



المركز الوطني للأمن السيبراني
National Cyber Security Center

توعية أمنية

تطبيقات الـ VPN استخداماتها ومخاطرها

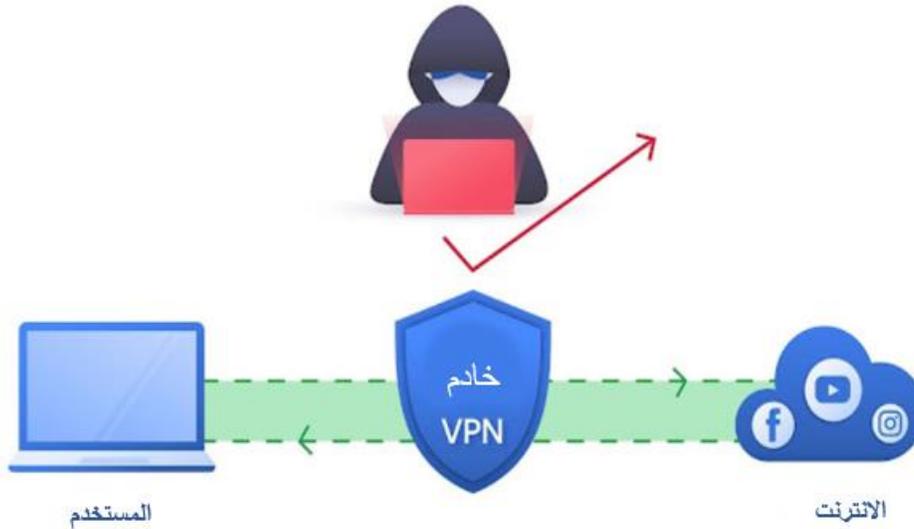
Document Status: Final
Document Version: 1.1
Document Date: 13 July 2023
Reference: N/A
Prepared by: NCSC Team
Approved by: NCSC Manager



مفهوم ال VPN واستخداماته

انتشر مؤخرًا استخدام الشبكة الخاصة الافتراضية (والمعروفة بال VPN) بشكل كبير جدا ومتزايد بين مستخدمي الإنترنت في العالم، ليتمكنوا من الوصول إلى جميع المواقع الإلكترونية بما فيها المواقع المحجوبة مع الحفاظ على خصوصيتهم.

VPN هي اختصار ل (Virtual Private Network) وهي عبارة عن شبكة افتراضية تنشأ اتصالاً مشفراً بين جهاز الكمبيوتر الخاص بالمستخدم والإنترنت. بحيث يتصل جهاز الكمبيوتر الخاص بالمستخدم بجهاز آخر يسمى الخادم، ويستخدم المعلومات الخاصة بهذا الخادم لتصفح الإنترنت بدلاً من استخدام معلومات الكمبيوتر الخاص به (كما هو موضح بالشكل التالي).



تقوم خدمة ال VPN بإخفاء العنوان الشبكي (IP Address) الخاص بجهاز المستخدم، وكذلك تشفير بياناته قبل أن يعاد توجيهها إلى خوادم بعيدة. وبالتالي عند تتبع أي موقع لبيانات المستخدم سوف يحصل على معلومات الخادم بدلاً من معلومات جهاز المستخدم.

يقوم العديد من المستخدمين حول العالم بالاتصال بالشبكة العنكبوتية من خلال تطبيقات ال VPN ليتمكنوا من الوصول إلى بعض المواقع المحجوبة وبعض مزايا التطبيقات التي يتم حجبها في بعض الدول أو لإخفاء هويتهم أثناء تصفح الإنترنت،

مخاطر وعيوب استخدام ال VPN

- التكلفة المرتفعة نسبياً لتطبيقات ال VPN التجارية مما يدفع العديد من الأشخاص للبحث عن تطبيقات بديلة مجانية.
- تعد تطبيقات ال VPN المجانية غير آمنة، حيث يقوم مزودي خدماتها بحفظ بيانات المستخدم وإنشاء سجل لأنشطته على الإنترنت والاستفادة منها لاحقاً الأمر الذي يعد انتهاكاً واضحاً للخصوصية. وقد تكون معلومات المستخدم الشخصية عرضة للمتاجرة بها وبيعها في مواقع الإنترنت المظلم (Dark Web)، إضافة إلى أن بعض شركات ال VPN قد تقوم ببيع معلومات المستخدم الشخصية إلى أطراف ثالثة مثل الشركات الخاصة بالإعلانات التجارية.



- قد تكون برامج الـ VPN غير الموثوقة مصممة لإلحاق الضرر بجهاز المستخدم واصابته بالبرمجيات الخبيثة، او لكي تقوم بتعطيل برامج مكافحة الفيروسات.
- انخفاض سرعة الاتصال مع شبكة الانترنت، وذلك بسبب زيادة مسار الاتصال والوقت اللازم للتشفير.
- تتعامل بعض المواقع (التي لا تسمح بالوصول إليها إلا من خلال عنوان شبكي حقيقي) مع مستخدمي تطبيقات الـ VPN برؤية وحذر شديدين، بحيث قد تمنعه من تصفح الموقع أو بعض مزاياه، وقد تطلب من المستخدم القيام باختبارات تحقق للتأكد من أنه شخص حقيقي أو تقوم بحظره كليا.
- الإعدادات الخاطئة لـ VPN قد تكشف هوية المستخدم وتعرضه لخطر التجسس والاختراق.
- قد يعتقد بعض مستخدمي VPN بأنهم مخفيون تماما ولا يمكن الوصول إليهم وبالتالي القيام بأنشطة غير قانونية أو ضارة للآخرين، والصحيح انه يمكن تتبعهم والوصول إليهم من قبل المختصين في حال قيامهم بأنشطة محظورة.
- بعكس الاعتقاد السائد، لا يمنع الـ VPN إلحاق الضرر بجهاز المستخدم، حيث أنه في حال إصابة الجهاز ببرمجيات خبيثة، فإن عملية الاختراق ممكنة باستخدام شبكة الـ VPN المتاحة.

التوصيات

نظرا لعدم وجود رقابة على تطبيقات الـ VPN، يُنصح الأفراد بعدم تنزيل مثل هذه التطبيقات على الأجهزة الخاصة بهم سواء أجهزة الهواتف المحمولة أو أجهزة الكمبيوتر، وذلك حفاظا على البيانات الشخصية الخاصة بهم من مخاطر التجسس والاختراق، بالإضافة لخطر بيعها إلى جهات أخرى وبالتالي استغلالها لتنفيذ هجمات إلكترونية أخرى كهجوم الفدية والابتزاز.