PETIT GUIDE

DU TÉLÉTRAVAIL SÉCURISÉ

A L'USAGE DES SALARIÉS PENDANT LE #COVID19

PAR EQUIPAGES IT SOLUTIONS

Les appareils personnels

PC et portables privés utilisés à des fins professionnelles

Il est possible que votre entreprise n'ait pas anticipé une situation de télétravail généralisé due au confinement, et que vous ne disposiez par exemple pas de PC portable. Vous vous retrouvez donc avec pour seuls outils de travail vos propres équipements : PC personnel, téléphone privé…

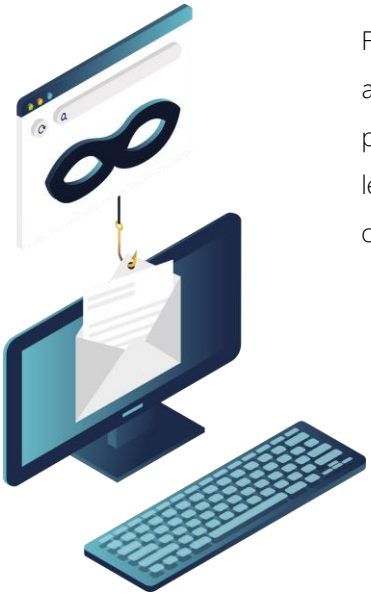
Si vous avez l'avantage de bien connaître ces derniers, il faut bien prendre conscience que vous allez travailler sur des documents et des données d'entreprise. L'utilisation de vos appareils doit évoluer en conséquence !

Les points à vérifier

- ☐ Vous êtes équipé d'un des antivirus reconnus et/ou imposés par votre entreprise
- ☐ Votre antivirus est à jour
- ☐ Tous vos logiciels et systèmes d'exploitation sont à jour
- ☐ Vos appareils sont protégés par un mot de passe (ou autre système d'authentification choisi par l'entreprise) unique, connu de vous seul et changé régulièrement
- ☐ Vos appareils sont utilisés par vous et vous seul

Le phishing

Vol de données personnelles via une fausse page web



Face à une situation nouvelle et inédite, des acteurs malveillants vont rivaliser d'imagination pour créer des emails plus vrais que nature dans le but de vous piéger, obtenir des codes d'accès ou infecter vos appareils.

Vous pourriez ainsi recevoir un email imitant un collègue, une communication corporate ou officielle et vous menant à une fausse page de connexion pour récupérer vos identifiants ou d'autres informations confidentielles.

Les points à vérifier

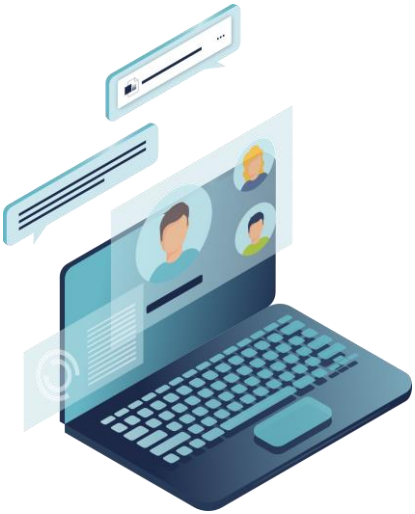
- ☐ Votre antivirus comprend une protection contre le phishing
- ☐ Vérifiez toujours l'adresse email de l'émetteur
- ☐ Vérifiez les liens hypertexte en passant votre souris dessus pour voir l'url
- ☐ Connectez-vous directement sur un site en tapant l'url dans la barre de recherche plutôt qu'en cliquant sur un lien envoyé par email
- ☐ Soyez particulièrement attentif aux mails abordant le coronavirus
- ☐ Vérifiez que les sites sur lesquels vous vous connectez soient sûrs (url commençant par « https » avec un petit cadenas à gauche)

La collaboration

Échanger avec vos collègues et partenaires à distance

Fini les réunions avec le télétravail ? Pas si sûr… Il est temps pour votre entreprise, si ce n'est déjà fait, d'adopter un outil de visioconférence, mais également de partage et de stockage en ligne.

Bien sûr, nous utilisons tous déjà ce genre d'outil au quotidien (WeTransfer, Google Drive, DropBox…), et la tentation est grande d'utiliser ces mêmes outils gratuits pour travailler : vous les connaissez bien, vous avez déjà un compte…
Mais attention ! Vous travaillez sur les données de l'entreprise, potentiellement sensibles, et la manière dont vous les utilisez doit respecter les politiques de protection des données de la société. Or, des acteurs malveillants vont profiter de la situation pour mettre à disposition des services de collaboration infectés, gratuits ou imitant vos outils habituels

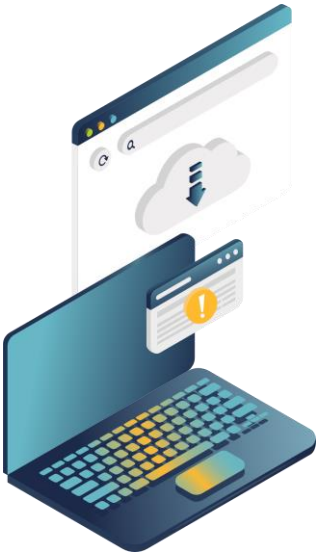


Les points à vérifier

- ☐ N'utilisez pas d'autres outils que ceux indiqués par votre société
- ☐ Vos outils de collaboration sont à jour
- ☐ Assurez-vous d'être sur le site officiel des logiciels que vous souhaitez télécharger (allez sur le site en tapant l'url dans la barre de recherche et non en cliquant sur un lien reçu)

Les téléchargements

Equiper ses appareils privés des logiciels et outils d'entreprise



En temps normal, il faut être attentif à ce que vous téléchargez. Mais en situation de télétravail généralisé, où vous êtes amenés à vous échanger beaucoup de mails et à envoyer beaucoup de documents en ligne à vos collègues et partenaires, il est d'autant plus important de vérifier tous vos téléchargements.

Des acteurs malveillants vont profiter de la peur du coronavirus pour créer des email anxiogènes imitant une communication officielle ou corporate ; ou encore des logiciels censés faciliter le télétravail dans le but d'infecter votre ordinateur

Les points à vérifier

- ☐ Assurez-vous d'être sur le site officiel des logiciels que vous souhaitez télécharger
- ☐ N'ouvrez et ne téléchargez les pièces jointes que des émetteurs en lesquels vous avez confiance
- ☐ Ne laissez pas l'accès à vos appareils à des tierces personnes (ex: enfants qui pourraient télécharger un jeu infecté)
- ☐ Ne téléchargez que le strict minimum, et uniquement les logiciels recommandés par votre entreprise

Les sauvegardes

Éviter la perte de travail et de données en cas de problème

Si vous n'êtes pas connecté au réseau de l'entreprise via un VPN, cette dernière doit s'assurer que vous disposiez d'un système de sauvegarde des données performant. Car les ransomwares, ces logiciels qui chiffrent vos données et vous demandent de l'argent en échange de la clé de décryptage, ne sont pas touchés par le coronavirus !

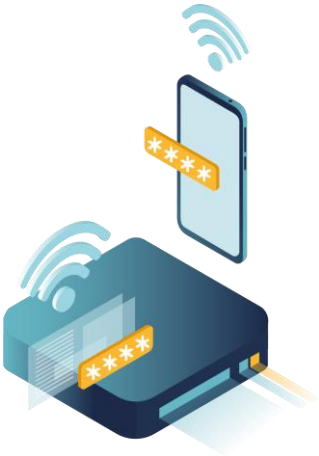
Votre système de sauvegarde peut prendre la forme d'un NAS (Network Attached Storage – un serveur de stockage en réseau sous forme d'un petit boitier contenant des baies de stockage) ou d'une solution Cloud.
Quelle que soit la solution choisie, il vous incombe d'assurer son bon fonctionnement et le respect des procédures de sauvegarde. Dans tous les cas, rapprochez vous de votre service informatique pour connaître les modalités de sauvegarde des données

Les points à vérifier

- ☐ Contactez votre service informatique pour avoir des informations concernant le type de stockage choisi par votre entreprise et les démarches à suivre de votre côté

Les réseaux

Se connecter pour accéder aux ressources de l'entreprise



Idéalement, votre entreprise dispose d'un VPN auquel vous pouvez vous connecter pour accéder à toutes les ressources de votre société. Cependant, si ce n'est pas le cas, et que vous y accédez via un réseau Wi-Fi privé ou partage de connexion, il est judicieux de procéder à quelques ajustements afin de sécuriser votre connexion. Si vous n'avez pas la main sur votre réseau (réseaux publics, d'hôtel…), la solution la plus sûre reste encore d'utiliser un VPN. Dans tous les cas, rapprochez vous des services informatiques de votre entreprise afin de connaître les démarches d'installation de VPN et/ou de sécurisation de vos nouveaux postes de travail.

Les points à vérifier

- ☐ Changez le mot de passe de votre Wi-Fi ou partage de connexion
- ☐ Utilisez toujours le VPN d'entreprise si existant, éventuellement un VPN personnel le cas échéant
- ☐ *Option* : désactiver le SSID afin que votre réseau n'apparaisse plus aux appareils non configurés - il faudra entrer manuellement chaque appareil dont vous souhaitez autoriser la connexion
- ☐ *Option* : appliquer le filtrage MAC si disponible sur votre Box afin de n'autoriser la connexion qu'à certains appareils manuellement définis au préalable

Le confort

S'installer confortablement pour travailler efficacement

Dernier point mais non des moindres, votre confort ! Si vos espaces de travail au bureau sont en général ergonomiquement pensés, la transition soudaine au télétravail ne permet pas toujours de mettre en place des conditions de travail idéales : espace fermé / peu ou trop lumineux / mal aéré, chaise inconfortable, petits écrans, distractions, environnement bruyant…

Un mauvais espace de travail peut causer des douleurs physiques et accélérer la fatigue. Il convient donc d'aménager un peu votre environnement personnel pour travailler dans de bonnes conditions.

Les points à vérifier

- ☐ Définissez un espace de travail clairement identifié et si possible isolé
- ☐ Prenez des pauses régulières (15min toutes les 2h au minimum)
- ☐ Suivez des horaires réguliers
- ☐ Placez votre écran à hauteur des yeux
- ☐ Nettoyez et désinfectez régulièrement clavier, souris et tout autre équipement
- ☐ Positionnez-vous de manière à ce que les bras soient en angle droit
- ☐ Reposez vos pieds à plat sur le sol (ou un repose pied)

Le respect des règles

La sortie de la crise #Covid19, c'est l'affaire de tous

Pour faire face à cette situation inédite, votre entreprise vous a probablement fourni des règles de sécurité et cybersécurité afin de vous protéger et protéger l'entreprise. Il est important de respecter ces mesures afin de garantir votre sécurité et l'intégrité des données sur lesquelles vous travaillez.

En cas de non respect, vous exposez vos collègues, vous-même et votre entreprise à une cyberattaque qui pourrait d'autant plus impacter son activité. En cas de doute, pensez toujours à contacter votre service informatique.

Prenez soin également de suivre l'actualité et respecter les consignes données par le gouvernement et l'OMS afin de limiter la propagation du virus, protéger vos proches et assurer un retour à la normal le plus rapide possible

Bon télétravail à tous !

EQUIPAGES
IT SOLUTIONS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Santé publique France

COVID-19

CORONAVIRUS, POUR SE PROTÉGER ET PROTÉGER LES AUTRES

Lavez-vous très régulièrement les mains

Toussez ou éternuez dans votre coude

Utilisez un mouchoir à usage unique et jetez-le

SI VOUS ÊTES MALADE

Portez un masque chirurgical jetable

Vous avez des questions sur le coronavirus ?

GOUVERNEMENT.FR/INFO-CORONAVIRUS

0 800 130 000
(appel gratuit)