Digital Business Strategy

RÈGLES D'HYGIÈNE DE SÉCURITÉ INFORMATIQUE

#1 MOTS DE PASSE : FAITES PREUVE D'IMAGINATION !

Aimez-les complexes, uniques, secrets et régulièrement renouvelés !

#2 MISES À JOUR : JE NE LE FERAI PAS DEMAIN !

La mise à jour des logiciels et applications corrige les vulnérabilités appréciées des attaquants. N'attendez plus !

#3 PRIVILÈGES : À QUOI BON AVOIR TOUS LES 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.

#4 SAUVEGARDES : L'ATOUT SÉRÉNITÉ.

Pour préserver vos données, effectuez des sauvegardes régulières sur un support externe déconnecté.

#5 N'OUVREZ PAS LA PORTE À N'IMPORTE QUI !

Les services ou équipements qui vous sont offerts peuvent avoir été configurés à des fins malveillantes. Par prévoyance, évitez-les ou demandez l'avis d'un spécialiste.

#6 TABLETTE, TÉLÉPHONE, PC, MAC : MÊME COMBAT !

Vos appareils mobiles aussi sont vulnérables ! Qu'attendez-vous pour les protéger ?

En 2022 :

- **85% des violations de la CyberSécurité sont causées par une erreur humaine (source VERIZON)**
- **94% de tous les logiciels malveillants arrivent par email (source OSC)**

Chaque collaborateur doit lutter activement contre le risque Cyber.

#7 NOMADISME : MOBILITÉ RIME AVEC SÉCURITÉ.

En déplacement, attention et discrétion doivent guider l'usage que vous faites de vos appareils mobiles. N'emportez que l'essentiel !

#8 MESSAGERIE : MÉFIEZ-VOUS DES APPARENCES...

Les courriels, les pièces jointes ou les liens qu'ils contiennent réservent parfois de mauvaises surprises... Les incohérences de fond ou de forme et les requêtes indiscrètes sont à prendre avec des pincettes !

#9 TÉLÉCHARGEMENT : GARE AUX ARNAQUES !

Restez prudents lorsque vous téléchargez programmes et logiciels, préférez les sites officiels.

#10 PAIEMENT EN LIGNE : ÉVITEZ LES FRAIS.

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.

#11 SÉPARATION DES USAGES : UN JEU D'ENFANT ?

Pour limiter l'effet boule de neige d'une action malveillante, séparez vos usages professionnels et personnels (messagerie, équipements...).

#12 IDENTITÉ NUMÉRIQUE : ATTENTION, DOSSIER !

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...

Conseils fournis par l'Agence Nationale de la Sécurité des Systèmes d'Information.

Retrouvez tous les conseils sur le site : https://www.ssi.gouv.fr