نصائح لاستخدام شبكات Wi-Fi العامة بأمان

قد يحاول المحتالون استغلالك عندما تستخدم الإنترنت. اقرأ النصائح التالية لتقرر ما إذا كنت بحاجة لاستخدام شبكة Wi-Fi عامة.

نتيجة لتفشي فيروس كورونا وإغلاق المنشآت التجارية والمكتبات، يقضي الكثير منا المزيد من الوقت عبر الإنترنت. ولهذا، فقد نحتاج إلى استخدام شبكة Wi-Fi عامة للاتصال بالإنترنت. إذا احتجت لاستخدام شبكة Wi-Fi عامة، فيرجى مراعاة التوصيات التالية من كبير موظفي حماية الخصوصية لمساعدتك في حماية بياناتك:

1- تأكد من سلامة الشبكة المتاحة لديك.

تأكد من اتصالك بالشبكة الصحيحة، فقد يحاول المحتالون إنشاء شبكات تبدو آمنة وفقًا لأسمائها ولكنها في الواقع تقوم بتوجيهك للاتصال بشبكة تم إعدادها للاطلاع على تصفحك للإنترنت. وهذا يعني أنك إذا أدخلت بيانات اعتماد تسجيل الدخول أو كلمات المرور لمواقع الويب، فسيتمكن المخترقون من سرقة بياناتك. لحماية بياناتك، اقرأ اسم الشبكة بعناية، وإن أمكن، فتأكد من أحد الموظفين أو تحقق من لافتة أو لوحة المنشأة للتأكد من سلامة الشبكة.

الشبكات المعروفة، مثل شبكات سلاسل المقاهي المشهورة، غالبًا ما تكون آمنة لأن الشركة تقدم الشبكة كجزء من الخدمات في المقهى. عادة ما تكون الشبكات المعروفة أكثر أمانًا من شبكات Wi-Fi المجانية العشوائية التي قد تظهر على هاتفك في مكان عام.

2- أغلق الاتصال التلقائي.

تحتوي العديد من الأجهزة (الهواتف الذكية وأجهزة الكمبيوتر المحمول والأجهزة اللوحية) على إعداد الاتصال التلقائي، وهذا الإعداد يتيح لأجهزتك الاتصال بالشبكات القريبة بسهولة. لا يشكل الأمر مشكلة مع الشبكات الموثوق بها، ولكنه يمكن أن يؤدي إلى اتصال جهازك بشبكات غير آمنة. يمكنك تعطيل هذه الخاصية من خلال الإعدادات على جهازك. أغلق دومًا هذا الإعداد، خاصة عند الذهاب لأماكن غير مألوفة، وكإجراء احتياطي إضافي، يمكنك تحديد "إزالة الشبكة" بعد استخدام شبكة Wi-Fi عامة.

عليك أيضًا الانتباه لاتصال Bluetooth لديك أثناء التواجد في الأماكن العامة. يتيح اتصال Bluetooth تواصل العديد من الأجهزة معًا، ويمكن للمخترق البحث عن إشارات Bluetooth المفتوحة للوصول إلى أجهزتك. أغلق هذه الميزة في هاتفك وأجهزتك الأخرى دائمًا عندما تكون في منطقة غير مألوفة.

3- أغلق مشاركة الملفات.

تأكد من إغلاق خيار مشاركة الملفات عند الاتصال بشبكة Wi-Fi عامة، ويمكنك إغلاق مشاركة الملفات من تفضيلات النظام أو لوحة التحكم، تبعًا لنظام التشغيل الذي تستخدمه. خدمة AirDrop هي مثال على إحدى ميزات مشاركة الملفات التي ينبغي إغلاقها. تقوم بعض أنظمة التشغيل مثل Windows أو نظام تشغيل الكمبيوتر الشخصي بإغلاق مشاركة الملفات عن طريق تحديد خيار "عامة" عند الاتصال بشبكة عامة جديدة لأول مرة.

خطوات إغلاق مشاركة الملفات

على جهاز كمبيوتر شخصي:

1. انتقل إلى "الشبكة" و"مركز المشاركة".
2. ثم قم بتغيير إعدادات المشاركة المتقدمة.
3. أغلق مشاركة الملفات والطابعات.

بالنسبة لأجهزة Mac:

1. انتقل إلى "تفضيلات النظام".
2. اختر "المشاركة".
3. قم بإلغاء تحديد كل الخيارات.
4. ثم من الباحث، انقر على AirDrop، وحدد السماح باكتشافي بواسطة: "لا أحد".

بالنسبة لأجهزة iOS، ابحث عن AirDrop في "مركز التحكم" وقم بإغلاقه.

4- استخدم شبكة VPN.

فكر في تثبيت شبكة VPN (شبكة ظاهرية خاصة) على جهازك. إن استخدام شبكة VPN هو الخيار الأكثر أمانًا للخصوصية الرقمية عند استخدام شبكة Wi-Fi عامة، فهي تقوم بتشفير البيانات عند مرورها من وإلى جهازك وتعمل "كنفق" بحيث لا تكون بياناتك مرئية أثناء مرورها عبر شبكة.

5- FBI تحذر من المواقع الإلكترونية المشفرة – HTTPS.

حذرت FBI من المواقع الإلكترونية التي يبدأ عنوانها بـ "https". يفترض أن يشير وجود "https" ورمز القفل إلى أن مرور الشبكة مشفر وأنه يمكن للزائرين مشاركة البيانات بأمان، ولكن مرتكبي الجرائم الإلكترونية يستغلون الآن ثقة العامة من الجمهور باستدراجهم إلى المواقع الخبيثة التي يتضمن عنوانها https وتبدو آمنة ولكنها عكس ذلك.

توصيات FBI:

- لا تثق ببساطة في الاسم الموجود بعنوان البريد الإلكتروني: تحقق من غرض محتوى البريد الإلكتروني.
- إذا تلقيت رسالة بريد مريبة تحتوي على رابط من شخص تعرفه، فتأكد من صحة الرسالة بالاتصال بالشخص أو مراسلته عبر البريد الإلكتروني، ولا ترد بشكل مباشر على رسالة بريد إلكتروني مريبة.
- ابحث عن الأخطاء الإملائية أو أسماء المجالات الخاطئة في الرابط (على سبيل المثال، إذا كان العنوان ينتهي بـ ".com" بدلًا من أن ينتهي بـ ".gov").
- لا تثق في موقع إلكتروني لمجرد أنه يحتوي على رمز القفل أو يتضمن "https" في شريط عنوان المتصفح.

6- لا نوصي بالوصول إلى المعلومات الحساسة.

حتى وإن كنت تستخدم شبكة VPN، فلا نوصي بالوصول إلى الحسابات المصرفية الشخصية أو البيانات الحساسة المشابهة مثل أرقام الضمان الاجتماعي عبر الشبكات العامة غير الآمنة. حتى الشبكات العامة الآمنة قد تمثل خطرًا. فكر جيدًا قبل اتخاذ قرار الوصول إلى هذه الحسابات على شبكة Wi-Fi عامة. وبالنسبة للمعاملات المالية، ربما من الأفضل استخدام وظيفة نقطة الاتصال اللاسلكية بهاتفك الذكي بدلاً من الشبكة العامة.

7- الشبكات الآمنة وغير الآمنة.

يوجد في الأساس نوعان من شبكات Wi-Fi العامة: شبكات آمنة وغير آمنة.

اتصل بالشبكات العامة الآمنة كلما أمكن. يمكن الاتصال بالشبكات غير الآمنة بحيث لا تتطلب استخدام أي نوع من ميزات الأمان مثل كلمة المرور أو تسجيل الدخول، بينما تتطلب الشبكات الآمنة عادة موافقة المستخدم على الشروط والأحكام، أو تسجيل حساب، أو إدخال كلمة مرور قبل الاتصال بالشبكة.

8- قم بتشغيل جدار الحماية دائمًا.

إذا كنت تستخدم جهاز كمبيوتر محمول، فقم بتشغيل جدار الحماية أثناء استخدام شبكة Wi-Fi عامة. يعمل جدار الحماية كحاجز لحماية جهازك من تهديدات البرامج الخبيثة. قد يعطل المستخدمون جدار حماية Windows بسبب الشاشات المنبثقة والإخطارات ثم ينسون ذلك. إذا كنت تريد إعادة تشغيل جدار الحماية على كمبيوتر شخصي، فانتقل إلى لوحة التحكم، "النظام والأمان"، وحدد "جدار حماية Windows". إذا كنت من مستخدمي Mac، فانتقل إلى "تفضيلات النظام"، ثم "الأمان والخصوصية"، ثم علامة تبويب "جدار الحماية" لتمكين هذه الميزة.

9- استخدم برنامج مكافحة الفيروسات.

تأكد كذلك من تثبيت أحدث إصدار من برنامج مكافحة الفيروسات على الكمبيوتر المحمول الخاص بك. قد تساعد برامج مكافحة الفيروسات في حمايتك عند استخدام شبكة Wi-Fi عامة من خلال اكتشاف البرامج الخبيثة التي قد تصل لنظامك أثناء استخدام شبكة مشتركة. سيتم تنبيهك في حالة تحميل فيروسات معروفة إلى جهازك أو عند وجود نشاط أو هجوم مشتبه به أو عند دخول برنامج خبيث إلى نظامك.

10- استخدم المصادقة الثنائية أو متعددة العوامل.

استخدم المصادقة متعددة العوامل (MFA) عند تسجيل الدخول إلى المواقع الإلكترونية باستخدام بياناتك الشخصية. ويعني هذا تلقيك لرمز تحقق إضافي (يتم إرساله إلى هاتفك في رسالة نصية أو عن طريق تطبيق أو مفتاح فعلي) لتوفير المزيد من الحماية، وبالتالي، حتى في حالة حصول المخترق على اسم المستخدم وكلمة المرور، فلن يمكنه الوصول إلى حساباتك دون رمز المصادقة.

11- تتبع أجهزتك الشخصية.

لا تترك الكمبيوتر المحمول أو الجهاز اللوحي أو الهاتف الذكي الخاص بك دون مراقبة في مكان عام أو داخل سيارة، لن يمنع توخيك الحذر أثناء استخدام شبكة Wi-Fi أي شخص من سرقة ممتلكاتك أو استراق النظر إلى بياناتك. انتبه لمحيطك ولمن حولك.

12- نصائح أخرى للأمان على الإنترنت.

فيما يلي بعض نصائح للبقاء آمنًا أثناء اتصالك بالإنترنت، خاصة عند استخدام شبكة Wi-Fi عامة:

- استخدم كلمات مرور قوية.
- قم بتشفير أجهزتك.
- احذر من رسائل البريد الإلكتروني الاحتيالية.
- انتبه عند قيامك بالنشر على وسائل التواصل الاجتماعي، فتقديم الكثير من التفاصيل الشخصية يمكن أن يساعد المخترق في تخمين كلمات المرور.

- احذف البيانات القديمة التي لا تحتاجها بعد الآن.
- إذا طلبت منك شبكة تثبيت أي برامج إضافية أو ملحقات للمتصفح، فلا تتصل بها.
- تأكد من تثبيت أحدث تصحيحات وتحديثات البرامج على أجهزتك لحمايتها من المشكلات المعروفة.