EUROPEAN ENDOWMENT FOR DEMOCRACY

الدليل المبسط

لتأمين الاتصال بالإنترنت

الدليل المبسط لتأمين الاتصال بالإنترنت

مقدمة

صار اعتمادنا على الإنترنت في حياتنا اليومية أكبر من أي وقت مضى، ومع التزايد المستمر لاستخدام الإنترنت وتداخله مع حيواتنا اليومية، زادت الانتهاكات الرقمية ومن أهمها تقنيات المراقبة والتجسس، والتي صارت أيضا في تطور مستمر، ولإدراكنا حجم هذا الأمر وأهمية أن يحافظ كل مستخدم على خصوصيته الرقمية، نقدم الدليل المبسط لتأمين الاتصال بالإنترنت، فنبدأ بشرح كيف نتصل بالإنترنت ونتتبع المسار الذي تسلكه بياناتنا حتى نتمكن من تحديد ما نحتاج تأمينه، ثم نتناول أهم طرق تأمين الاتصال، ونأمل من خلال هذا الدليل المبسط أن نساعد أكبر عدد من المستخدمين على الخروج من نطاق المراقبة المستمرة وتحقيق قدرٍ مرضٍ من الخصوصية.

المحتويات

الطريق إلى الإنترنت

إذا استخدمت سميرة هاتفها لإرسال رسالة تقول "أهلا" إلى صديقتها علياء عبر تطبيق واتساب، ستصل الرسالة في جزء من الثانية لكنها في هذا الجزء من الثانية ستغادر هاتف سميرة وتمر بالعديد من المحطات التي يمكننا اختصارها كالآتي:

المحطة الأولى جهاز الراوتر

ستتحرك الرسالة من هاتف سميرة إلى جهاز الراوتر، وقد لا تكون سميرة الشخص الوحيد الذي يستخدم هذا الراوتر، ومن يمثل خطرا في هذه المرحلة هم الأشخاص الآخرون المتصلون بنفس الراوتر، خصوصا إذا كانت لدى أحدهم صلاحيات إدارية وكانت لديه المعرفة التقنية الكافية.

المحطة الثانية مقدم خدمة الإنترنت

سيقوم الراوتر بإرسال الرسالة إلى مقدم خدمة الإنترنت (شركة الاتصالات التي تزود سميرة بالإنترنت)، وفي هذه المحطة فإن شركة الإنترنت بوسعها الوصول إلى كل ما يمر من خلالها.

المحطة الثالثة خوادم واتساب

ستقوم شركة الاتصالات بإرسال الرسالة إلى وجهتها في حواسيب أو خوادم شركة ميتا (التي تشغل واتساب)، والتي ستقوم بمعالجة الرسالة ثم إرسالها إلى الطرف المقصود، وبوسع شركة ميتا رؤية من أين أتت تلك الرسالة لأنها ترى عنوان الـ IP الذي جاءت منه، وهو يدل على الموقع الجغرافي التقريبي.

الجيد في هذا السيناريو هو أن رسائل واتساب مشفرة، وبالتالي فإنها عندما تمر خلال تلك المحطات لا يظهر محتواها بشكل مفهوم، أي أنه بالرغم من قدرة العديد من الأطراف على رؤية البيانات التي تخرج من هاتف سميرة وتصل إليها، إلا أن هؤلاء الأطراف لن يتمكنوا من فهم المحتوى بسبب تشفير الرسائل. أما إذا لم يكن المحتوى الذي نتلقاه أو نرسله مشفرا سيكون بوسع جميع تلك الأطراف الاطلاع على هذا المحتوى.

استخدام منصات مشفرة

واتساب مجرد مثال واحد على المنصات التي تهتم بتشفير البيانات، وهو ليس المثال الأفضل، فهناك خدمات تراسل تقدم معايير أفضل في التشفير مثل سيجنال. التشفير عموما يوفر أمانا جيدا عند إرسال واستقبال البيانات، حتى عبر الشبكات غير الآمنة، وهو لا يقتصر على منصات التراسل فحسب، إنما يشمل أيضا الخدمات السحابية وخدمات نقل البيانات والاجتماعات والمكالمات عبر الإنترنت. لهذا ننصح عموما بالاعتماد على المنصات التي تستخدم تشفيرا جيدا لنقل البيانات، لكن ماذا عن المواقع التي نزورها؟

استخدام HTTPS

العديد من البيانات التي نرسلها ونتلقاها على الإنترنت مشفرة بدرجات متفاوتة، فمثلا مواقع الإنترنت التي نزورها عادة ما تستخدم بروتوكول HTTPS وهو يشفر تفاعلنا مع الموقع، فلا يعرف من لديهم وصول إلى بيانات اتصالنا بالإنترنت سوى أننا نتصفح الموقع الفلاني، دون أن يعرفوا ماذا نفعل بداخله تحديدا، لهذا فإن أسهل خطوات تأمين الاتصال بالإنترنت هي التأكد

من استخدامنا لبروتوكول HTTPS وليس HTTP عند تصفح المواقع، وهذا يمكن إعداده بسهولة في جميع المتصفحات الشهيرة.

جوجل كروم

Settings → Privacy and security → Security →
Always use secure connections

فايرفوكس

Settings → Privacy & Security → Enable HTTPS-Only Mode

يحمينا تفعيل هذا الخيار من التجسس على المعلومات التي نتبادلها مع المواقع التي نزورها، فبدون بروتوكول HTTPS يمكن للآخرين المتواجدين على نفس الشبكة ومقدم خدمة الإنترنت رؤية المعلومات التي نرسلها للمواقع مثل كلمات السر وبيانات البطاقات البنكية، ويحمينا هذا الخيار كذلك من التلاعب في محتوى هذه المواقع من طرف من بوسعهم اعتراض اتصالنا بها، لكنه لا يمنع هذه الأطراف من معرفة عناوين المواقع التي نزورها.

استخدام VPN

الـ VPN هو اختصار virtual private network (باللغة العربية: شبكة خاصة افتراضية)، ولفهم كيف يعمل الـ VPN علينا العودة إلى المثال الذي ذكرناه في البداية عندما قلنا إن رسالة الواتساب تخرج من هاتفنا إلى جهاز الراوتر ثم إلى مقدم خدمة الإنترنت ثم إلى خوادم واتساب.

ما يفعله الـ VPN هو تشفير البيانات التي نرغب بإرسالها بداية من الهاتف فتمر عبر جهاز الراوتر ومقدم خدمة الإنترنت في صورة مشفرة غير مفهومة، ثم يرسلها الـ VPN لأحد خوادمه في مكان آخر ويقوم بفك التشفير وتستكمل الرسالة مسارها إلى خادم واتساب، لكن هذه المرة باعتبارها قادمة من خادم

الـ VPN وليس من شركة الاتصالات التي تزودنا بالإنترنت، فإذا كنا نحن في مصر وكان خادم الـ VPN الذي اخترناه في الولايات المتحدة الأمريكية، تبدو الرسالة كأنها قادمة من الولايات المتحدة الأمريكية وليس من مصر.

ويمكن تلخيص فوائد الـ VPN في الآتي:

- منع من يمكنهم اعتراض الاتصال (مثل من لهم وصول على نفس الراوتر ومقدم خدمة الإنترنت) من معرفة المواقع التي نزورها والخدمات التي نستخدمها.
- منع المواقع التي نزورها والخدمات التي نستخدمها من معرفة عنوان الـIP الحقيقي، وبالتالي معرفة موقعنا الجغرافي التقريبي الذي يحتوي البلد والمدينة (لكن ليس نقطة محددة بشكل دقيق على الخريطة).
- الوصول إلى المحتوى المقيد جغرافيا، فإذا كانت حكومة البلد التي نتواجد فيها تحجب الوصول إلى مواقع إلكترونية معينة، يمكن للـ VPN مساعدتنا في تخطي هذا الحجب، وكذلك إذا كانت بعض المواقع أو الخدمات حصرية لبلاد معينة، يمكننا الوصول إليها عبر استخدام VPN لديه خوادم في هذه البلاد.

تقدم بعض خدمات الـ VPN مزايا إضافية مثل حجب الإعلانات أو منع ملفات تعريف الارتباط (الكوكيز)، لكن كل تلك الأشياء يمكن فعلها بإضافات بسيطة للمتصفح، فأهمية الـ VPN تكمن بشكل أساسي في تشفير محتوى الاتصال أمام مقدم خدمة الإنترنت ومن لديهم وصول لنفس شبكة الإنترنت التي تستخدمها، وينبغي هنا الإشارة إلى أن مقدمي خدمات الـ VPN كثيرا ما يبالغون في وصف دور الـ VPN في حماية الأمن الرقمي للمستخدمين، لهذا يجب معرفة حدود الحماية التي يقدمها الـ VPN، فهو لن يحمينا من التصيد الاحتيالي أو من الاحتيال المالي عبر الإنترنت، وبالتأكيد لن يحمي هويتنا إذا ما لم نكن نحن على حذر كافٍ في تقديم معلومات عن أنفسنا على الإنترنت.

عند الاشتراك في VPN يجب أيضا التأكد من شيئين مهمين؛ أولا ثقتنا في مقدم خدمة الـ VPN، لأن تفعيل الـ VPN هي عملية نقل ثقة، فنحن نحجب

محتوى اتصالنا عن مقدم خدمة الإنترنت ونعطيه لمقدم خدمة الـ VPN، لذلك يجب اختيار مقدمي خدمات الـ VPNs الموثوق بهم فقط، وثانيا يجب التأكد من عمل هذه الخدمة في بلدنا، لأن بعض البلدان تحاول حجب الشبكات الخاصة الافتراضية، وهذا يتسبب في تعطيل عمل بعض خدمات الـ VPN. ننصح كذلك بعدم الاستسلام بسهولة عندما يفشل الاتصال بالـ VPN وتجربة البروتوكولات المختلفة المتاحة فيه.

هل سيعرف أحد أنني متصل بخدمة VPN؟

إذا قامت إحدى الجهات بالتحقق من اتصالك ستجد أنه متجه إلى خادم تابع إلى خدمة VPN، لكن هذا الأمر ليس دليل إدانة دوما، فكثيرا ما يستخدم الناس خدمات VPN للوصول إلى محتويات نتفلكس أو التطبيقات أو الخدمات الحصرية في بلاد معينة.

لماذا لا ننصح بخدمات الـ VPN المجانية؟

الشبكات الخاصة الافتراضية تعتمد على وجود خوادم تنقل سعات كبيرة من البيانات طوال الوقت، وتشغيل هذه الخوادم أمر مكلف، فلماذا نتوقع أن نستفيد بهذه الخدمة المكلفة مجانا؟ خدمات الـ VPN المجانية أحيانا ما تكون فخًا لسرقة بيانات مستخدميها (كما أوضحنا سابقا أن استخدام الـ VPN هي عملية نقل ثقة). يوجد بالطبع استثناءات لهذا الأمر، مثل الخدمات التي تعمل بطرق لا مركزية مثل أوتلاين (Outline VPN) وشبكة تور (Tor).

ما خدمات الـ VPN التي ترشحونها؟

عند استخدام خدمات مدفوعة يجب مراجعة معلومات عن الشركات التي تقدمها مثل سمعتها في الانتهاكات الرقمية وما إذا كانت الخدمة تتعرض للتدقيق والمراجعة الخارجية أو لا، وما إذا كانت سياساتها تمنع الاحتفاظ بسجلات تصفح المستخدمين (رغم أن هذا الأمر لا يمكن الاعتماد عليه تماما)،

وبالطبع يجب التأكد من أن هذه الخدمة لديها بروتوكولات تعمل في البلد الذي سنستخدمها فيه.
الخدمات المجانية التي نرشحها هي الخدمات المبنية على Outline VPN مثل BeePass وكذلك شبكة تور (Tor).

استخدام Tor

تور أو Tor (لاختصار The Onion Router) هو متصفح يساعد في الوصول إلى الإنترنت بحيث يصعب بشدة على المواقع تتبع مصدر الاتصال فيوفر درجة عالية من المجهولية، ويعتمد تور على تشفير البيانات 3 مرات، وتمريرها عبر 3 خوادم تعمل ضمن شبكة تور.

تحذير بخصوص استخدام تور
إذا قامت إحدى الجهات بتحليل البيانات من أجهزتك ستتمكن من معرفة أنك تستخدم تور، لكنها لن تعرف المواقع التي تزورها.

عند استخدام تور، يفضل استخدام جسر خصوصا إذا كان تور محجوبا في البلد الذي تستخدمه فيه، ولتقليل فرصة التعرف على اتصالك به، ويوفر تور بعض أنواع الجسور من خلال إعدادات البرنامج.

ويجب ملاحظة أن هذه الجسور لا تضمن دوما عدم التعرف على استخدامك لتور، خصوصا عند الفحص الدقيق لاتصالك، ولهذا قد يكون من الأفضل الاتصال بتور من خلال VPN، لكن يجب معرفة أن هذا الأمر من شأنه إبطاء سرعة الإنترنت بشكل ملحوظ، لكنه يزيد من مجهوليتك.

النصائح الأساسية

النصائح العامة التي قد يكون معظمنا سمع بها من قبل هي في الواقع نصائح مهمة جدا وفعالة.

الحذر من الشبكات العامة

الشبكات العامة هي شبكات الواي فاي التي يمكن لأي أحد الاتصال بها، ويجب أن نتساءل دوما عن مصلحة أي جهة في توفير إنترنت مجاني، والخطر

هنا يكمن في قدرة المسؤول عن الشبكة، بل وأحيانا أي شخص متصل بنفس الشبكة ولديه المعرفة التقنية الكافية، على رؤية المواقع التي يزورها الآخرين على نفس هذه الشبكة، وكذلك يمكن له التلاعب بمحتوى المواقع التي لا تستخدم HTTPS، وتنزيل محتوى ضار على أجهزتنا، لهذا يُفضل تجنب الشبكات العامة، وعند الاضطرار إلى استخدامها يجب الاتصال بخدمة VPN موثوقة.

حماية شبكة الواي فاي

حتى لا نجلب مشاكل شبكات الواي فاي العامة إلى شبكات الواي فاي الخاصة بنا يجب علينا الحرص على عدم قدرة أي شخص غير مرغوب فيه على الوصول إلى شبكة الواي فاي الخاصة بنا، ويكون ذلك من خلال اختيار كلمة مرور قوية للشبكة، وإلغاء تفعيل خيار WPS، ويمكن أيضا لزيادة تأمين الشبكة إخفاء اسمها وهو ما يجعل الاتصال بها أمر أصعب يضطر المستخدم إلى معرفة اسم الشبكة أولا ثم معرفة كلمة مرورها.

عدم مشاركة الشبكة مع أي شخص

انضمام أي شخص إلى شبكة الواي فاي الخاصة بك يعني أن بوسعه، إذا كانت لديه المعرفة التقنية اللازمة، أن يصبح مصدر تهديد وتتبع للمحتوى الذي تصل إليه عبر الإنترنت. نحن هنا لا ندين الكرم، لكن نشجع على تحري الثقة فيمن نسمح لهم بالانضمام إلى شبكاتنا الخاصة.

استخدام متصفحات حديثة

المتصفحات الجيدة تحرص على اتباع البروتوكولات الآمنة وإتاحتها دوريا، نحن نرشح متصفح موزيلا فايرفوكس ونوصي بإبقائه محدثا طوال الوقت.

يبدو الاتصال بالإنترنت في وقتنا هذا عملية مباشرة وسهلة، لكنه في الواقع يتطلب يتطلب جهدا إضافيا لمنع أي طرف غير مرغوب فيه من تتبع اتصالنا أو استهدافنا من خلاله، لهذا يجب أن نبذل هذا الجهد في تثقيف أنفسنا حول المخاطر المحتملة وتثقيف من حولنا كذلك من أجل تضييق الخناق على الراغبين في التجسس على الآخرين أو إيذائهم على الإنترنت.