MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

COVID-19

Télétravail et travail à distance

Suite à la décision visant à réduire très fortement tous les déplacements, le télétravail - pour tous les postes qui le permettent – et le travail à distance deviennent la règle impérative. Seuls les agents publics participant aux plans de continuité de l'activité en présentiel se rendent effectivement sur leur lieu de travail. Pour les autres agents, en cas d'impossibilité de télétravailler, l'agent est placé en autorisation spéciale d'absence (ASA).

La généralisation de ces pratiques professionnelles pour répondre à la crise sanitaire COVID-19, sollicite fortement les systèmes d'information du ministère et augmente de façon importante les risques de compromission ou d'atteinte aux ressources ou aux services numériques.

5 bonnes pratiques pour un usage responsable du télétravail

Pour préserver l'accès aux outils informatiques professionnels à partir des outils mis à votre disposition par le service du numérique (SNum), nous vous remercions d'appliquer 5 bonnes pratiques :

1. **Réservez vos consultations internet à un usage strictement professionnel**

2. **Évitez les téléchargements de fichiers lourds**

COVID-19

3 **Limitez l'utilisation d'internet entre 10 h 30 et 15 h 30**

4 **Supprimez les images de ma signature de mail ou redussiez-là au maximum (nom, prénom, numéro de téléphone)**

5 **Déconnectez-vous du réseau à distance ou utilisez votre ordinateur ou smartphone personnel pour des usages gourmands (comme le visionnage de vidéos) ou pour des recherches/consultations personnnelles**

Travailler à distance avec des moyens personnels

La généralisation du travail à distance pour répondre à la crise sanitaire COVID-19 favorise par ailleurs le recours à des équipements personnels. Or, les ordinateurs et équipements personnels sont moins bien protégés que ceux fournis par le ministère. Ils constituent des cibles de choix pour les cybercriminels, qui espèrent profiter de la situation pour les piéger.

Face aux différentes cyber menaces, l'utilisation de moyens personnels doit respecter a minima les bonnes pratiques suivantes :

· Vérifiez que votre équipement dispose bien d'un système d'exploitation et d'un antivirus à jour et si possible d'un pare-feu activé. En cas de doute, évitez de l'utiliser à titre professionnel ;

COVID-19

- Assurez-vous qu'un mot de passe ou un code PIN protège bien l'accès au système d'exploitation de votre équipement ;
- Limitez au strict nécessaire l'usage de votre messagerie électronique personnelle pour des échanges professionnels ;
- En cas de traitement ou de transmission de données professionnelles de type Office, protégez les en utilisant la protection native de Windows Office (fichier > protéger le document > chiffrer avec mot de passe) ou le logiciel gratuit de l'éditeur Prim'X : https://www.zedencrypt.com/download
- Privilégiez l'utilisation des services de communication de l'État tels : TCHAP https://www.tchap.gouv.fr ou Web conférence https://webconf.numerique.gouv.fr pour communiquer avec vos collègues ou votre entité(groupe de discussion) ;
- Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs ;
- Limitez pendant cette période, autant que possible, l'utilisation d'Internet aux sites officiels ou gouvernementaux.

En cas de doute

Éviter d'utiliser vos équipements et ordinateur personnels à titre professionnel car vous exposez ainsi directement la sécurité du ministère et plus largement de l'Etat. Le service du numérique (SNum) du ministère n'assure aucun support sur vos logiciels, matériels et connexions réseaux personnels. En cas de suspicion de risque informatique, il vous est demandé de joindre la structure de gestion de la Cybermalveillance en mettant en copie le service HFDS covide19-SSI@justice.gouv.fr. Cette structure publique a notamment pour missions d'aider les particuliers victimes de cybermalveillance, de les informer sur les menaces numériques et de leur donner les moyens de se défendre.

https://www.cybermalveillance.gouv.fr/