# Rencontres virtuelles: Vidéoconférences avec le personnel de Service Coordination Soutien, incluant les Services de l'Ontario pour les personnes ayant une déficience intellectuelle - Région de l'Est

## Risques à la sécurité et Pratiques Exemplaires

## Avril 2020

# Table des matières

# Rencontres virtuelles: Vidéoconférences avec le personnel de SCS (incluant le SOPDIRE)

## Introduction

Compte tenu de la situation actuelle concernant la COVID-19 et des mesures visant la distanciation physique (sociale), nos employés ont reçu comme directive de continuer à rencontrer les clients/familles par téléphone ou par vidéoconférence, si possible.

SCS, incluant le SOPDIRE, utilise le logiciel de conférence BlueJeans, une plateforme sécurisée pour mener des rencontres virtuelles (vidéoconférences) avec les clients. Il est important de noter qu'il existera toujours des risques de sécurité avec toute plateforme de communication en ligne - voir dans le document ci-dessous les *Risques et Conseils reliés à la sécurité*. Nos employés qui organisent une rencontre virtuelle par vidéoconférence avec le logiciel BlueJeans seront responsables d'héberger celle-ci. Nos employés doivent organiser des rencontres virtuelles uniquement par l'entremise du logiciel BlueJeans.

Nos employés sont autorisés à participer à une rencontre virtuelle sur une autre plateforme ou logiciel au choix du client et/ou de la famille (par exemple Zoom). Toutefois, nos employés doivent s'assurer que vous connaissez les risques pour la sécurité en vous posant certaines questions avant de participer à une rencontre sur une plateforme autre que BlueJeans.

En vous posant ces questions, SCS (incluant le SOPDIRE) ne sera pas tenue responsable de toute atteinte à la vie privée ou problèmes qui pourraient en résulter. Vous serez demandé d'être responsable d'organiser la rencontre virtuelle sur une plateforme autre que BlueJeans.

Les questions qui vous seront posées lorsque vous initierez une rencontre virtuelle sur le logiciel ou la plateforme de votre choix seront les suivantes :

- Êtes-vous conscient des risques de sécurité associés à l'utilisation de plateformes ou logiciels pour des rencontres virtuelles?
- Cette plateforme ou logiciel est-il sécurisé par un nom d'usager unique et un mot de passe?
- Cette plateforme ou logiciel a-t-il la capacité de connaître l'identité des participants lorsqu'ils entrent dans la rencontre virtuelle
- À votre connaissance, cette plateforme ou logiciel a-t-il été mis à jour avec la version la plus récente?

Il est possible que nos employés refusent de participer sur la plateforme de votre choix s'ils ont des inquiétudes sur la sécurité de l'information de celle-ci, dépendamment des réponses aux questions ci-dessus.

## Risques liés à la sécurité des vidéoconférences

Avec la popularité croissante de la vidéoconférence pour les réunions d'affaires, l'enseignement à distance et les rencontres sociales virtuelles en raison de la situation actuelle, les fraudeurs ont lancé une série de nouvelles attaques visant les technologies de vidéoconférence et leurs utilisateurs.

Voici quelques exemples de ces attaques :

- **Bombardement d'une rencontre** – Dans ce type d'attaque, le fraudeur se joint à une rencontre par vidéoconférence, soit pour écouter la conversation, soit pour perturber la réunion en partageant des renseignements inappropriés. Prévenez les intrusions en utilisant des identifiants et des mots de passe uniques pour chaque rencontre.
- **Liens malveillants dans la conversation –** Une fois que les fraudeurs ont accès à votre salle de rencontre virtuelle, ils peuvent tromper les participants en leur faisant cliquer sur des liens malveillants partagés dans le clavardage, ce qui permet aux attaquants de voler leurs identifiants. Cela renforce le fait qu'il est plus que jamais essentiel d'exiger des mots de passe pour toutes les rencontres.
- **Vol des liens aux rencontres** – La réutilisation des liens aux rencontres facilite leur vol par les fraudeurs. Pour éviter tout accès non autorisé à vos rencontres, activez des avertissements qui vous permettront de savoir quand quelqu'un a rejoint votre salle de rencontre sans votre consentement. Ou mieux encore, n'autorisez pas d'autres personnes à rejoindre votre rencontre avant vous en désactivant "Rejoindre avant l'hôte".
- **Données partagées avec des tiers –** Assurez-vous que des contrôles de sécurité sont en place pour protéger vos données, puis assurez-vous que ces contrôles sont configurés correctement. Soyez attentifs aux participants dans la rencontre et aux fichiers que vous partagez qui contiennent des renseignements confidentiels ou personnels. Il est important d'avoir des

ententes sur la protection des données avec des tiers assurant les contrôles de sécurité appropriés.

- **Logiciels malveillants ou attaques « Zero Day »** – Lorsqu'il s'agit d'attaques « Zero Day », les anciens logiciels antivirus ne font pas le poids. Vous devrez vous protéger contre les activités malveillantes en renforçant la sécurité au niveau des points d'accès et du réseau.

## Conseils de sécurité pour la vidéoconférence

- Ne jamais réutiliser un identifiant de rencontre
- Protéger toutes les rencontres par un mot de passe
- Obliger les participants à s'identifier par le biais d'une vidéo ou d'une acceptation verbale
- Ne partagez jamais de liens ou d'identifiants à une rencontre sur les médias sociaux
- Le partage de fichiers ne doit être effectué qu'avec les participants appropriés (autorisations de partage)
- Le partage d'écran doit se faire avec les participants appropriés afin de protéger les renseignements personnels
- Signalez toute activité suspecte à votre administrateur

## Responsabilités pour la création et l'organisation des rencontres (modérateur)

1. **Exiger des mots de passe :** En tant qu'hôte de la rencontre, c'est la première mesure que vous pouvez prendre pour sécuriser vos rencontres : rendez les mots de passe obligatoires pour toutes vos rencontres afin de vous protéger contre les fraudeurs et de sécuriser les renseignements concernant la rencontre, notamment le nom de la rencontre et l'organisateur.
2. **Vérifiez les participants :** Veillez à vérifier la liste des participants lorsque vous envoyez l'invitation à la rencontre, et examinez la liste des participants pendant l'appel. Supprimez toute personne qui n'est pas censée participer à la rencontre.
3. **Vérifiez le lien de la rencontre :** Lorsque vous recevez une invitation à une rencontre, vérifiez qu'elle provient d'un expéditeur connu et digne de confiance.

Vérifiez également le lien de la rencontre avant de cliquer, en faisant attention aux liens malveillants avec l'extension « .exe », par exemple. Les tentatives d'hameçonnage sont de plus en plus fréquentes. Les liens malveillants contiennent le nom du logiciel ou la plateforme de vidéoconférence, mais ils vous conduisent à de faux sites vous invitant à entrer vos identifiants. En utilisant des liens protégés par des mots de passe, vous augmenterez la sécurité et réduirez le « war dialing », une technique utilisée pour découvrir ou deviner l'identifiant d'une rencontre.

4. **Correctifs** : Assurez-vous que votre logiciel de vidéoconférence est doté des dernières mises à jour fournies par le fournisseur et que les mises à jour automatiques sont activées.
5. **Préservez la confidentialité :** Gardez les conversations confidentielles privées, et assurez-vous de ne rien partager de confidentiel par accident sur votre ordinateur portable ou dans votre arrière-plan. Les arrière-plans virtuels ont gagné en popularité pour un dépaysement total !
6. **Passez en revue vos paramètres de sécurité :** Examinez et activez les paramètres de sécurité et de confidentialité appropriés pour empêcher les fraudeurs d'exploiter des vulnérabilités connues.
7. **Signalez toute activité suspecte :** N'oubliez pas de signaler toute activité suspecte aux équipes chargées de la sécurité et des technologies de l'information de votre entreprise.