Les services de Remote Support en toute sécurité

Le Remote Support ou assistance à distance est une technologie qui permet de bénéficier d'une aide extérieure sur un dispositif, sans la présence physique d'un technicien sur place. Cette possibilité est utilisée notamment par les éditeurs de logiciels et les instituts bancaires dans le cadre de leurs services d'assistance/helpdesks. Mais pour profiter de ces services en toute sécurité, il convient de respecter un certain nombre de règles.

Principaux conseils à suivre :

- établissez une connexion uniquement avec des personnes dignes de confiance. Soyez particulièrement méfiant, lorsque vous n'êtes pas l'initiateur de la connexion (par ex. lorsque vous recevez un appel téléphonique sans l'avoir sollicité).
- utilisez une connexion chiffrée.
- utilisez un mot de passe ou un ID de réunion.
- n'autorisez pas le contrôle total de votre système. La personne qui vous aide devrait se limiter à observer passivement ce que vous faites.
- sachez que tout ce qui s'affiche à l'écran peut être vu et enregistré par votre interlocuteur.
- saisissez le moins de mots de passe possible pendant votre session.
- ne naviguez pas sur des sites Internet n'ayant aucune pertinence avec l'objet de votre session, même si votre interlocuteur vous le demande.
- assurez-vous, une fois votre prise en charge terminée, que la connexion avec le centre de Remote Support est bien coupée pour empêcher tout accès futur à votre appareil.

De nombreuses entreprises utilisent les logiciels de Remote Support afin que le personnel d'assistance informatique puisse rapidement jeter un œil au dispositif d'un utilisateur en difficulté, sans avoir besoin de se déplacer physiquement.

Malheureusement, les cyberpirates ont eux aussi recours à cette technologie pour obtenir l'accès aux dispositifs des internautes. En se faisant passer pour des collaborateurs du service d'assistance d'une société, ils profitent de la connexion pour voler des mots de passe, installer des logiciels malveillants ou effectuer des virements par e-banking. Alors faites attention et n'accordez pas votre confiance à n'importe qui !

Consultez également notre fiche « Comment vous protéger contre les arnaques par téléphone ».

Copyright © 2020 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_fr.pdf)

Les logiciels d'assistance à distance ou Remote Support permettent d'accéder à un système distant à travers un réseau local (LAN) ou Internet. De cette manière, l'interface de l'appareil distant s'affiche sur le système local et peut même être partiellement commandé à distance.

Copyright © 2020 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Pour aller plus loin

L'invitation
Les connexions ne doivent être établies qu'avec des personnes dignes de confiance. Soyez particulièrement méfiant, lorsque vous n'êtes pas l'initiateur de la connexion (par ex. lorsque vous recevez un appel téléphonique sans l'avoir sollicité). Un piège classique désormais couramment utilisé par les cyberpirates est de se présenter au téléphone comme un collaborateur Microsoft par exemple, ou d'une société informatique ou d'un institut financier, dans le but d'accéder à votre dispositif. La session ne doit être ouverte que sur une invitation explicite. Avant d'accepter une connexion via le logiciel, vous devriez avoir la possibilité de l'autoriser de manière explicite.

Le chiffrement
Choisissez un logiciel offrant un niveau de cryptage suffisant pour que les données ne soient pas transmises en clair La longueur de clé devrait être au moins de 128 Bit.

L'authentification
La personne qui établit une connexion avec votre appareil doit s'identifier au moyen d'un identifiant de réunion (Meeting-ID) et/ou d'un mot de passe. La méthode d'authentification peut être différente selon le logiciel utilisé. Pour s'assurer que ces informations confidentielles ne tombent pas entre de mauvaises mains, le mot de passe ou l'identifiant sont la plupart du temps transmis par téléphone.

Les droits d'accès
N'autorisez pas un contrôle total de votre système. En règle générale, la personne qui vous aide devrait se limiter à observer passivement ce que vous faites et à vous donner des instructions. De cette manière, vous serez sûr de garder toujours le contrôle exclusif de votre système et qu'aucune modification ne pourra être effectuée à votre insu.

L'enregistrement
Attention : sachez que la session de téléassistance peut être enregistrée. Tout ce qui apparaît sur votre écran pendant la durée de la session peut être vu et enregistré par l'autre personne.

La session
Pendant toute la durée de votre session, il convient de ne taper que les mots de passe strictement nécessaires pour la résolution de votre problème (l'idéal serait de n'en saisir aucun) et de ne pas visiter les sites Internet n'ayant rien à voir avec votre session. Si vous utilisez le service d'assistance d'un institut bancaire par exemple, il convient de rester uniquement sur le site Web de la banque concernée.

Fin de session
Assurez-vous, une fois votre prise en charge terminée, que la connexion avec le centre de Remote Support est bien coupée pour empêcher tout accès futur sur votre appareil. Tant que la connexion est établie, une fenêtre de rappel indiquant que vous utilisez un service de téléassistance devait constamment être affichée à l'écran (sans la possibilité d'être réduite). Il convient donc de vous reporter aux instructions fournies dans la documentation du logiciel.

Copyright © 2020 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique