Conseils pratiques à la mise en place du télétravail pour les particuliers et les entreprises

Pour les particuliers

La pandémie du coronavirus (COVID-19) a incité de nombreuses entreprises à mettre en place des solutions de télétravail. Si vous êtes concerné(e)s par ce type de dispositif, vous devez suivre quelques règles pour garantir votre propre sécurité et celle de votre entreprise.

Suivez les instructions de votre employeur

- Si votre entreprise dispose d'une **charte informatique dans le cadre du télétravail**, prenez-en connaissance et appliquez-la rigoureusement.
- **Ne faites pas en télétravail ce que vous ne feriez pas au bureau.** Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels, notamment sur votre navigation web, en veillant à bien séparer les usages professionnels et les usages personnels. Vous pouvez par exemple créer des comptes distincts si vous utilisez une même application pour ces deux sphères.

Sécurisez votre connexion Internet

- **Assurez-vous du bon paramétrage de votre box Internet**. Vérifiez son mot de passe d'accès administrateur, changez-le s'il est faible et mettez à jour son logiciel interne. Le site web de votre opérateur (par exemple celui de Bouygues, Free, Orange et SFR), vous accompagnera dans la bonne mise en œuvre de ces étapes.
- **Si vous utilisez le Wi-Fi**, activez l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe (l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande par exemple une vingtaine de caractères). Désactivez la fonction WPS et supprimez le Wi-Fi invité. Ne vous connectez qu'à des réseaux de confiance et évitez les accès partagés avec des tiers.

Favorisez l'usage d'équipements fournis et contrôlés par votre entreprise

- Si vous en avez la possibilité, utilisez autant que possible le VPN (Virtual Private Network ou réseau privé virtuel) mis à disposition par votre entreprise :
  - **privilégiez l'échange de données à travers les stockages disponibles depuis le VPN** plutôt que par la messagerie électronique;
  - **connectez-vous au moins une fois par jour au VPN** pour appliquer les mises à jour;
  - **désactivez votre VPN seulement lorsque vous utilisez des services consommateurs de bande passante**, comme le streaming vidéo, qui ne nécessitent pas de passer par le réseau de votre entreprise.

Si vous devez utiliser un ordinateur personnel, assurez-vous qu'il est suffisamment sécurisé

- Cela doit passer par:
  - **l'installation d'un antivirus et d'un pare-feu**. Si vous êtes sur le système d'exploitation *Windows 10*, vérifiez l'état de vos systèmes de protection au moyen du centre de sécurité ;
  - **l'utilisation d'un compte personnel avec des droits limités**, protégé par un mot de passe fort et non partagé avec d'autres personnes (par exemple avec d'autres membres de votre famille) et sur lequel les applications installées se limitent au strict nécessaire ;
  - **la mise à jour régulière du système d'exploitation et des logiciels utilisés**, notamment le navigateur web et ses extensions. Supprimez ou passez au plus vite à une version récente des logiciels dont le support ou la mise à jour sont abandonnés, comme le système d'exploitation *Windows 7* (et les versions antérieures comme *Windows XP*) dont le support n'est plus assuré depuis le 14 janvier 2020;
  - **des sauvegardes régulières de votre travail** de préférence sur les infrastructures de votre entreprise, si possible en activant une solution de sauvegarde automatique ;
  - **l'utilisation de mots de passe forts sur l'ensemble de vos services** et l'activation de l'authentification à deux facteurs (clef d'authentification, jeton, sms) dès que cela est proposé par le service. Les gestionnaires de mots de passe, par exemple les logiciels KeePass et ZenyPass, vous permettront également de sécuriser leur stockage et leur gestion. La site de la CNIL propose un outil pour créer rapidement des mots de passe robustes ainsi qu'un tutoriel pour utiliser le gestionnaire de mots de passe Keepass.

Si vous devez utiliser votre téléphone personnel, protégez vos données et limitez les accès

- Parce qu'ils vous accompagnent partout, les téléphones portables sont particulièrement exposées à la perte et aux vols:
  - **Evitez d'y enregistrer des informations confidentielles**: codes secrets, codes d'accès, coordonnées bancaires, etc ;
  - **Activez le code PIN et mettez en place un délai de verrouillage automatique du téléphone**. Évitez les codes trop faciles (date de naissance, 0123, etc.) ;
  - **Activez le chiffrement des informations** sur votre téléphone lorsque c'est possible;
  - **Notez le numéro "IMEI" du téléphone** pour le bloquer en cas de perte ou de vol ;
  - **N'installez des logiciels que depuis les plateformes officielles** et évitez à tout prix les applications de sources inconnues ;
  - Lorsque vous installez de nouvelles applications sur votre appareil, **lisez les conditions d'utilisation et la politique de confidentialité et limitez les données auxquelles elles peuvent avoir accès au strict nécessaire**;

- Réglez les paramètres de géolocalisation afin de toujours contrôler **quand et par qui être géolocalisé**.

Communiquez en toute sécurité

- **Évitez de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries.** A défaut, chiffrez les données avant de les transmettre et transmettez les clés de chiffrement via un canal de communication distinct (par exemple, communication du mot de passe par téléphone ou SMS). Des logiciels grand public comme 7-zip et Zed! permettent de chiffrer les données avec des algorithmes réputés fiables.
- **Installez uniquement des applications autorisées par votre entreprise.** Si votre entreprise ne propose pas de système de déploiement d'application, téléchargez celles-ci depuis les sites ou les magasins officiels des éditeurs.
- **Privilégiez des outils de communication chiffrés de bout en bout**, si votre entreprise ne vous fournit pas d'outils de communication sécurisé. Evitez les applications gratuites qui ne vous offrent pas de garanties fortes de sécurité. Dans tous les cas, respectez toujours les instructions de votre employeur.
- **Privilégiez les systèmes de visioconférence qui protègent la vie privée**. Vérifiez les conditions d'utilisation de votre logiciel pour vous assurez que ces outils garantissent la confidentialité de vos données et ne les réutilisent pas pour d'autres finalités. L'ANSSI a certifié Tixeo pour les administrations, les Opérateurs d'Importance Vitale (OIV) et les entreprises soucieuses de leur sécurité. La direction interministérielle du numérique (DINUM) et la Direction Générale de l'Administration et de la Fonction Publique (DGFAP) fournissent un tableau comparatif pour vous accompagner dans le choix d'une solution qui convient à votre besoin.

Soyez particulièrement vigilant sur les tentatives d'hameçonnage

- Les pirates profitent des périodes de crise ou de trouble pour inventer de nouvelles escroqueries et tirer profit de ces événements. Soyez vigilant à tout contact :
  - *de personnes que vous ne connaissez pas*, surtout si elles vous invitent à cliquer sur des liens ou à ouvrir un fichier;
  - *d'une personne connue vous envoyant une communication inhabituelle.* Essayez de vérifier cette information par un autre canal (téléphone, SMS, mail);
  - *de personnes cherchant à créer un sentiment d'urgence ou de danger.* Le cas échéant, toujours utiliser un autre canal pour vérifier les informations communiquées, par exemple en effectuant une recherche sur Internet.
- **En cas de doute, demandez de l'aide à votre directeur des systèmes d'information (DSI) ou votre responsable de la sécurité des systèmes informatiques(RSSI)**.

Pour les entreprises

Dans le contexte du COVID-19, le télétravail est une solution qui doit s'accompagner de mesures de sécurités renforcées pour garantir la sécurité des systèmes d'information et des données qu'ils traitent. La CNIL publie des recommandations pour aider à la bonne sécurisation des données personnelles durant cette transition.

Sécurisez votre système d'information

- Éditez une **charte de sécurité dans le cadre du télétravail** ou, dans le contexte actuel, au moins un socle de règles minimales à respecter, et communiquez ce document à vos collaborateurs suivant votre règlement intérieur.
- Si vous devez modifier les règles de gestion de votre SI pour permettre le télétravail (changement des règles d'habilitation, accès des administrateurs à distance, etc.), **mesurez les risques encourus** et, au besoin, **prenez les mesures nécessaires** pour maintenir le niveau de sécurité.
- **Équipez tous les postes de travail de vos salariés au minimum d'un pare-feu, d'un anti-virus et d'un outil de blocage de l'accès aux sites malveillants.**
- **Mettez en place un VPN pour éviter l'exposition directe de vos services sur Internet**, dès que cela est possible. Activez l'authentification du VPN à deux facteurs si c'est possible.
- Mettez à disposition de vos salariés une liste d'outils de communications et de travail collaboratif appropriés au travail distant, qui garantissent la confidentialité des échanges et des données partagées. Favorisez des outils dont vous conservez la maîtrise et assurez-vous qu'ils fournissent au minimum une authentification et un chiffrement des communications conformes à l'état de l'art et que les données transitant ne sont pas réutilisées pour d'autres finalités (amélioration du produit, publicitaire, etc.). Certains logiciels grand public peuvent transmettre à des tiers les données sur leurs utilisateurs, et s'avèrent donc particulièrement inadaptés pour un usage en entreprise. En outre, la direction interministérielle du numérique (DINUM) déconseille l'usage de certains logiciels, tels que Zoom, pour échanger des informations non publiques et recommande d'autres solutions telles que Jitsi. Vous pouvez également vous appuyer sur la liste des produits certifiés Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'ANSSI.

Si vos services sont accessibles depuis Internet

- **utilisez des protocoles garantissant la confidentialité et l'authentification du serveur destinataire**, par exemple *HTTPS* pour les sites web et *SFTP* pour le transfert de fichiers, en utilisant les versions les plus récentes de ces protocoles ;
- **appliquez les derniers correctifs de sécurité** aux équipements et logiciels utilisés (VPN, solution de bureau distant, messagerie, vidéoconférence etc.). Consultez régulièrement le bulletin d'actualité CERT-FR pour être prévenu des dernières vulnérabilités sur les logiciels et des moyens pour s'en prémunir ;
- **mettez en œuvre des mécanismes d'authentification à double facteur** sur les services accessibles à distance pour limiter les risques d'intrusions ;

- **consultez régulièrement les journaux d'accès aux services accessibles à distance** pour détecter des comportements suspects ;
- **ne rendez pas directement accessibles les interfaces de serveurs non sécurisées**. De manière générale, limitez le nombre de services mis à disposition au strict minimum pour limiter les risques d'attaques.

Références pour vous accompagner dans cette sécurisation

- Le guide du NIST sur le télétravail (en anglais uniquement).
- Le bulletin d'actualité du CERTFR-2020-ACT-002.
- Les différents guides de l'ANSSI, notamment le guide d'hygiène informatique, les recommandations de sécurité relatives aux réseaux Wi-Fi, les bonnes pratiques pour se prémunir des rançongiciels et la liste des produits et services qualifiés.
- La plateforme cybermalveillance.gouv.fr d'aide nationale d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace en France, notamment les recommandations de sécurité informatique pour le télétravail en situation de crise.
- Le guide de la sécurité des données personnelles et les bonnes pratiques du BYOD de la CNIL ainsi que la cartographie des outils et pratiques de protection de la vie privée du LINC.

Vous souhaitez contribuez à ce guide ?

- Ce guide est publié sous licence GPLv3 et sous licence ouverte 2.0 (explicitement compatible avec CC-BY 4.0 FR). **Il est donc librement partageable**. Vous en trouverez une version PDF dans l'onglet "Releases".
- **Vous pouvez contribuer à son enrichissement.** Cela se fait en quelques étapes :
- inscrivez-vous sur la plateforme Github ;
- rendez-vous sur la page du projet ;
- vous pouvez :
  - utiliser l'onglet "Issue" pour ouvrir des commentaires ou participer à la discussion
  - utiliser l'option "Fork" en bannière de cette page pour faire vos propres modifications et proposer leur inclusion via le bouton "Pull Requests"
- **Toutes vos propositions de contribution seront examinées par la CNIL avant publication**.