

#1



Verrouillez systématiquement votre ordinateur lorsque vous ne l'utilisez pas.

- 1) Paramétrez le verrouillage automatique après un temps d'inactivité sur votre PC.
- 2) Verrouillez manuellement votre PC, en tapant la combinaison de touche clavier :



#2



Protégez votre ordinateur contre les programmes malveillants (virus, trojan, vers, etc.)



- 1) Installez un bon antivirus et mettez le régulièrement à jour (automatiquement).
- 2) Effectuez des « scan » réguliers de votre ordinateur.
- 3) Scannez tous les supports usb avant de les ouvrir sur votre ordinateur.

#3



Adoptez une bonne hygiène de mot de passe, afin de protéger vos comptes.

- 1) Utilisez des mots de passe forts, comportant au moins 12 caractères (ex: @2£*c7zw!9nH).**
- 2) Changez régulièrement vos mots de passe et gardez les absolument secrets.**
- 3) Ayez un mot de passe différent pour chacun de vos comptes.**

4



**Chiffrez les données sensibles
contenues sur vos supports USB
afin de garantir la confidentialité
en cas de perte ou de vol.**

- 1) Utilisez des outils de chiffrement de données (ex: TrueCrypt, Rohos mini drive, etc.).
- 2) Chiffrez vos disques durs avec des logiciels de chiffrement (ex: Bitlocker).
- 3) Ne conservez pas de données sensibles sur les supports USB que vous partagez.

#5



Evitez le téléchargement de fichiers (jeu, musique, logiciel, etc.) sur des sites internet inconnus ou de mauvaise réputation, car ils peuvent contenir des logiciels malveillants.

- 1) Téléchargez les fichiers à partir de sites officiels (ex microsoft, avast, etc.).**
- 2) Utilisez des extensions web pour vérifier la fiabilité du site avant de télécharger (ex WDT).**
- 3) Scannez systématiquement les fichiers avec votre antivirus avant de les ouvrir.**

#6



Réduisez les risques et l'impact des «spam», car ces messages non sollicités peuvent être dangereux.

- 1) N'ouvrez jamais un e-mail d'un émetteur inconnu et marquez le comme «spam».
- 2) Supprimez systématiquement les e-mails non sollicités (spam).
- 3) Evitez de publier votre adresse e-mail sur les forums, réseaux sociaux, etc.

#7



Appliquez les mêmes règles de sécurité de votre PC sur votre smartphone, car il contient aussi des données sensibles.

- 1) Installez un bon antivirus et scannez régulièrement votre smartphone.**
- 2) Chiffrez vos données et verrouillez votre smartphone avec un mot de passe fort.**
- 3) N'installez pas d'applications inutiles téléchargées sur des sites inconnus.**

#8



MISE À JOUR...



Installez les dernières mises à jour de votre système d'exploitation (windows, android, linux, etc.) et des logiciels que vous utilisez.

- 1) Activez la mise à jour automatique de votre système d'exploitation.
- 2) Installez les dernières mises à jour des logiciels utilisés.
- 3) Utilisez des outils de gestion automatique des mises à jour de logiciels.

#9



Evitez d'accéder à vos comptes ou effectuer des transactions sensibles en vous connectant à des points d'accès WIFI publics, car ils peuvent cacher des pirates.

- 1) Utilisez toujours une connexion privée pour ce genre de transactions.
- 2) Contentez-vous de visiter uniquement des sites Web si vous devez utiliser ces points d'accès.

#10



Adoptez les bons réflexes de base en cas d'incident informatique et demandez l'assistance d'experts.

- 1) En cas d'incident de sécurité, déconnectez votre machine du réseau internet.
- 2) Prévenez automatiquement votre responsable sécurité ou un spécialiste.
- 3) Adressez-vous au **CI-CERT** pour une assistance et suivez ses recommandations.