**ANNEXE AU CONTRAT DE TRAVAIL**

Lorsque vous travaillez depuis chez vous, vous êtes exposés à de nouveaux dangers et votre niveau de vigilance n'est plus le même. N'oubliez pas que les pirates profitent des moments de panique pour piéger les personnes en jouant sur leur naïveté, leur empressement et leur peur. Pour cela ils vont potentiellement vous proposer de télécharger une multitude de logiciel améliorant "soi-disant" la qualité de votre navigation, augmentant la sécurité de votre vie privée, protégeant votre ordinateur contre le COVID-19.

Mais vous allez également subir, très certainement, une myriade de canulars vous invitant à renseigner des informations personnelles voire des mots de passe.

Restez donc vigilants et naviguez sur des sites officiels.

Il faut aussi garder à l'esprit que la charte informatique de votre entreprise reste applicable et qu'il est donc nécessaire de respecter la politique de sécurité de votre entreprise.

**Rappel de bonnes pratiques universelles :**

1. Connecter votre PC professionnel uniquement à un réseau connu, correctement sécurisé (WPA2 : mentionné sur votre box)
Si cela est possible pour vous, et que vous utilisez votre réseau personnel, durcissez votre mot de passe wifi pour éviter une éventuelle intrusion.
2. Ne pas naviguer sur des sites inutiles à votre métier (divertissement etc.)
3. Ne pas utiliser sa boite mail personnelle sur son PC professionnel
4. Ne branchez pas vos équipements personnels à votre PC professionnel
5. Naviguez uniquement sur des sites utilisant HTTPS. Attention aux certificats des sites sur lesquels vous naviguez (ne pas accepter les erreurs de certificat).
Faites attention également aux noms de domaines des sites web visités, comme il l'a été mentionné, il s'agit d'une période à risque ou les pirates sont peut-être de sortie.
6. Gardez à jour votre PC, n'installez aucun logiciel sans en avertir votre DSI. Prévenez votre DSI dès que vous détectez un comportement anormal de votre PC.