LES MESURES ESSENTIELLES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

- PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES 
  - ✔ Utilisez des mots de passe suffisamment longs, complexes
  - ✔ Différents sur tous vos équipements et services qu'ils soient personnels ou professionnels
  - ✔ Au moindre doute, et régulièrement , changez-les
  - ✔ Utilisez un gestionnaire de mots de passe
  - ✔ Activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité.

- SÉCURITÉ NUMÉRIQUE : SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT 
  - ✔ En cas de piratage, ou en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages…)
  - ✔ Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

- APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ, DÈS QU'ELLES VOUS SONT PROPOSÉES 
  - ✔ Sur tous vos appareils
  - ✔ Vous corrigez ainsi les failles de sécurité pour éviter que des pirates s'introduisent dans vos appareils

- UTILISEZ UN ANTIVIRUS 
  - ✔ Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus.
  - ✔ Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour
  - ✔ Faites des analyses approfondies.

- TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS 
  - ✔ Éditeurs (exemple: AppleApp, Store, Google Play Store, ...)
  - ✔ Vérifiez l'adresse sécurisée en https://
  - ✔ De même, évitez les sites internet suspects ou frauduleux (téléchargement, vidéo, streamings illégaux)

- SÉCURITÉ NUMÉRIQUE : MÉFIEZ-VOUS DES MESSAGES INATTENDUS 
  - ✔ Dès réception d'un message inattendu ou alarmiste par message rie (e-mail), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime.

- VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS 
  - ✔ IL existe malheureusement de nombreux sites de vente douteux, voire malveillants
  - ✔ Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel
  - ✔ Vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

- MAÎTRISEZ VOS RÉSEAUX SOCIAUX 
  - ✔ Les réseaux sociaux contiennent souvent des informations personnelles qui ne doivent pas tomber dans de mauvaises mains
  - ✔ Mot de passe solide
  - ✔ Définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas trop publiques
  - ✔ Ne relayez pas d'informations non vérifiées (fake news).

- SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS 
  - ✔ Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent mince
  - ✔ Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise
  - ✔ Inversement, qu'une faille de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles.

- SÉCURITÉ NUMÉRIQUE : ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS 
  - ✔ En mobilité, privilégiez la connexion de votre abonnement téléphonique 3G, 4G ou 5G aux réseaux WiFi publics
  - ✔ Ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

Source : https://www.cybermalveillance.gouv.fr