أشياء عادية يمكن للقراصنة تتبعك من خلالها

ترجمة وتحرير: نون بوست

يعتبر عالم التكنولوجيا الحديثة عالمًا جذابًا ومثيرًا للاهتمام وقابلًا للتطور بصفة مستمرة، إذ دائمًا ما تظهر أجهزة جديدة قادرة على تسهيل حياتنا. ولكن في المقابل، تستمر الجرائم الإلكترونية في تعكير صفو حياتنا. فعلى سبيل المثال، لا يكتفي المتحيّلون والقراصنة بسرقة الحسابات المصرفية فقط؛ وإنما يراقبون أيضًا مستخدمي بطاقات الائتمان، ويحاولون اختراع طرق جديدة لتتبع ضحاياهم والتجسس عليهم.

المكانس الكهربائية

ساهم ظهور هذه الأجهزة المنزلية في تبسيط حياة ربات البيوت بشكل كبير، إذ لم يعد عليهن قضاء وقت طويل في تنظيف المنازل. ولكن يبدو أنه بات من الممكن استخدام هذه المكانس الكهربائية ضد أصحابها. فأثناء عملية التنظيف تقوم هذه الأجهزة بمسح كامل الغرفة ومختلف زوايا المنزل مما يمكنها من حفظ خريطته وتخزين البيانات في ذاكرتها.

فضلا عن ذلك، يسهّل وصل هذه الأجهزة مع أدوات إلكترونية أخرى من اختراقها من قبل القراصنة. أما إذا كان الهاتف الذكي أو الجهاز اللوحي المتصل بهذه المكانس الآلية، متصلا بوحدات التخزين السحابية فسيصبح من السهل على القراصنة الحصول على معلومات قيمة.

سماعة الرأس

يستخدم الجميع سماعات الرأس للاستماع إلى الموسيقى أو لإجراء محادثات على الهاتف المحمول، لكن لا أحد يعلم أن هذه الأدوات الصغيرة قد تجعل منك هدفا للتجسس. فمكبّرات الصوت والميكروفونات تعمل بنفس الطريقة، وفي حال كنت تستخدم سماعات الرأس فإنه من الممكن تهيئتها للعمل في وضع الميكروفون. وبهذه الطريقة، لا يحتاج القراصنة سوى لتثبيت برنامج ضار يسمى "سبيكر" على الحاسوب لاصطياد الضحية والتجسس على جميع محادثاتها في أي مكان من العالم.

السيارات

إن النماذج الحديثة للسيارات مزودة بالكثير من الإلكترونيات لتحسين وظائفها بشكل كبير. وتحتوي السيارات العصرية على تكنولوجيات قادرة على تسجيل البيانات والمعلومات المتعلقة بجميع المواقع والسرعة والطرق المفضلة التي يسلكها السائق. وترسل جميع هذه البيانات إلى خادم "أوتوماكر" الذي يُستخدم لدراسة اختيارات المستهلكين وسلوكياتهم بهدف تحسين جودة المنتجات التي يصنعونها. لكن من الممكن أن تقع هذه المعلومات بين أيدي القراصنة.

فرشاة الأسنان الكهربائية

تعتبر فرشاة الأسنان الكهربائية من الأدوات الذكية التي ظهرت منذ فترة في مراكز البيع والصيدليات. وسنة 2014، قدمت شركة "أورال بي" نموذجا ذكيا يدعم اتصال هذه الأدوات مع الهواتف الذكية عبر البلوتوث من خلال تطبيق خاص. ويمكن لهذه الفرشاة أن تراقب عملية تنظيف الفم وتقدم تقريرا كاملا يتضمن نصائح مفصلة حول كيفية العناية بالفم بشكل أفضل. ويمكن نقل هذه المعلومات لطبيب الأسنان للتمكن من مراقبة صحة الأسنان والاطلاع على المزيد من الإجراءات الوقائية والعلاجية. ولكن قد تُنقل هذه البيانات تلقائيا إلى الشركات المصنعة أو تقع بين أيدي القراصنة.

أليكسا

أشياء عادية يمكن للقراصنة تتبعك من خلالها

إيكاترينا بيتروف | نشر في ٥ مايو ٢٠١٩,

قامت شركة أمازون الأمريكية بتطوير المساعد الرقمي "أليكسا" لتبسيط عملية التسوق واستهداف فئات مختلفة من المستخدمين. ويراقب هذا البرنامج الرقمي سلوك الأشخاص ويحصل على معلوماتهم الشخصية. وقد تحول هذا البرنامج إلى خوارزمية تتيح للمستخدم التحكم فيها عن طريق الأوامر الصوتية. وبناء على تجربة المستخدمين، فإن هذا البرنامج قادر على نقل البيانات الحساسة مثل أرقام البطاقات المصرفية والمحادثات الخاصة، ما يجعل هذه المعطيات عرضة لخطر القرصنة عبر الإنترنت.

مصابيح الصمام الثنائي الباعث للضوء

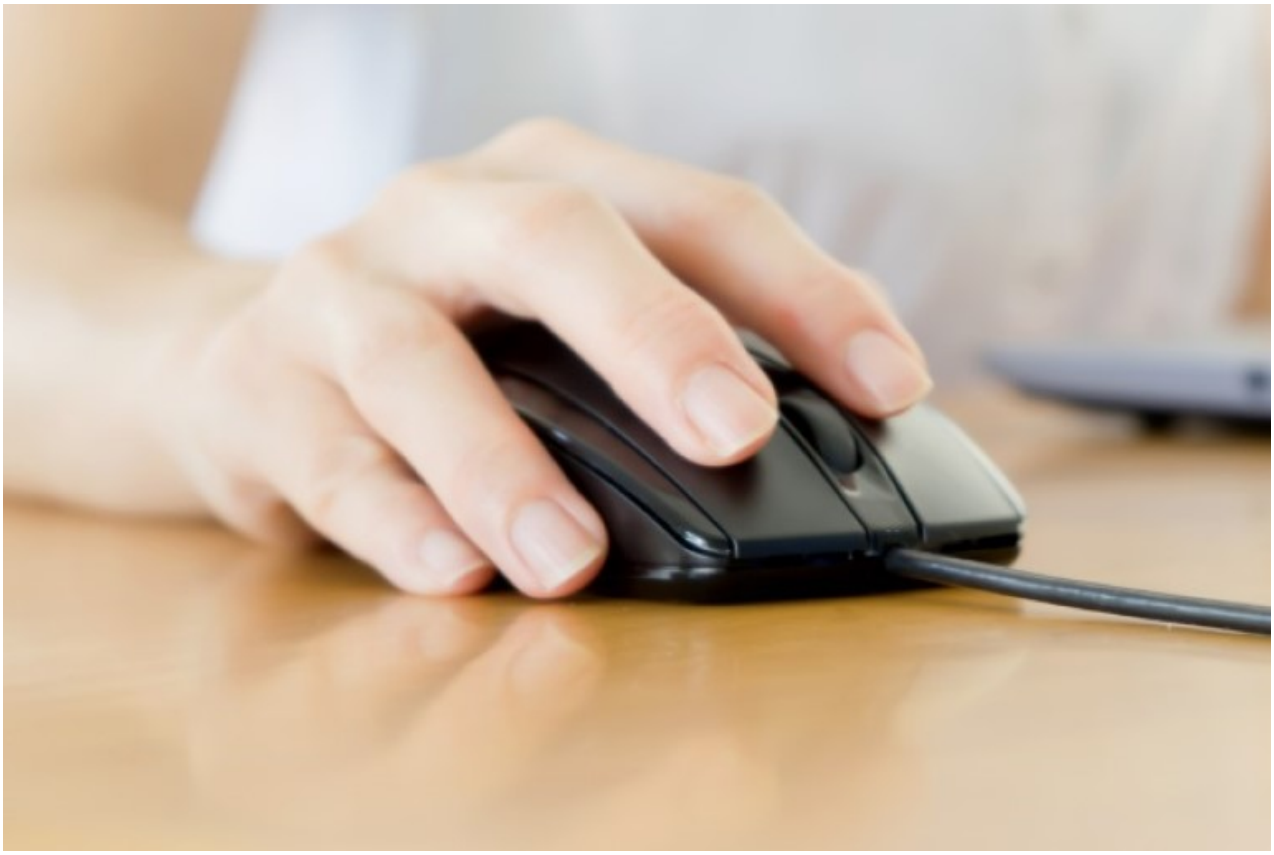
في الوقت الراهن، أصبحت تجهيزات الإضاءة العادية مصممة على تقديم أكثر من مجرد إضاءة. فعلى سبيل المثال، تم تجهيز محطة مطار نيوارك ليبرتي الدولي في نيو جيرسي بتجهيزات إضاءة متصلة بمجموعة متنوعة من أجهزة الاستشعار وكاميرات المراقبة لضمان أمن الركاب. ووفقا للمعلومات الرسمية، يتم استخدام هذه الأنظمة بشكل حصري لمراقبة الخطوط الطويلة وأرقام السيارات والأنشطة المشبوهة وغيرها من النشاطات الكثيرة الأخرى. وتخزن جميع هذه البيانات في أجهزة الاستشعار وكاميرات المراقبة على خوادم المطار مما يعني أنها قد تكون عرضة للقرصنة.

الألعاب

يحب الأطفال الدمى المتحدثة والروبوتات القادرة على القيام بحركات مختلفة وتقليد الأصوات. ويمكن لبعض الألعاب الذكية الاستجابة إلى الأصوات واتباع الأوامر، وقد تكون مجهزة بكاميرات فيديو وميكروفونات مدمجة ترسل المعلومات في بعض الأحيان إلى الشركات المصنعة.

لدى شركة جينيسيس معامل لتصنيع لعب الأطفال في كل من لوس أنجلوس وهونغ كونغ، وقد سجلت أجهزة أمن الشركة المصنعة عمليات تجسس على الناس. وقد تبين أن إحدى ألعاب هذه الشركة كانت تسجل المحادثات وترسلها إلى طرف ثالث، أي القراصنة، مما يعني أن هذا النوع من الألعاب فريسة سهلة للقراصنة. وفي وقت لاحق، قامت الشركة المصنعة بعدة إجراءات لحماية هذه الألعاب من الاختراق.

فأرة الحاسوب



لا يمكن لأحد أن يشك في أن أجهزة الحاسوب الخاصة بهم من الممكن أن تكون وسيلة للتجسس عليهم. ولكن تبين أن العديد من معدات الحاسوب مثل لوحة المفاتيح أو الفأرة قد تزيد من احتمالات التجسس عليك. ففي سنة 2012، تمكن صاحب عمل في سنغافورة من مراقبة ما يقوم به موظفوه من خلال تجهيز فأرة الحاسوب العادية بميكروفونات مدمجة وبطاقات سيم كارد يُمكن من خلالها تسجيل المحادثات التي تدور في دائرة قطرها 10 أمتار. لذلك من الضروري توخي الحذر نظرا لأن هذه الأداة البسيطة قد تكون أداة تجسس حقيقية.

كاميرات مراقبة المنزل

في سبيل ضمان أمنهم وحماية منازلهم من السرقة واللصوص يعمد الكثيرون إلى تثبيت أنظمة مراقبة بالفيديو في منازلهم. ولكن يمكن للمتسللين مراقبة أهل المنزل من خلال اختراق هذه الأجهزة. فضلا عن ذلك، يمكن لقراصنة الإنترنت تنزيل تسجيلات فيديو وصوت تلقائيا على الشبكة ومن ثم نقلها إلى خدمات التخزين السحابية. وهذا يعني أن هذه الكاميرات قد تشكل تهديدا خطيرا على خصوصية الأفراد.

الساعات الذكية

لقد ازدادت شعبية هذه الأجهزة مؤخرا. ومن بين جميع الأجهزة الإلكترونية، تعتبر الساعات الذكية وأجهزة تتبع اللياقة البدنية من بين أكثر برامج التجسس التي يعول عليها قراصنة الإنترنت. فهذه الأجهزة تُسجّل وتخزّن معلومات حول الممارسات التي يقوم بها الشخص والحركات البدنية المفضلة لديه. كما تظهر الإحصائيات أن القراصنة تمكنوا من سرقة كلمات المرور من جهاز حاسوب عبر الساعات الذكية بنسبة 94 بالمائة من مجمل الحالات، والرموز البريدية والبطاقات المصرفية بنسبة 87 بالمائة. وبناء على ما ذكر آنفا، فإنه لا بد من توخي الحذر من الأجهزة العادية التي نستخدمها بصفة يومية نظرا لأنها قد تكون سبيلا لمراقبتنا أو التحيل علينا.

المصدر: آف بي. ري

رابط المقال: https://www.noonpost.com/27646/