LES RECOMMANDATIONS DE SÉCURITÉ POUR LES TÉLÉTRAVAILLEURS

SICTIAM
OPÉRATEUR PUBLIC DE SERVICES NUMÉRIQUES

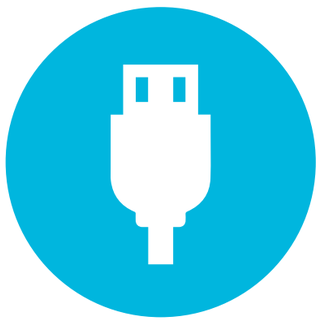
Parce que la sécurité est l'affaire de tous, y compris vous,
voici les 12 points de sensibilisation pour respecter
une hygiène informatique et garantir la sécurité de tous pour tous.

RENFORCEZ VOS MOTS DE PASSE

Utilisez des mots de passe longs, complexes et différents sur tous les équipement et services auxquels vous accédez, qu'ils soient personnels ou professionnels. Pensez à les renouveler assez souvent.

N'OUBLIEZ PAS LES MISES À JOUR !

Les mises à jours des logiciels vous permettent de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès.



EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES

La sauvegarde vous permets de retrouver vos données en cas de cyberattaques, mais également en cas de panne ou de perte de son équipement. Sauvegardez régulièrement votre travail sur un support externe (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

BIEN CONNAÎTRE SES DROITS

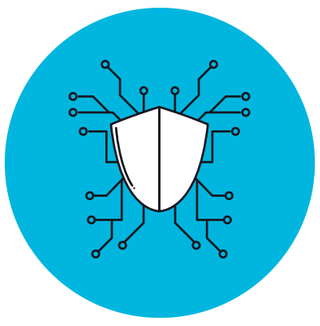
Un compte administrateur vous ouvre tous les droits (configuration de votre ordinateur, réseaux, etc.). Préférez le compte utilisateur pour vos usages courants (navigation, bureautique, etc.) : c'est plus sûr.

SÉCURISER L'ACCÈS WI-FI

Il est important de bien sécuriser la connexion WiFi pour éviter toute intrusion sur votre réseau qui pourrait être utilisée pour attaquer votre collectivité. Utilisez un mot de passe complexe et pensez également à mettre à jour régulièrement votre « box Internet » (rapprochez-vous de votre opérateur pour plus d'informations).

SÉPAREZ LES USAGES

Séparez bien vos usages professionnels et personnels afin d'éviter de générer des fautes de sécurité. L'activité professionnelle doit se faire seulement sur vos moyens professionnels et l'activité personnelle doit se faire seulement sur vos moyens personnels.



UTILISEZ UN ANTIVIRUS

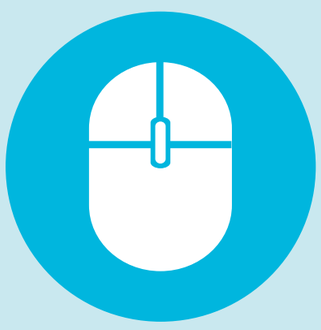
Vérifiez que tous vos équipements connectés (PC, téléphones, tablettes…) sont bien protégés par un antivirus, qu'il est bien à jour, et effectuez une analyse complète (scan) de vos matériels.

MÉFIEZ-VOUS DES MESSAGES INATTENDUS

En cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur. Il peut s'agir d'une attaque par hameçonnage visant à vous dérober des informations confidentielles, de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque.

ATTENTION AUX TÉLÉCHARGEMENTS

Restez prudents lorsque vous téléchargez programmes et logiciels, préférez toujours le téléchargement sur les sites officiels des éditeurs pour limiter les risques d'installation d'une application piégée pour pirater votre équipement. Évitez aussi les sites Internet suspects ou frauduleux qui pourraient également piéger vos équipements.



SOYEZ VIGILANT LORS DES PAIEMENTS EN LIGNE

Soyez vigilants lors de vos achats sur Internet. Gardez en tête quelques bons réflexes : vérifiez que figure la mention « https:// » dans la barre d'adresse du site consulté et dans certains cas, un cadenas.

NE FAITES PAS EN TÉLÉTRAVAIL CE QUE VOUS NE FERIEZ PAS AU BUREAU

Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels. Si vous utilisez vos moyens personnels en télétravail, ayez conscience que vos activités personnelles peuvent faire prendre un risque aussi à votre collectivité, redoublez donc d'attention et de prudence.

PRENEZ SOIN DE VOS INFORMATIONS ET DE VOTRE IDENTITÉ NUMÉRIQUE

Une fois sur Internet, vos données vous échappent et font le bonheur des adeptes de l'« ingénierie sociale » (usurpation d'identité, espionnage…). Faites-vous discret…

WWW.SICTIAM.FR

Source : www.cybermalveillance.gouv.fr