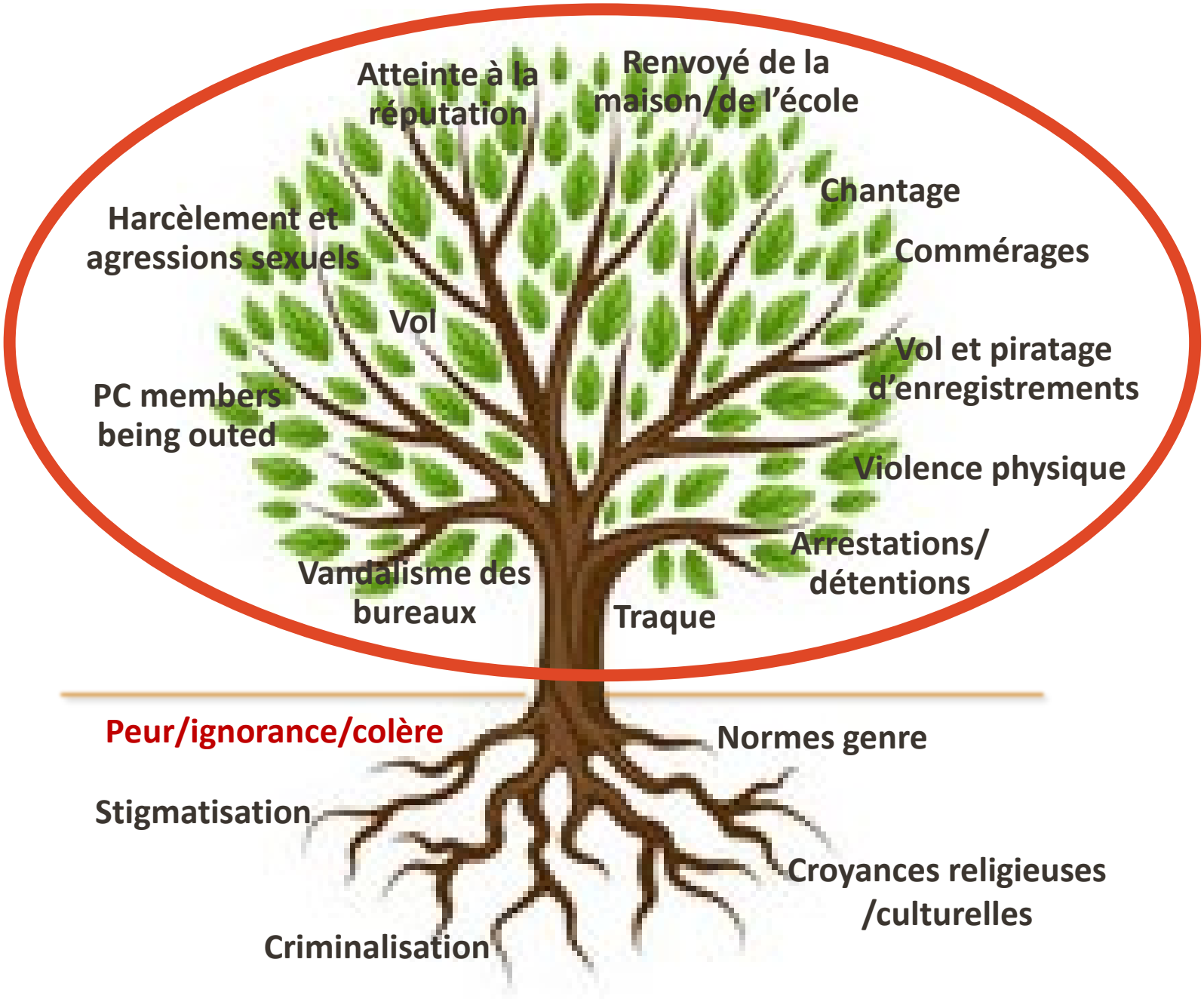
En pensant à votre programme PC, quelle est la fréquence de chacun de ces incidents de sécurité ?



The code lets your audience join the presentation. It expires in 2 days.

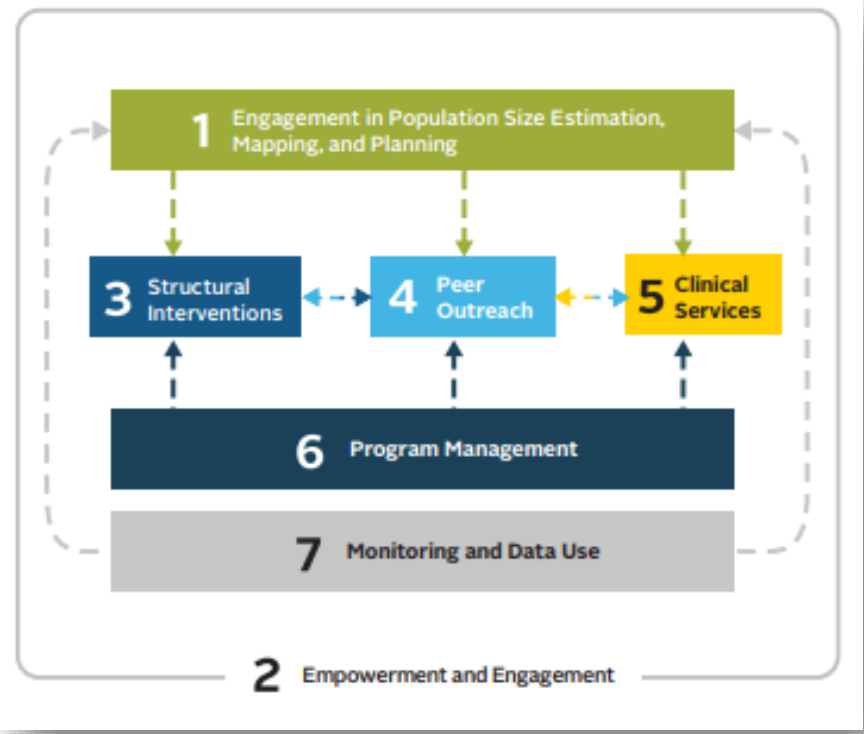
Qui commet des violences à l'encontre des exécutants du programme PC ?




Atteinte à la réputation
Renvoyé de la maison/de l'école
Chantage
Harcèlement et agressions sexuels
Commérages
Vol
Vol et piratage d'enregistrements
PC members being outed
Violence physique
Arrestations/ détentions
Vandalisme des bureaux
Traque
Peur/ignorance/colère
Normes genre
Stigmatisation
Croyances religieuses /culturelles
Criminalisation

Comment les problèmes de sécurité affectent-ils les programmes des PC ?

Sept domaines de programmes destinés aux populations clés[1]



1. Il peut être difficile d'entreprendre des enquêtes comportementales ou biomédicales limitant les données fiables.
2. Il est plus difficile d'embaucher des membres du groupe de pression ou d'engager des organisations de la société civile (OSC) dirigées par des membres du groupe de pression.
3. Nécessité de formations intensives sur la réduction de la stigmatisation pour les travailleurs de santé, en particulier si le travail avec les membres des PC entraîne une stigmatisation et des abus secondaires.
4. Le harcèlement limite le travail de proximité.
5. L'épuisement du personnel clinique augmente.
6. Les changements d'orientation de la direction rendent difficile la réalisation des objectifs du programme.
7. Si les données ne peuvent pas être sécurisées, ce qui peut être collecté est sévèrement limité.

1. Key Population Program Implementation Guide. Washington (DC): FHI 360/LINKAGES; March 2016.

Termes clés et recommandations majeures

Objectif de la session

Définissez les termes "sécurité", "risque", "menace", "capacité" et "vulnérabilité", et discutez des principales recommandations relatives à la sécurité des exécutants des programmes des PC.

Activité D. Définition: Sécurité

Que signifie le terme "sécurité" ?

A. Être sûr d'être en totale sécurité.
B. Être à l'abri de toute violence intentionnelle.
C. Avoir une trousse de premiers soins.

Bien que le terme "sécurité" soit parfois utilisé de manière interchangeable avec celui de sûreté, la sécurité est axée sur l'absence de dommages intentionnels. La sûreté comprend l'absence de dommages tels que la maladie et les catastrophes naturelles, qui ne seront pas abordés dans cette formation.

Activité D. Définition: Risque

Que signifie le terme "risque" ?

A. La probabilité que quelque chose de nuisible se produise.
B. Être prudent.
C. Planifier à l'avance pour éviter le danger.

Bien que le terme "risque" puisse faire référence à la fois à la possibilité d'un dommage et à quelqu'un/quelque chose qui crée un danger, dans cette formation, nous parlerons du risque comme de la probabilité que quelque chose de dangereux se produise.

Activité D. Définition: Menace

Que signifie le mot "menace" ?

A. Une indication/signe que quelqu'un veut nous faire du mal, nous nuire ou nous punir.
B. Une déclaration de soutien.
C. Un mauvais présage.

Les menaces peuvent être verbales, par exemple : "Je vais te faire du mal". Cependant, les menaces peuvent aussi être des actions. Dans cette formation, nous parlerons des menaces comme venant de l'extérieur de nous-mêmes (c'est-à-dire que nous n'aborderons pas des idées telles que l'automutilation).

Activité D. Définition : Capacité

Que signifie le terme "capacité" ?

A. Un signe que quelqu'un veut nous faire du mal, nous nuire ou nous punir.
B. Toute ressource (financière, capacité, contacts, infrastructure, personnalité, etc.) que nous pouvons utiliser pour améliorer notre sécurité.
C. Le degré de dangerosité de quelque chose.

Les capacités peuvent inclure presque tout. Un grand sens de l'humour peut aider à désamorcer une situation tendue. Être relié à quelqu'un du programme national de lutte contre le sida peut empêcher les autres de vous importuner. Une voiture avec des serrures solides peut vous protéger contre le vol.

Activité D. Définition : Vulnérabilité

Que signifie le terme "vulnérabilité" ?

A. Tout ce qui augmente notre exposition à ceux qui veulent nous faire du mal.
B. Tout ce que nous faisons pour nous protéger.
C. Un signe que quelqu'un veut nous faire du mal.

Not objectif n’est pas de nous rendre complétement non vulnérables. Être vivant c’est être vulnérable. Cependant, nous pouvons identifier nos vulnérabilités et déterminer si certaines d’entre elles peuvent être réduites.

La vulnérabilité est un concept délicat

- Une "vulnérabilité" n'est pas la même chose qu'une "faiblesse".
- Une capacité dans un contexte donné peut être une vulnérabilité dans le contexte suivant.
- Certaines capacités/vulnérabilités ne peuvent être modifiées.
- L'objectif est de prendre conscience de vos vulnérabilités et de vos capacités et d'agir de manière à en tenir compte, chaque personne décidant de ce qui lui convient.

Activité E. Devoirs : Recommandations majeures

A	1.	**Faire des principes et des approches du programme VIH le fondement des efforts de sécurité.**
B	2.	**Faites de la sécurité une priorité et attribuez-lui des ressources de manière explicite.**
C	3.	**Faites de la sécurité du lieu de travail la responsabilité de l'employeur.**
D	4.	**Planifiez à l'avance et assurez-vous que tout le monde connaît le plan (tout en restant flexible).**
E	5.	**Discutez explicitement du niveau de risque acceptable pour l'organisation et les individus.**
F	6.	**Agissez en connaissant à la fois les risques réels et leurs causes sous-jacentes (y compris les cadres juridiques).**
G	7.	**Reconnaissez les différentes vulnérabilités et capacités de chaque travailleur dans la planification de la sécurité.**
H	8.	**Apprenez à connaître toutes les parties prenantes, et pas seulement les alliés évidents.**
I	9.	**Identifiez les menaces (physiques, numériques, psychologiques) et les stratégies de sécurité de manière holistique.**
J	10.	**Être ensemble, travailler en coalition et apprendre les uns des autres.**

Devoir #1: Réflexions sur les recommandations

- Après cette session, chaque groupe se verra attribuer une recommandation.
- Vous trouverez plus d'informations sur votre recommandation dans « l'aide-mémoire » de la formation.
- Soyez prêt, lors de la prochaine session, à (1) décrire cette recommandation, (2) partager comment votre programme utilise déjà cette recommandation, et (3) comment il pourrait utiliser cette recommandation.

Identification et évaluation des menaces

Objectif de la session

- Identifier les menaces et déterminer leur gravité.

Types de menaces

- **Menace directe -** Indication que quelqu'un veut me faire souffrir ou nuire à mon organisation en particulier.
- **Menace indirecte** - Indication que quelqu'un veut me faire souffrir ou nuire à un groupe plus large de personnes dont je fais partie, mais pas à moi ou à mon organisation en particulier.
- **Incident de sécurité** - Situations dans lesquelles un dommage se produit, mais nous ne savons pas si l'incident est une menace ou plutôt une coïncidence.

Activité F. Étiqueter chaque menace

Incident	Type de menace qui pèse sur vous (menace directe, menace indirecte, incident de sécurité)
A. Vous êtes le directeur de l'OSC 1, une organisation qui fournit des services VIH aux HSH. Un leader local influent accuse l'OSC 2 de promouvoir l'homosexualité. L'OSC 2 offre les mêmes services aux HSH que votre organisation. Quelqu'un casse les fenêtres de l'OSC 2 et fait des graffitis sur le domicile du directeur de l'OSC 2.	**Menace indirecte :** Ce n'est pas une menace directe pour vous mais elle vise un groupe dont vous faites partie (personnes fournissant des services VIH aux HSH).
B. Vous êtes un travailleur de proximité pour les pairs qui distribue des préservatifs. Un policier vous arrête et vous dit que s'il vous revoit, il vous fera arrêter.	**La menace directe :** Cette menace vous concerne et est dirigée contre vous
C. Vous êtes infirmière. Une cliente vous donne le nom et l'adresse de son partenaire sexuel. Lorsque vous vous rendez au domicile du partenaire nommé, il refuse de vous parler. Plus tard dans la journée, vous recevez trois appels d'un numéro inconnu. L'appelant ne dit jamais rien, mais respire fort dans le téléphone.	**Incident de sécurité :** Vous ne savez pas qui appelle et si vous êtes visé pour une raison précise.

Enregistrement des menaces

Il est important de pouvoir répertorier ces trois menaces et cela peut vous aider à fournir des documents, y compris au donateur, et à suivre les tendances

- Si une menace indirecte pèse sur un groupe plus large
- Lieux ou activités à risque
- Les auteurs communs
- Si la violence s'intensifie
- Qui est le plus à risque ?

Journal de sécurité

Security Incident Log			
	Question	**How to Answer**	**Response**
1	Security incident number	Begin with number 1 and continue; the numbering allows security incidents to be linked to one another (see question #14)	
2	Date of incident	Type as YEAR-MONTH-DAY (e.g., 2019-02-17 for February 17, 2019) in order to organize this security event log by date	
3	Time of incident	Specific time of day (if known), or more general (morning, afternoon, evening, night)	
4	Perpetrator	If known and safe to list, or use a more general term such as “law enforcement officer”	
5	Affected organization	Name of HIV program implementing partner (i.e., community-based organization’s name)	
6	Target	Specific person or type of staff, physical space (e.g., name of a specific hot spot), website, database, etc. Do not name individuals here unless you have their permission to do so.	
7	Where incident occurred	Physical address, online, by phone, etc.	

Évaluer les menaces : Quelle est la gravité réelle de la situation ?

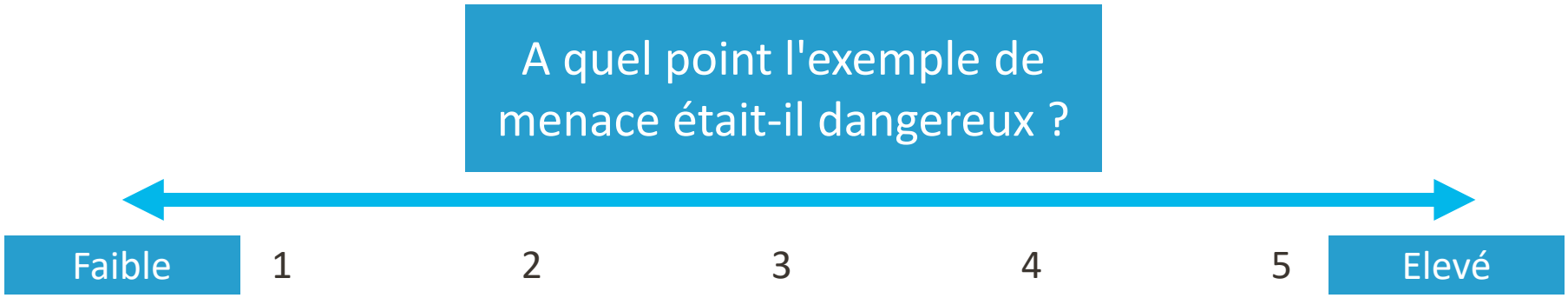
1. Quels sont les faits entourant la menace ?
2. La menace fait-elle partie d'une série qui est devenue plus systématique ou plus fréquente au fil du temps ?
3. Qui est la personne qui profère les menaces ?
4. Quel est l'objectif de la menace ?
5. Pensez-vous que la menace soit sérieuse ?

Exemple

Question	Réponse
Quels sont les faits entourant la menace ?	Un groupe a suivi deux éducateurs pairs dans trois points chauds différents. Le groupe a crié sur les éducateurs en disant qu'ils encourageaient l'immoralité.
Les menaces font-elles partie d'une série qui est devenue plus systématique ou plus fréquente au fil du temps ?	Oui, c'est la troisième fois que ces camarades sont la cible d'agressions verbales. La première fois, c'était il y a un mois, dans un seul point chaud. Maintenant, ils suivent les pairs entre les points chauds.
Qui est la ou les personnes qui profèrent les menaces ?	Il semble s'agir de membres de la communauté locale qui vivent près du point chaud. Plusieurs d'entre eux sont connus pour être membres d'une église qui prêche constamment contre l'homosexualité.
Quel est l'objectif de la menace ?	Pour prévenir la sensibilisation et suivre l'enseignement du ministère.
Pensez-vous que la menace soit sérieuse ?	Un peu. La santé mentale de nos pairs éducateurs est affectée, ce qui est une grande préoccupation. Nous ne pensons pas que le groupe deviendra physiquement violent.

Activité G. Évaluer les menaces en fonction de leur impact

- Après avoir déterminé la gravité d'une menace (c'est-à-dire la probabilité qu'elle se produise), n'oubliez pas de tenir compte de son impact lorsque vous évaluez son potentiel de nuisance.
- Par exemple, une menace qui pourrait entraîner la fermeture de votre organisation est plus dangereuse qu'une menace qui pourrait perturber quelques jours de services.
- À votre avis, quel était le degré de dangerosité de l'exemple de menace ? (tapez votre réponse dans le chat)



Activité H. Considérer nos propres menaces

Question	Réponse
Quels sont les faits entourant la menace ?	
Les menaces font-elles partie d'une série qui est devenue plus systématique ou plus fréquente au fil du temps ?	
Qui est la ou les personnes qui profèrent les menaces ?	
Quel est l'objectif de la menace ?	
Pensez-vous que la menace soit sérieuse ?	

A quel point cette menace est-elle dangereuse ?

Faible 1 2 3 4 5 Elevé

Clôture du premier jour

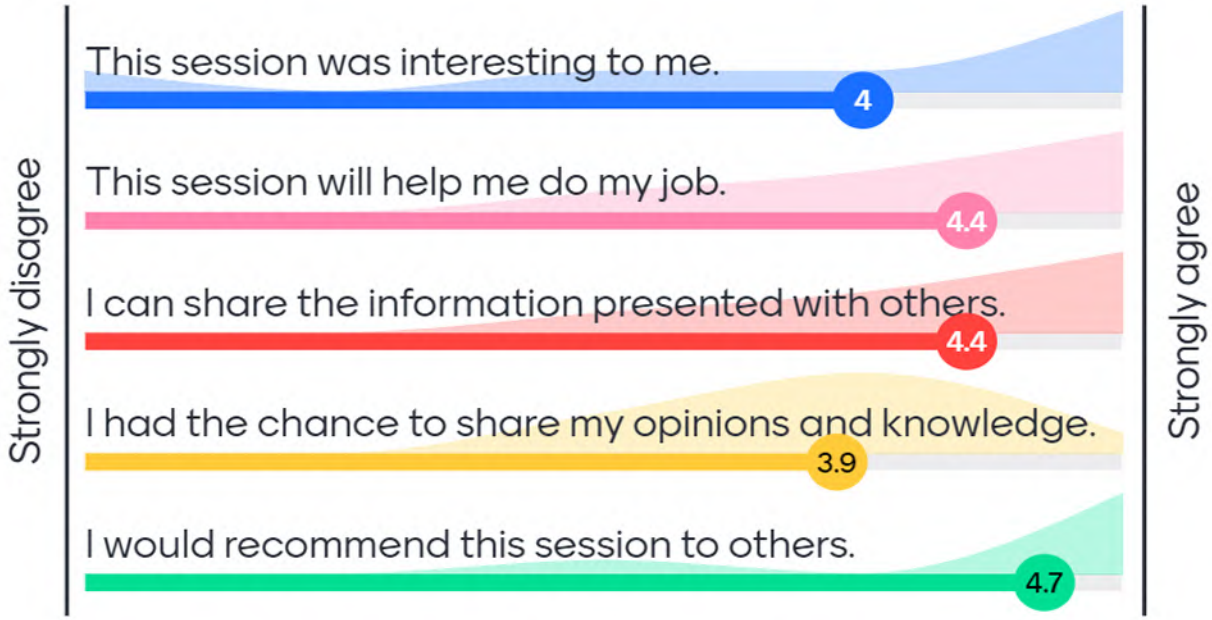
Objectifs de la session

- Évaluer la journée

Activité I. Menti, Clôture du premier jour

Go to **www.menti.com** and use the code **88 64 96 0**

Veuillez vous rendre sur Menti.com et utiliser le code pour partager vos opinions sur la journée.



Jour 2

Nom
Organisation

Récapitulation du premier jour et du devoir # 1

Objectifs de la session

- Partagez les réponses du devoir #1.
- Rappelez-vous les sujets abordés le premier jour.

Activité J. Réflexions sur les recommandations

1. Faire des principes et des approches du programme VIH le fondement des efforts de sécurité.
2. Faites de la sécurité une priorité et attribuez-lui des ressources de manière explicite.
3. Faites de la sécurité du lieu de travail la responsabilité de l'employeur.
4. Planifiez à l'avance et assurez-vous que tout le monde connaît le plan (tout en restant flexible).
5. Discutez explicitement du niveau de risque acceptable pour l'organisation et les individus.
6. Agissez en connaissant à la fois les risques réels et leurs causes sous-jacentes (y compris les cadres juridiques).
7. Reconnaissez les différentes vulnérabilités et capacités de chaque travailleur dans la planification de la sécurité.
8. Apprenez à connaître toutes les parties prenantes, et pas seulement les alliés évidents.
9. Identifiez les menaces (physiques, numériques, psychologiques) et les stratégies de sécurité de manière holistique.
10. Être ensemble, travailler en coalition et apprendre les uns des autres.

Devoir #1

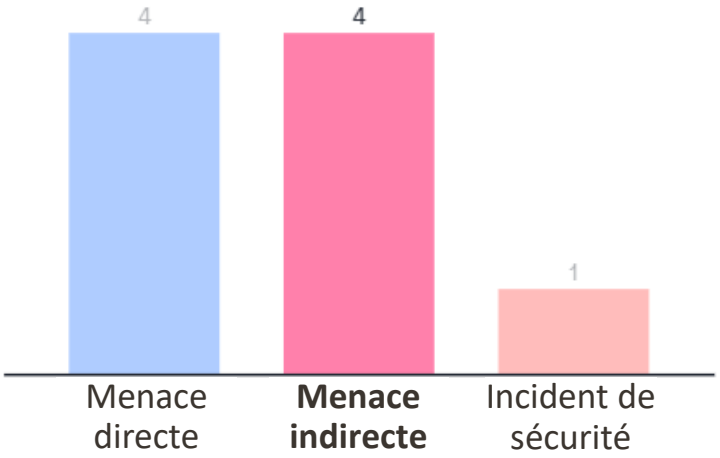
Décrivez : (1) la recommandation, (2) comment votre programme utilise déjà cette recommandation, ET (3) comment le programme pourrait utiliser cette recommandation.

Activité K. Menti Récapitulatif du Jour 1

Go to **www.menti.com** and use the code **38 86 45 9**

Mentimeter

Vous êtes un pair éducateur. Vous apprenez que deux autres pairs éducateurs de votre province ont été arrêtés lors d'une action de sensibilisation. Quel type de menace cela représente-t-il pour vous ?



Press ENTER to hide correct

9

Limiter la capacité de nuire d'un agresseur

Objectif de la session

Décrivez ce qui peut être fait, et par qui, pour limiter la capacité d'un agresseur à causer du tort.

Activité L. De quoi a besoin un attaquant potentiel ?

Un attaquant a besoin :

- D'un accès : à la victime physiquement ou virtuellement.
- Ressources : tout ce qui peut être utilisé pour mener à bien l'attaque - informations sur l'emplacement ou les faiblesses de la victime ; arme ; transport ; argent ; etc.
- Impunité : légale et/ou sociale
- Motif : raison d'agir

Tapez dans le chat : de quoi un attaquant a-t-il besoin pour pouvoir mener une attaque (dans un espace physique ou virtuel) ?

Activité M. Scénario 1 : Sensibilisation

Marvin est un travailleur de proximité pour une organisation qui distribue des préservatifs et des lubrifiants. Il se rend seul dans des lieux, tels que des boîtes de nuit, où les hommes homosexuels se rencontrent. Sur place, il fournit trois préservatifs et trois lubrifiants à chaque personne (dans des sacs pré-emballés, conformément à la politique de l'organisation). Plusieurs semaines de suite, différents hommes dans un bar spécifique ont exigé de manière agressive plus de préservatifs. À chaque fois, Marvin a refusé, expliquant la politique de l'OSC. Un soir, un homme qui avait crié sur Marvin à plusieurs reprises lui jette une bouteille de bière pleine, le frappant durement à la tête.

Que pourrait-on faire pour limiter l'accès, les ressources, le mobile et l'impunité afin d'éviter que cette situation ne se reproduise ?

Scénario 1 réponses possibles

- L'organisation de Marvin pourrait :
  - changer sa politique de distribution de préservatifs (motif)
  - Envoyer des pairs par groupes de deux ou plus (accès/impunité).
  - Cesser de fournir des services à ce point chaud OU ne fournir des services que si les propriétaires du point chaud offrent une meilleure protection au personnel de proximité OU laisser les préservatifs/lubrifiants dans une salle de bain ou un autre endroit (accès/impunité).
  - Engager un champion local au point chaud qui peut distribuer les préservatifs ou expliquer la politique (accès/motivation).
- Marvin pourrait :
  - Signaler les incidents à son organisation pour qu'elle puisse réagir (tous)
  - rencontrer les gens à l'extérieur avant qu'ils n'entrent dans le bar (ressources).

Activité M. Scénario 2 : Clinique

Crystal est une infirmière dans une clinique soutenue par une OSC. Elle fournit des services de santé sexuelle et reproductive aux travailleurs du sexe. Elle a aidé plusieurs d'entre eux à obtenir des conseils pour faire face à des relations violentes. Un matin, un inconnu se présente à la clinique et demande à voir Crystal. La réceptionniste le laisse entrer. Il trouve Crystal et la menace avec un couteau, lui disant qu'elle ferait mieux de "rester en dehors de ma vie privée". Crystal découvre plus tard que l'inconnu est le petit ami violent de l'une des travailleuses du sexe qu'elle a aidées.

Que pourrait-on faire pour limiter l'accès, les ressources, le mobile et l'impunité afin d'éviter que cette situation ne se reproduise ?

Scénario 2 réponses possibles

- L'organisation de Crystal pourrait :
  - Développer et mettre en place une politique d'admission qui inclut le fait de
    - Noter le nom de chaque visiteur et la raison de sa visite (impunité/accès),
    - Rappeler le personnel concerné pour demander si le visiteur est attendu avant de l'admettre (accès),
    - Avoir des zones publiques bien marquées où le personnel vient rencontrer les visiteurs qui ne sont pas des clients (accès/impunité).
    - Vérifier que chaque visiteur n'est pas armé (ressources)
  - Rappelez à tout le personnel de parler aux clients des circonstances dans lesquelles il peut être préférable de ne pas partager des informations avec un partenaire violent (motif).
- Crystal pourrait :
  - Rappeler à ses clients qu'il n'est peut-être pas approprié de partager la nature du soutien qu'ils reçoivent à la clinique avec des partenaires violents (motif).
  - Rappeler à ses clients de ne pas ramener chez eux des documents sur la violence que leur partenaire pourrait voir et auxquels il pourrait réagir négativement (motif).

Activité M. Scénario 3 : Passer de la connexion au hors-ligne

Un travailleur de proximité en ligne, Patrick, rencontre de nouveaux utilisateurs potentiels du service sur Grindr et les encourage à se faire dépister. Les hommes qu'il rencontre sur Grindr veulent souvent le rencontrer hors site avant d'accepter de se rendre dans un établissement clinique. Plusieurs fois, lorsque Patrick a rencontré des utilisateurs potentiels en personne, ils ont voulu avoir des relations sexuelles avec lui. Un homme, Andrew, a été incroyablement insistant. Après que Patrick ait dit qu'il ne souhaitait pas avoir de relations sexuelles, Andrew est venu au bureau de l'OSC à la recherche de Patrick à plusieurs reprises et s'est même présenté à l'autre emploi de Patrick (serveur dans un restaurant) après avoir trouvé des informations sur lui en ligne.

Que pourrait-on faire pour limiter l'accès, les ressources, le mobile et l'impunité afin d'éviter que cette situation ne se reproduise ?

Scénario 3 réponses possibles

- L'organisation de Patrick pourrait
  - Avoir des politiques et des formations claires concernant les informations que chaque travailleur de proximité/sensibilisation en ligne peut partager ; par exemple, pas de photos, pas de noms de famille, pas d'informations personnelles (accès, ressources).
  - Avoir des politiques claires stipulant que les travailleurs de proximité ne peuvent pas avoir de relations avec les clients ; les politiques pourraient être accompagnées de scripts à utiliser si les clients leur demandent d'être impliqués dans une relation (motif)
  - Disposer d'une politique stipulant que les travailleurs de proximité en ligne ne doivent jamais rencontrer hors site les clients qui passent d'une relation en ligne à une relation hors ligne ou qu'un nouvel que le travailleur de proximité doit être la personne chargée de la transition (accès).
  - Avoir une politique sur la façon de protéger le personnel qui pourrait être en danger, y compris des fonds pour la relocalisation (accès).
- Patrick pourrait :
  - Limiter les informations disponibles sur lui-même en ligne (par exemple, ne pas créer un profil LinkedIn comprenant son organisation, son nom complet et sa photo).
  - Signaler immédiatement à l'organisation les clients inquiétants et demander conseil.

Activité M. Scénario 4 : Test d’indexation

Un client indexé partage les noms de trois partenaires sexuels. Mary, un agent de santé, réussit à mettre en relation les partenaires nommés #1 et #3 avec les services mais ne peut pas joindre le partenaire #2 par téléphone. Mary essaie de trouver le partenaire n°2 à domicile. Elle utilise les transports publics, conformément à la politique du programme. Lorsque Marie explique au partenaire n°2 la raison de sa venue, le partenaire n°2 menace Marie avec une casserole d'eau bouillante. Mary part immédiatement. Pendant que Mary doit attendre les transports en commun pour retourner au bureau, elle est extrêmement effrayée.

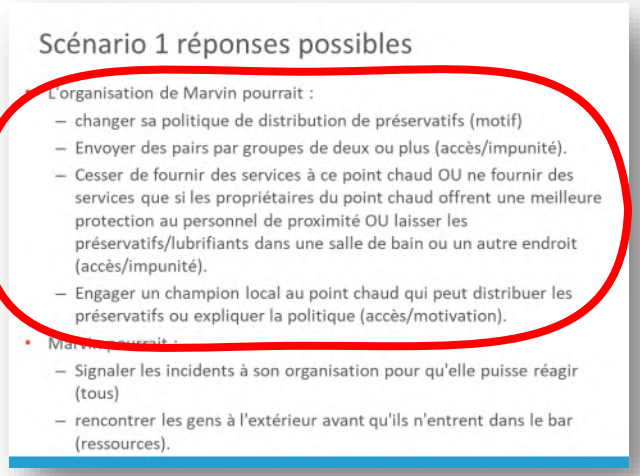
Que pourrait-on faire pour limiter l'accès, les ressources, le mobile et l'impunité afin d'éviter que cette situation ne se reproduise ?

Scénario 4 réponses possibles

- L'organisation de Mary pourrait :
  - S'assurer que tous les clients indexés font l'objet d'un dépistage de la violence du partenaire intime (VPI) afin que les travailleurs de proximité ne se rendent pas au domicile de clients violents (accès).
  - Avoir des politiques qui interdisent les visites au domicile des clients sans autorisation/volontariat (accès)
  - Avoir des politiques qui autorisent le transport privé lors des visites communautaires ou dans des circonstances particulières (accès).
  - Disposer de lignes directrices claires pour les tests d'indexation qui dictent les modalités appropriées dans différentes circonstances (accès, motif).
  - Avoir des politiques qui stipulent que personne ne doit faire de la sensibilisation seul (accès/impunité).
- Mary pourrait :
  - Suggérer qu'un événement de sensibilisation ait lieu dans la communauté du partenaire n°2 ; plusieurs personnes peuvent être invitées à y assister, y compris le partenaire n°2 (motif).

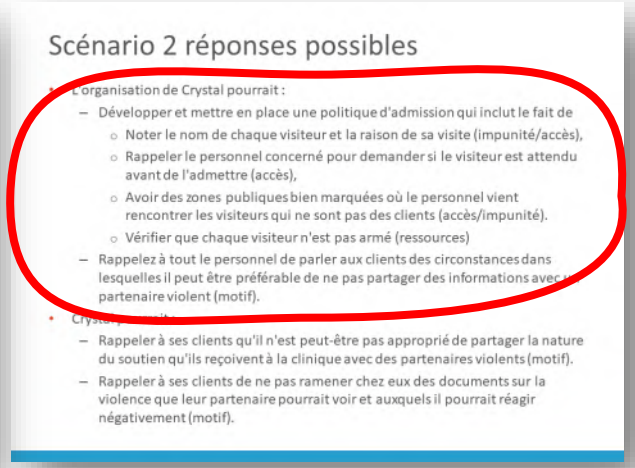
Activité N. Qu'est-ce que ces solutions ont en commun ?

Dans chaque scénario, les solutions relèvent principalement de la responsabilité de l'organisation et non de l'individu. Les organisations reconnaissent leur responsabilité envers la sécurité de leurs travailleurs. Elles ne se contentent pas de s'en remettre au meilleur jugement du personnel ou des bénévoles.



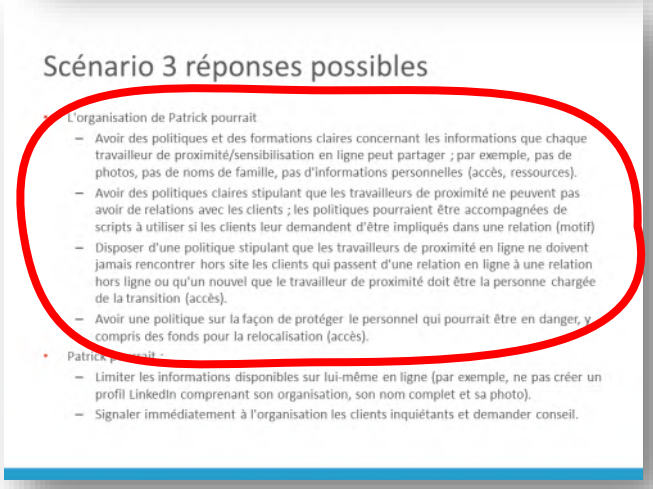
Scénario 1 réponses possibles

- L'organisation de Marvin pourrait :
  - changer sa politique de distribution de préservatifs (motif)
  - Envoyer des pairs par groupes de deux ou plus (accès/impunité).
  - Cesser de fournir des services à ce point chaud OU ne fournir des services que si les propriétaires du point chaud offrent une meilleure protection au personnel de proximité OU laisser les préservatifs/lubrifiants dans une salle de bain ou un autre endroit (accès/impunité).
  - Engager un champion local au point chaud qui peut distribuer les préservatifs ou expliquer la politique (accès/motivation).
- Marvin pourrait :
  - Signaler les incidents à son organisation pour qu'elle puisse réagir (tous)
  - rencontrer les gens à l'extérieur avant qu'ils n'entrent dans le bar (ressources).



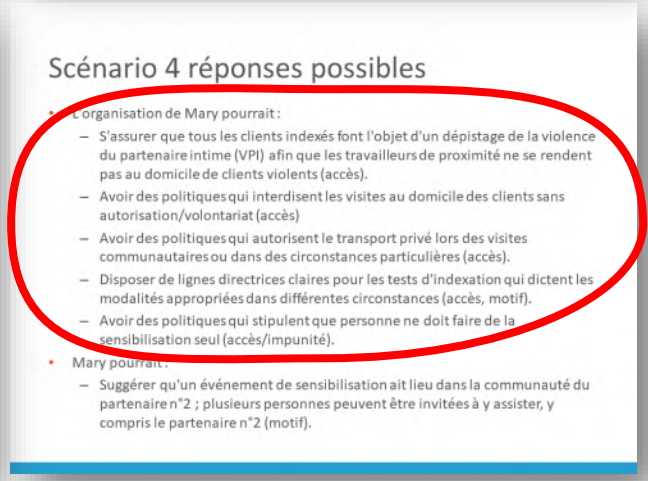
Scénario 2 réponses possibles

- L'organisation de Crystal pourrait :
  - Développer et mettre en place une politique d'admission qui inclut le fait de
    - Noter le nom de chaque visiteur et la raison de sa visite (impunité/accès),
    - Rappeler le personnel concerné pour demander si le visiteur est attendu avant de l'admettre (accès),
    - Avoir des zones publiques bien marquées où le personnel vient rencontrer les visiteurs qui ne sont pas des clients (accès/impunité).
    - Vérifier que chaque visiteur n'est pas armé (ressources)
  - Rappelez à tout le personnel de parler aux clients des circonstances dans lesquelles il peut être préférable de ne pas partager des informations avec [illegible] partenaire violent (motif).
- Crystal pourrait :
  - Rappeler à ses clients qu'il n'est peut-être pas approprié de partager la nature du soutien qu'ils reçoivent à la clinique avec des partenaires violents (motif).
  - Rappeler à ses clients de ne pas ramener chez eux des documents sur la violence que leur partenaire pourrait voir et auxquels il pourrait réagir négativement (motif).



Scénario 3 réponses possibles

- L'organisation de Patrick pourrait
  - Avoir des politiques et des formations claires concernant les informations que chaque travailleur de proximité/sensibilisation en ligne peut partager ; par exemple, pas de photos, pas de noms de famille, pas d'informations personnelles (accès, ressources).
  - Avoir des politiques claires stipulant que les travailleurs de proximité ne peuvent pas avoir de relations avec les clients ; les politiques pourraient être accompagnées de scripts à utiliser si les clients leur demandent d'être impliqués dans une relation (motif)
  - Disposer d'une politique stipulant que les travailleurs de proximité en ligne ne doivent jamais rencontrer hors site les clients qui passent d'une relation en ligne à une relation hors ligne ou qu'un nouvel que le travailleur de proximité doit être la personne chargée de la transition (accès).
  - Avoir une politique sur la façon de protéger le personnel qui pourrait être en danger, y compris des fonds pour la relocalisation (accès).
- Patrick pourrait :
  - Limiter les informations disponibles sur lui-même en ligne (par exemple, ne pas créer un profil LinkedIn comprenant son organisation, son nom complet et sa photo).
  - Signaler immédiatement à l'organisation les clients inquiétants et demander conseil.



Scénario 4 réponses possibles

- L'organisation de Mary pourrait :
  - S'assurer que tous les clients indexés font l'objet d'un dépistage de la violence du partenaire intime (VPI) afin que les travailleurs de proximité ne se rendent pas au domicile de clients violents (accès).
  - Avoir des politiques qui interdisent les visites au domicile des clients sans autorisation/volontariat (accès)
  - Avoir des politiques qui autorisent le transport privé lors des visites communautaires ou dans des circonstances particulières (accès).
  - Disposer de lignes directrices claires pour les tests d'indexation qui dictent les modalités appropriées dans différentes circonstances (accès, motif).
  - Avoir des politiques qui stipulent que personne ne doit faire de la sensibilisation seul (accès/impunité).
- Mary pourrait :
  - Suggérer qu'un événement de sensibilisation ait lieu dans la communauté du partenaire n°2 ; plusieurs personnes peuvent être invitées à y assister, y compris le partenaire n°2 (motif).

Sécurité numérique

Objectif de la session

Décrire les vulnérabilités inhérentes aux plateformes numériques et identifier les stratégies de réduction des risques dans chacune d'elles.

Activité O. Menti : Quels appareils utilisez-vous et que disent-ils de vous ?

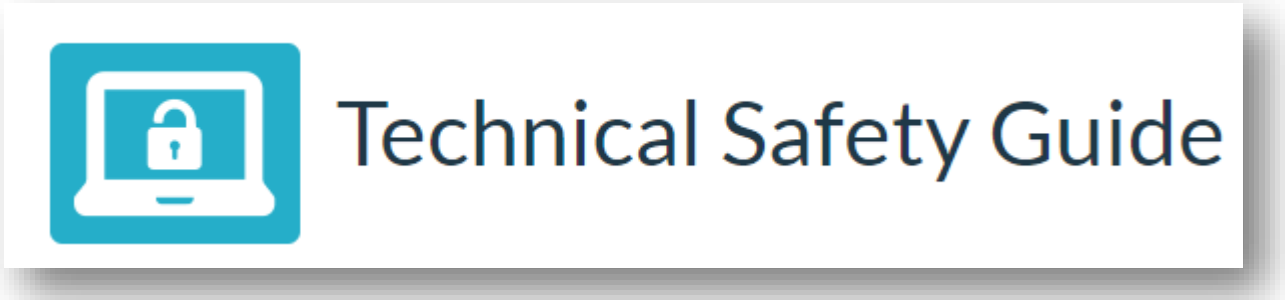
- Quels appareils utilisez-vous dans votre vie quotidienne ?
- Que pourrait-on apprendre sur vous si l'on avait accès à votre téléphone/tablette/ordinateur ?

Utilisez des mots de passe et renforcez-les

- Ayez-en plus d'un.
- Changez régulièrement vos mots de passe (conseil : réinitialisez vos mots de passe, puis programmez un rappel sur votre téléphone trois mois après ce jour pour les changer, et répétez).
- Un mot de passe fort comporte environ 10 caractères ou plus, dont idéalement : des lettres majuscules, des lettres minuscules, des chiffres et des symboles.

Utilisez la vérification en deux étapes

- Les courriels, les médias sociaux et d'autres sites vous permettent d'activer la vérification en deux étapes, qui vous demande un code à partir d'une application ou vous envoie par SMS un numéro à saisir lorsque vous ou quelqu'un d'autre tente de se connecter à votre compte depuis un navigateur ou un ordinateur inconnu.
- C'est une petite gêne pour vous, mais une énorme gêne pour quelqu'un qui essaie de s'introduire dans votre compte.
- https://iheartmob.org/resources/tech

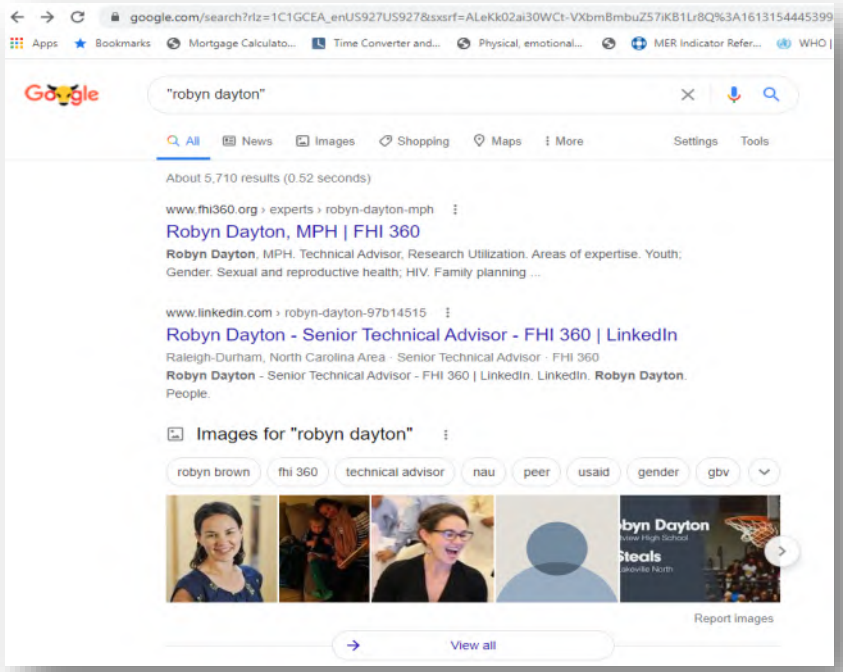


KeePass

- Gestionnaire de mots de passe gratuit et libre (open source)
- Maintien de la sécurité des mots de passe
- Vous n'avez qu'à vous souvenir d'un seul passe-partout pour déverrouiller toute la base de données de vos mots de passe.
- https://keepass.info/

Recherchez vous

- Tout, depuis notre nom et notre adresse électronique jusqu'à notre adresse personnelle et nos informations bancaires, est en ligne.
- Une fois que vous avez trouvé des informations vous concernant en ligne, faites en sorte de les supprimer.



Limitez ce que vous partagez sur vous-même

- Ne donnez pas de détails sur votre lieu de résidence ou sur les endroits que vous aimez fréquenter.
- Ne marquez pas l'endroit où vous vous trouvez et ne publiez pas de photos permettant aux gens de vous localiser.
- Méfiez-vous du partage automatique de l'emplacement sur les médias sociaux (appareils équipés d'un GPS).

Crédit Photo: Tomas Nozina

Où sont ces gens ?

Crédit Photo : Loly Galina

Limitez ce que vous partagez sur vous-même (suite)

- Évitez de partager des informations qui permettraient à d'autres de connaître votre emploi du temps quotidien.
- Évitez de publier des informations qui pourraient être utilisées pour connaître les réponses à vos questions de sécurité :
  - le nom d'un animal de compagnie de votre enfance
  - votre date de naissance complète
- https://safequeers.org/ a plus d'informations sur l'utilisation sûre des sites de rencontre, etc.

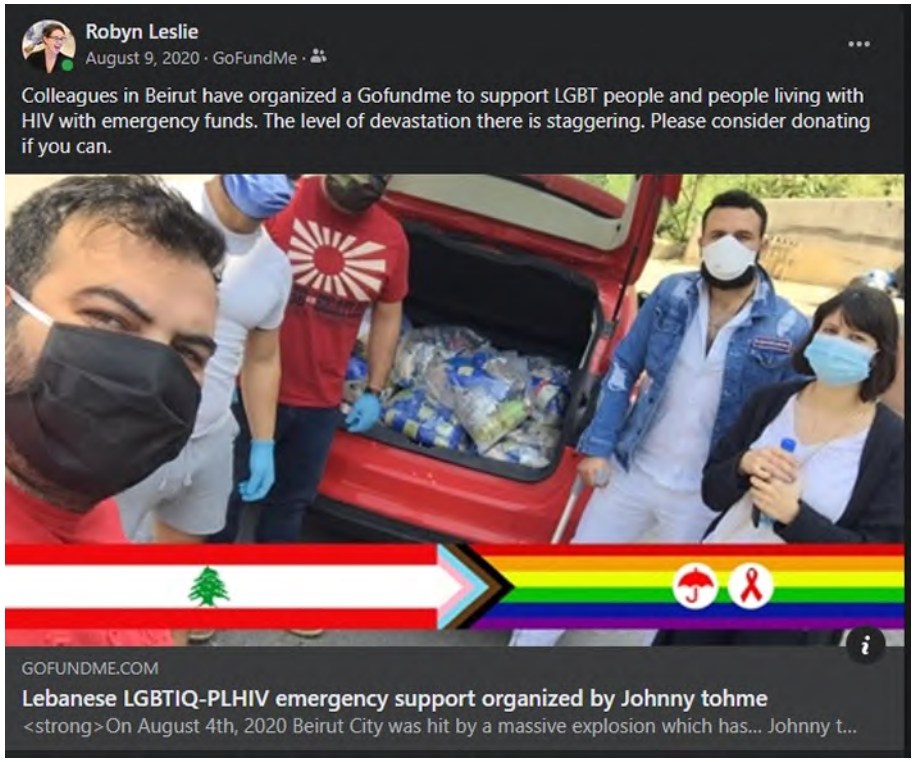
Lorsque les informations sont utilisées contre nous

- On parle de "doxxing" lorsque des personnes recherchent et publient sur internet des informations privées sur une autre personne à laquelle elles souhaitent nuire.
- Il s'agit d'une tactique utilisée pour que les individus se sentent en danger.
- Le doxxing est plus facile que jamais car la plupart de nos informations sont en ligne.

Activité P : Que partageons-nous sur les médias sociaux ?

- Quels sont les médias sociaux que vous utilisez ?
- Que pourrait-on y apprendre sur vous ?

Question Q. Qu'est-ce que quelqu'un pourrait apprendre sur moi à partir de ces publications sur les médias sociaux ?



Limitez ce que vous partagez sur les autres

- Les photos et les vidéos révèlent rapidement des identités, des lieux et des informations personnelles.
- Obtenez un consentement avant de prendre et de publier des photos.
- Les appareils photo intègrent des données cachées. Les sites de partage de photos peuvent inclure ce contenu lorsque vous téléchargez la photo. Faites attention !
- Si les photos sont interdites dans certains espaces, diffusez largement cette information.

Si vous êtes harcelé en ligne, vous pouvez agir

- **Ignorez-les ou bloquez-les -** s'engager peut devenir accablant.
- **Signalez-les -** et demandez à vos amis de les signaler ! Utilisez les guides de sécurité des médias sociaux pour en savoir plus sur la manière de signaler un cas sur Facebook, Instagram, etc.
- **Dénoncez-les** - vous pouvez prendre des photos du harcèlement et les tenir pour responsables en partageant la preuve de leur harcèlement.
- **Engagez-le**s - en expliquant la position que vous avez adoptée.
- **Cherchez du soutien** - cela peut être traumatisant ; parlez-en à quelqu'un qui vous soutient.
- **Restez anonyme** - par exemple, joignez un autre courriel à votre compte de médias sociaux.

Activité R. Avez-vous utilisé l'une de ces méthodes ? Quel a été le résultat ?

Social Media Safety Guides

Staying safe on social media- We've got your back!

Introducing our new Social Media Safety Guides for Facebook, Twitter, Reddit, Tumblr, and Youtube! We have worke… …er for you to stay safer online. Every guide gives user-friendly information on how use different platforms' reporting and privacy tools – and for t… …ation is gathered in one location.

Twitter Facebook Instagram Tumblr Reddit Youtube

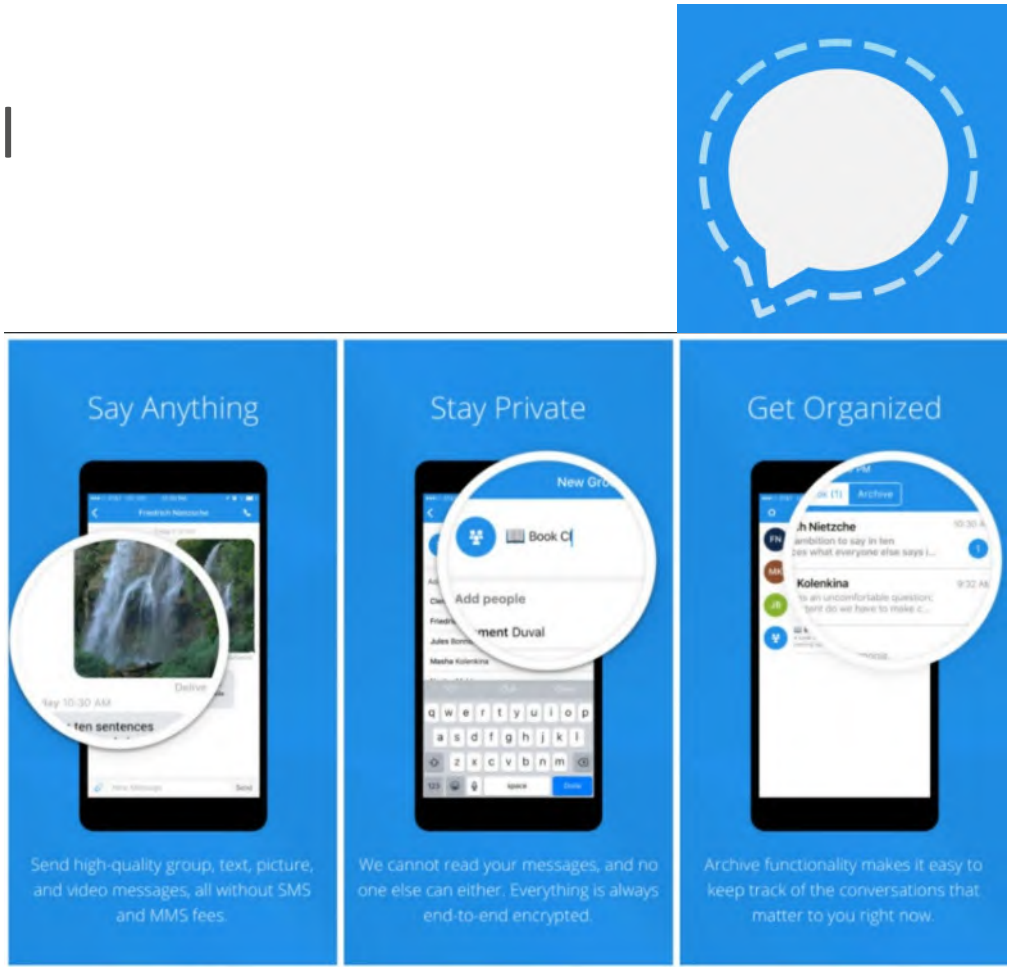
Options de messages

- WhatsApp est une option de communication populaire (2 milliards d'utilisateurs mensuels) appartenant à Facebook.
- La communication est cryptée de bout en bout, mais de grandes lacunes en matière de sécurité subsistent :
  - Toute personne disposant de votre numéro de téléphone peut voir : votre texte de présentation et votre photo, la date de votre dernière connexion et si vous avez lu un message (vérifiez les paramètres de confidentialité pour les modifier).
  - Facebook peut accéder aux informations suivantes : qui vous contactez, quand, à quelle fréquence et à partir de quel endroit (ces informations ne peuvent pas être désactivées).
  - Les policiers munis d'un mandat peuvent demander à Facebook : vos appels et messages entrants et sortants.
  - Si vous choisissez de sauvegarder vos données WhatsApp sur iCloud ou Google Drive, les messages n'y sont pas cryptés.

https://www.consumerreports.org/privacy/how-to-use-whatsapp-privacy-settings/?EXTKEY=YSOCIAL_FB&fbclid=IwAR2du8xBV9DPWCBUyELt5kxQdd41glfDyzhe0_tRe7TXbC8n3ScqZ7m1kCY

Si ce n'est pas WhatsApp, quoi d'autre ?

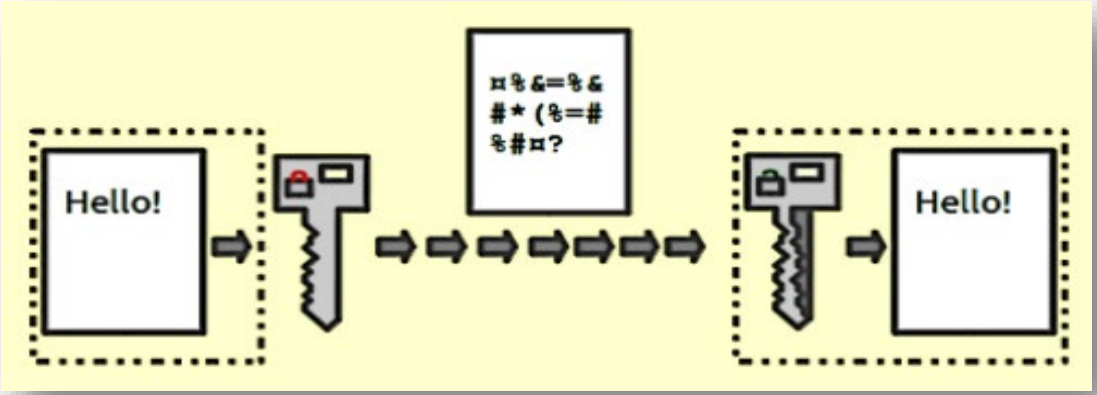
- Signal (application gratuite) est plus sûr ; il est crypté de bout en bout.
- Possibilité d'effectuer des appels audio de groupe
- Vous pouvez envoyer des messages qui disparaîtront au bout d'un certain temps.



Cryptage et protection des documents

- Envisagez le cryptage (Veracrypt vous permet de créer un dossier secret qui ne sera visible que si vous savez comment le chercher).
- Envisagez de changer les noms de fichiers sur votre ordinateur
- Au lieu de " HSH proximité location_X ".
- Utilisez "Activités du projet_Nom de code pour l'emplacement X".

Qu’est ce que le cryptage ?



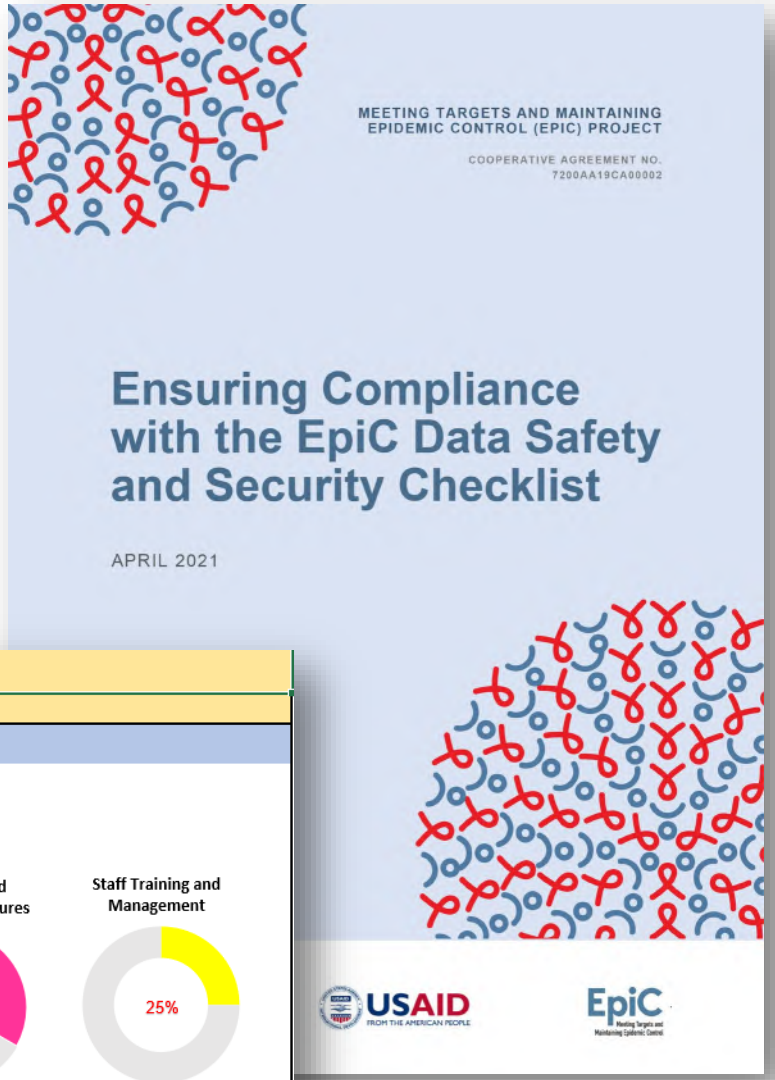
https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537

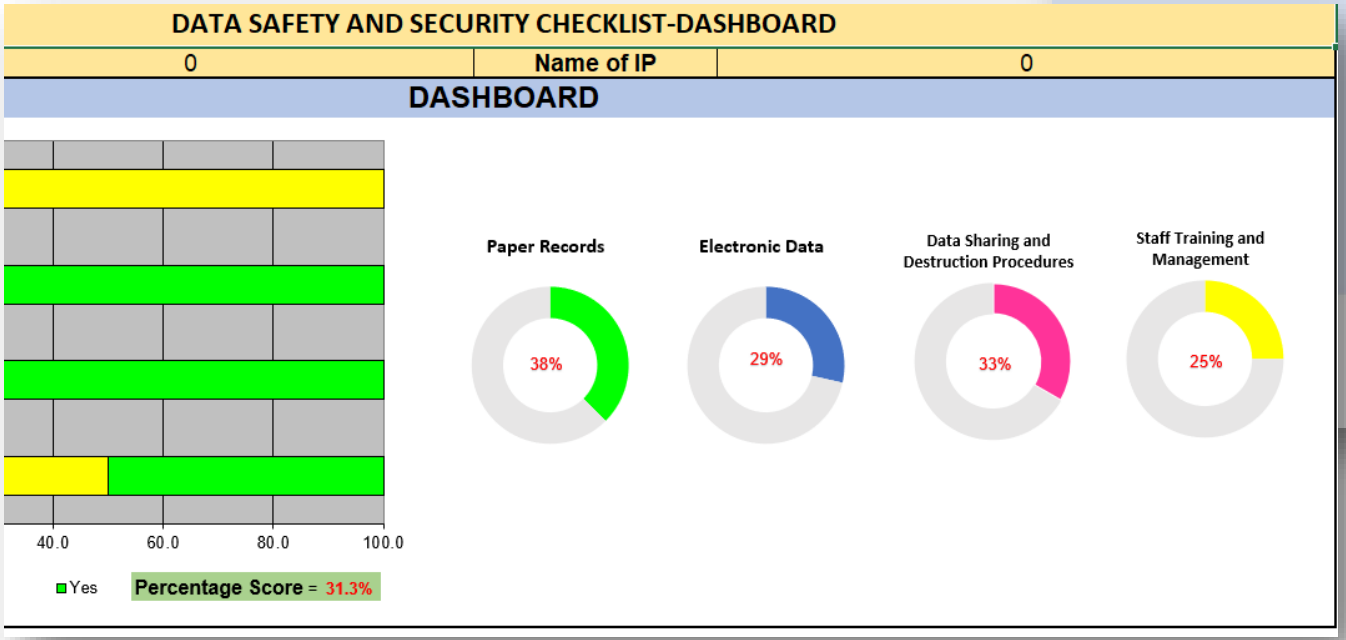
Activité S. Relier les problèmes aux solutions

Problème	Réponse	Options de solution
1. Les travailleurs de proximité en ligne reçoivent des avances sexuelles non désirées	**A, B, C D, E**	A. Inclure des conseils sur ce que les travailleurs en ligne peuvent partager, y compris les noms/photos/localisations.
2. Les travailleurs de proximité en ligne sont harcelés par des clients	**A, B, C, D, E**	B. Fournir des scripts pour guider les conversations en ligne et répondre aux avances sexuelles
3. Des clients font du chantage à leurs pairs en utilisant des captures d'écran de conversations en ligne.	**A, B, C, D, E**	C. Utilisez des groupes fermés sur Facebook (ou une autre plateforme) et mettez en place un processus de vérification de l'identité des personnes avant qu'elles n'y adhèrent.
		D. Partagez les noms/photos des harceleurs habituels afin qu'ils ne participent pas à des programmes en ligne.
		E. Avoir des politiques qui empêchent les travailleurs d'avoir des relations amoureuses avec les clients

Outils et conseils supplémentaires spécifiques à l'information stratégique

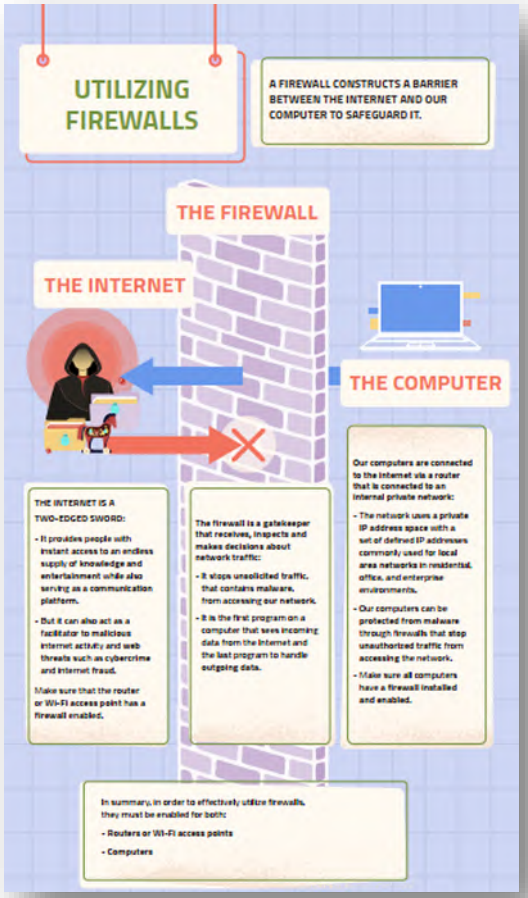
https://www.fhi360.org/resource/implementer-and-data-security





Outils et indication supplémentaires : Sécurité en ligne générale

- En collaboration avec LINKAGES, la [Fondation arabe pour les libertés et l'égalité] a développé une formation virtuelle sur la sécurité numérique à la fois pour les exécuteurs et les bénéficiaires de programmes pour une utilisation sure d'internet.
- Les formations en ligne adaptées à votre rythme sont disponibles sur: https://afemena.org/digital-security-sessions/



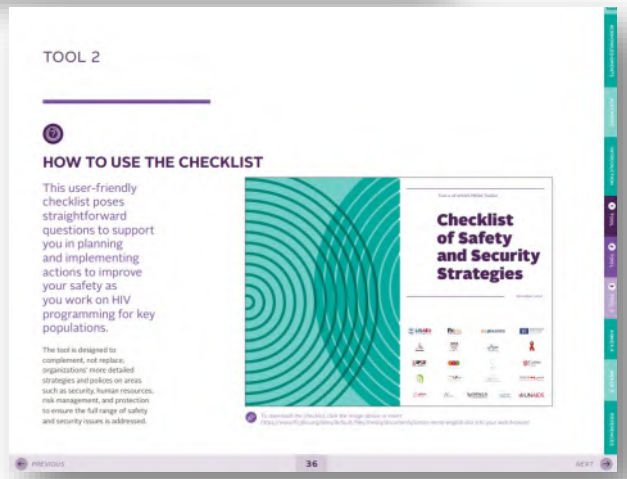
Outils et indication supplémentaires : Sécuriser l'utilisation des appareils et applications mobiles

- Soutenir les organisations à sécuriser les appareils et applications mobiles
- Sujets:
  - Choisir les appareils
  - Déployer/gérer les appareils
  - Gestion de cas virtuelle
  - Protection et vie privée du client
- Site web: https://www.fhi360.org/sites/default/files/media/documents/resource-secure-mobile-devices-apps.pdf

Examiner nos propres capacités et planifier le partage des compétences

Objectifs de la session

- Passez en revue les réponses collectives aux évaluations de sécurité (listes de vérification).
- Affectez chaque partenaire de mise en œuvre à une compétence qui sera présentée lors de la prochaine session.



La liste de vérification que chaque partenaire doit remplir fait partie de la boîte à outils AMAN MENA (Secure in MENA). Un hyperlien vers la liste de vérification se trouve au début de l'outil 2 de la boîte à outils, disponible en arabe, anglais et français. Les trois boîtes à outils sont disponibles ici : https://www.fhi360.org/resource/aman-mena-toolkit

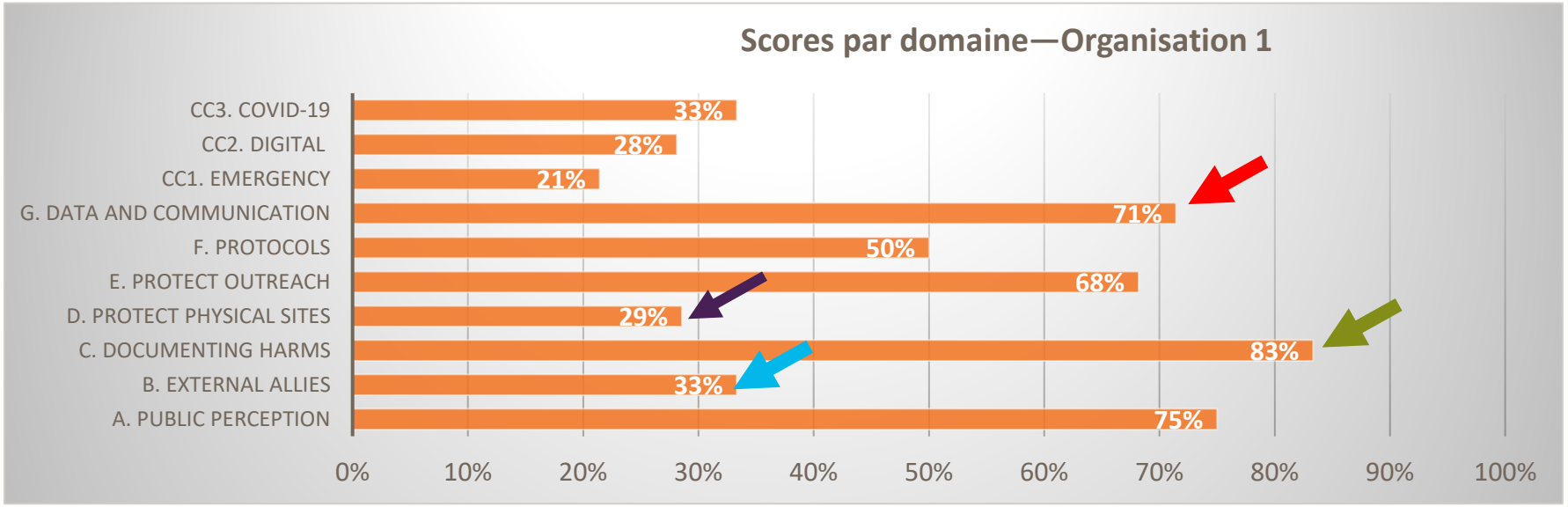
Etape 1

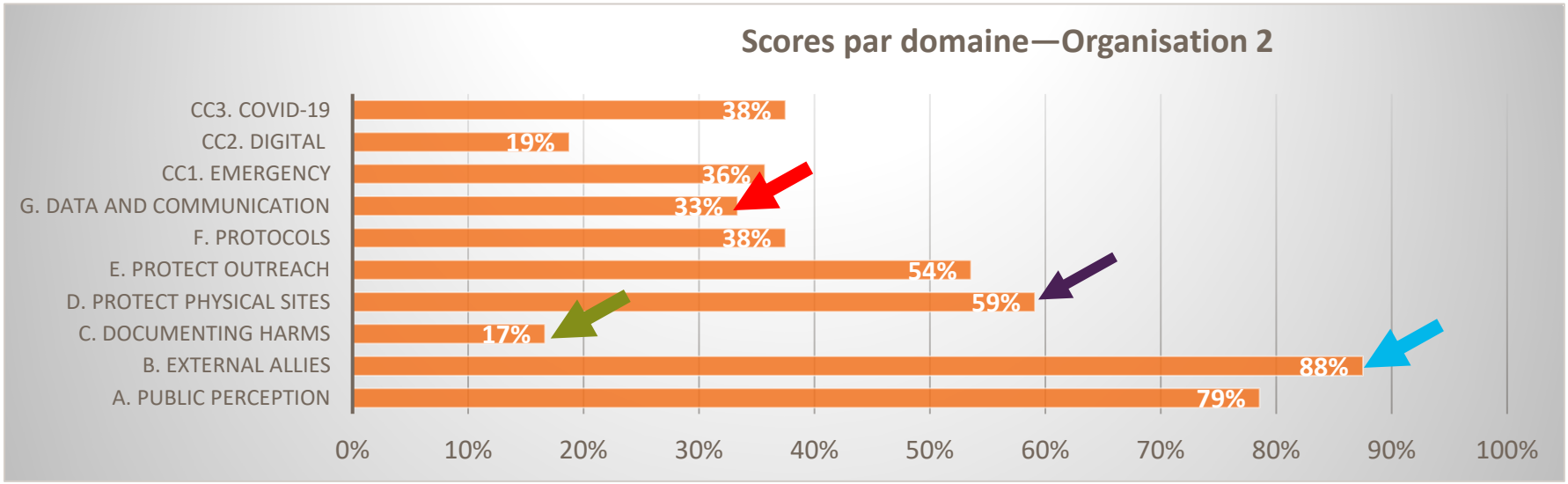
Domaines de sécurité évalués dans la liste de vérification

A. Cultiver et sensibiliser les alliés externes
B. Influencer la perception publique du projet ou de l'organisation
C. Documenter les préjudices pour le suivi et le plaidoyer
D. Protection des bureaux, des centres d'accueil et d'autres lieux physiques
E. Assurer la sécurité des travailleurs lors des actions de sensibilisation physiques et numériques
F. Développer des protocoles de sécurité fonctionnels et institutionnalisés, y compris pour les urgences.
G. Assurer la sécurité des données et des communications
H. Questions transversales : préparation aux situations d'urgence, sécurité numérique, COVID-19

	Strategy	Yes	No	Somewhat	Not applicable	Notes and score
	C. Documentation of harms for tracking and advocacy To be completed by both (1) the organization leading the project and/or the umbrella agency and (2) individual organizations implementing activities (with each organization filling out their own survey)					
23	Does the organization document abuses against its beneficiaries and/or staff?	1				
24	Does the organization keep an anonymized list of security incidents that have affected their operations?		1			
25	Does the organization analyze documented abuses or threats to predict future safety issues or perform advocacy?			1		
26	Does the organization document surges in abuse related to crises such as COVID-19?				1	
	TOTAL	1	1	1	1	
	SCORE PART C					50.0%

Activité T (partie 1). Missions d'apprentissage de l'exécutant





Activité T (partie 2). Missions d'apprentissage de l'exécutant

- Examinez le domaine que vous allez enseigner
- Choisissez au moins une stratégie dans ce domaine que vous aimeriez partager avec les autres.
- Créez quatre diapositives
- Diapositive de titre : Nom de l'organisation et nom du sujet
- Comment mettre en œuvre cette stratégie
- Tout outil pour soutenir la mise en œuvre
- Résultats des preuves anecdotiques sur la façon dont cette stratégie a été utile.
- Vous disposerez de 10 minutes pour votre présentation, puis de 5 minutes pour les questions.
- Les présentations auront lieu à X heure, à Y date.

Devoirs :

? ?? = perception du public (A)

? ?? = alliés extérieurs (B)

? ?? = documentation des préjudices (C)

? ?? = protéger les sites physiques (D)

? ?? = protéger la sensibilisation (E)

? ?? = protocoles (F)

? ?? = données et communication (G)

? ?? = urgences (CC1)

? ?? = sécurité numérique (CC2)

? ?? = COVID-19 (CC3)

Activité T (partie 3). Exemple

- L’OSC "Santé pour tous et pour chacun" est affectée au domaine C : Documentation des préjudices.
- L’OSC examine les stratégies du domaine C et en choisit au moins une à partager avec l'ensemble de l'équipe.

	Strategy	Yes	No	Somewhat	Not applicable	Notes and score
	C. Documentation of harms for tracking and advocacy To be completed by both (1) the organization leading the project and/or the umbrella agency and (2) individual organizations implementing activities (with each organization filling out their own survey)					
23	Does the organization document abuses against its beneficiaries and/or staff?	1				
24	Does the organization keep an anonymized list of security incidents that have affected their operations?		1			
25	Does the organization analyze documented abuses or threats to predict future safety issues or perform advocacy?			1		
26	Does the organization document surges in abuse related to crises such as COVID-19?				1	
	TOTAL	1	1	1	1	
	SCORE PART C					50.0%

Clôture du jour 2

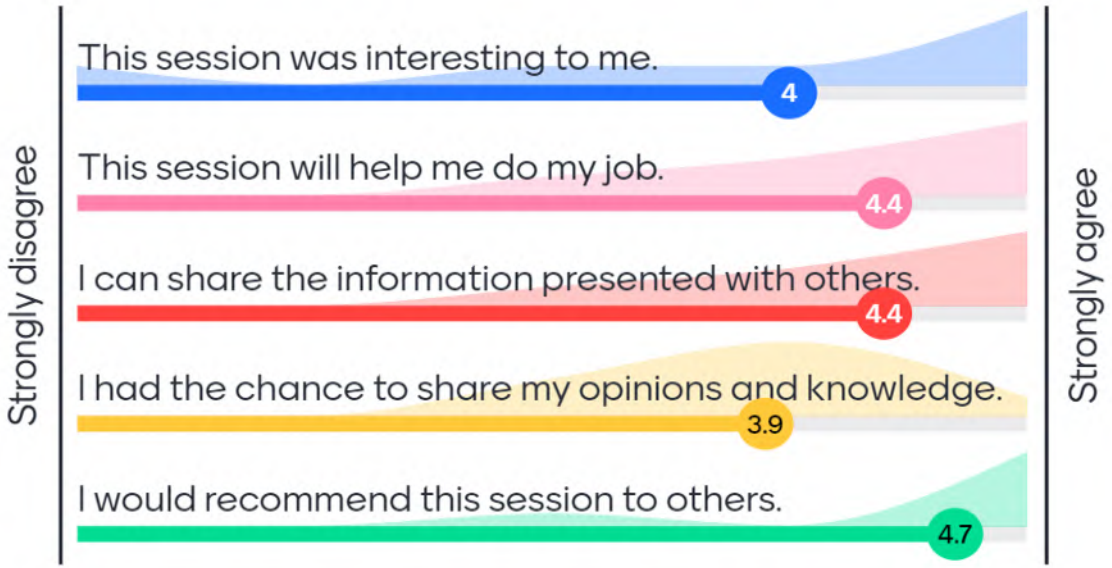
Objectif de la session

Compléter l'évaluation du jour 2

Activité U. Clôture jour 2

Go to **www.menti.com** and use the code **88 64 96 0**

Veuillez vous rendre sur Menti.com et utiliser le code pour partager vos opinions sur la journée.



JOUR 3
Présentations du groupe

Nom
Organisation

Objectifs de la session

- Partagez une stratégie de sécurité attribuée à votre OSC.
- Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.

Activité V. Présentations des partenaires exécutants

- Chacune doit comporter
  - Une diapositive de titre : Nom de l'organisation et nom du sujet
  - Comment mettre en œuvre cette stratégie
  - Tout outil pour soutenir la mise en œuvre
  - Résultats des preuves anecdotiques sur la façon dont cette stratégie a été utilisée.

JOUR 4

NOM
OrganiSation

Récapitulatif du jour 2 et réflexions de la session spéciale

Objectifs de la session

- Réfléchissez aux stratégies présentées lors de la session spéciale.
- Se souvenir des sujets abordés le deuxième jour.

Activité W. Principaux points à retenir

- En pensant aux compétences et aux stratégies que vous avez apprises de vos collègues lors de la dernière session, partagez quelques idées que vous comptez utiliser dans votre organisation.

Activité X. Rappel du Jour 2

- Menti.com

Utiliser ce que vous avez appris : Scénarios de défis de sécurité

Objectifs de la session

- Réfléchissez à ce que votre organisation pourrait faire si elle était confrontée à divers problèmes de sécurité.
- Discutez si les "solutions possibles" après chaque scénario seraient appropriées dans le contexte local.

Huit scénarios d'incidents de sécurité

1. Les chefs religieux locaux affirment que votre organisation encourage le péché en distribuant des préservatifs et des lubrifiants. En conséquence, les violences physiques et verbales à l'encontre des éducateurs pour les pairs se multiplient.
2. Un travailleur signale qu'il a été harcelé par un autre travailleur.
3. Une travailleuse de proximité est arrêtée alors qu'elle distribue des préservatifs ; elle est détenue par la police.
4. Après une activité de sensibilisation au VIH dans un point chaud, un bénéficiaire met des photos des travailleurs de proximité et des membres des PC sur Facebook et les étiquette.
5. Le bureau de votre organisation fait l'objet d'une descente ; la police prend tous les dossiers et les ordinateurs.
6. Un article hostile à votre organisation est publié dans le journal. Il donne l'adresse de votre clinique et comprend des photos de deux de vos cliniciens.
7. Un bénéficiaire menace de chantage l'un de vos travailleurs de proximité. Le bénéficiaire dit qu'il dira aux parents du travailleur de proximité que celui-ci est homosexuel.
8. Une infirmière se rend au domicile d'un homme nommé par un client indexé. L'homme réagit violemment. Il attaque le travailleur de proximité et lui inflige plusieurs blessures. Il le retient également contre sa volonté pendant trois heures.

Activité Y. Utiliser ce que vous avez appris

Nom de l'exécutant partenaire	Etude de cas
	1
	2
	3
	4

Nom de l'exécutant partenaire	Etude de cas
	5
	6
	7
	8

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne se produise, pour atténuer ou prévenir les préjudices causés ?

Une fois que le groupe présente ses réponses, quelques solutions possibles seront montrées. Le groupe qui présente ses réponses doit réagir aux solutions possibles, en notant si certaines d'entre elles sont inappropriées ou non pertinentes dans leur contexte ou si elles pourraient être de bons compléments à ce qu'il a déjà présenté.

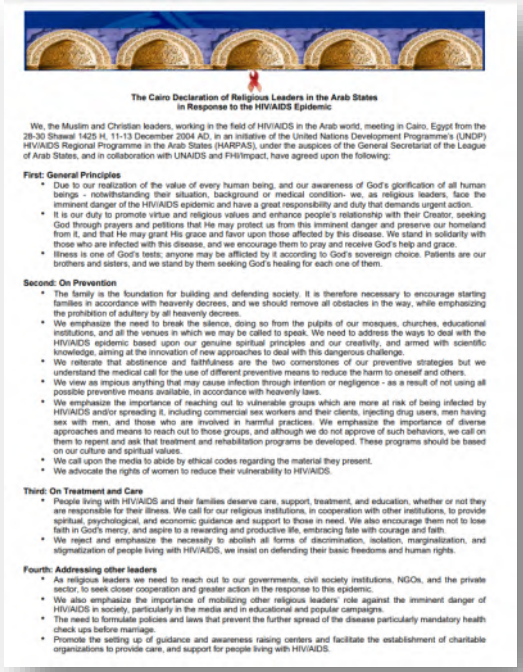
Activité Y. Scénario 1

Les chefs religieux locaux affirment que votre organisation encourage le péché en distribuant des préservatifs et des lubrifiants. En conséquence, les violences physiques et verbales à l'encontre des éducateurs pairs se multiplient.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 1 – Solutions possibles

- À l'avance :
  - Travaillez avec les chefs religieux pour expliquer votre travail. Fournir des soins de santé aux plus vulnérables s'aligne sur l'enseignement de la plupart des grandes religions. Les chefs religieux peuvent être de puissants défenseurs des programmes de lutte contre le VIH.
  - Tenez un registre de suivi des incidents de sécurité afin de savoir clairement quelles sont les zones où les abus se multiplient.
- Après l'incident :
  - Fournir un soutien aux éducateurs pour les pairs touchés (y compris les soins de santé mentale et physique, les services juridiques et autres services psychosociaux).
  - Réduire les activités de sensibilisation dans les zones particulièrement touchées, au moins temporairement.
  - Rendre compte au donateur du problème, des réponses proposées et de tout changement prévu dans la capacité à atteindre les objectifs/cibles.
  - Demandez aux responsables locaux de la santé d'entrer en contact avec les chefs religieux et/ou de convoquer une réunion où il est possible d'expliquer la nature de votre travail et son alignement sur les objectifs du gouvernement en matière de santé publique.



The Cairo Declaration of Religious Leaders in the Arab States In Response to the HIV/AIDS Epidemic

We, the Muslim and Christian leaders, working in the field of HIV/AIDS in the Arab world, meeting in Cairo, Egypt from the 28-30 Shawal 1425 H, 11-13 December 2004 AD, in an initiative of the United Nations Development Programme's (UNDP) HIV/AIDS Regional Programme in the Arab States (HARPAS), under the auspices of the General Secretariat of the League of Arab States, and in collaboration with UNAIDS and FHI/Impact, have agreed upon the following:

First: General Principles

- Due to our realization of the value of every human being, and our awareness of God's glorification of all human beings - notwithstanding their situation, background or medical condition- we, as religious leaders, face the imminent danger of the HIV/AIDS epidemic and have a great responsibility and duty that demands urgent action.
- It is our duty to promote virtue and religious values and enhance people's relationship with their Creator, seeking God through prayers and petitions that He may protect us from this imminent danger and preserve our homeland from it, and that He may grant His grace and favor upon those affected by this disease. We stand in solidarity with those who are infected with this disease, and we encourage them to pray and receive God's help and grace.
- Illness is one of God's tests; anyone may be afflicted by it according to God's sovereign choice. Patients are our brothers and sisters, and we stand by them seeking God's healing for each one of them.

Second: On Prevention

- The family is the foundation for building and defending society. It is therefore necessary to encourage starting families in accordance with heavenly decrees, and we should remove all obstacles in the way, while emphasizing the prohibition of adultery by all heavenly decrees.
- We emphasize the need to break the silence, doing so from the pulpits of our mosques, churches, educational institutions, and all the venues in which we may be called to speak. We need to address the ways to deal with the HIV/AIDS epidemic based upon our genuine spiritual principles and our creativity, and armed with scientific knowledge, aiming at the innovation of new approaches to deal with this dangerous challenge.
- We reiterate that abstinence and faithfulness are the two cornerstones of our preventive strategies but we understand the medical call for the use of different preventive means to reduce the harm to oneself and others.
- We view as impious anything that may cause infection through intention or negligence - as a result of not using all possible preventive means available, in accordance with heavenly laws.
- We emphasize the importance of reaching out to vulnerable groups which are more at risk of being infected by HIV/AIDS and/or spreading it, including commercial sex workers and their clients, injecting drug users, men having sex with men, and those who are involved in harmful practices. We emphasize the importance of diverse approaches and means to reach out to those groups, and although we do not approve of such behaviors, we call on them to repent and ask that treatment and rehabilitation programs be developed. These programs should be based on our culture and spiritual values.
- We call upon the media to abide by ethical codes regarding the material they present.
- We advocate the rights of women to reduce their vulnerability to HIV/AIDS.

Third: On Treatment and Care

- People living with HIV/AIDS and their families deserve care, support, treatment, and education, whether or not they are responsible for their illness. We call for our religious institutions, in cooperation with other institutions, to provide spiritual, psychological, and economic guidance and support to those in need. We also encourage them not to lose faith in God's mercy, and aspire to a rewarding and productive life, embracing fate with courage and faith.
- We reject and emphasize the necessity to abolish all forms of discrimination, isolation, marginalization, and stigmatization of people living with HIV/AIDS, we insist on defending their basic freedoms and human rights.

Fourth: Addressing other leaders

- As religious leaders we need to reach out to our governments, civil society institutions, NGOs, and the private sector, to seek closer cooperation and greater action in the response to this epidemic.
- We also emphasize the importance of mobilizing other religious leaders' role against the imminent danger of HIV/AIDS in society, particularly in the media and in educational and popular campaigns.
- The need to formulate policies and laws that prevent the further spread of the disease particularly mandatory health check ups before marriage.
- Promote the setting up of guidance and awareness raising centers and facilitate the establishment of charitable organizations to provide care, and support for people living with HIV/AIDS.

https://www.fhi360.org/resource/cairo-declaration-religious-leaders-arab-states-response-hivaids-epidemic-pdfs-arabic-and

Activité Y. Scénario 2

Un travailleur signale qu'il a été harcelé par un autre travailleur.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 2 – Solutions possibles

- À l'avance :
  - Créez des codes de conduite pour le personnel ; élaborez des politiques pour traiter les griefs qui garantissent plusieurs niveaux de responsabilité, comme les plaintes directement adressées au conseil d'administration, et sensibilisez tous les travailleurs à ces politiques dans le cadre de l'intégration.
- Après l'incident :
  - Suivez les politiques existantes pour traiter le harcèlement sans exposer la victime à des risques de représailles OU élaborez de nouvelles politiques si aucune politique pertinente n'existe.
  - Formez à nouveau les travailleurs au code de conduite (ou offrez une formation initiale).
  - Offrez un soutien en matière de santé mentale à la personne harcelée.

Activité Y. Scénario 3

Un travailleur de proximité est arrêté alors qu'il distribuait des préservatifs et est détenu par la police.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 3 – Solutions possibles

- À l'avance :
  - Travaillez avec les autorités locales pour obtenir l'autorisation de toutes les activités de proximité, et formez les agents chargés de l'application des lois, qu'ils soient de haut rang ou de première ligne, sur leur rôle dans la riposte au VIH, y compris la création d'un environnement favorable aux activités de proximité.
  - Formez le personnel de proximité à expliquer la nature de ses activités aux forces de l'ordre et fournissez-leur des documents officiels (tels que des cartes d'identité ou des lettres des autorités locales ou du ministère de la Santé) décrivant leur objectif.
  - Identifiez des avocats qui peuvent soutenir l'organisation en cas de besoin si des problèmes surviennent.
- Après l'incident :
  - Appelez des avocats alliés ou un avocat interne pour assurer un suivi immédiat (s'il n'y a pas de financement pour un avocat et qu'il n'y a pas de possibilité d'engager un avocat à titre gracieux, adressez-vous à Dignité pour tous [axé sur les communautés LGBT], Frontline Defenders, The Lifeline Embattled CSO Assistance Fund, ou d'autres fonds pour obtenir un soutien).
  - Si des contacts avec la police existent, appelez ces personnes pour discuter des prochaines étapes.
  - S'il y a un désir de rendre le problème plus visible publiquement (par exemple, en activant des alliés), assurez-vous que ce cas fait l'objet d'une enquête approfondie avant de prendre cette mesure.

Activité Y. Scénario 4

Après une activité de sensibilisation au VIH avec des membres des PC, un bénéficiaire publie sur Facebook des photos des agents de sensibilisation et des membres de la communauté et les marque.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 4 – Solutions possibles

- À l'avance :
  - Informez les personnes qui viennent à un événement si l'espace est propice à la prise de photos (cela peut également aider les bénéficiaires qui voient d'autres personnes prendre des photos à leur rappeler les politiques ou à les signaler si nécessaire).
- Après l'incident :
  - Si les photos sont publiées sans intention négative, contactez la personne pour qu'elle les retire et expliquez-lui l'importance de ne plus publier de telles photos à l'avenir.
  - Si une personne a sciemment enfreint des règles claires ou ne veut pas retirer ses photos, ne l'autorisez pas à participer à des événements futurs.
  - Signalez la personne aux administrateurs de Facebook qui peuvent suspendre son profil.
  - Informez les personnes identifiées et expliquez-leur les mesures prises pour résoudre le problème. Fournissez-leur le soutien nécessaire si la publication entraîne une violence émotionnelle ou physique.

Activité Y. Scénario 5

Le bureau de l'organisation est perquisitionné par la police, qui emporte tous les dossiers et les ordinateurs.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 5 – Solutions possibles

- À l'avance :
  - Protégez toutes les technologies qui contiennent des informations stockées à l'aide de mots de passe et de cryptage.
- Après l'incident :
  - Créez un plan qui décrit ce qui se passera pour soutenir les personnes nommées en cas de fuite de données.
  - Contactez des alliés de haut rang au sein des forces de police pour qu'ils vous conseillent sur la marche à suivre. Par exemple, précisez ce qui sera fait de ces documents et encouragez-les à ne pas faire un mauvais usage ou à ne pas partager les dossiers médicaux et autres informations personnelles.
  - Si la saisie n'était pas légale, envisagez de contacter un avocat pour contester les documents pris sans mandat.
  - Faites un rapport au donateur sur le problème, les réponses proposées et tout changement prévu dans la capacité à atteindre les objectifs/cibles.

Activité Y. Scénario 6

Un article hostile sur votre organisation est publié dans le journal ; il mentionne l'adresse de votre clinique et comprend des photos de deux de vos cliniciens.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 6 – Solutions possibles

- À l'avance :
  - Prenez contact avec les autorités locales et les forces de l'ordre pour expliquer, en collaboration avec un responsable du ministère de la Santé (MS), la nature des activités de votre organisation.
  - Enregistrez votre organisation
  - Établissez des relations avec les détenteurs du pouvoir, tels que les chefs religieux ou les autorités locales, qui peuvent défendre votre organisation.
  - Mettez en place une politique claire décrivant la manière dont votre organisation interagit avec les journalistes et préférez les déclarations à la presse aux interviews. Dans une interview, les propos tenus par le personnel ou les membres de votre organisation peuvent être déformés ou sortis de leur contexte.
- Après l'incident :
  - Renforcer la sécurité de la clinique
  - Informez les autorités locales alliées du problème et demandez leur soutien en cas de violence contre l'organisation ou les prestataires individuels.
  - Soutenez les cliniciens à se reloger provisoirement ou à modifier leurs responsabilités (par exemple en ne les faisant travailler qu'en journée ou en arrêtant les activités communautaires) s'ils pensent qu'ils seront en danger.
  - Demander au ministère de la Santé de rédiger un article clarifiant le rôle de l'organisation et son importance pour la santé de la communauté.

Activité Y. Scénario 7

Un travailleur de proximité paire de votre organisation fait l'objet d'un chantage de la part d'un bénéficiaire qui menace de dire à ses parents que celui-ci est homosexuel.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 7 – Solutions possibles

- À l'avance :
  - Disposez d'un code de conduite clair pour les participants au programme, qui inclut les attentes en matière de confidentialité et décrit les conséquences d'un manquement à ces attentes.
  - Parlez aux pairs et aux autres membres du personnel des risques auxquels ils peuvent être confrontés, y compris dans leur vie personnelle, en raison de leur travail et aidez-les à décider s'ils souhaitent assumer un rôle susceptible d'augmenter les chances que leur famille ou leurs amis découvrent leur statut de membre des PC, s'il n'est pas déjà le cas.
- Après l'incident :
  - Soutenez la santé mentale du travailleur en lui offrant une écoute active et en le mettant en relation avec un conseiller, s'il le souhaite.
  - Proposez d'aider à faciliter une conversation avec le travailleur et ses parents, si vous le souhaitez.
  - Expliquez au travailleur le contexte juridique local (par exemple, l'action du bénéficiaire est-elle illégale) et les options qui s'offrent à lui, notamment ne rien faire (le chantage n'est souvent pas exercé) et bloquer le bénéficiaire sur les médias sociaux et au téléphone. Une fois que le travailleur a choisi une option, apportez-lui le soutien nécessaire à réaliser son choix.
  - Empêchez le bénéficiaire de participer à tout événement futur du programme.

Activité Y. Scénario 8

Un travailleur de proximité se rend au domicile d'un homme nommé par un client indexé. L'homme réagit violemment. Il attaque le travailleur de proximité et lui inflige plusieurs blessures. Il le retient également contre sa volonté pendant trois heures.

- Que pouvez-vous faire maintenant ?
- Qu'auriez-vous pu faire, avant que ce problème ne survienne, pour atténuer ou prévenir les préjudices causés ?

Scénario 8 – Solutions possibles

- À l'avance :
  - Proposer plusieurs modalités de test d'indexation (avec un dépistage de la VPI pour éclairer la sélection).
  - Avoir des directives claires sur le moment où les visites à domicile doivent avoir lieu (par exemple, la personne visitée doit donner son consentement à l'avance) et sur la manière dont ces visites doivent être effectuées (par exemple, toujours en binôme).
  - Disposer d'un système pour suivre les travailleurs de proximité (par exemple, savoir où ils vont, leur arrivée et leur retour prévus ; envisager un suivi par GPS).
  - Proposez une assurance médicale aux travailleurs et/ou développez un système leur permettant de recevoir des soins médicaux gratuits s'ils sont blessés au travail.
- Après l'incident :
  - Demandez au superviseur d'alerter la direction du retour tardif du travailleur de proximité.
  - Orientez le travailleur de proximité vers un traitement gratuit en cas de blessures
  - Fournir au travailleur de proximité des ressources psychologiques
  - Contactez la police pour porter plainte contre l'auteur de l'agression (si cela correspond aux souhaits du travailleur de proximité).
  - Inscrire le client potentiel sur une liste d'interdiction de contact pour référence future.

Activité Z. Réflexions sur les scénarios

Q : Si l'on considère les huit scénarios que nous venons d'examiner, pourquoi les mesures prises avant le défi de la sécurité sont-elles si importantes ?

R : Il y a trois raisons principales :

1. Lorsque vous disposez d'un plan de sécurité avant qu'un problème de sécurité ne survienne, vous pouvez réagir plus rapidement et de manière plus organisée/efficace que si vous essayez d'élaborer un plan au milieu d'une crise.
2. La planification de la sécurité met en place des structures et des relations qui empêchent les problèmes de sécurité de se produire ou les rendent moins nuisibles s'ils se produisent.
3. Il est beaucoup moins coûteux (temps et argent) de prévenir un incident de sécurité que d'y répondre.

Réflexion finale sur les scénarios de sécurité

Si votre organisation a des préoccupations spécifiques qui n'ont pas été abordées ici, notez-les. Ensuite, faites cet exercice en utilisant ces préoccupations.

Planifiez maintenant pour éviter des conséquences négatives plus tard !

Formule d'évaluation des risques

Objectif de la session

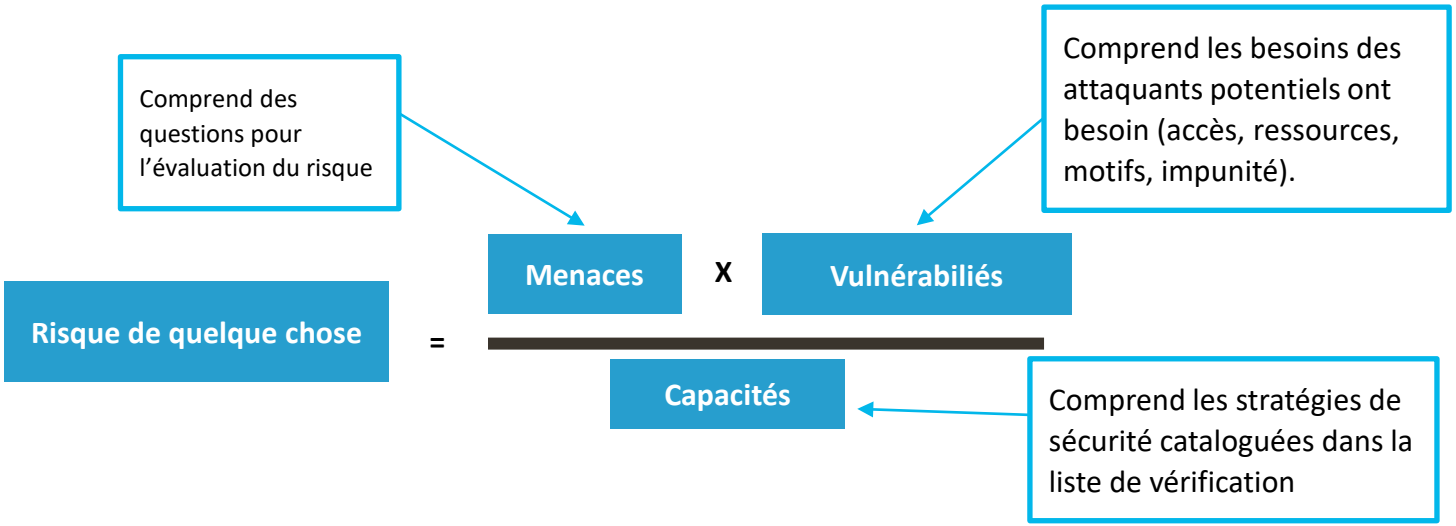
Se familiariser avec la formule permettant de déterminer la probabilité qu'un dommage donné se produise.

Compromis

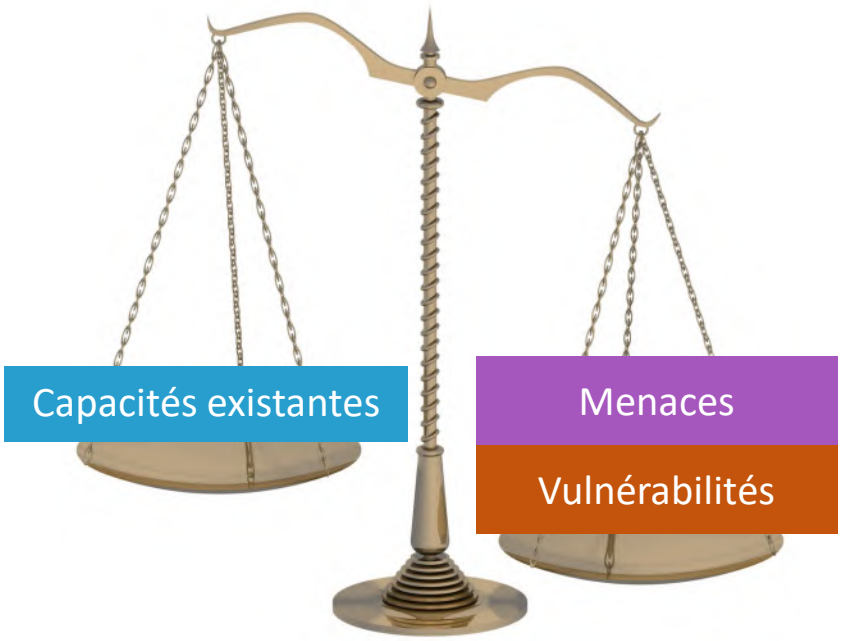
- Limiter l'accès, les ressources et les motivations d'un attaquant peut impliquer des compromis pour vous en tant qu'individu et en tant qu'organisation.
- Comment décidez-vous des vulnérabilités à accepter ?

Prenez des actions pour réduire le risque

- **Menaces** - vous pouvez évaluer ces indications et peut-être les modifier au fil du temps, mais vous avez un contrôle limité sur elles (externe)
- **Vulnérabilités** - inhérentes à vous/votre communauté ; vous pouvez en contrôler certaines, mais pas d'autres (interne).
- **Capacité** - ce que vous voulez constamment travailler à augmenter (interne)

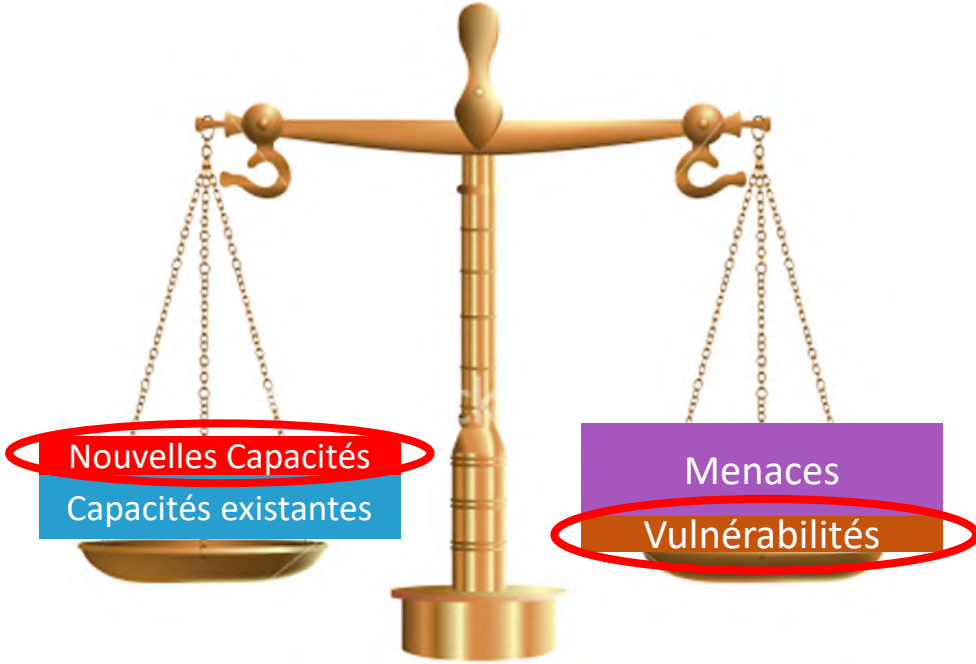


Nous voulons partir de cela...



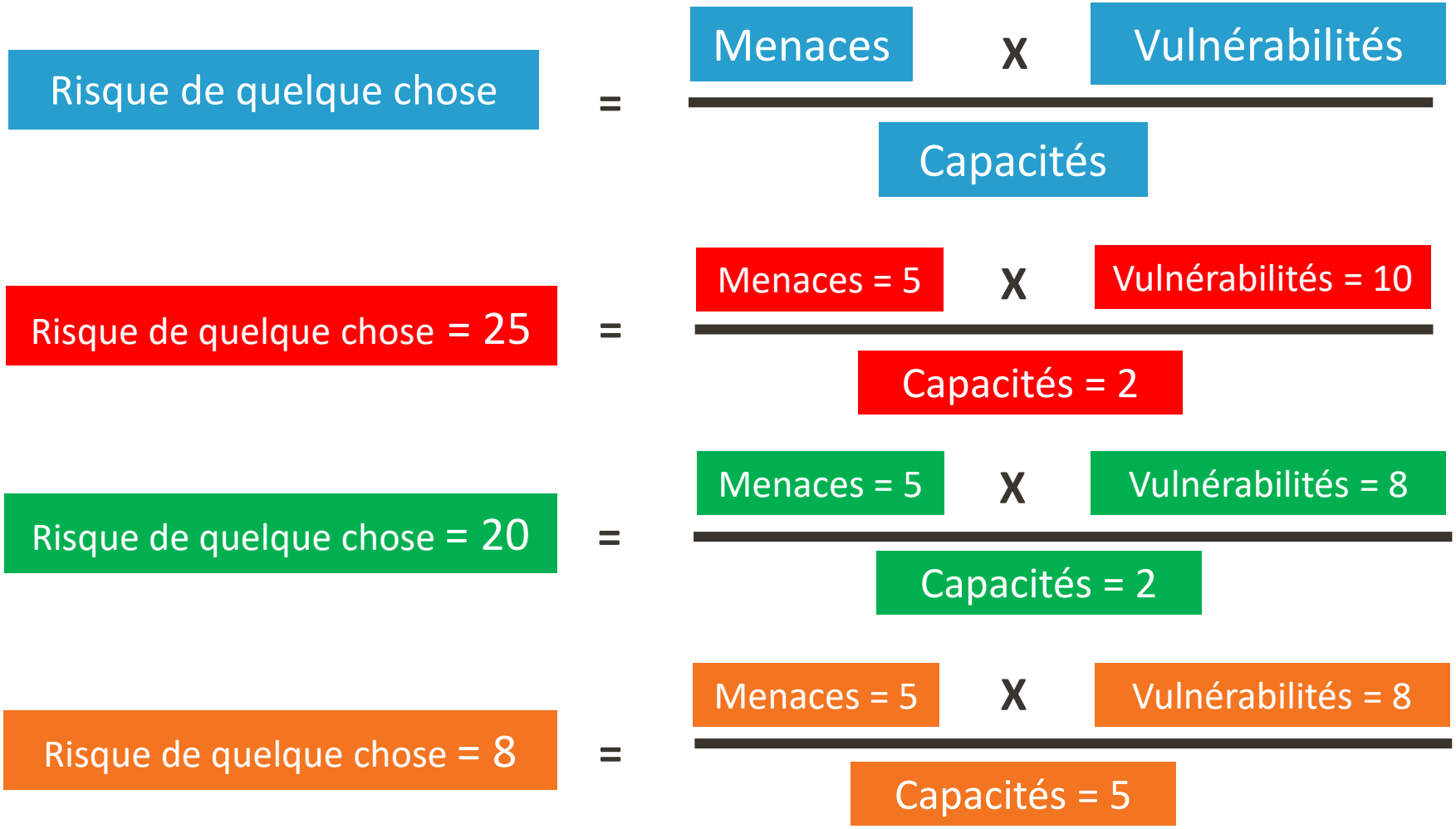
Les menaces et les vulnérabilités dépassent largement les capacités.

Pour nous approcher de cela…



Les capacités sont égales ou supérieures aux menaces et aux vulnérabilités.

Formule de calcul du risque



En réalité, le risque zéro n'existe pas et les situations évoluent rapidement. Cet outil vous donne une idée de la probabilité de différents préjudices pour comparer les risques et comparer votre niveau de risque au fil du temps.

Exemple d'évaluation du risques

$$\text{Risque de quelque chose} = \frac{\text{Menaces} \times \text{Vulnérabilité}}{\text{Capacité}}$$

- Choisir un risque spécifique (lieu, activité, personne)
  - Notre CSO craint que nos pairs travailleurs de proximité ne soient agressés physiquement lors des actions de sensibilisation.
- Tenez compte des menaces qui rendent le risque probable
  - Des abus verbaux, y compris des menaces de violence physique, ont eu lieu dans le passé ; les auteurs sont souvent les propriétaires de bars. Les menaces verbales sont en augmentation.
- Nommez vos vulnérabilités :
  - Le travail de proximité est effectué par des travailleurs du sexe ; il a lieu la nuit ; le transport se fait à pied.
- Nommez vos capacités :
  - Les travailleurs de proximité pairs portent des cartes d'identité indiquant qu'ils sont liés au ministère de la Santé et un numéro de téléphone permettant de joindre un officier de police formé localement ; les pairs sortent en binôme ; les pairs ont des téléphones avec du crédit prépayé en cas de problème.

Activité AA. Exemple d'évaluation du risques

$$\text{Risque de quelque chose} = \frac{\text{Menaces} \times \text{Vulnérabilité}}{\text{Capacité}}$$

- Choisir un **risque spécifique** (lieu, activité, personne)
  - Notre OSC craint que les travailleurs de proximité ne soient agressés physiquement pendant la sensibilisation.
- Tenir compte des **menaces** qui rendent le risque plus ou moins probable
  - Des abus verbaux, y compris des menaces de violence physique, se sont produits dans le passé ; les auteurs sont souvent les propriétaires de bars.
- Nommez vos **vulnérabilités** :
  - Le travail de proximité est effectué par des travailleurs du sexe ; il doit avoir lieu la nuit ; le transport se fait à pied.
- Nommez vos **capacités** :
  - Les travailleurs de proximité pairs portent des cartes d'identité qui montrent qu'ils sont liés au ministère de la Santé et un numéro de téléphone pour joindre un officier de police formé localement ; les pairs sortent en binôme ; les pairs ont des téléphones avec du crédit prépayé en cas de problème.

Discussion: Que pourriez-vous faire pour réduire les vulnérabilités et augmenter les capacités ?

Activité AA. Exemple d'évaluation du risques

$$\text{Risque de quelque chose} = \frac{\text{Menaces} \times \text{Vulnérabilité}}{\text{Capacité}} \quad -1 \quad +4$$

- Choisir un **risque spécifique** (lieu, activité, personne)
  - Notre OSC craint que les travailleurs de proximité ne soient agressés physiquement pendant la sensibilisation.
- Tenir compte des **menaces** qui rendent le risque plus ou moins probable
  - Des abus verbaux, y compris des menaces de violence physique, se sont produits par le passé ; les auteurs sont souvent les propriétaires de bars.
- Nommez vos **vulnérabilités** :
  - Le travail de proximité est effectué par des travailleurs du sexe ; il doit avoir lieu la nuit ; le transport se fait ~~à pied~~. en taxi.
- Nommez vos **capacités** :
  - Les travailleurs de proximité pairs portent des cartes d'identité qui montrent qu'ils sont liés au ministère de la Santé et incluent un numéro de téléphone pour joindre un officier de police formé localement ; les pairs sortent en binôme ; les pairs ont des téléphones avec du crédit prépayé en cas où ils rencontreraient des problèmes ; les pairs ont un message non controversé pour décrire leur travail ; les allées et venues des pairs sont suivies via un journal de bord et un GPS ; les pairs ont des refuges pré-identifiés dans chaque quartier où ils travaillent ; les travailleurs du sexe sont accompagnés par une escorte connue et respectée de la région.

Plan de sécurité

Objectifs de la session

- Reconnaissez les éléments d'un plan de sécurité et entraînez-vous à utiliser le modèle pour élaborer le vôtre.

- Identifiez vos trois principaux risques et créez un plan de sécurité pour chacun d'eux en tenant compte des vulnérabilités, des capacités existantes et des capacités nécessaires..

Plan de sécurité

Risque (de quelque chose): Un cambriolage à la clinique avec vol de dossiers de clients.			
Menaces	Vulnérabilités	Capacité existante	Capacité requise
Elevé • Des travailleurs de proximité ont été suivis jusqu'à la clinique par des groupes de hurleurs qui disent que nous encourageons l'homosexualité. • Des messages menaçants ont été graffités sur la clinique.	• Nous sommes dans un quartier où il y a peu de circulation le soir. • Nous n'avons pas d'agents de sécurité à la clinique après 17 heures. • Nous n'avons pas de moyen de contrôler les visiteurs pendant la journée. • Le personnel ne verrouille pas toujours les dossiers des patients. • Les fenêtres et les portes n'ont pas de barreaux ; elles peuvent être brisées avec des pierres.	• Nous disposons d'un agent de sécurité pendant les heures d'ouvertures de la clinique (de 9 h à 17 h). • Nous avons le logo de l'USAID et du MS sur notre panneau. • Nous nous sommes présentés et avons expliqué notre travail aux officiers de police travaillant dans le district. • Nous avons des armoires fermées à clé pour stocker tous les dossiers papier des clients. • Nous utilisons des CIU et conservons principalement des informations électroniques cryptées.	• Journaux de bord des visiteurs • Formation de tout le personnel sur le stockage sécurisé des documents (politique de bureau propre). • Discuter avec le propriétaire de la nature de notre travail. • Installer des mesures de sécurité physique pour les fenêtres et les portes. • Créer un journal des incidents de sécurité pour suivre les tendances ; envisager d'utiliser ce journal pour plaider auprès du donateur en faveur de fonds pour une présence de sécurité accrue.

Plan de sécurité à faible coût ou sans coût

Risque (de quelque chose): Un cambriolage à la clinique avec vol de dossiers de clients.			
Menaces	Vulnérabilités	Capacité existante	Capacité requise
Elevé • Des travailleurs de proximité ont été suivis jusqu'à la clinique par des groupes de hurleurs qui disent que nous encourageons l'homosexualité. • Des messages menaçants ont été graffités sur la clinique.	• Nous sommes dans un quartier où il y a peu de circulation le soir. • Nous n'avons pas d'agents de sécurité à la clinique après 17 heures. • Nous n'avons pas de moyen de contrôler les visiteurs pendant la journée. • Le personnel ne verrouille pas toujours les dossiers des patients. • Les fenêtres et les portes n'ont pas de barreaux ; elles peuvent être brisées avec des pierres.	• Nous disposons d'un agent de sécurité pendant les heures d'ouvertures de la clinique (de 9 h à 17 h). • Nous avons le logo de l'USAID et du MS sur notre panneau. • Nous nous sommes présentés et avons expliqué notre travail aux officiers de police travaillant dans le district. • Nous avons des armoires fermées à clé pour stocker tous les dossiers papier des clients. • Nous utilisons des CIU et conservons principalement des informations électroniques cryptées.	• Journaux de bord des visiteurs • Formation de tout le personnel sur le stockage sécurisé des documents (politique de bureau propre). • Discuter avec le propriétaire de la nature de notre travail. • Installer des mesures de sécurité physique pour les fenêtres et les portes. • Créer un journal des incidents de sécurité pour suivre les tendances ; envisager d'utiliser ce journal pour plaider auprès du donateur en faveur de fonds pour une présence de sécurité accrue.

Activité BB. Exemple local

Risque (de quelque chose): XXXX			
Menaces	Vulnérabilités	Capacité existante	Capacité requise
• XXXX • XXXX	• XXXX • XXXX	• XXXX • XXXX	• XXXX • XXXX

Activité CC. Vos risques prioritaires

1. Faites un brainstorming sur les plus grands risques de sécurité de votre organisation
2. Sélectionnez vos trois principaux risques
3. Élaborez un plan de sécurité pour chacun de vos trois principaux risques.

   - Consultez la liste de vérification que vous avez remplie pour comprendre vos capacités actuelles et trouver des idées sur ce qui peut être fait de plus.
4. Terminez les plans de sécurité et envoyez-les à XXXX avant XXXX pour obtenir un retour d'information.

Prochaines étapes

Objectifs de la session

- Discutez des possibilités d'action immédiate sans frais ou à faible coût, de la poursuite de l'apprentissage inter-OSC, du lien entre les activités de sécurité et la prévention et la réponse à la violence en cours, et de la recherche d'un soutien international.
- Identifiez les mesures à prendre pour finaliser et faire accepter les plans de sécurité par chaque OSC.

Finalisation et financement des plans

- La finalisation des plans de sécurité peut inclure
  - Obtenir l'adhésion des autres membres de votre organisation
  - demander aux autres parties prenantes quels engagements spécifiques elles prendront (propriétaires, LINKAGES/EpiC, ministère de la Santé, etc.).
- De nombreuses actions seront gratuites ou très peu coûteuses.
  - Celles qui nécessitent un financement doivent être documentées afin d'aider à la planification de futurs conférences des parties et opportunités d'autres financements.

Activité DD. Planification des actions

- Après avoir complété vos plans de sécurité, choisissez parmi les capacités que vous devez construire
- Choisissez 10
- Remplissez le plan d'action et renvoyez-le à XXXXXX
- Si l'un de vos projets est de déployer cette formation à un groupe plus large au sein de votre organisation, élaborez vos propres politiques et procédures opérationnelles standard en matière de sécurité avant cette formation.

	Top 10 Required Capacities to be Pursued	Requires additional monetary resources? (Y/N)	Time capacity will be fully implemented	Main person(s) responsible
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Possibilités de soutien (financement)

DIGNITY FOR ALL

International HIV/AIDS Alliance

Together to end AIDS

FRONT LINE DEFENDERS

URGENT ACTION FUND FOR WOMEN'S HUMAN RIGHTS

Nouvelles opportunités pendant le COVID-19

Le financement peut couvrir :

- Pénurie alimentaire, création de moyens de subsistance à moyen et long terme
- Résilience des mouvements
- la lutte contre la violence : (violence liée au sexe, violence domestique et violence familiale), peut inclure un soutien en matière de santé mentale.
- Documentation des violations des droits de l'homme

https://outrightinternational.org/outright-covid-19-global-lgbtiq-emergency-fund

Réflexions et clôture

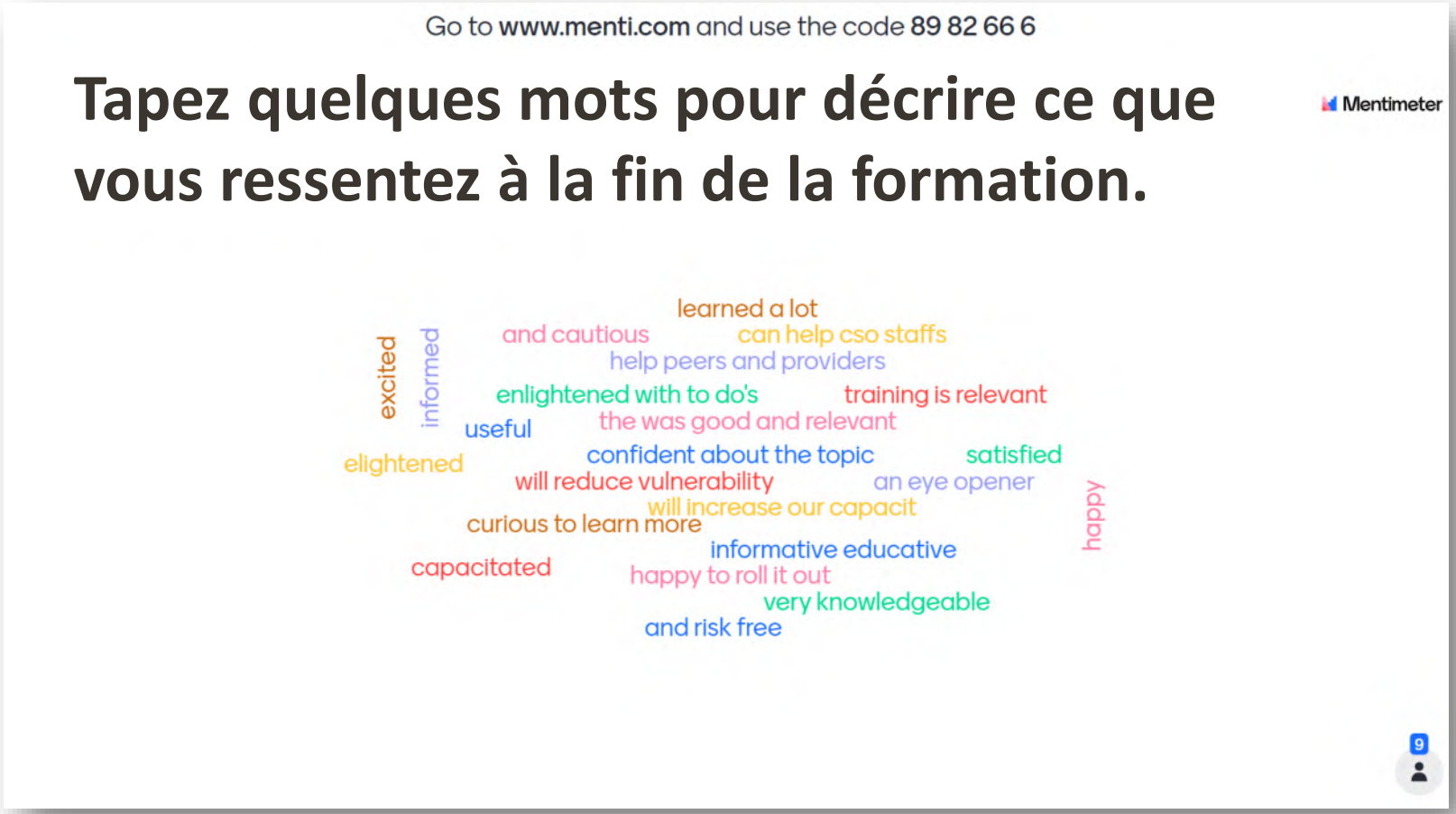
Objectif de la session

Partagez vos réflexions sur l'atelier et évaluez-le ; formulez des réflexions de clôture.

Activité EE. Évaluation et post-test

- Une évaluation pour noter la formation peut être trouvée ici : XXXXXX
- Le post-test peut êter trouvé ici : XXXXXX

Activité FF. Dans vos propres mots



Remerciements