**٥ من أجهزة إنترنت الأشياء البسيطة التي يمكن أن تصبح نقاط دخول للمتسللين**

على الرغم من ضخامة عدد الأجهزة والخوادم والشبكات المتصلة ببعضها، إلا أن الإنترنت لا زال في توسع دائم، وأحد مجالاته الكبيرة أثناء التوسع هو إنترنت الأشياء والذي سيشهد على توسع الإنترنت بشكل لم يسبق له مثيل في كل منزل والجانب السلبي هو أن هذه التكنولوجيا الجديدة يمكن أن تسمح أيضًا لبعض الغرباء غير المرغوب فيهم داخل المنزل.

لم يكن يٌنظر إلى الأثاث المنزلي التقليدي كبوابة للإنترنت، من كان يظن أنه قد يحتاج إلى محمصة متصلة بالإنترنت؟ ومن الواضح أن شخصًا ما أحتاج إلى ذلك لأنه موجود الآن بالفعل محمصة متصلة بالإنترنت!

من الضروري أم لا، أصبحت الأدوات المنزلية اليومية مثل الثلاجات والغسالات والكاميرات وأجهزة التلفاز وحتى الأفران جزءًا من إنترنت الأشياء. الغرض من إنترنت الأشياء هو منح المستخدمين وسيلة لمراقبة أجهزتهم والتحكم فيها عن بُعد. يمكن لبعض هذه الأجهزة التحدث مع بعضها البعض، لكن كل نقاط الاتصال هذه قد تصبح نقاط دخول محتملة للمتسللين الذين يجوبون الإنترنت.

تابع القراءة لترى لماذا يجب أن يكون هذا مصدر قلق لأي شخص يستخدم أو يخطط لاستخدام أجهزة إنترنت الأشياء في منزله.

**يمكن أن يؤدي استخدام أحد أجهزة إنترنت الأشياء الخمسة هذه إلى السماح للمتسللين بالدخول:**

إن استخدام هذه الأنواع الخمسة من أجهزة إنترنت الأشياء قد يسبب مخاطر في صورة التجسس والاستغلال والابتزاز والسرقة. لا تقتصر كل هذه الأمور على المجال الافتراضي أيضًا، ولكنها قد تتحول إلى تهديدات حقيقية.

**1. الكاميرات اللاسلكية:**

وضع الناس كاميرات خارج منازلهم لراحة البال ومع ذلك، فإن الكاميرا التي ترسل باستمرار لقطات عبر الإنترنت يمكن أن تصبح كارثة أمنية إذا تمكن المتسللين من الوصول إليها.

هذا التهديد يمثل مشكلة متنامية بين مالكي المنازل في جميع أنحاء العالم، هناك الآن مواقع ويب كاملة مخصصة لعرض البث المباشر من نظام كاميرات المراقبة الكامل (CCTV) مباشرة أو لقطات الكاميرا المنزلية من الكاميرات اللاسلكية المخترقة وكاميرات الويب.

**اتخذ هذه الاحتياطات عند استخدام أحد أجهزة إنترنت الأشياء:** تأكد من تغيير كلمة المرور الافتراضية عند شراء الكاميرا وأثناء إعدادها. غالبًا ما تكون كلمات المرور التي تأتي "مثبتة مسبقًا" مع الكاميرات بمثابة كلمات مرور عشوائية أو من السهل جدًا تخمينها. وقم بإعداد المصادقة الثنائية كطبقة أمان إضافية.

**2. أجهزة مراقبة الأطفال:**

تشكل أجهزة مراقبة الأطفال المتصلة بالإنترنت تهديدًا مشابهًا جدًا لتهديد الكاميرا المنزلية. حيث أنها تسمح للمتسللين بالتجسس على الأسرة أو الرضيع عن بعد ومع ذلك، لا يلتزم المتسللون دائمًا بالتجسس على ضحاياهم. كما أثبتت حادثة الاختراق التي تم إطلاق اسم "العش" عليها، والتي سمع فيها الأب صوت شخص غريب في غرفة طفله!

هناك تقارير متعددة عن اختراق أجهزة مراقبة الأطفال في المنازل في جميع أنحاء العالم وقد يكون للمتسللين أسباب مختلفة للدخول إلى هذه الأجهزة ولكن أيا كان سببها فإنها تعتبر حادثة مرعبة لا يريد أي من الوالدين المرور بها.

**اتخذ هذه الاحتياطات عند استخدام أحد أجهزة إنترنت الأشياء:** لا تعيد استخدام كلمات المرور في الأجهزة والحسابات، وضع في اعتبارك أنه غالبًا ما يتم اختراق العديد من أجهزة مراقبة الأطفال بسهولة.

**3. مساعد المنزل الذكي:**

يقترب السوق أن يمتلئ من مجموعة واسعة من مساعدين المنزل الذكي التي يتم تصنيعها من الشركات الكبرى ويعتبرون هؤلاء في طليعة التكنولوجيا المتطورة مثل أليكسا من أمازون أو مساعد جوجل الذكي والذين يزدادون شعبية بين أصحاب المنازل مع الوقت. ومع ذلك، فإن هذه الأجهزة ليست آمنة دائمًا كما أثبت الباحثون الصينيون مؤخرًا، في حين لم يتم الإعلان عن أي اختراق رئيسي لمساعدي المنازل الذكية حتى الآن، إلا أنها مسألة وقت فقط.

**اتخذ هذه الاحتياطات عند استخدام أحد أجهزة إنترنت الأشياء:** تصل الشركات إلى أبعد الحدود للتأكد من أن أجهزتها آمنة وأنه لا يمكن اختراقها لكن يجب على أولئك الذين يشترون مساعدًا منزليًا ذكيًا التأكد من أنهم يفعلون إعدادات أمان الجهاز وغالبًا ما يكون هناك الكثير من التدابير الأمنية الإضافية التي يمكن تفعيلها يدويًا ويجب أيضًا تحديث البرامج على هذه الأجهزة دائمًا.

**4. أجهزة تنظيم الحرارة المنزلية الذكية:**

قد يبدو الأمر وكأنه شيء من فيلم خيال علمي، ولكن يمكن للمتسللين (وقد قاموا بذلك) مهاجمة أجهزة تنظيم الحرارة المنزلية الذكية.

وجود درجة حرارة مرتفعة باستمرار أو منخفضة من قبل شخص متسلل هو أكثر من مجرد إزعاج ولا يمكن للمتسللين فقط قفل الأجهزة والمطالبة بفدية بل يمكنهم أيضًا الدخول إلى أجهزة أخرى وإحداث الفوضى.

**اتخذ هذه الاحتياطات عند استخدام أحد أجهزة إنترنت الأشياء:** من الصعب تتبع كل جهاز والتأكد من بقائه آمنًا وهنا يصبح تثبيت برنامج الشبكة الخاصة الافتراضية (VPN) مغير رئيسي في مجال الأمن السيبراني المنزلي.

حاول كتابة "ما هو عنوان بروتوكول الأنترنت (IP) الخاص بي" في محرك بحث (أو يمكنك التحقق منه على الفور [هنا](https://nordvpn.com/what-is-my-ip/)) ويكشف العنوان المعروض في الموقع تفاصيل مثل هوية الشخص وموقعه الفعلي.

يمكن للمتسللين العثور على عنوان بروتوكول الأنترنت الخاص بك واستخدامه لاستغلال أي من أجهزة إنترنت الأشياء غير المؤمنة التي تقوم باستخدام العنوان. سيساعد تثبيت برنامج الشبكة الخاصة الافتراضية على تأمين هذه المعلومات من خلال توفير عنوان مزيف من خلال خادم بعيد وتشفير الاتصال. يعد تثبيت برنامج الشبكة الخاصة الافتراضية على جهاز توجيه (Router) هو الخيار الأفضل في هذه الحالة لأنه سيحمي كل جهاز متصل به.

**5. أقفال الأبواب الذكية:**

أقفال الأبواب الذكية هي الأحدث في مجال أمن المنازل عالي التقنية وتأتي مع مجموعة من المميزات المفيدة. على عكس الأقفال التقليدية، فإنها تسمح لمالكي المنازل بمعرفة من هو على الباب والتحدث إليهم.

يمكن عادةً أن يتم إقفالها أو فتحها من أي مكان أيضًا ومع ذلك، على عكس الأقفال التقليدية فإن الأقفال الذكية عرضة للقرصنة والكسر دون أي مخاطر بالنسبة للمتسلل.

**اتخذ هذه الاحتياطات عند استخدام أحد أجهزة إنترنت الأشياء:** ابحث عن الشركة المصنعة ونوع القفل بشكل مكثف قبل شرائه وبمجرد تثبيته تأكد من تحديث البرامج المثبتة على الجهاز دائمًا وتغيير الرقم الذي على لوحة المفاتيح كثيرًا (إذا كان القفل يستخدم واحدًا). أخيرًا، لا تقم بتثبيت التطبيق الذي يفتح الباب على العديد من الأجهزة.

**كلمة أخيرة**

يمكن أن يكون الحصول على أحدث أدوات تكنولوجيا الأمان أمرًا مثيرًا للتكنولوجيا والمستخدمين الأوائل.

لا أحد يستطيع أن يجادل بحقيقة أن هذه الأدوات تضيف الراحة إلى حياة أصحابها ولكن لا يمكن تجاهل المخاطر المحتملة الملازمة لاستخدام الأجهزة المتصلة.

لن يتم إيقاف الهجمات المستندة إلى إنترنت الأشياء في أي وقت قريب، لذا تأكد من اتخاذ بعض الخطوات لتجنب الوقوع ضحية لهجوم إلكتروني.

**المرجع:**

<https://www.cpomagazine.com/cyber-security/5-simple-iot-devices-that-can-become-entry-points-for-hackers/>