10 نصائح لتأمين شبكة واي فاي ومنع اختراقها

الأحد 2 نوفمبر 2025 03:00 م

في زمن أصبح فيه الاعتماد على الإنترنت متزايدًا، يصبح من الضروري تأمين شبكة الإنترنت وبياناتك الشخصية، وتوفير الحماية لشبكة "الواي فاي" من أية محاولات اختراق قد تتعرض لها. لذلك، يُعد اختيار رواتر المناسب وتأمين شبكة منزلك أمرًا بالغ الأهمية للحفاظ على أمانك.

إذا لم تكن شبكة "الواي فاي" مؤمّنة بشكل صحيح، فقد تُعرّضها، للاختراق وسرقة البيانات وغيرها من التهديدات الرقمية. ويتم التحكم في الأجهزة المتصلة، أو تثبيت برامج ضارة، أو الوصول إلى بياناتك الحساسة، مثل أرقام البطاقات البنكية وبث الكاميرا المباشر.

لذا، فإن الحفاظ على شبكة منزلية آمنة يُقلل من خطر الاختراق، ويُبعد أيضًا الأشخاص غير المرغوب فيهم أو غير المصرح لهم والأجهزة التي قد تُبطئ اتصالك بخدمة الإنترنت.

وعلى الرغم من أنه لا يوجد ما يضمن الحماية المطلقة من محاولات الاختراق، لكن هناك مجموعة من الخطوات التي تُصعّب على أي شخص اختراق شبكتك وبياناتك.

نصائح لتأمين شبكة واي فاي

1. ضع جهاز الراوتر في مكان مركزي

ضع جهاز الراوتر في مكان مركزي بالمنزل. يُرسل الجهاز إشارات لاسلكية في جميع الاتجاهات، لذا فإن وضعه في موقع مركزي مُحكم يُساعد في الحفاظ على اتصالك داخل حدود منزلك. ومن المزايا الإضافية، أنه يُؤمّن أفضل جودة اتصال.

على سبيل المثال، إذا وضعت جهاز الراوتر بجوار جدار مشترك قد يرسل إشارة قوية ومغرية إليهم. إذ يمكن للجهاز الجيد بث الإشارات إلى الجيران أو عبر الشارع، حتى لو لم تكن في شقة. في حين أن وضعه في موقع مركزي يقلل من مدى انتشار هذه الإشارات خارج المنزل.

2. إنشاء كلمة مرور قوية لشبكة واي فاي وتغييرها بشكل متكرر

إنشاء كلمة مرور فريدة لشبكة "الواي فاي" أمرٌ أساسي للحفاظ على اتصال آمن. تجنب كلمات المرور أو العبارات سهلة التخمين، مثل اسم الشخص أو تاريخ ميلاده أو رقم هاتفه أو أي معلومات شائعة أخرى.
وبينما يسهل تذكر كلمات مرور الواي فاي البسيطة، يسهل على الآخرين تخمينها أيضًا. يمكنك بسهولة الوصول إلى إعدادات جهاز الراوتر لتحديث كلمة مرور "الواي فاي".
تأكد من تغيير كلمة مرورك كل ستة أشهر تقريبًا، أو كلما شككت في تعرض أمان شبكتك للاختراق. كلما غيّرت كلمة مرورك بانتظام، قلّت احتمالية اختراقها.

3. تغيير بيانات الوصول إلى إعددات الراوتر

على نفس المنوال الذي تستخدمه لحماية شبكة واي فاي الخاصة بك بكلمة مرور، ستحتاج أيضًا إلى منع أي شخص من الوصول مباشرة إلى إعدادات جهاز الراوتر الخاص بك.
للقيام بذلك، غيّر اسم المسؤول وكلمة المرور لجهاز الراوتر. يمكنك تسجيل الدخول إلى إعدادات جهاز الراوتر بكتابة عنوان IP الخاص به في شريط URL، لكن معظم أجهزة الإنترنت وموفري الخدمة لديهم تطبيق يتيح لك الوصول إلى نفس الإعدادات والمعلومات.

بيانات تسجيل الدخول لجهاز الراوتر منفصلة عن اسم شبكة واي فاي وكلمة المرور. إذا لم تكن متأكدًا من الإعداد الافتراضي، ستجده أسفل جهاز الراوتر. أما إذا تم تغييره، فإليك كيفية الوصول إلى إعدادات جهاز الراوتر لتحديث اسم المستخدم وكلمة

المرور.

4. تشغيل جدار الحماية وتشفير شبكة واي فاي
تحتوي معظم أجهزة الراوتر على جدار حماية لمنع الاختراق الخارجي، وتشفير واي فاي لمنع أي شخص من التنصت على البيانات المتبادلة بين جهاز الراوتر والأجهزة المتصلة. عادةً ما يكون كلا الخيارين مفعلين افتراضيًا، لكن يجب عليك التأكد من تفعيلهما في إعدادات جهاز الراوتر. إذا كانا معطلين لأي سبب، فقم بتشغيلهما.

5. إنشاء شبكة واي فاي للضيوف
قبل مشاركة الوصول إلى شبكة واي فاي الخاصة بك، فكّر في إنشاء شبكة ضيوف منفصلة للزوار، لأنه قد تُصاب أجهزتهم أو أي شيء يُنزّلونه أثناء اتصالهم بشبكتك ببرامج ضارة أو فيروسات تستهدف شبكتك دون علمهم.

تعتبر شبكة الضيوف مثالية أيضًا لأجهزة إنترنت الأشياء الخاصة بك، مثل كاميرات واي فاي وأجهزة التحكم في درجة الحرارة الذكية ومكبرات الصوت الذكية - وهي أجهزة قد لا تحتوي على الكثير من المعلومات الحساسة وربما تكون أكثر عرضة للاختراق من جهاز أكثر ذكاءً مثل الكمبيوتر أو الهاتف.

6. استخدم **VPN**
هناك عدة أسباب لاستخدام "شبكة افتراضية خاصة" (VPN)، وهي تقنية تنشئ اتصالاً آمنًا ومشفرًا بين جهازك والإنترنت، مما يحمي بياناتك ويخفي عنوان IP الخاص بك. تعمل كـ "نفق" خاص عبر الشبكة العامة، مما يضمن خصوصية نشاطك ويسمح لك بتجاوز الحظر الجغرافي أو الرقابة على الإنترنت.

شبكات VPN تكون أكثر فائدة عند الاتصال بشبكة عامة، لكنها توفر أيضًا مستوى من الأمان والخصوصية إلى شبكتك المنزلية. بعض شبكات VPN أفضل من غيرها، لكن ذلك قد يتطلب منك دفع رسوم مادية مقابل الاستفادة منها.

7. تحديث الراوتر والأجهزة المتصلة
قد تكون تحديثات البرامج مزعجة، لكنها غالبًا ما تتضمن تحديثات أمنية. عندما تدرك الشركات وجود ثغرات أمنية محتملة أو مكشوفة، تُصدر تحديثات وتصحيحات لتقليل المخاطر أو القضاء عليها. ابقَ على اطلاع دائم لتنزيلها بانتظام.

تحديث جهاز الراوتر والأجهزة المتصلة به باستمرار يضمن لك أفضل حماية ضد البرامج الضارة ومحاولات الاختراق المعروفة. إن أمكن، اضبط جهاز الراوتر على التحديث التلقائي في إعدادات المسؤول، وتحقق دوريًا من تحديثه.

8. تعطيل الوصول إلى جهاز الراوتر عن بُعد
يتيح الوصول عن بُعد لجهاز الراوتر لأي شخص غير متصل مباشرةً بشبكة واي فاي الوصول إلى إعداداته. ما لم تكن بحاجة إلى الوصول إلى الراوتر أثناء وجودك خارج المنزل (مثلاً للتحقق من إعدادات جهاز طفل متصل أو تغييرها)، فلا داعي لتفعيل الوصول عن بُعد.

يمكنك تعطيل الوصول عن بُعد من إعدادات مسؤول جهاز الراوتر. بخلاف إجراءات الأمان الأخرى، قد لا يكون تعطيل الوصول عن بُعد لجهاز التوجيه هو الخيار الافتراضي.

9. التحقق من الأجهزة المتصلة
افحص الأجهزة المتصلة بشبكتك بانتظام وتأكد من معرفتك بها. إذا لاحظت اتصال أي جهاز من خارج المنزل بها، افصله وغيّر كلمة مرور واي فاي. بعد تغيير كلمة المرور، ستحتاج إلى إعادة توصيل جميع أجهزتك المتصلة سابقًا، لكن سيتم إيقاف تشغيل أي مستخدم أو جهاز غير مصرح له باستخدام شبكتك.

قد تحمل بعض الأجهزة، وبخاصةً أجهزة إنترنت الأشياء غير المعروفة، أسماءً افتراضية غريبة لأرقام وحروف عشوائية لا تتعرف عليها فورًا. إذا واجهتَ مشكلةً كهذه أثناء تدقيق أجهزتك المتصلة، فافصلها. لاحقًا، عندما لا تتمكن من تشغيل مكنسة الروبوت الكهربائية من هاتفك، ستعرف أن هذا هو السبب.

10. جهاز **WPA3**
WPA3 هو أحدث معيار أمان لشبكات واي فاي. يجب أن تكون جميع أجهزة الراوتر الجديدة مزودة به، إذا كان جهازك مصنوعًا قبل عام 2018، فقد يكون لديك جهاز WPA2، الذي يفتقر إلى نفس بروتوكولات الأمان الموجودة في أجهزة WPA3 الأحدث.

سيُظهر لك بحث سريع عن طراز جهازك تاريخ إصداره وأي ميزات خاصة به، مثل ما إذا كان يدعم WPA2 أو WPA3. إذا كان لديك جهاز راوتر يدعم WPA2، فاتصل بمزود الخدمة واحصل على جهاز أحدث وأفضل.