FO ÉNERGIE ET MINES

Avril 2020

Communiqué

COMPLÉMENT D'INFORMATION QUANT À L'UTILISATION DES MOYENS INFORMATIQUES

La période de confinement est une réelle opportunité pour les attaques malveillantes en tout genre sur nos postes informatiques, téléphones, tablettes…

Si les entreprises ont mis à disposition des salariés des moyens informatiques « protégés », il n'en est pas de même pour les outils digitaux personnels. Il arrive parfois d'utiliser son matériel au motif que la sécurisation des outils de l'entreprise nous bloque pour télécharger des applications courantes dans le but de suivre des visioconférences, de pouvoir échanger via des outils de discussions.

La CNIL met en garde sur l'utilisation d'applications dites « VoIP ». Ces logiciels sont basés sur une technologie permettant à l'utilisateur d'utiliser le micro et/ou la webcam de son matériel personnel en étant connecté à Internet.

Pourquoi cette mise en garde de la CNIL ?

Ces applications apparaissant comme « gratuites » peuvent vous proposer des services supplémentaires moyennant un abonnement. Mais elles peuvent rentabiliser leurs services en captant et traitant des informations vous concernant tels que vos nom, prénom, adresse mail, numéro de téléphone… qui peuvent être complétées à votre insu par d'autres données beaucoup plus personnelles via votre adresse IP, alors que c'est interdit de ne pas informer l'utilisateur des données collectées.

En cette période de fort piratage de données, la CNIL a rappelé quelques règles utiles à destination des utilisateurs :

- Privilégier les solutions protégeant la vie privée recommandées par l'ANSSI (Agence Nationale de la Sécurité Informatique).
- Éviter de télécharger une application depuis un site web inconnu.
- Utiliser les applications affichant clairement comment vos données seront réutilisées.
- Vérifier que les mesures de sécurité ont été mises en place (mot de passe, chiffrement…).
- S'assurer que l'antivirus et le pare-feu sont à jour sur votre matériel.
- Ne jamais renseigner l'intégralité des données demandées à l'inscription sauf si elles sont obligatoires.

- Utiliser un mot de passe distinct pour toutes ces applications spécifiques.

- Penser à vérifier dans les paramètres de l'application la mention se rapportant à la protection de votre vie privée.

- Fermer l'application sur le PC ou le téléphone quand vous ne l'utilisez plus et pensez à désactiver le microphone et la webcam (quitte à lui mettre un cache).

Les données des utilisateurs sont des mines d'or pour toutes ces entreprises. Elles les vendent à des sociétés de marketing dans le meilleur des cas, mais ce sont aussi des portes ouvertes pour les personnes ou organismes malveillants.

N'oubliez pas vos données sont précieuses, pensez à les protéger !