عمل شبكات VPN

م/ عادل إبراهيم

ما هي عمل شبكاتVPN ؟

تخفي شبكات VPN عنوان IP الخاص بك من خلال السماح للشبكة بإعادة توجيهه عبر خادم مهيأ خصيصا ويعمل عن بعد تحت إدارة مستضيف شبكةVPN وهذا يعني أنه إذا قمت بالتصفح عبر الإنترنت باستخدام شبكةVPN فإن خادم VPN يصبح مصدر بياناتك. هذا يعني أن مزود خدمة الإنترنت (ISP) والأطراف الثالثة الأخرى لا يمكنهم معرفة مواقع الويب التي تزورها أو البيانات التي ترسلها وتستقبلها عبر الإنترنت. تعمل شبكة VPNمثل عامل تصفية يحول جميع بياناتك إلى "بيانات مبهمة". حتى لو نجح أي طرف في الوصول إلى هذه البيانات فستكون بلا فائدة.

ما هي فوائد اتصالVPN ؟

يخفي اتصال VPN حركة البيانات عبر الإنترنت ويحميها من الوصول الخارجي. فالبيانات غير المشفرة يمكن عرضها من قبل أي شخص يمكنه الولوج إلى الشبكة ويريد رؤيتها لكن عند استخدام VPNيصبح من الصعب على المخترقين ومجرمي الإنترنت فك تشفير هذه البيانات.

التشفير الآمن :تحتاج إلى مفتاح تشفير لقراءة البيانات. وبدون امتلاك مفتاح سيستغرق الكمبيوتر ملايين السنين لفك الشفرة في حالة الهجوم المكثف .بمساعدةVPN يتم إخفاء أنشطتك عبر الإنترنت حتى على الشبكات العامة.

إخفاء أماكن تواجدك :تعمل خوادم VPN بشكل أساسي كخوادم وكيلة لك على الإنترنت. ونظراً لأن بيانات الموقع الديموجرافي تأتي من خادم في دولة أخرى لا يكون بالإمكان تحديد موقعك الفعلي. إضافة إلى ذلك فإن معظم خدمات VPN لا تخزن سجلات نشاطك من ناحية أخرى يقوم بعض مقدمي الخدمة بتسجيل سلوكك لكنهم لا يمررون هذه المعلومات إلى أطراف ثالثة. وهذا يعني أن أي سجل محتمل لسلوكك كمستخدم يظل مخفياً بشكل دائم.

الوصول إلى المحتوى المحلي :لا يكون من الممكن دائماً الوصول إلى محتوى الويب المحلي من كل مكان حيث تحتوي الخدمات والمواقع في كثير من الأحيان على محتوى لا يمكن الوصول إليه إلا من أجزاء معينة من العالم. وهنا تستخدم الاتصالات القياسية الخوادم المحلية في البلد لتحديد موقعك وهذا يعني أنه لا يمكنك الوصول إلى المحتوى في بلدك أثناء السفر ولا يمكنك الوصول إلى المحتوى الدولي من بلدك. هنا تتدخل خدمة تغيير الموقع عبر VPNلتسمح لك بتبديل الخادم إلى بلدان أخرى و"تغيير" موقعك بشكل فعال.

النقل الآمن للبيانات :إذا كنت تعمل عن بُعد فقد تحتاج إلى الوصول إلى الملفات المهمة على شبكة شركتك. ولأسباب أمنية يتطلب هذا النوع من المعلومات اتصالاً آمناً. غالباً ما يلزم وجود اتصال VPN للوصول إلى الشبكة حيث تتصل خدمات VPN

بالخوادم الخاصة وتستخدم أساليب التشفير للحد من خطر تسرب البيانات.

لماذا ينبغي عليك استخدام اتصالVPN ؟

عادة ما يقوم مزود خدمة الإنترنت بإعداد اتصالك عند الاتصال بالإنترنت ومن ثم يكون بإمكانه تعقبك باستخدام عنوان IP. يتم توجيه حركة بياناتك على الشبكة من خلال خوادم مزود خدمة الإنترنت والذي يمكنه تسجيل وعرض كل ما تفعله عبر الإنترنت.

قد يبدو مزود خدمة الإنترنت الخاص بك جديراً بالثقة لكنه قد يشارك سجل التصفح الخاص بك مع المعلنين والشرطة أو الحكومة و/أوجهات خاجية أخرى. كما يمكن أن يقع مزود خدة الإنترنت الخاص بك ضحية لهجمات مجرمي الإنترنت: وإذ تم اختراقه فإن بياناتك الشخصية والخاصة يمكن أن تتعرض للخطر.

ويكون هذا مهماً بشكلٍ خاص إذا كنت تستخدم شبكات Wi-Fi عامة كثيراً فأنت لا تعرف أبداً من الذي قد يراقب حركة المرور على الإنترنت وما الذي قد يسرقه منك بما في ذلك كلمات المرور أو البيانات الشخصية أو معلومات الدفع أو حتى هويتك بالكامل.

ما الدور الذي ينبغي أن تقوم به شبكات VPN الجيدة؟

يمكنك أن تعتمد على قيام شبكة VPN الخاصة بك بمهمة واحدة أو أكثر. وينبغي أن تكون شبكة VPN نفسها محمية من الاختراق. إليك المميزات التي يمكنك توقعها من أي حل VPN شامل:

تشفير عنوان IP الخاص بك :تتمثل المهمة الأساسية لشبكة VPNفي إخفاء عنوان IP الخاص بك عن مزود خدمة الإنترنت الخاص بك والأطراف الثالثة الأخرى. ويسمح هذا لك بإرسال واستقبال المعلومات على الإنترنت دون التعرض لخطر رؤيتها بواسطة أي طرف بخلافك ومزود خدمة.VPN

تشفير البروتوكولات :ينبغي لشبكات VPN كذلك أن تمنع بقاء أي أثر لاستخدامك مثل تاريخ التصفح أو تاريخ البحث أو ملفات تعريف الارتباط. ويعد تشفير ملفات تعريف الارتباط مهمًا بشكل خاص لأنه يمنع الجهات الخارجية من الوصول إلى المعلومات السرية مثل البيانات الشخصية والمعلومات المالية والمحتويات الأخرى على مواقع الويب.

إيقاف الاتصال :إذا انقطع اتصال VPN الخاص بك فجأة فسيتم أيضاً قطع اتصالك الآمن. يمكن لشبكات VPN الجيدة اكتشاف هذا التوقف المفاجئ وإنهاء البرامج المحددة مسبقاً مما يقلل من احتمال تعرض البيانات للخطر.

المصادقة ثنائية العوامل :من خلال استخدام مجموعة متنوعة من أساليب المصادقة تقوم شبكات VPN القوية بفحص كل من يحاول تسجيل الدخول. على سبيل المثال قد يُطلب منك إدخال كلمة مرور ومن ثم يتم إرسال رمز إلى جهازك المحمول. وهذا يزيد ما صعوبة وصول أي أطراف ثالثة غير مدعوة إلى اتصالك الآمن.

تاريخ شبكاتVPN

منذ أن بدأ الناس في استخدام الإنترنت كانت هناك حركة لحماية بيانات تصفح الإنترنت وتشفيرها. وقد شاركت وزارة الدفاع الأمريكية بالفعل في مشاريع تعمل على تشفير بيانات اتصالات الإنترنت في الستينيات.

النواة الأولى لشبكاتVPN

ساهمت تلك الجهود في إنشاء شبكة وكالة مشاريع الأبحاث المتقدمة(ARPANET) وهي شبكة تبديل حزم أدت بعد ذلك إلى تطوير بروتوكول التحكم بالنقل/بروتوكول الإنترنت(TCP/IP)

والذي كان له أربع طبقات :الرابط والإنترنت والنقل والتطبيق . عند طبقة الإنترنت يمكن توصيل الشبكات والأجهزة المحلية بالشبكة العالمية - وهنا بدا واضحا خطر التعرض. في عام ١٩٩٣ نجح فريق من جامعة كولومبيا ومختبرات AT&T Bell أخيراً في إنشاء ما يعتبر أول شكل من أشكال شبكات VPN العصرية وأطلقوا عليها اسم swipe أي بروتوكول تشفير بروتوكول الإنترنت.

وفي العام التالي عمل Wei Xu على تطوير شبكة IPSec وهو بروتوكول لأمن الإنترنت يعمل على مصادقة حزم المعلومات التي يتم مشاركتها عبر الإنترنت وتشفيرها. ثم في عام ١٩٩٦ قام موظف في Microsoft يُدعى Gurdeep Singh-Pall بإنشاء بروتوكول الاتصال النفقي من نظير إلى نظير.(PPTP)

أوائل شبكاتVPN

بالتزامن مع قيام Singh-Pall بتطوير بروتوكولPPTP كانت شعبية الإنترنت تزداد مع ظهور الحاجة إلى أنظمة أمان متطورة وجاهزة لاستخدام المستهلكين. في ذلك الوقت، كانت برامج مكافحة الفيروسات فعالة حقًا في منع البرامج الضارة وبرامج التجسس من إصابة أنظمة الكمبيوتر. ولكن الأشخاص والشركات بدأوا في طلب برنامج تشفير يمكنه إخفاء سجل التصفح الخاص بهم على الإنترنت أيضًا.

وبهذا بدأت أولى شبكات VPN في أوائل العقد الأول من القرن الحادي والعشرين، لكنها استخدامها كان قاصرًا بشكل حصري تقريبًا على الشركات. لكن بعد فيضٍ من الانتهاكات الأمنية خاصة في أوائل عام ٢٠١٠ بدأت السوق الاستهلاكية لشبكات VPN في السير على طريق النمو.

شبكات VPN واستخداماتها الحالية

وفقاً لشركة أبحاث السوق GlobalWebIndex فإن عدد مستخدمي شبكات VPN حول العالم قد تضاعف أربع مرات بين عامي ٢٠١٦ و٢٠١٨ يوجد في بلاد مثل تايلاند وإندونيسيا والصين قيود كثيرة على استخدام الإنترنت ويتم مراقبته دائماً لذلك فإن شخص من بين كل ٥ أشخاص من مستخدمي الإنترنت هناك يستعينون بشبكات .VPN ولكن تقل نسبة مستخدمي VPN إلى حوالي ٥ % في الولايات المتحدة الأمريكية وبريطانيا العظمى وألمانيا إلا أنها في تزايد.

يتمثل أحد أكثر الدوافع لاعتماد VPN في السنوات الأخيرة في زيادة عدد المستخدمين الراغبين في الوصول إلى المحتويات التي يوجد عليها قيود جغرافية أي أنها متاحة في بلاد معينة فقط. على سبيل المثال تجعل خدمات بث الفيديو مثل Netflix أو YouTube مقاطع فيديو معينة متاحة في بلدان معينة فقط. باستخدام شبكات VPN الحديثة يمكنك تشفير عنوان IP الخاص بك بحيث تبدو وكأنك تتصفح من بلد آخر مما يتيح لك الوصول إلى هذا المحتوى من أي مكان.

إليك كيفية التصفح بأمان باستخدامVPN

تقوم شبكة VPN بتشفير سلوك تصفحك والذي لا يمكن فك تشفيره إلا بمساعدة مفتاح. ولا يعرف هذا المفتاح إلا جهاز الكمبيوتر الخاص بك وشبكة VPN فقط لذلك لا يستطيع مزود خدمة الإنترنت التعرف على المكان الذي تتصفح منه. تستخدم شبكات VPN المختلفة عمليات تشفير مختلفة ولكنها تعمل بشكل عام في ثلاث خطوات:

بمجرد اتصالك بالإنترنت ابدأ تشغيل شبكة VPN الخاصة بك. حيث تعمل شبكة VPN كنفق آمن بينك وبين الإنترنت ولا يمكن لمزود خدمة الإنترنت الخاص بك والجهات الخارجية الأخرى اكتشاف هذا النفق.

يصبح جهازك الآن على الشبكة المحلية الخاصة باتصالVPN ويمكن تغيير عنوان IP الخاص بك إلى عنوان IP الذي يوفره خادم VPN.

يمكنك الآن تصفح الإنترنت كما تشاء لأن VPN تحمي جميع بياناتك الشخصية.

ما أنواع شبكات VPN المتاحة؟

يوجد الكثير من أنواعVPN لكن ما يهم معرفته منها هي ثلاثة أنواع رئيسية:

SSL VPN

لا يستطيع جميع موظفي الشركة في كثيرٍ من الأحيان الوصول إلى كمبيوتر محمول للشركة يمكنهم استخدامه للعمل من المنزل. خلال أزمة كورونا في ربيع ٢٠٢٠ واجهت العديد من الشركات مشكلة عدم وجود معدات كافية لموظفيها. في مثل هذه الحالات غالباً ما يتم اللجوء إلى استخدام جهاز خاص (كمبيوتر شخصي كمبيوتر محمول جهاز لوحي هاتف محمول). في هذه الحالة تلجأ الشركات إلى حل SSL-VPN والذي يتم تنفيذه عادة عبر صندوق أجهزة مطابق.

وعادة ما يكون المتطلب الأساسي هو متصفح يدعم HTML-5 والذي يُستخدم لاستدعاء صفحة تسجيل الدخول الخاصة بالشركة. تتوفر المتصفحات التي تدعم HTML-5 لأي نظام تشغيل تقريباً ويكون الوصول محمياً باسم مستخدم وكلمة مرور.

VPNمن موقع لموقع

شبكة VPNمن موقع لموقع هي في الأساس عبارة عن شبكة خاصة تهدف إلى إخفاء اتصالات الشبكات الداخلية مع السماح لمستخدمي هذه الشبكات الآمنة بالوصول إلى موارد بعضهم بعضاً

تعد شبكة VPN من موقع لموقع مفيدة إذا كان لديك مواقع متعددة في شركتك لكل منها شبكة محلية (LAN) خاصة به متصلة بشبكة المنطقة الواسعة .(WAN) تعد شبكات VPN من موقع لموقع مفيدة أيضاً إذا كان لديك شبكتان منفصلتان تريد إرسال الملفات بينهما دون وصول المستخدمين بإحدى الشبكات الداخلية إلى الشبكة الداخلية الأخرى بشكل صريح.

تستخدم شبكات VPN من موقع إلى موقع بشكل أساسي في الشركات الكبيرة. إذ إنها تكون معقدة التنفيذ ولا تقدم نفس المرونة التي توفرها شبكات .VPN SSL إلا أنها تعتبر الطريقة الأكثر فعالية لضمان التواصل ضمن الأقسام الكبيرة وبينها.

VPNالعميل إلى خادم

يمكن تخيل الاتصال عبر عميل VPN كما لو كنت تقوم بتوصيل جهاز الكمبيوتر المنزلي الخاص بك بشبكة الشركة باستخدام وصلة تمديد حيث يمكن للموظفين الاتصال بشبكة الشركة من مكاتبهم المنزلية عبر الاتصال الآمن والتصرف كما لو كانوا جالسين في المكتب. ولكن يجب أولاً تثبيت عميل VPN وتكوينه على الكمبيوتر

وهي عملية تتطلب عدم اتصال المستخدم بالإنترنت عبر مزود خدمة الإنترنت الخاصة به وإنشاء اتصال مباشر عبر مزود خدمة VPNالخاص به. هنا لا يوجد مرحلة النفق المعتادة في اتصالات VPN فبدلاً من استخدام VPN في إنشاء نفق تشفير يخفي اتصال الإنترنت الموجود بالفعل يمكن لخدمة VPN أن تعمل تلقائياً على تشفير البيانات قبل إتاحتها إلى المستخدم.

يزداد استخدام هذا النوع حالياً نظراً لأنه مفيد بشكل خاص لمزودي خدمات شبكات WLAN العامة غير الآمنة فهو يمنع الأطراف الخارجية من الوصول إلى اتصال الشبكة واختراقه عبر تشفير جميع البيانات حتى وصولها إلى مزود الخدمة. كما أنه يمنع مزودي خدمات الإنترنت من الوصول إلى البيانات التي تظل غير مشفرة لأي سبب من الأسباب ويتجاوز أي قيود على وصول المستخدم إلى الإنترنت على سبيل المثال إذا كانت حكومة ذلك البلد تقيد الوصول إلى الإنترنت

تتمثل ميزة هذا النوع من وصول VPN في زيادة الكفاءة والوصول العالمي إلى موارد الشركة وذلك شريطة توفر نظام هاتف مناسب حيث يمكن للموظف على سبيل المثال الاتصال بالنظام باستخدام سماعة رأس والتصرف كما لو كان في مكان عمل الشركة. حتى عملاء الشركة لن يتمكنوا من معرفة إذا ما كان الموظف يعمل من الشركة أم من مكتبه المنزلي.

كيف يمكنني تثبيت VPN على جهاز الكمبيوتر لدي؟

قبل تثبيت VPN من المهم معرفة الطرق المختلفة للقيام بهذا:

عميلVPN

يجب تثبيت البرنامج لتطبيقات عميل VPN المستقلة. ويتم تكوين هذا البرنامج بحيث يتوافق مع متطلبات نقطة النهاية. عند إعداد شبكةVPN فإن نقطة النهاية سوف تشغل رابط VPN وتوصله بنقطة النهاية الأخرى مما ينشئ نفق التشفير. وعادة ما تتطلب هذه الخطوة في الشركات إدخال كلمة مرور صادرة عن الشركة أو تثبيت شهادة مناسبة حيث يمكن لجدار الحماية التعرف على أن هذا اتصال مصرح به من خلال استخدام كلمة مرور أو شهادة. ثم يقوم الموظف بعد ذلك بتعريف نفسه عن طريق تقديم بيانات الاعتماد المعطاة له.

ملحقات المتصفحات

يمكن تثبيت ملحق VPN لمعظم متصفحات الويب مثل Google Chrome Firefox حتى أن بعض المتصفحات مثل Opera تأتي بملحق VPN مدمج. تسهل الملحقات على المستخدمين عملية تشغيل وتكوين اتصال VPN بسرعة أثناء تصفح الإنترنت. لكن اتصال VPN يكون صالحاً فقط للمعلومات التي تتم مشاركتها في هذا المتصفح حيث لا يمكن تشفير الاستخدام على المتصفحات الأخرى واستخدامات الإنترنت الأخرى خارج المتصفح (مثل الألعاب عبر الإنترنت) بواسطة اتصال VPN هذا.

على الرغم من أن ملحقات المتصفحات ليست شاملة تماماً مثل عملاء VPN إلا أنها قد تكون خياراً مناسباً لمستخدمي الإنترنت من حين لآخر الذين يريدون طبقة إضافية من الأمان على الإنترنت. لكن الأبحاث أظهرت أنها تكون أكثر عرضة للاختراقات. يُنصح المستخدمون أيضاً باختيار ملحق مشهور إذ قد يحاول حاصدو البيانات استخدام ملحقات VPN وهمية. حصد البيانات هي عملية جمع البيانات الشخصية مثل ما يفعله خبراء التسويق لإنشاء ملف تعريف شخصي لك حتى يتم تخصيص المحتوى الإعلاني لك شخصياً

VPN للراوتر

إذا كانت هناك عدة أجهزة متصلة بنفس شبكة الإنترنت فقد يكون من الأسهل تطبيق VPN مباشرة على جهاز الراوتر بدلاً من تثبيت VPNمنفصل على كل جهاز. تعد شبكة VPN للراوتر مفيدة بشكل خاص إذا كنت ترغب في حماية الأجهزة التي تحتوي على اتصال إنترنت لا يسهل تكوينه مثل أجهزة التلفزيون الذكية. كما يمكنها أن تساعد في الوصول إلى المحتوى المقيد على مناطق محددة عبر جميع أنظمة الترفيه في منزلك.

من السهل تثبيت VPN للراوتر وهي توفر دائماً الأمان والخصوصية وتمنع اختراق شبكتك عند تسجيل دخول أجهزة غير آمنة. ولكن قد يكون من الصعب إدارتها إذا لم يكن لجهاز

الراوتر الخاص بك واجهة مستخدم خاصة به وهذا بدوره قد يؤدي إلى حظر الاتصالات الواردة.

VPN للشركة

شبكة VPN للشركات هي حل مخصص يتطلب إعداداً مخصصاً ودعماً فنياً إذ عادة ما يتم إنشاء VPN من أجلك بواسطة فريق تكنولوجيا المعلومات بالشركة. كمستخدم لا يكون لك أي تأثير إشرافي من VPN نفسها مع تسجيل أنشطتك وعمليات نقل البيانات الخاصة بك بواسطة شركتك. وهذا يسمح للشركة بتقليل المخاطر المحتملة لتسرب البيانات. تتمثل الميزة الرئيسية لشبكة VPNللشركات في وجود اتصال آمن تماماً بالشبكة الداخلية والخادم الخاصين بالشركة حتى بالنسبة للموظفين الذين يعملون خارج الشركة باستخدام اتصال الإنترنت الخاص بهم.

هل يمكنني أيضاً استخدام VPN على هاتفي الذكي أو أجهزتي الأخرى؟

بالتأكيد فهناك عدد من خيارات VPN المتوفرة للهواتف الذكية والأجهزة الأخرى التي تتصل بالإنترنت. يمكن أن تكون شبكة VPN ضرورية لجهازك المحمول إذا كنت تستخدمه لتخزين معلومات الدفع أو البيانات الشخصية الأخرى أو حتى لتصفح الإنترنت فقط. ويقدم العديد من مزودي خدمات VPN أيضاً حلولاً للهاتف المحمول - يمكن تنزيل العديد منها مباشرة من متجر Google

Play أو متجر تطبيقات Apple مثل Kaspersky VPN Secure Connection.

هل خدمات VPN آمنة فعلاً؟

من المهم ملاحظة أن شبكات VPN لا تعمل مثل برامج مكافحة الفيروسات الشاملة فبينما تحمي عنوان IP الخاص بك وتقوم بتشفير سجل الإنترنت الخاص بك إلا أن اتصال VPN لا يحمي جهاز الكمبيوتر الخاص بك من التدخل الخارجي. بل للقيام بذلك ينبغي عليك بالتأكيد استخدام برامج مكافحة الفيروسات مثل Kaspersky Internet Security لأن استخدام اتصال VPN وحده لا يحميك من أحصنة طروادة أو الفيروسات أو الروبوتات أو البرامج الضارة الأخرى.

فبمجرد أن تجد البرامج الضارة طريقها إلى جهازك يمكنها سرقة بياناتك أو إتلافها سواء كنت تقوم بتشغيل VPN أم لا. لذلك من المهم أن تستخدم VPN مع برنامج شامل لمكافحة الفيروسات لضمان أقصى درجات الأمان.

اختيار مزود خدمة VPN آمن

من المهم أيضاً أن تختار مزود خدمة VPN يمكنك الوثوق به. ففي حين أن مزود خدمة الإنترنت الخاص بك لا يمكنه رؤية حركة البيانات فإن مزود خدمة VPN يمكنه ذلك. وإذا تم اختراق مزود خدمة VPN الخاص بك فسيتم اختراقك أيضاً لهذا السبب يكون

من المهم أن تختار مزود VPN موثوقاً به لضمان إخفاء أنشطة الإنترنت الخاصة بك وضمان أعلى مستوى من الأمان.

كيفية إعداد اتصال VPN على هاتفك الذكي

كما ذكرنا سابقاً يوجد أيضاً اتصالات VPN للهواتف الذكية التي تعمل بنظام Android وهواتف iPhone. ولحسن الحظ تتميز خدمات VPN للهواتف الذكية بسهولة الاستخدام وستتضمن عموماً ما يلي:

عادة ما تقوم عملية التثبيت بتنزيل تطبيق واحد فقط من متجر تطبيقات iOS أو متجر Google Play. على الرغم من وجود مزودي خدمة VPN بالمجان فمن الحكمة اختيار مزود محترف عندما يتعلق الأمر بالأمان.

إن عملية الإعداد سهلة للغاية حيث تكون الإعدادات الافتراضية مصممة بالفعل في الغالب لمستخدمي الهواتف الذكية العاديين. فقط قم بتسجيل الدخول باستخدام حسابك، وستوجهك معظم التطبيقات بعد ذلك عبر الوظائف الرئيسية لخدمات VPN.

يشبه تشغيل اتصال VPN حرفياً مفتاح إضاءة في العديد من تطبيقات VPN للهواتف الذكية وسوف تجد الخيار مباشرة على الشاشة الرئيسية في أغلب الأحيان.

عادة ما يتم تبديل الخادم يدوياً إذا كنت تريد التلاعب بموقعك حيث يمكنك ببساطة تحديد البلد المطلوب من القائمة المتوفرة.

تتوفر إعدادات متقدمة للمستخدمين الذين يتطلبون درجة أعلى من حماية البيانات. قد تتمكن أيضاً من تحديد بروتوكولات أخرى لأسلوب التشفير الخاص بك اعتماداً على تطبيق VPN الذي تستخدمه. يمكن كذلك العثور على التشخيصات وبعض الوظائف الأخرى في تطبيقك تعرف على هذه الميزات لاكتشاف شبكة VPN المناسبة لاحتياجاتك قبل أن تقوم بالاشتراك.

من أجل تصفح الإنترنت بأمان من الآن فصاعداً كل ما عليك فعله هو تنشيط اتصال VPN من خلال التطبيق أولاً

لكن ضع في اعتبارك ما يلي :تكون شبكة VPN آمنة بقدر ما تنص عليه سياسات استخدام وتخزين البيانات الخاصة بمزودها. تذكر أن خدمة VPN تقوم بتحويل بياناتك إلى خوادمها ومن ثم تتصل هذه الخوادم عبر الإنترنت نيابة عنك. فإن قامت الخدمة بتخزين سجلات البيانات فتأكد من توضيح الغرض من تخزين هذه السجلات.

عادة ما يضع مزودو خدمات VPN المحترفون خصوصيتك في المقام الأول لذلك ينبغي عليك اختيار مزود خدمة موثوق به مثل Kaspersky Secure Connection.

تذكر أن بيانات الإنترنت فقط هي التي تُشفر حيث لن يتم نقل أي شيء لا يستخدم اتصالاً خلوياً أو اتصال Wi-Fi عبر الإنترنت. ونتيجة لذلك لن تقوم شبكة VPN الخاصة بك بتشفير مكالماتك الصوتية أو رسائلك النصية القياسية.

الخاتمة

ينشئ اتصال VPN اتصالاً آمناً بينك وبين الإنترنت. يتم توجيه كل حركة بياناتك عبر نفق افتراضي مشفر عبر شبكةVPN ويعمل هذا على إخفاء عنوان IP الخاص بك عندما تستخدم الإنترنت مما يجعل موقعه مخفياً عن الجميع. كذلك يكون اتصال VPN آمناً ضد الهجمات الخارجية وذلك لأنه لا يمكن الوصول إلى البيانات في النفق المشفر إلا من خلالك أنت فقط - ولا يمكن لأي جهة أخرى الوصول لأنها لا تمتلك المفتاح. يتيح لك اتصال VPN الوصول إلى المحتوى المقيد إقليمياً من أي مكان في العالم. لا تكون كل منصات البث متاحة في كل البلاد ومع ذلك يمكنك الوصول إليها باستخدام VPN