Renforcer la sÃ©curitÃ© numÃ©rique des voyageurs pendant les fÃªtes de fin dâ□□annÃ©e

SÃ©curitÃ©

PostÃ© par : JerryG

PubliÃ©e le : 18/12/2023 14:00:00

Avec l'augmentation des voyages pendant la pÃ©riode des fÃªtes, il est important de garder en tÃªte la question de la cybersÃ©curitÃ©.Â

Les dÃ©placements prÃ©sentent en effet divers risques, allant du vol ou de la perte d'appareils Ã la compromission des comptes personnels ou professionnels.Â

Selon une Ã©tude rÃ©cente du site Allaboutcookies, plus de 40 % des voyageurs internationaux ont reconnu avoir frÃ©quemment utilisÃ© des rÃ©seaux Wi-Fi non sÃ©curisÃ©s pendant leurs dÃ©placements, exposant ainsi leurs donnÃ©es sensibles Ã des menaces potentielles.

Pour Fabrice de VÃ©sian, Sales Manager chez Yubico, si lâ□□activation rapide de l'authentification multi-facteur (MFA) est un premier pas pour contrecarrer toute compromission, il est essentiel de sensibiliser les consommateurs Ã des pratiques de sÃ©curitÃ© complÃ©mentaires.

Â« Alors que les voyageurs se prÃ©parent aux vacances de NoÃ«l, il est essentiel de garder Ã lâ□□esprit la sÃ©curitÃ© en ligne. En effet, dans le monde numÃ©rique d'aujourd'hui, la mise en pratique de mesures prÃ©ventives lors de dÃ©placements est primordiale pour dÃ©jouer toute tentative de fraude.

Ã□viter les rÃ©seaux Wi-Fi publics est une recommandation de base Ã suivre pour assurer sa sÃ©curitÃ© en voyage. Bien qu'ils offrent une connectivitÃ© pratique dans des endroits trÃ¨s frÃ©quentÃ©s tels que les aÃ©roports et les gares, ils reprÃ©sentent une porte d'entrÃ©e potentielle pour les cybercriminels.

Ces points dâ□□accÃ¨s, souvent non sÃ©curisÃ©s, peuvent en effet permettre aux hackers d'accÃ©der aux donnÃ©es sensibles des utilisateurs, compromettant ainsi leur vie privÃ©e et leur sÃ©curitÃ© en ligne. Aussi, pour prÃ©venir toute connexion involontaire Ã des rÃ©seaux Wi-Fi publics, dÃ©sactiver la fonction de connexion automatique dans les rÃ©glages des appareils s'avÃ¨re essentiel.

Cette dÃ©marche rÃ©duit l'exposition aux cybermenaces. Alternativement, les voyageurs peuvent activer le partage de connexion sur leur smartphone pour accÃ©der Ã internet si jamais ils ont besoin de faire quelque chose rapidement, les risques Ã©tant limitÃ©s contrairement au rÃ©seau public.

De la mÃªme maniÃ¨re, il est conseillÃ© d'Ã©viter l'utilisation directe des ports USB au sein des Ã©tablissements publics ou dans les hÃ´tels, ainsi que des cÃ¢bles mis Ã disposition dans ces lieux ou encore des bornes de recharge pour les tÃ©lÃ©phones, car ils sont potentiellement des vecteurs de cyberattaques.

Afin de contrÃ´ler les informations exposÃ©es sur l'Ã©cran de verrouillage des appareils mobiles, il est important dâ□□ajuster les paramÃ¨tres pour limiter la visibilitÃ© des donnÃ©es sensibles, pour prÃ©venir l'accÃ¨s non autorisÃ© en cas de regard indiscret.

La fonction Bluetooth constitue, elle aussi, une porte dâ□□entrÃ©e pour les cybercriminels.

Lorsquâ□□elle est activÃ©e, ils peuvent soustraire des informations sensibles en se connectant aux appareils prÃ©cÃ©demment connectÃ©s.

Il convient donc de la mettre hors ligne ou en mode â□□cachÃ©â□□, ce qui peut empÃªcher les appareils inconnus de sâ□□appairer Ã un tÃ©lÃ©phone. En outre, le rÃ©glage des paramÃ¨tres d'Airdrop sur â□□contacts uniquementâ□□, Ã©vite aux appareils inconnus de partager des contenus en public.

Enfin, le fait dâ□□Ã©teindre complÃ¨tement les ordinateurs et tÃ©lÃ©phones portables au moment de passer les contrÃ´les de sÃ©curitÃ© dans les aÃ©roports ou les douanes par exemple, permet d'exploiter pleinement leur fonction de sÃ©curitÃ© matÃ©rielle, telle que le chiffrement intÃ©gral du disque. Cela aide en effet Ã protÃ©ger ses donnÃ©es en cas de perte ou de vol de lâ□□appareil.

En ces pÃ©riodes de fÃªtes, la vigilance en ligne est un impÃ©ratif dans le cadre des dÃ©placements, les cybercriminels Ã©tant Ã lâ□□affÃ»t de la moindre faille. En adoptant des mesures simples, les utilisateurs rÃ©duiront significativement les risques et pourront profiter dâ□□une expÃ©rience de voyage plus sÃ»re. Â»