SANS SECURITY AWARENESS

Votre bulletin mensuel sur la sensibilisation à la sécurité

Réseaux Privés Virtuels (VPN)

Aperçu

Vous vous êtes peut-être retrouvé dans la situation où vous aviez besoin d'utiliser le WiFi public à l'extérieur, comme quand vous êtes au restaurant, au café ou lors d'un voyage, à l'hôtel ou à l'aéroport. Mais comment mesurer le niveau de sécurité de ces réseaux publics ? Qui espionne ou enregistre ce que vous faites en ligne ? Peut-être vous ne faites même pas confiance à votre FAI (Fournisseur d'Accès Internet) à la maison et voulez vous assurer qu'il ne surveille pas ce que vous faites en ligne. Protégez vos activités en ligne et votre vie privée avec quelque chose appelé VPN (réseau privé virtuel). Un VPN est une technologie qui crée un tunnel privé et chiffré pour vos activités en ligne, rendant ainsi l'accès bien plus difficile pour ceux qui veulent espionner ou surveiller ce que vous faites en ligne. De plus, un VPN vous aide à dissimuler votre localisation. Il est donc bien plus difficile pour les sites de déterminer où vous êtes.

Comment ça fonctionne ?

Un VPN fonctionne en créant un tunnel privé et chiffré allant vers un fournisseur de VPN que vous sélectionnez. Toute votre activité en ligne passe dans ce tunnel, puis part du réseau de votre fournisseur de VPN vers la destination choisie. Par exemple, vous êtes basé à Nantes et vous vous connectez à un serveur VPN à Munich en Allemagne. Tous les sites que vous visitez vont croire que vous êtes basé à Munich. Un VPN est simple à utiliser. La première étape, c'est trouver un fournisseur de VPN de confiance, puis créer un compte avec eux (vous devrez sûrement acheter leurs services). Une fois le compte créé, vous téléchargez, installez et configurez leur logiciel VPN. Une fois installé et configuré, vous vous connectez à internet comme d'habitude. Le logiciel VPN va discrètement creuser le tunnel chiffré et commencer à protéger votre vie privé sans que vous vous en rendiez compte.

Sélectionner un fournisseur de VPN

Le niveau de sécurité de vos activités en ligne s'arrête à celui de votre fournisseur de VPN. Soyez sûr d'en sélectionner un de confiance. Voici quelques points clés quand vous sélectionnez votre fournisseur de VPN.

Enregistrement : cherchez un service qui n'enregistre pas vos données et se concentre sur votre vie privée. Si votre fournisseur de VPN ne conserve pas les données, il est alors plus difficile pour quiconque de retourner voir ce que vous avez fait en ligne.

Où est basée l'entreprise : des fournisseurs de VPN différents sont basés dans différents pays. Soyez sûr de sélectionner un fournisseur de VPN basé dans un pays où la loi sur la vie privée est importante. Dans un pays où la loi sur la vie privée est faible, un fournisseur de VPN peut être contraint à devoir partager des informations qu'ils récupèrent sur vous.

Serveurs : cherchez un service VPN avec des serveurs basés dans les pays ou les villes voulus. Certains fournisseurs de VPN ont des milliers de serveurs basés tout autour du globe. Devez-vous prétendre que votre connection vient d'un pays spécifique ? Votre fournisseur de VPN peut-il vous apporter cela ?

Compatibilité : cherchez des services qui fonctionnent sur différents ordinateurs ou appareils mobiles. Par exemple, vous pouvez utiliser un PC sous Windows, une tablette et un iPhone. Vous voulez un service qui fonctionne sur tous ces appareils.

Évitez les « gratuits » : soyez méfiant des services VPN « gratuits ». Comment font-ils de l'argent pour rester actifs ? Les services gratuits peuvent collecter et vendre vos informations.

Un VPN est une moyen fantastique pour protéger votre vie privée en ligne. Par contre, un VPN ne sert en rien à sécuriser votre PC, appareils ou comptes en ligne. Donc, même si vous utilisez un VPN, assurez-vous de toujours suivre les étapes de sécurité de base : s'assurer que vos appareils soient à jour, utiliser un verrouillage d'écran et toujours utiliser un mot de passe fort et unique pour tous vos comptes.

Rédacteur Invité

Phil Johnsey *(@peakreflections) est un professionnel de l'informatique à Palm Beach County, expérimenté dans la sécurité, le légl et l'audit. Certifié SANS en informatique légale, en sécurité sur internet et membre de la commission d'évaluation de OUCH. Sa passion, c'est rendre la sécurité simple pour les autres.*

Ressources

Attaques personnalisées :	https://www.sans.org/u/Sd8
Sécuriser vos appareils mobiles :	https://www.sans.org/u/Sdd
Arrêter les maliciels :	https://www.sans.org/u/Sdi