

كيف تحمي هاتفك عند الاتصال بشبكة واي فاي في الأماكن العامة؟



الاثنين 3 نوفمبر 2025 03:00 م

مع توفير خدمة "واي فاي" المجانية في المطارات والفنادق والمقاهي، وحتى في بعض الحدائق، أصبح استخدام أجهزتك للاتصال بالإنترنت أثناء التنقل أسهل من أي وقت مضى.

على عكس الشبكات الخاصة، لا توفر نقاط اتصال "واي فاي" العامة دائمًا حماية عالية، وهو ما قد يؤدي إلى سرقة البيانات الشخصية، مثل كلمات المرور أو أرقام البطاقات البنكية. لذا، فإن هناك أمرًا واحدًا يجب مراعاته عند استخدامها: الأمان.

تقدم (Avast) شركة برمجيات الأمن السيبراني، مجموعة من الطرق التي تساعدك على الحفاظ على هاتفك أثناء استخدام واي فاي في الأماكن العامة.

من أسهل الطرق للحفاظ على أمان هاتفك على شبكات "الواي فاي" العامة استخدام أحد أفضل متصفحات الخصوصية، واتباع بعض نصائح السلامة الأساسية، مثل التحقق من أمان الشبكة، وعدم الكشف عن معلوماتك الشخصية أثناء الاتصال، واستخدام شبكة افتراضية خاصة (VPN) لإخفاء عنوان IP الخاص بك.

يجب عليك اتباع نصائح السلامة المتعلقة بشبكات واي فاي العامة مهما كان اتصالك. ويمكنك حماية شبكتك بشكل أكبر من خلال إعداد اتصال VPN الخاص بك، وهي من أفضل الطرق لحماية نفسك بالكامل على الإنترنت.

كيفية التحقق من أمان شبكة واي فاي العامة

تأكد من أن اسم الشبكة يتطابق مع اسم المكان العام الذي تتواجد فيه. إذا لم تكن متأكدًا من أن المكان الذي تتواجد فيه يوفر خدمة واي فاي عامة، فاسأل قبل الاتصال. غالبًا ما تُدوّن المقاهي اسم الشبكة في قوائمها، وغالبًا ما تعرض الأماكن العامة اسم الشبكة في محطات المواصلات أو في الإعلانات الرسمية.

تأكد من اتصالك بشبكة شركة موثوقة، والتزم بالمواقع الآمنة التي تستخدم اتصالات HTTPS فقط. تحقق من عنوان URL لكل موقع تزوره - يجب أن يبدأ بـ HTTPS، وليس HTTP. حرف "s" يعني "آمن". المواقع التي تحتوي على "https" في عناوين URL الخاصة بها أكثر أمانًا من تلك التي لا تحتوي على "https".

اطلب كلمة مرور الواي فاي

يساعدك استخدام كلمة مرور واي فاي على التحقق من هوية الشبكة وتقييم أمانها. لا تستحق طرق الاتصال الأخرى المخاطرة الأمنية، لأن اتصالاتك قد لا تكون مشفرة.

استخدم أقل عدد ممكن من الشبكات العامة

مع أن أفضل ممارسة هي التحقق من شبكة واي فاي المفتوحة قبل الاتصال، إلا أنه من الأفضل الحد من تكرار اتصالك بالشبكات العامة المفتوحة بدلاً من الاعتماد بشكل عشوائي على إجراءات أمان شبكة واي فاي، تحقق من سلامة بعض المواقع، والتزم بالشبكات التي تثق بها.

إذا لم تتمكن من الحفاظ على اتصال واي فاي على شبكات محددة فقط، فحاول إصلاح اتصالات واي فاي على نظام أندرويد أو آي أو إس قبل اللجوء إلى شبكة أخرى غير معروفة. إذ أن تمكين جهازك من الاتصال تلقائيًا بشبكات واي فاي موثوقة يوفر عليك الوقت ويضمن اتصالك آمنًا.

الشروط والأحكام

يجب عليك قراءة الشروط والأحكام لضمان أمان شبكة الواي فاي المجانية التي تستخدمها. افهم تأثير استخدام شبكة واي فاي غير آمنة على بياناتك الشخصية ونشاط تصفحك. قد تفاجأ بما توافق عليه مقابل اتصال مجاني.

لا تكشف الكثير من التفاصيل

أحيانًا، يلزم تقديم معلومات شخصية للوصول إلى الشبكات واي فاي العامة. لا تُفصح عن معلومات حساسة، مثل كلمات المرور أو تفاصيل حسابك المصرفي.

حتى لو طلبت منك شبكة واي فاي عامة إنشاء كلمة مرور لتسجيل الدخول فقط، فلا تستخدم كلمة مرور من حساب شخصي آخر. أنشئ كلمة مرور قوية وأصلية لا تُعرض حساباتك الأخرى للخطر. فكر أيضًا في استخدام عنوان بريد إلكتروني بديل، مُصمّم خصيصًا لهذه الحالات.

تجنب المواقع التي تتطلب معلوماتك

عند استخدام شبكة واي فاي عامة، راقب مواقع الويب التي تزورها. إذا كنت بحاجة إلى تسجيل الدخول أو التسجيل أو بيانات البطاقة البنكية، فاستخدم بيانات هاتفك المحمول، أو انتظر حتى تتصل بشبكة خاصة آمنة.

ونظرًا لأنه من السهل على المتسللين الحصول على معلوماتك الشخصية عبر شبكات واي فاي العامة، فلا تستخدم المواقع التي تتطلب معلومات حسابك المصرفي، مثل الخدمات المصرفية عبر الإنترنت أو منصات التجارة الإلكترونية.

استخدم VPN لشبكة واي فاي العامة

نُشئ شبكة VPN، أو الشبكة الافتراضية الخاصة، اتصالاً آمنًا بين خادم VPN الخاص بك والإنترنت. وكما هو الحال في تفعيل تشفير واي فاي على جهاز (الراوتر)، والذي يُؤمّن جميع البيانات الداخلة والخارجة من شبكتك، تُرسل شبكة VPN بياناتك إلى خادم آمن حيث تُشفّر قبل أن تنتقل إلى الإنترنت. جميع المعلومات، بما في ذلك نشاط تصفحك وبياناتك الشخصية - مثل كلمات المرور وتفاصيل تسجيل الدخول - في مأمن من أعين المتطفلين.

تُخفي شبكات VPN أيضًا عنوان IP الخاص بك لتوفير طبقة إضافية من الخصوصية. وينطبق هذا سواء كنت تستخدم عنوان IP عامًا أو خاصًا. عند استخدام شبكة VPN، يتصل جهازك بخادم خاص، والذي بدوره يربطك بالمواقع الإلكترونية التي تزورها بدلاً من مرور اتصالك بالكامل عبر شبكة واي فاي عامة واسعة، عند استخدام شبكة VPN على شبكة واي فاي عامة، تُستخدم الشبكة العامة فقط لتوصيل جهازك بخادم VPN الخاص. عند وصول اتصالك إلى خادم VPN، تُشفّر اتصالاتك ثم تُمرّر إلى الإنترنت الأوسع.

استخدام VPN على شبكات واي فاي العامة آمن ويوفر حماية قوية من التهديدات الإلكترونية على الشبكات المفتوحة. بالإضافة إلى ذلك، يمكن فتح المواقع المحظورة باستخدام VPN، ومنع المتطفلين من تتبع أنشطتك والحصول على كلمات مرورك ومعلومات بطاقتك البنكية.

استخدم برنامج مكافحة الفيروسات

تُعد حماية شبكات واي فاي العامة ميزة شائعة في العديد من أفضل برامج مكافحة الفيروسات. لذا، ينصح تثبيت أداة إزالة الفيروسات على جهازك لحماية جهازك.

تمكين جدار الحماية

نصيحة أخرى فعّالة للحفاظ على خصوصية شبكة واي فاي هي استخدام جدار حماية لمنع وصول البيانات الضارة إلى شبكتك الشخصية. معظم أجهزة الكمبيوتر، بما في ذلك أجهزة الكمبيوتر الشخصية وأجهزة ماك - وبعض هواتف أندرويد وآي فون الحديثة - مزودة بجدران حماية مدمجة. تحقق من إعدادات الأمان لديك للتأكد من توفر حماية جدار الحماية، وشغلها قبل استخدام اتصال واي فاي مفتوح.

تقييد مشاركة الملفات

بدون اتصال واي فاي آمن، تجنب أو قلل من مشاركة الملفات AirDrop. يمكن لأي شخص آخر على الشبكة سرقة أي شيء تنقله بسهولة. إذا لم يكن من الممكن تجنب مشاركة الملفات، فاستخدمها باعتدال.