Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DES ARDENNES

Cabinet

Charleville-Mézières, le 26 FEV. 2018

Affaire suivie par : Aude Bernier
Tel : 03 24 59.66.21

@ : aude.bernier@ardennes.gouv.fr

Le Préfet

à

Messieurs les présidents des chambres consulaires

Mesdames et messieurs les présidents des fédérations professionnelles

En communication à :

Mesdames et Monsieur les sous-préfets

Mesdames et Messieurs les chefs de service de l'Etat

Objet : Les vulnérabilités liées à l'utilisation professionnelle des smartphones

Je souhaite appeler votre attention sur les cas de compromission ou de captation d'informations liés à l'utilisation de smartphones dans un cadre professionnel qui sont régulièrement observés. Ils surviennent bien souvent à l'occasion de déplacements à l'étranger ou, plus communément, à la suite d'un usage non sécurisé.

L'utilisation des smartphones, très largement répandue dans l'environnement professionnel, permet de consulter les courriels professionnels, de naviguer sur Internet ou encore de se connecter sur des réseaux d'entreprise pour travailler, comme il serait possible de le faire depuis un poste fixe de travail.

En outre, de nombreux utilisateurs ont un usage dual de leur téléphone professionnel, l'utilisant également à des fins personnelles pour télécharger, notamment, des applications ludiques ou un accès aux différents réseaux sociaux. Comme le souligne l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il est illusoire d'espérer atteindre un haut niveau de sécurité avec un smartphone, quel que soit le soin consacré à son paramétrage. Il est toutefois nécessaire de protéger au mieux les données qu'il contient.

Afin de limiter les risques liés à leur utilisation, il convient de mettre en œuvre les préconisations suivantes :

Risque de vol :

- Protéger les données contenues dans le smartphone par un verrouillage systématique de l'écran
- Verrouiller son téléphone portable par un code alphanumérique de 8 caractères
- Chiffrer les données sensibles grâce à des solutions de chiffrement pour smartphones

- Prévenir la police ou la gendarmerie en cas de vol ou de perte d'un téléphone professionnel pouvant contenir ou contenant des informations sensibles ou stratégiques

Vulnérabilité du système :

- Mettre à jour régulièrement le système d'exploitation et l'ensemble des applications téléchargées sur le smartphone
- Afin de se protéger contre l'installation d'une application malveillante, ne jamais cliquer sur un lien d'origine inconnue et éviter de scanner des QR codes
- Avant de télécharger une application, vérifier sa provenance et ses droits d'accès aux données du téléphone
- S'assurer du téléchargement des applications et de leur mise à jour à partir d'une plateforme officielle
- Rester vigilant aux potentielles atteintes à la confidentialité liées à l'accès aux données personnelles

Géolocalisation :

- Désactiver systématiquement la fonction géolocalisation une fois utilisée
- Les photos et vidéos indiquent par ailleurs le lieu, la date et l'heure de la prise de vue dans les métadonnées

Wi-Fi2 :

- Installer un VPN (Virtual Private Network) permettant la transmission chiffrée des données. Certains VPN sont directement téléchargeables sur les smartphones via des applications
- Ne pas laisser le Wi-Fi actif sans nécessité, celui-ci transmettant en permanence l'historique et la géolocalisation de vos anciennes connexions

Bluetooth :

- Désactiver la fonction après utilisation

Utilisation :

- Limiter le plus possible l'utilisation du smartphone professionnel à des fins personnelles et inversement
- Dans le cadre d'un déplacement professionnel à l'étranger, privilégier l'utilisation d'un téléphone dédié.

Je vous appelle donc à la plus grande prudence et vous invite à relayer le plus largement possible cette information auprès de vos adhérents.

Mes services restent à votre disposition pour tout renseignement complémentaire.

Pascal JOLY