2023

5 RÈGLES CYBER À RESPECTER EN DÉPLACEMENT

RÉDIGÉ PAR

LES EXPERTS UBCOM

www.ubcom.eu
contact@ubcom.eu

PRÉFACE

Malgré une augmentation significative des risques cyber ces dernières années, et particulièrement depuis la pandémie de Covid-19, on constate que les utilisateurs n'ont encore pas adopté pour autant tous les bons gestes. Nous pourrions penser que les données d'un utilisateur sont plus en sécurité lors de ses déplacements que connecté chez lui. Et pourtant ! Lorsque nous voyageons, à l'époque moderne du smartphone et des Wi-Fi publics, nous emportons l'ensemble de nos données avec nous et les mettons souvent en danger sans le savoir. Si les risques en milieu professionnel et privé sont importants, ils le sont d'autant plus lors des déplacements : un utilisateur connecté en dehors de son environnement représente une cible privilégiée pour les pirates informatiques.

Dans la majeure partie des cas, les victimes de cyberattaques créent leurs propres failles, en adoptant des comportements inadaptés face aux menaces. En s'exposant ainsi, ce ne sont pas seulement les données de la victime qui sont en jeu, mais également celles de son environnement : entreprise, familles, amis.

Dès qu'un pirate informatique réussit à s'introduire dans la machine de la victime, nombreuses sont les opportunités d'endommagement dont celui-ci dispose. Pour pallier à cela, UBCOM vous propose 5 règles cyber à respecter en déplacement, pour qu'à l'avenir, **la cyber-quiétude soit au cœur de tous vos déplacements.**

INTRODUCTION

PENSER "CYBERSÉCURITÉ"

Tel que nous l'entendons, la **cybersécurité** est la mise en œuvre de moyens techniques pour protéger la confidentialité, l'intégrité et la disponibilité d'une information.

Qu'il s'agisse d'un e-mail, d'un SMS, d'une conversation téléphonique ou même d'un post sur un forum, ces informations nécessitent d'être sécurisées tout au long de leur «cycle de vie»; depuis leur création dans un milieu sécurisé, à leur destruction totale quand cela est possible. Entre temps, leur stockage, leur transfert et leur accessibilité sont des questions de cybersécurité.

En déplacement, l'ensemble des données que nous transportons avec nous, via nos objets connectés (ordinateurs, tablettes, smartphones, montres connectées ou autres) sont plus vulnérables que dans un environnement « contrôlé », tel qu'à la maison ou au travail par exemple. Encore faut-il, là aussi, avoir adopté les bons gestes pour protéger ses systèmes d'information, nous vous renvoyons pour cela au livre blanc d'UBCOM sur les 5 conseils pour préparer votre cyberdéfense.

Chaque réseau propre dispose d'un minimum de protections, lesquelles se voient malheureusement amoindries lorsqu'elles dépendent d'un lieu public et d'un environnement non maîtrisé.

Dans les aéroports et les trains, dans une chambre d'hôtel ou même en soirée chez des amis, soyez particulièrement vigilants pour ne pas entacher votre effort de cybersécurité quotidien en un déplacement !

À RETENIR

01 Mon chargeur, mes données

02 Wi-Fi gratuit ou partage de connexion ?

03 Gardez toujours un œil sur vos équipements

04 La confidentialité pour les yeux et les oreilles

05 Faire des sauvegardes régulières

01 Mon chargeur, mes données

Oui, un câble de chargeur peut suffire à voler des données.

Oui, une clé USB peut être infectée par un virus et paralyser votre ordinateur.

Oui, un simple câble de branchement peut propager une cyberattaque.

On ne le dira jamais assez : méfiez-vous des connectiques et accessoires des inconnus !

UBCOM vous recommande fortement de n'utiliser que vos câbles de connexion et vos chargeurs, mais aussi et surtout d'éviter de les prêter à des inconnus. Dans le même sens, évitez tout branchement aux ports USB du train, d'un hall de gare ou d'aéroport, ou encore de votre chambre d'hôtel. Sans tomber dans la paranoïa, pensez simplement à privilégier les prises électriques classiques pour recharger les batteries de vos appareils.

Tout comme dans la série à succès Le Bureau des Légendes, les pirates informatiques peuvent effectivement utiliser le moindre appareil de connectique (chargeur d'ordinateur, câble de branchement, clé USB, etc.) pour y insérer un virus et bloquer ou voler vos données à votre insu.

NOTRE CONSEIL

Inscrivez un signe distinctif et reconnaissable sur votre connectique et vos accessoires de branchement afin de les identifier plus facilement et n'utilisez que vos propres câbles et chargeurs.

02 Wi-Fi gratuit ou partage de connexion ?

Préférez les partages de connexion à l'aide de votre smartphone, aux réseaux Wi-Fi disponibles gratuitement dans les lieux publics. Les réseaux Wi-Fi accessibles gratuitement ne sont, dans la plupart des cas, pas ou très peu protégés.

Cela signifie qu'un pirate informatique n'aura aucune difficulté à s'introduire dans votre ordinateur ou votre smartphone en passant par ce réseau, si vos outils ne sont pas eux-mêmes correctement protégés.

NOTRE CONSEIL

Si en cas de force majeure, vous devez vous connecter à un réseau Wi-Fi public, pensez à activer votre VPN afin de protéger votre identité numérique et vos données. N'oubliez pas non plus de désactiver votre Bluetooth lorsque vous n'en avez pas l'utilité. En effet, cette fonction est une porte d'entrée pour les pirates informatiques les plus rusés.

03 Gardez toujours un œil sur vos équipements

Règle immuable : Gardez toujours sous votre surveillance tous vos appareils électroniques et leurs équipements (ordinateur, smartphone, chargeur, câble de branchement, clé USB, etc.). Tous ces effets personnels peuvent contenir des données sensibles dont vous devez assurer la protection et la sécurité par ces gestes simples.

On constate encore bien trop souvent, dans le train notamment, un ordinateur laissé apparent, voire déverrouillé, à la place d'un voisin de wagon négligent, qui s'absente quelques instants pour passer un appel téléphonique ou se rendre aux toilettes.

Cette imprudence peut coûter très cher et mettre en péril non seulement ses informations personnelles, mais également celles de l'ensemble de ses collaborateurs et de son entreprise.

NOTRE CONSEIL

Dans un train ou dans un avion, gardez toujours votre portable et votre ordinateur avec vous ou rangez-les dans votre sac. En cas d'information particulièrement sensible à transporter, il est de bonne augure de l'isoler des autres afin d'y accorder une protection spécifique. Surtout n'oubliez pas de verrouiller systématiquement vos écrans après utilisation et de programmer un verrouillage automatique au-delà d'une minute d'inactivité.

04 La confidentialité pour les yeux et les oreilles

Lors de vos déplacements, les informations que vous partagez dans vos conversations (SMS, e-mails, notes, etc.) mais aussi lors de vos recherches (sites internet consultés, connexion à votre espace de travail en ligne, etc.) peuvent aussi grandement intéresser des individus malveillants, qui parfois peuvent se trouver juste à côté de vous. Si une information peut se lire, elle peut aussi facilement s'entendre, surtout dans un environnement cloisonné comme dans un wagon (finalement, passer ses appels depuis la plateforme permet non seulement de garantir la tranquillité des autres voyageurs mais aussi votre confidentialité !). Lors de vos déplacements, si votre attention peut être distraite par l'environnement changeant, il convient de toujours être attentif à votre confidentialité.

De manière générale, veillez à protéger vos données, qu'elles soient écrites ou orales, et à vous prémunir face à toute sorte d'espionnage industriel et/ou d'intelligence économique. En une phrase : ne laissez pas l'opportunité à qui que ce soit, de récolter une information vous concernant d'un simple coup d'œil sur votre écran ou grâce à une oreille un peu trop attentive...

NOTRE CONSEIL

Pour plus de protection, il est fortement recommandé de poser un filtre de confidentialité sur vos écrans d'ordinateur et de smartphone. Nos experts insistent sur le besoin de discrétion que requièrent des sujets sensibles, et dont vous pourriez faire mention lors d'un appel téléphonique en déplacement, dans un lieu public, en présence potentielle d'oreilles malintentionnées.

05 Faire des sauvegardes régulières

Afin de limiter les risques de pertes de données, notamment en cas de vol ou de perte de vos appareils en déplacement, nous vous recommandons de faire des sauvegardes régulières de votre ordinateur et de votre téléphone sur un disque dur que vous garderez en lieu sûr.

Il est recommandé de ne pas emporter avec vous le disque dur externe sur lequel vous avez sauvegardé vos données, afin qu'en cas de vol de vos effets personnels vous ne perdiez pas votre ordinateur et ses sauvegardes. Finalement, UBCOM vous recommande de réaliser de telles sauvegardes régulièrement, même en cas d'utilisation d'un cloud, que vous soyez ou non en déplacement.

NOTRE CONSEIL

Pour éviter le vol de vos données, chiffrez le disque de votre ordinateur mais aussi de votre volume de sauvegarde, et protégez vos appareils par des mots de passe robustes. Réalisez des sauvegardes sur disque dur externe et, si possible, ne transportez pas votre ordinateur et votre disque de stockage dans le même sac.

CONCLUSION

De manière générale, un environnement spécifique mène à des comportements spécifiques. En effet, un environnement particulier peut : faciliter ou empêcher certains types d'attaques, révéler certaines vulnérabilités du système ou encore vous faire rencontrer – par hasard ou non – des dangers inhabituels. Sans sombrer dans la paranoïa, il convient de prendre en compte sa situation, de l'analyser objectivement afin de protéger au mieux vos données personnelles.

Les risques d'être la cible d'une cyberattaque sont bien réels et les conséquences peuvent être multiples et souvent désastreuses. Les conséquences possibles liées à une cyberattaque sont variées et peuvent aller d'une e-réputation entachée entraînant la perte de confiance de vos clients et/ou partenaires, à un arrêt total de votre activité, en passant par des risques juridiques et des amendes pénales. De plus, il convient de garder à l'esprit les coûts directs et indirects que peuvent impliquer une cyberattaque. Pour ce faire, vous pouvez consulter notre article dédié à ce sujet : "Les coûts directs et indirects d'une cyberattaque".

Dans cette optique, et en fonction de votre secteur d'activité et de votre environnement, il peut s'avérer nécessaire, voire indispensable, de réfléchir en amont à la protection de vos informations personnelles et professionnelles, souvent entremêlées par les outils connectés.

Ladite protection reposera principalement sur le recours à des outils plus performants et sécurisés, mais aussi sur les bonnes pratiques qu'il convient d'adopter. Nos experts peuvent vous aider à choisir les meilleures solutions pour garantir la bonne sécurité de vos données.

Vous voilà fin connaisseur des bonnes pratiques cyber à respecter lors de vos déplacements. À votre tour de transmettre et partager votre savoir, à vos collaborateurs, amis et familles, et de leur expliquer pourquoi il faut emporter son ordinateur aux toilettes dans le train...

UBCOM

CYBER PROTECTION & SOVEREIGNTY

5 RÈGLES CYBER À RESPECTER EN DÉPLACEMENT

www.ubcom.eu
contact@ubcom.eu