PROBLÈMES DE SÉCURITÉ LIÉS AU TÉLÉTRAVAIL

MARS 2019

ITSAP.10.016

Le télétravail est un régime de travail souple et pratique qui vous permet de travailler à l'extérieur de l'environnement de bureau traditionnel. En vous connectant au réseau de votre organisation à distance, vous pouvez continuer d'utiliser les applications et d'accéder à l'information comme si vous étiez au bureau.

PROBLÈMES DE SÉCURITÉ POSÉS PAR LE TÉLÉTRAVAIL

Lorsque vous utilisez de l'équipement à des fins opérationnelles à l'extérieur des périmètres de sécurité TI de votre organisation, vous pourriez créer un maillon faible dans l'infrastructure TI globale de votre organisation. Des auteurs de menace peuvent exploiter ces connexions à distance si celles-ci ne sont pas protégées de manière appropriée. Il importe donc de protéger vos dispositifs mobiles ainsi que les renseignements et les données de nature délicate, qu'ils soient inactifs ou en transit. Les menaces sont susceptibles de mettre en péril la confidentialité, l'intégrité et la disponibilité de l'information.

RISQUES LIÉS AU TÉLÉTRAVAIL

Soyez conscient que le télétravail augmente la possibilité d'occurrence des incidents suivants :

- L'accès physique à votre dispositif par des utilisateurs non autorisés qui pourraient trafiquer, voler ou endommager votre dispositif.
- L'insertion de code malveillant dans votre dispositif, ce qui peut entrainer :
  - La manipulation du trafic (un attaquant insère son propre trafic pour modifier les données et obtenir l'accès au dispositif mobile ou au réseau de l'organisation).
- Le piratage psychologique, dans le cadre duquel des auteurs de menace essaient de vous inciter à communiquer de l'information ou à accorder l'accès à votre dispositif.
- La compromission de vos justificatifs d'ouverture de session, l'oubli de votre mot de passe, paramètres de système de sécurité faibles, etc.
- La compromission des liaisons de communications par les moyens suivants :
  - Écoute électronique : un attaquant écoute le trafic, réseau ou Wi-Fi, ou enregistre vos activités en ligne, ce qui comprend la journalisation de votre nom d'utilisateur et de vos mots de passe.
  - Vol de service : un attaquant tente d'utiliser votre service internet ou puissance de traitement à ses propres fins (p. ex. en envoyant des pourriels), sans aucun intérêt pour le trafic transmis.

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

Généralement, le télétravail demande la protection de **deux éléments essentiels** : le dispositif et la liaison de communication. Vous devriez envisager d'autres mesures de protection lorsque vous utilisez des dispositifs personnels et organisationnels pour le télétravail.

MESURES DE PROTECTION POUR LES DISPOSITIFS PERSONNELS :

- Limitez l'utilisation votre ordinateur de travail à vous seulement (c.-à-d. ne laissez pas les membres de votre famille ou d'autres personnes l'utiliser votre compte créé pour le télétravail).
- Respectez les politiques de stockage des données de l'entreprise, stockez toujours les données de l'entreprise dans un stockage infonuagique ou local approuvé.
- Mettez en œuvre le chiffrement intégral du disque dur en cas de perte ou de vol de votre ordinateur.
- Utilisez un logiciel antimaliciel qui fournit une protection en temps réel ainsi qu'un balayage intégral hebdomadaire (au minimum) du disque dur.
- Utilisez un économiseur d'écran protégé par mot de passe qui s'active après un certain délai d'inactivité.
- Assurez-vous que les mises à jour de correctifs sont installées régulièrement sur votre système d'exploitation et vos applications.
- Protégez votre routeur sans fil domiciliaire à l'aide de phrases de passe robustes, du chiffrement WPA-2 (et non le chiffrement WEP non sécurisé) et de l'adressage MAC, dans la mesure du possible.
- Lors d'un séjour à l'hôtel, protégez votre dispositif en le verrouillant dans le coffre-fort de votre chambre ou de la réception ; ne le laissez jamais sans surveillance dans une chambre d'hôtel.
- Lorsque vous devez laisser votre ordinateur portatif sans surveillance, mettez un cadenas sur la mallette contenant votre ordinateur portatif afin de le protéger contre le vol.
- N'utilisez jamais de clé USB ou de disque dur portatif non approuvé ou non chiffré pour stocker des renseignements opérationnels.
- En plus de votre nom d'utilisateur et de votre mot de passe, employez des méthodes d'identification et d'authentification robustes telles que l'authentification à deux facteurs ou l'authentification fondée sur l'infrastructure à clé publique (ICP).
- Déchiquetez toutes les documents imprimés dans une déchiqueteuse approuvée ou déposez-le dans un bac de déchiquetage sécurisé à votre lieu de travail.
- Ne laissez pas sans surveillance sur un ordinateur des données de nature délicate pouvant être vues ou copies.
- Désactivez les services de réseautage Wi-Fi et Bluetooth lorsque vous ne les utilisez pas et lorsque vous voyagez en transport en commun.
- Signalez immédiatement les événements de sécurité soupçonnés, suspects et réels à l'équipe responsable de la sécurité des TI de votre organisation.

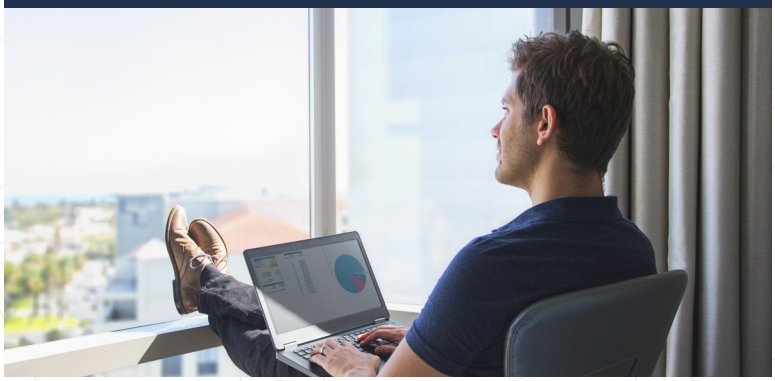
MESURES DE PROTECTION DES DISPOSITIFS ORGANISATIONNELS :

L'équipe responsable des TI au sein de votre organisation peut appliquer des mesures de sécurité à votre dispositif et à votre connexion. Ces mesures comprennent notamment (Si votre organisation ne le fait pas, assurez-vous de suivre les règles de sauvegarde pour les appareils personnels) :

- La surveillance et l'entretien courants de votre dispositif.
- La configuration et la mise à jour du système d'exploitation, des applications principales et des logiciels de sécurité.
- L'utilisation de systèmes de sécurité réseau pour surveiller le trafic.
- L'utilisation de coupe-feux pour bloquer le trafic non autorisé. .

De plus, n'oubliez pas les pratiques exemplaires suivantes :

- Utilisez votre dispositif à des fins professionnelles uniquement.
- Ne configurez pas et n'installez pas de logiciel ou de matériel sur votre dispositif.
- Apprenez à utiliser en toute sécurité le dispositif qui vous a été remis.
- Observez toujours les politiques de sécurité de votre organisation et comprenez vos obligations en matière de sécurité.
- Ne connectez jamais de clé USB ou tout autre périphérique non chiffré à votre dispositif.
- Effectuez des sauvegardes sur votre dispositif pour éviter de perdre de l'information opérationnelle.
- Assurez-vous que l'information conservée sur votre dispositive est chiffrée lorsqu'elle est inactive.
- Accédez uniquement à de l'information non classifiée ou de nature non délicate.
- Suivez les politiques de stockage de données de votre employeur.
- Utilisez toujours l'équipement fourni pour vous connecter au réseau de votre organisation afin d'établir une voie chiffrée et sécurisée au moyen d'un réseau privé virtuel (RPV).



Vous avez des questions ou vous avez besoin d'aide ? Vous voulez en savoir plus sur les questions de cybersécurité ? Consultez le site Web du Centre canadien pour la cybersécurité (CCC) à **cyber.gc.ca**