

OUCH!

نشرت الشهرية للتوعية بأمن المعلومات

الشبكات الخاصة الافتراضية (VPN)

نظرة عامة

قد تجد نفسك بحاجة لاستخدام شبكة Wi-Fi العامة للوصول إلى الإنترنت عندما تكون بعيدًا عن المنزل، مثلًا عندما تكون في أحد المطاعم المحلية أو المقاهي أو عند سفرك في فندق أو مطار ما. ولكن هل فكرت بمدى أمان هذه الشبكات العامة ومن الذي يشاهد أو يسجل ما تفعله عبر الإنترنت؟ ربما لا تتق في مزود خدمة الإنترنت (ISP) الخاص بك في المنزل وتريد أن تتأكد من أنهم لا يستطيعون مراقبة ما تفعله عبر الإنترنت. لذلك قم بحماية أنشطتك عبر الإنترنت وخصوصيتك باستخدام ما يسمى بالشبكة الافتراضية الخاصة VPN فهي تقنية تنشئ نفقًا خاصًا ومشفرًا لنشاطك عبر الإنترنت، مما يجعل من الصعب على أي شخص التجسس عليك ومشاهدة ما تقوم به عبر الإنترنت أو مراقبته. بالإضافة إلى ذلك، تساعد VPN على إخفاء موقعك مما يجعل الأمر أكثر صعوبة بالنسبة لمواقع الويب التي تزورها لتحديد مكان وجودك.

كيف تعمل ال VPN؟

تعمل VPN من خلال إنشاء نفق خاص مشفر لمزود خادم VPN الذي تختاره. بحيث يتم توجيه كل نشاطك عبر الإنترنت إليها مروراً عبر هذا النفق، من ثم تغادر شبكة مزود VPN الخاص بك إلى وجهتك المقصودة. على سبيل المثال، إذا كنت مقيمًا في تامبا بولاية فلوريدا وقمت بالاتصال بخادم VPN في ميونيخ، ألمانيا، فإن أي موقع ويب تتصل به سيعتقد أنك تتصل من ميونيخ، ألمانيا. ال VPN هي خدمة سهلة الاستخدام. لكن يتطلب منك كخطوة أولى العثور على مزود VPN تثق به، ثم إنشاء حساب معهم (يتطلب ذلك عادةً شراء خدمتهم). وبمجرد أن يكون لديك حساب، يمكنك تنزيل وتثبيت وإعداد برامج VPN الخاصة بهم. بعدها، ستتمكن الاتصال بالإنترنت كما تفعل دائمًا. سيقوم برنامج VPN بصمت بإنشاء النفق المشفر الخاص بك والبدء في حماية خصوصيتك آلياً وبدون أن تشعر بذلك

اختيار مزود VPN

أمان أنشطتك عبر الإنترنت وخصوصيتها من أمان شبكة VPN التي تختار. لذلك تأكد من اختيار مزود يمكنك الوثوق به. فيما يلي النقاط الرئيسية عند اختيار مزود خدمة VPN

التسجيل: ابحث عن خدمة لا تحتفظ بأي سجلات وترتكز على الخصوصية. إذا لم يقدم مزود خدمة VPN الخاص بك بجمع أي سجلات، فسيكون من الصعب جدًا على أي شخص الرجوع والتعرف على ما قمت به عبر الإنترنت.



أين يقع مقر الشركة: يوجد العديد من مزودي خدمات VPN في بلدان مختلفة. لكن تأكد من تحديد مزود VPN يوجد مقره في بلد به قوانين خصوصية قوية. قد يتم إجبار مزودي VPN الموجودين في البلدان التي لديها قوانين خصوصية قليلة أو ضعيفة جدًا على كشف وإرسال المعلومات التي يجمعونها عنك.



الخوادم: ابحث عن خدمة VPN والتي يكون لها خوادم في البلدان أو المدن التي تحتاج إليها. يوجد لدى بعض مزودي VPN الآلاف من الخوادم والمواقع في جميع أنحاء العالم. تأكد إن كنت تحتاج لجعل اتصالاتك تظهر كما لو كانت قادمة من بلد معين، هل يمكن لمزود VPN الخاص بك توفيرها؟



التوافق: ابحث عن الخدمات التي تعمل عبر أجهزة الكمبيوتر والأجهزة المحمولة المختلفة. على سبيل المثال: إن كنت تريد استخدام كمبيوتر محمول يعمل بنظام Windows وجهاز لوحي وجهاز iPhone. فستحتاج إلى خدمة VPN تعمل على جميع هذه الأجهزة.



تجنب استخدام ال VPN المجاني: كن حذرًا جدًا من خدمات VPN «المجانية»، فكر معي للحظة كيف يكسبون المال ويستثمرون في العمل؟ الخدمات المجانية غالباً ما تكون أنت السلعة فيها وقد تجمع وتبيع معلوماتك.



تعد VPN وسيلة رائعة للمساعدة في حماية خصوصيتك عبر الإنترنت. ومع ذلك، لا تفعل VPN أي شيء لتأمين الكمبيوتر أو الأجهزة أو حساباتك عبر الإنترنت. لذلك حتى إذا كنت تستخدم VPN، فتأكد دائماً من اتباع خطوات الأمان الأساسية، بما في ذلك التأكد من تحديث أجهزتك، واستخدام قفل الشاشة واستخدام كلمات مرور قوية وفريدة من نوعها لجميع حساباتك دائماً.



الضيف المحرر

فيل جونسي (@peakreflections) متخصص في تكنولوجيا المعلومات في مقاطعة بالم بيتش ويتمتع بخبرة في مجال الأمن الرقمي والتحريرات والتدقيق. معتمد من SANS في البحث الجنائي الرقمي وأساسيات الأمان، وعضو في مجلس مراجعات مجتمع OUCH. شغفه هو جعل الأمن الرقمي سهل للآخرين.

مصادر إضافية

<https://www.sans.org/u/Sd8>

:Making Passwords Simple

<https://www.sans.org/u/Sdd>

:Securing Your Mobile Devices

<https://www.sans.org/u/Sdi>

:Stop Malware

OUCH! من قبل فريق الوعي الأمني في SANS وتوزع بموجب Creative Commons BY-NC-ND 4.0. يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو إستخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: www.sans.org/security-awareness/ouch-newsletter. | المجلس التحريري: والت سكريفنز، فل هوفمان، ألان واجونير، شيريل كونلي | ترجمها إلى العربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد