Loi 25

Protection des données personnelles au Québec

ATTRACTION

La **Loi 25**, c’est un peu comme le gardien vigilant de nos précieux secrets numériques. Elle est à nos données ce que le coffre-fort est à nos biens les plus précieux.

Cette loi québécoise, également connue sous le nom de loi sur la gouvernance des renseignements personnels, encadre méticuleusement comment les entreprises et les organismes publics collectent, utilisent et partagent nos **informations personnelles**.

En bref, cette loi est là pour s’assurer que nos données ne se retrouvent pas entre de mauvaises mains ou utilisées à mauvais escient, garantissant ainsi la confiance des Québécois dans la gestion de leurs informations.

Nom

Adresse courriel

Numéro de téléphone

Mot de passe

Adresse IP

Quizz

Quels autres éléments peuvent être considérés comme des données personnelles?

ATTRACTION

- **Numéro d’assurance sociale**
- **Numéro de passeport**
- **Numéro d’assurance maladie**
- **Adresse postale**
- **Empreintes digitales**
- **. . .**

C’est, en fait, tout ce qui permet d’identifier une personne spécifiquement.

Les entreprises qui ne respectent pas cette loi peuvent être soumises à des **amendes considérables**, qui peuvent atteindre des millions de dollars.

De plus, les incidents de confidentialité peuvent également entraîner la **perte de la confiance des clients** et causer des dommages importants à la **réputation de l'entreprise** et causer beaucoup de **problèmes à la personne** qui s'est fait voler ses données.

Il y a 3 possibilités de poursuite :

Poursuite pour dommages-intérêts punitifs

La personne dont les données ont été volées peut intenter une action en justice pour demander des dommages-intérêts punitifs et réclamer des montants d'argent.

Comme dans le cas du recours collectif contre Desjardins suite à la fuite de données.

Sanctions administratives pécuniaires

Il existe des sanctions administratives pécuniaires pouvant atteindre un montant maximal de 10 millions de dollars ou 2 %.

Sanctions pénales

Il existe également des sanctions pénales pouvant atteindre un montant maximal de 25 millions de dollars ou 4 %.

Les changements clés à connaître

Toutes les entreprises sont concernées et doivent:

1. **Tenir un inventaire des renseignements personnels qu'elles détiennent**
2. **Mettre à jour leur politique de confidentialité et la rendre accessible et claire à tous**
3. **Mettre en place des mesures pour assurer la sécurité des données qu'elles détiennent**

Chez Attraction, nous attachons une grande importance à la protection de la vie privée et à la conformité aux lois sur la protection des renseignements personnels. C'est pourquoi nous avons mis en place des procédures de conservation, de destruction et d'anonymisation des données personnelles. Par exemple, notre système ERP, Prextra, dispose d'un module pour anonymiser les données des anciens employés, et notre logiciel de paie masque les données sensibles. De plus, nous offrons la possibilité de détruire les informations lorsque qu'un employé quitte l'entreprise. Nous sommes engagés à préserver la confidentialité des données personnelles et à protéger la vie privée de tous.

1 Tenir un inventaire des renseignements personnels qu'elles détiennent

Un fichier Excel de suivis est complété. ✓

2 Mettre à jour leur politique de confidentialité et la rendre accessible et claire à tous

La politique au manuel de l’employé a été mise à jour. ✓

3 Mettre en place des mesures pour assurer la sécurité des données qu'elles détiennent

Nous avons des restrictions d’accès sur les dossiers et ou logiciels avec des informations critiques. ✓

Reconnaître un cyberincident

Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement. Voici certains indicateurs.

- Activité **excessive ou inhabituelle** de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.
- Accès distant **excessif ou inhabituel** dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers.
- L'apparition de tout **nouveau réseau sans fil** (Wi-Fi) visible ou accessible.
- Une activité inhabituelle liée à la **présence de logiciels** malveillants, de **fichiers suspects** ou de fichiers et programmes exécutables nouveaux ou non approuvés.
- Ordinateurs ou appareils **perdus, volés ou égarés** qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

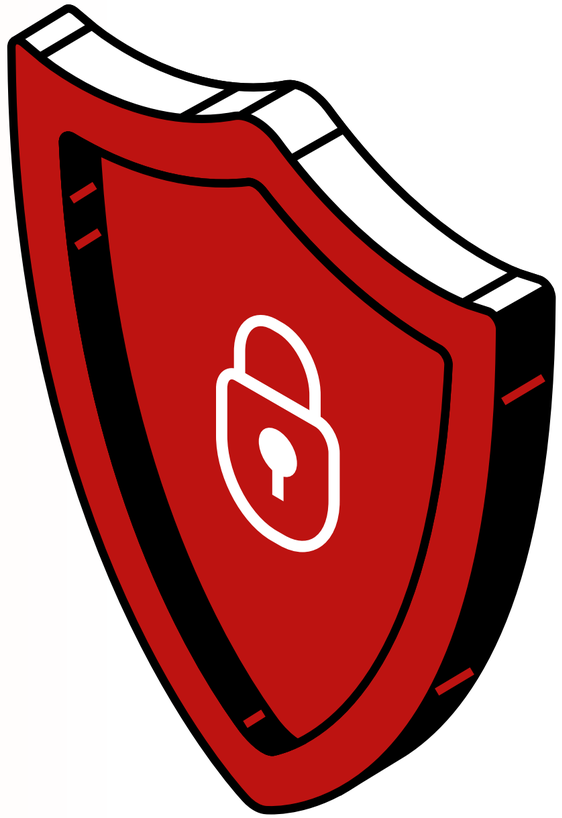
Reconnaître un cyberincident

Les cyberincidents ne sont pas uniquement le résultat d'actions malveillantes de pirates informatiques. Les erreurs humaines peuvent également entraîner des incidents de cybersécurité.

- Réception d'un **courriel** contenant des **informations confidentielles** qui ne nous étaient pas destinées.
- Accès à des **informations sensibles** auxquelles nous ne devrions pas avoir accès, comme des numéros de carte de crédit ou des adresses personnelles.
- Erreur de sécurité ou d'**accès attribuée à un utilisateur**, entraînant une violation de la confidentialité des données.

Atteinte à la protection des renseignements personnels

S’il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra :



Compléter le registre d’incidents de confidentialité pour documenter l’incident.

Examiner l’atteinte à la protection des renseignements personnels pour déterminer si des **renseignements personnels** ont été perdus en raison d'un accès ou utilisation non autorisés, d'une divulgation non autorisée ou de toute atteinte la protection de ces renseignements personnels et qu’il existe un risque de préjudice sérieux pour les personnes concernées.

o Dans un tel cas, le signaler à la Commission de l’accès à l’information au Québec.

o Et, le signaler également aux personnes dont les renseignements personnels sont visés par l’incident.

Rançongiciel

S’il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra:

Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.

Ne pas fermer l’ordinateur.
C’est essentiel afin de trouver la source et de faire les investigations nécessaires (informatique et policière)

Ne rien effacer sur de vos appareils (ordinateurs, serveurs, etc.).

Repartir à zéro (formater l’équipement, réinstaller le système d’exploitation et les logiciels. Remettre les données en les analysant méticuleusement pour s’assurer qu’aucune trace du rançongiciel n’y soit)

La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d’un chef de projet expert en cyberattaques (breach coach).

Protéger les systèmes en mettant en place des correctifs et des mises à jour pour prévenir de nouvelles infections et empêcher de potentielles attaques.

Piratage de compte

S’il a été confirmé qu'un piratage de compte s'est produit, il faudra:

- Aviser nos clients et fournisseurs qu’ils pourraient recevoir des courriels frauduleux de notre part, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.
- Vérifier si on a encore accès au compte en ligne.
- Changer le mot de passe utilisé pour se connecter à la plateforme.
- Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.
- Activer le double facteur d’authentification pour la plateforme.
- Supprimer les connexions et les appareils non légitimes de l’historique de connexion.

Perte ou vol d’un appareil

S’il a été confirmé qu'une perte d’équipement s'est produite, il faudra:

Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portatif ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. À la page 10, dans le document de formation, il n’y a pas juste la police à aviser, mais Attraction également (ou la personne responsable en informatique) afin que les accès soient bloquées le plus rapidement possible :

o *Cela inclut les pertes/vols en dehors des heures d’ouverture normale et pendant les week-ends.*

o *Si l'appareil perdu ou volé contenait des données sensibles et qu’il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.*

o *Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.*

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Utilisez des mots de passe forts

Utilisez des mots de passe comportant entre 16 et 20 caractères, composé d’une combinaison de lettres, de chiffres et de caractères spéciaux dans vos mots de passe. Évitez d'utiliser des informations personnelles évidentes et utilisez des mots de passe différents pour chaque compte.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Gestionnaires de mots de passe

Utilisez un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, Keepass ou 1Password pour générer, stocker et gérer vos mots de passe.

Certains d’entre eux ont la possibilité de conserver la clé de la double authentification.
(Dans les versions payantes le plus souvent)

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Activez l'authentification à deux facteurs

Utilisez des méthodes d'authentification à deux facteurs (2FA) lorsque cela est possible. Cela ajoute une couche de sécurité supplémentaire en demandant une deuxième preuve d'identité lors de la connexion.

Une histoire vrai de Josette Grégoire

Josette Grégoire, a eu une expérience avec son compte Facebook.
Pas une, mais deux fois cette année, son compte s'est retrouvé bloqué.

Mais heureusement, Josette avait eu la présence d'esprit d'activer l'authentification à deux facteurs ! Ainsi, même avec un mot de passe compromis, le pirate n'a pas pu accéder à ses informations sans ce précieux deuxième facteur.

Grâce à des mesures de sécurité comme l'authentification à deux facteurs, nous pouvons garder nos données en sécurité, même dans les situations les plus improbables !

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Méfiez-vous des messages suspects

Soyez vigilant avec les courriels, les messages instantanés et les appels téléphoniques non sollicités demandant des informations personnelles. Ne cliquez pas sur les liens suspects et n'ouvrez pas les pièces jointes sources inconnues.

Urgent: Release of Container Payment Required

FS

Francis St-Pitre
À Ana Bjelic

Répondre | Répondre à tous | Transférer

mer. 20-03-2024 15:30

Traduire le message en : Français | Ne jamais traduire à partir de : Anglais | Préférences en matière de traduction

Dear Ana,

I hope this email finds you well.
I recently spoke with Julia, and there seems to be an issue with one of our containers that is ready to be shipped.
In order to proceed with the release, we urgently need to make a payment of $20,000.

Please note that this is an urgent matter and requires immediate attention.
The payment should be made to the following bank account:

Account Name: XYZ Supplier Co.
Account Number: 123456789
Bank: ABC Bank
SWIFT Code: ABCD1234

Once the payment is made, kindly forward the payment confirmation to me so that I can release the container without any delays.

Thank you for your prompt action on this matter.
If you have any questions or concerns, please do not hesitate to contact me directly.

Best regards,

Francis St-Pitre
Purchasing Department
XYZ Supplier Co.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Mettez à jour régulièrement vos logiciels

Maintenez vos systèmes d'exploitation, vos applications et vos antivirus à jour en installant les dernières mises à jour et correctifs de sécurité. Les mises à jour contiennent souvent des correctifs pour les vulnérabilités connues. Une gestion proactive des mises à jour OS et matérielles limitent de beaucoup les risques de sécurité.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Limitez les informations personnelles partagées en ligne

Évitez de publier des informations personnelles sensibles, telles que votre adresse, votre numéro de téléphone ou vos détails financiers, sur les réseaux sociaux ou d'autres plateformes en ligne.
Évitez de partager des photos pendant que vous êtes en voyage.
Évitez de partager votre localisation lors d’une publication sur les réseaux sociaux.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Utilisez des réseaux Wi-Fi sécurisés

Évitez de vous connecter à des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des informations confidentielles. Privilégiez les réseaux Wi-Fi protégés par mot de passe ou utilisez un VPN en (presque) tout temps.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

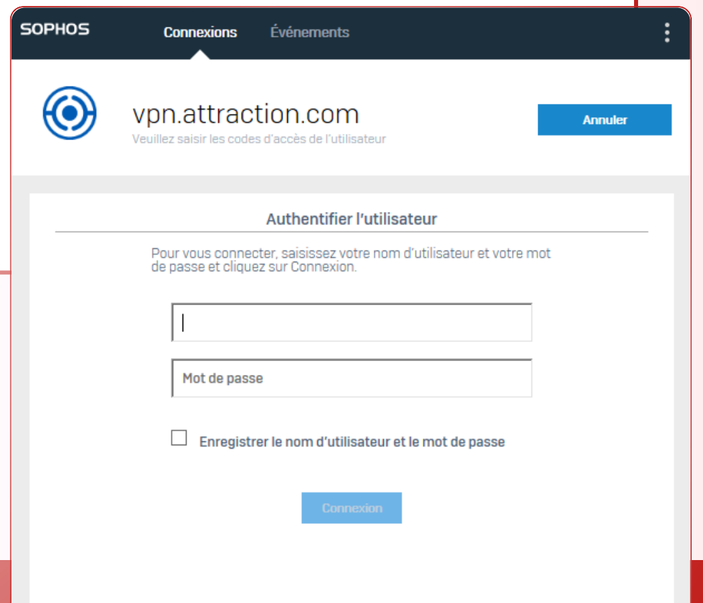
Suppression des cookies

Utilisez les outils de nettoyage du système d’exploitation pour supprimer les cookies de suivi et les données de navigation stockées sur vos appareils.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

VPN (Virtual Private Network)

Utilisez un VPN pour chiffrer votre connexion Internet et protéger votre vie privée en ligne. Des services populaires tels que NordLayer, ExpressVPN ou CyberGhost offrent des fonctionnalités de protection de la vie privée.
Chez Attraction, nous utilisons SOPHOS Connect.



ATTRACTION

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

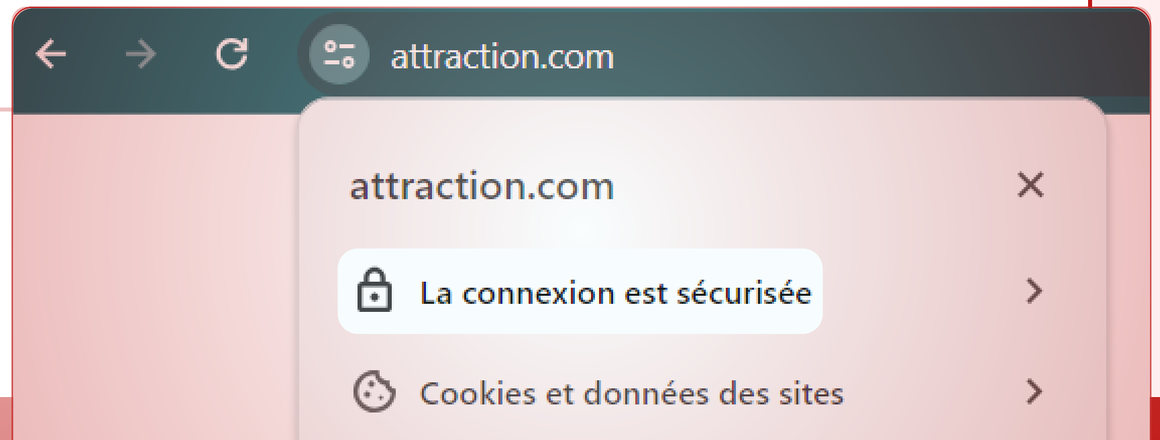
Chiffrement des communications

Utilisez des services de messagerie et de communication chiffrés, tels que Signal, WhatsApp ou Telegram, pour protéger la confidentialité de vos conversations. (Messenger en cours)

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Soyez prudent avec les informations de paiement en ligne

Lorsque vous effectuez des achats en ligne, assurez-vous de le faire sur des sites sécurisés et fiables. Vérifiez la présence d'un cadenas dans la barre d'adresse et utilisez des méthodes de paiement sécurisées, telles que PayPal ou les cartes de crédit protégées.



Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

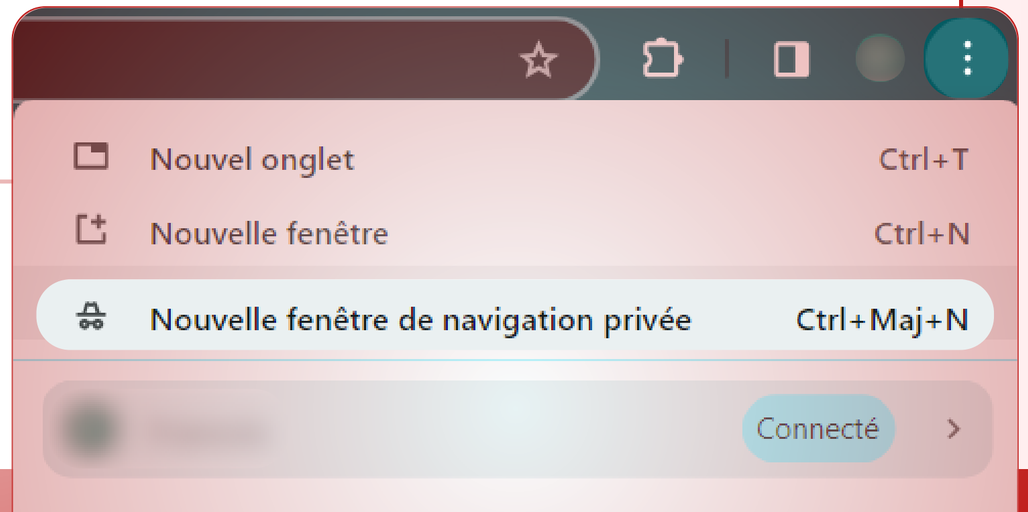
Chiffrement des fichiers

Utilisez des outils de chiffrement pour protéger vos fichiers sensibles. Des logiciels tels que VeraCrypt, AxCrypt ou BitLocker vous permettent de créer des conteneurs chiffrés ou de crypter des fichiers individuels.
Chez Attraction, tous les portables sont chiffrés avec BitLocker.
Gardez les clés de chiffrement en sécurité pour pouvoir récupérer les données en cas de panne de l'ordinateur ou de changement de disque.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Navigation privée

Utilisez le mode de navigation privée ou incognito de votre navigateur pour limiter la collecte de données et de cookies pendant vos sessions de navigation. Cela empêche également l'enregistrement de votre historique de navigation.



Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Vérification des paramètres de confidentialité

Passez en revue et ajustez les paramètres de confidentialité de vos comptes en ligne, tels que les réseaux sociaux, les services de messagerie et les applications, pour limiter la quantité d'informations personnelles partagées et restreindre l'accès à vos données.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Suppression des données personnelles

Supprimez régulièrement les données personnelles inutiles ou sensibles stockées sur vos appareils, tels que les anciens courriels, les fichiers temporaires, les caches de navigateur et les historiques de recherche.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Formation à la sensibilisation à la cybersécurité

Familiarisez-vous avec les meilleures pratiques de cybersécurité en suivant des cours en ligne, en lisant des ressources fiables et en restant informé des dernières menaces et techniques d'attaque.

Il est important de noter que la protection des renseignements personnels est un processus continu et qu'il est essentiel de rester vigilant et de se tenir au courant des dernières pratiques et outils de sécurité en ligne.

Des questions ?

EXTRA POUR LES SUPERVISEURS

Entrevue de départ ou mise à pied

o Éteindre les ordinateurs et appareils professionnels de l’employé.
o Désactiver l’accès de l’employé à tous les systèmes. Suivre la liste des rôles et des accès.
o Supprimer les données professionnelles des appareils appartenant aux employés :
o Observer l'utilisateur supprimer les comptes de messagerie de son téléphone.
o Une personne de l’équipe informatique peut le faire par effacement à distance, ce qui peut potentiellement supprimer des données personnelles (à utiliser avec prudence).
o S’assurer que l'employé retourne tout équipement appartenant à l’organisation : ordinateurs portables, tablettes, clés USB, etc.
o Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

EXTRA POUR LES SUPERVISEURS

Téléphone

o S’assurer que le numéro de téléphone de l'employé n'est pas transféré à un numéro externe, tel qu’un téléphone portable personnel.
o Changer le mot de passe de la messagerie vocale.
o Modifier le message vocal sortant conformément à vos directives de communication.
o Désigner une personne pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou réaffecté.

EXTRA POUR LES SUPERVISEURS

Accès aux courriels

o Ne jamais supprimer le compte courriel d’un employé. La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès tel que mentionné plus bas.
o Modifier le mot de passe du compte dans le système de courriels de l’organisation. Passer en revue la section 4.4 Accès au réseau et au Cloud avant de réactiver le compte.
o Si l'employé a utilisé un téléphone mobile personnel pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.
o Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de votre organisation.
o Supprimer l'employé des listes de diffusion de courriels internes.
o Supprimer l'employé des listes de diffusion de courriels spécialisées. S’assurer que quelqu'un d'autre est membre pour ne pas manquer ces communications.
o Contacter les fournisseurs avec lesquels l’employé a travaillé pour les informer du départ et leur fournir un nouveau contact.
o Désigner quelqu'un et lui donner les accès pour surveiller le courrier électronique de l'employé.

EXTRA POUR LES SUPERVISEURS

Accès au réseau et/ou au Cloud

o Supprimer l'employé de tous les groupes de contrôle d'accès pour la connexion au domaine de l’organisation, VPN, bureau à distance, système d'organisation et autres systèmes.
o Déplacer tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux de l’organisation vers un emplacement central.
o Révoquer l'accès de l’employé au compte infonuagique d'organisation.
o Supprimer les fichiers de travail de tout compte de stockage personnel.
o Passer en revue les règles d'accès au pare-feu pour confirmer que l'utilisateur ne dispose d'aucun autre accès, tel qu'un VPN direct depuis son pare-feu personnel à la maison.
o Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (LogMeIn ou TeamViewer), que l’employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.