HISCOX
CYBERCLEAR®

Loin de l'environnement de bureau sécurisé, le télétravail occasionne des failles de sécurité (utilisation d'appareils personnels, nouveau réseau Wifi, partage des écrans...). Les données sont ainsi plus exposées et les pirates y voient des opportunités de pièger de nouvelles victimes. Comment sécuriser vos objets connectés ?

CONSEILS POUR OPTIMISER LA SÉCURITÉ INFORMATIQUE DE VOS OBJETS CONNECTÉS

1. CONSEILS POUR OPTIMISER LA SÉCURITÉ INFORMATIQUE DE VOS OBJETS CONNECTÉS

57% des systèmes d'exploitation mobile Android et 20% des systèmes Apple ne sont pas à jour de la dernière version du système.

2. VÉRIFIER LES APPLICATIONS INSTALLÉES

Quelles sont les fonctions des applications et sont-elles nécessaires ? Quelles sont celles qui fonctionnent sans être ouvertes ?

3. PERMETTRE LES SYNCHRONISATIONS ET LES SAUVEGARDES AUTOMATIQUES

Cela sera utile en cas de vol de votre appareil.

4. DÉSINSTALLER OU DÉCONNECTER LES APPLICATIONS NON UTILISÉES

Attention : effacer les icônes de bureau n'équivaut pas à désinstaller complètement une application.

5. VÉRIFIER LES AUTORISATIONS QUE VOUS DONNEZ AUX APPLICATIONS

Les accès que vous approuvez permettent à l'application de mettre en place des actions potentiellement dangereuses.

6. UTILISER SI POSSIBLE UN APPAREIL PROFESSIONNEL

Si vous utilisez unn téléphone personnel pour des usages professionnels, assurez-vous de connaître les bons usages de cyber sécurité (votre entreprise doit vous y former).

RENFORCER ENCORE PLUS LA SÉCURITÉ SUR L'ENSEMBLE DE VOS OBJETS CONNECTÉS :

7. INSTALLER UN ANTI-VIRUS OU METTRE À JOUR L'ANTI-VIRUS EN PLACE AINSI QUE TOUS LES LOGICIELS DE SÉCURITÉ

8. SÉPARER VOS PROFILS PROFESSIONNELS ET PERSONNELS SUR VOS COMPTES RÉSEAUX SOCIAUX OU AUTRES

Vérifiez également les paramètres de confidentialité de vos comptes réseaux sociaux.

9. EVITER DE SUPPRIMER LES PARAMÈTRES DE SÉCURITÉ DU SYSTÈME DE VOTRE OPÉRATEUR

10. ASSURER VOUS QUE VOTRE CONNEXION WIFI EST SÉCURISÉE ET CHANGER LE MOT DE PASSE PAR DÉFAUT DE VOTRE MODEM

11. CRÉER DES MOTS DE PASSE RENFORCÉ ET ÉVITER D'UTILISER LE MÊME SUR DIFFÉRENTS VOS COMPTES

Se méfier de tout mail demandant de vérifier ou renouveler un identifiant de connexion ou un Mot de passe.

12. SAUVEGARDER LES FICHIERS IMPORTANTS ET UTILISER UN OUTIL DE CHIFFREMEN

Ce sera précieux en cas de ransomware.

13. VÉRIFIER LA SOURCE AVANT DE CLIQUER SUR UN LIEN OU D'OUVRIR UNE PIÈCE JOINTE

Attention : Les pirates savent créer un sentiment d'urgence pour vous inciter à cliquer. Des demandes inhabituelles de la part d'une personne connue doivent vous alerter, appelez la personne avant de cliquer.

14. VÉRIFIER VOS COMPTES EN BANQUES RÉGULIÈREMENT POUR REPÉRER D'ÉVENTUELLES OPÉRATIONS INHABITUELLES

15. CONTRÔLER LES DESTINATAIRES SI VOUS FAITES UN DON POUR UNE OEUVRE ASSOCIATIVE

16. SENSIBILISER VOS ENFANTS AUX RÈGLES ÉLÉMENTAIRES DE CYBER SÉCURITÉ

Utiliser le contrôle parental pour les protéger lorsqu'ils utilisent vos objets connectés et lorsqu'ils sont en ligne.

HISCOX ASSURANCES | Penser à tout, et surtout à vous

Pour plus d'informations
www.hiscox.fr
www.hiscox.fr/blog/teletravail-cybersecurite

20643 04/20