

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

في هذا العدد..

- ما المقصود بإترنت الأشياء (IoT)
- أبرز مشكلات إنترنت الأشياء
- حماية الأجهزة في إنترنت الأشياء

OUCH!

إنترنت الأشياء (IoT)

ما المقصود بإترنت الأشياء (IoT)؟

قبل عدة سنوات كانت التقنية نسيبًا أبسط من الوضع الحالي، كنت تقوم بوصول حاسبك الآلي بشبكة الإنترنت واستخدامه لإنجاز مهامك اليومية. مع تطور التقنية تحولت أجهزة الهاتف المتنقلة إلى هواتف ذكية وأنتشرت الأجهزة اللوحية بين الجميع. هذه الأجهزة لها نفس قدرة الحواسيب الآلية، ولكنها أصغر حجمًا لدرجة حملها في جيوبنا في كل مكان. مما جعل تقنيات «إنترنت الأشياء» (Internet of Things) من

المحرر الضيف

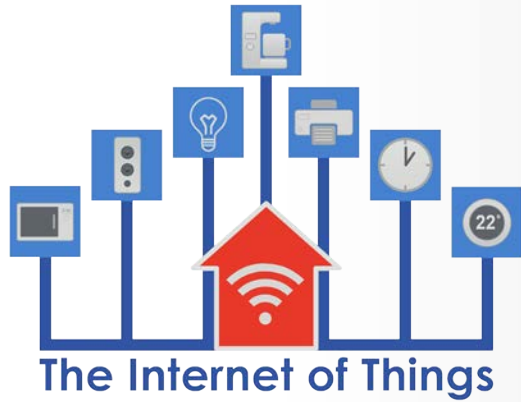
جايمس لين (@jameslyne) رئيس قسم أبحاث أمن المعلومات لشركة Sophos. يصف نفسه بـ «مهندس تقني» ، لديه خبرة واسعة في مختلف مجالات أمن المعلومات. وهو كذلك مدرب معتمد في معهد سانس ومحاضر رئيسي في العديد من ملتقيات أمن المعلومات.

أكبر التطورات التقنية مؤخرًا. إنترنت الأشياء وغالبًا تختصر بـ IoT ، هو كل ما يتعلق بإيصال أي جهاز بالإنترنت، بدءًا من جرس الباب والمصابيح الكهربائية حتى ألعاب الأطفال وأجهزة قياس الحرارة المنزلية. هذه الأجهزة المنزلية حين تربطها بالإنترنت ستجعل حياتنا أسهل، على سبيل المثال: تعرف المصابيح الكهربائية في منزلك على وجودك من عدمه من خلال التواصل مع هاتفك الذي عند قربك من المنزل! لذا فمنتجات إنترنت الأشياء في ارتفاع مذهل مؤخرًا، مع ظهور أجهزة جديدة بشكل أسبوعي. ولكن هذه الأجهزة صنعت تحديات أمنية جديدة وخاصة بإترنت الأشياء. في هذا العدد سنساعدك لفهم هذه المخاطر وحماية منزلك وأسرتك من خلال حماية أجهزة إنترنت الأشياء الخاصة بك.

أبرز مشكلات إنترنت الأشياء

أحد مميزات أجهزة إنترنت الأشياء أن معظم هذه الأجهزة بسيطة، فيمكنك ببساطة توصيل جهاز تحضير القهوة الخاص بك عند تشغيله سيطلب الجهاز الاتصال بشبكة الواي فاي الخاصة بك. ولكن هذه البساطة قد تتسبب في العديد من المشاكل الأمنية. حيث أن العديد من الشركات التي تصنع مثل هذه الأجهزة ليس لديها خبرة في أمن المعلومات، خبرتها تتركز في تصنيع الأجهزة المنزلية. أو ربما تسعى الشركة المصنعة لإنتاج جهاز يحقق لها أعلى ربح دون التركيز على الناحية الأمنية. كنتيجة لذلك، معظم أجهزة إنترنت الأشياء ضعيفة في جانب الأمن فمثلاً قد تكون كلمة المرور الخاصة بالجهاز هي نفسها لجميع الأجهزة المشابهة ولا يمكنك تغيير هذه الكلمة. وبالإضافة إلى ذلك، العديد من هذه الأجهزة لا يمكن تعديل أو ضبط الخيارات فيها، فعليك استخدامها بالاعدادات الأساسية من قبل الشركة المنتجة. مما يجعل الخطورة أكبر أن معظم هذه الأجهزة

إنترنت الأشياء (IoT)



اعرف أجهزتك المربوطة على الشبكة، قم بعزلها قدر الامكان، قم بتحديثها وحمايتها بكلمات مرور قوية.

لا يمكن تحديث برمجتها أو إعداداتها الأمنية حتى اذا تم اكتشاف ثغرة أمنية في تلك الاعدادات، ونتيجة لذلك سرعان ما ستصبح العديد من هذه الأجهزة غير آمنة بسبب نقاط ضعف معروفة لا يمكن إصلاحها وتترك مستخدمها عرضه للاختراق بشكل دائم.

حماية الأجهزة في إنترنت الأشياء

ماذا يمكن أن نفعل لنحمي أنفسنا من هذه المخاطر؟ نحن بالتأكيد نريد الاستفادة من مميزات إنترنت الأشياء بشكل آمن وفعال. يمكن أن توفر هذه الأجهزة ميزات رائعة تجعل الحياة أكثر بساطة، توفير المال، وربما تزيد من الأمن المادي لمنزلك. باضافة إلى ذلك، ربما تصبح جميع الاجهزة مستقبلاً تستخدم إنترنت الأشياء. فإليك بعض الإحتياطات التي يمكنك اتخاذها لحماية نفسك واجهزتك.

قم بتوصيل ما تحتاجه فقط: ببساطة أفضل طريقة لتأمين

أجهزة انترنت الاشياء هي عدم ربطها بالإنترنت اذا لم يكن هنالك حاجة لربطها.

نقطة وصول لاسلكية Wi-Fi منفصلة: اذا كنت بحاجة لربط أجهزة انترنت الأشياء بالإنترنت، قم بإنشاء نقطة وصول لاسلكية Wi-Fi

منفصلة خاصة بهم. العديد من وحدات الوصول Wi-Fi بها خصائص تسمح بإنشاء نقاط وصول Wi-Fi محمية ومغلقة. الخيار الاخر هو شراء نقطة وصول لاسلكية Wi-Fi فقط لأجهزة انترنت الأشياء. ذلك يحمي هذه الأجهزة ويبقيها معزولة عن الأجهزة الأخرى.

التحديث كلما كان ممكناً: تماما مثل أجهزة الحاسوب والأجهزة المحمولة، ابقى أجهزة انترنت الأشياء محدثة أولاً بأول. إذا كانت أجهزة

انترنت الأشياء تمتلك خاصية التحديثات التلقائية قم بتفعيلها.

كلمة مرور قوية: قم بتغيير كل كلمات المرور الافتراضية في أجهزة انترنت الأشياء الي كلمات قوية، فريدة لا أحد يعلمها سواك. انت لا

تذكر جميع كلمات المرور الخاصة بك؟! لا تقلق حتى نحن لا نستطيع ذلك. قم باستخدام إحدى برامج إدارة كلمات المرور لحفظها وتأمينها بشكل كامل.

خيارات الخصوصية: إذا كانت أجهزة انترنت الأشياء الخاصة بك تدعم خيارات الخصوصية، قم بالحد من كمية المعلومات التي تشارك بها.

الأفضل ان تقوم بتعطيل خيار مشاركة المعلومات للحفاظ على خصوصيتك.

إنترنت الأشياء (IoT)

استبدال الجهاز: في مرحلة ما قد ترغب في استبدال جهاز إنترنت الأشياء إذا أصبح به كثير من الثغرات الأمنية المعروفة والتي لا يمكن إصلاحها. دائما يمكنك استبدالها بأجهزة أحدث لديها إمكانيات وخصائص أمنية أفضل.

لا يوجد إجراءات موحدة لجميع الأجهزة، لذلك من الأفضل اتباع أفضل الممارسات والمنشورات الخاصة بالأجهزة لتأمينها. للأسف معظم أجهزة إنترنت الأشياء لم يتم تطويرها لمواجهة هجمات القرصنة، والكثير من مزودي الخدمات لا يقدمون الكثير لأمن المعلومات. لكن مع ازدياد الوعي بأهمية أمن المعلومات، نحن نأمل أن نرى المزيد والمزيد من مقدمي خدمات أجهزة إنترنت الأشياء يبنون أنظمتهم على تقنيات آمنه وتوفير المعلومات حول كيفية حمايتها وتحديثها.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة

<http://www.securingthehuman.org>

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_aa.pdf

<https://securingthehuman.sans.org/ouch/2015#october2015>

<https://securingthehuman.sans.org/ouch/2016#january2016>

http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_aa.pdf

عدد أوتش "عبارات المرور":

عدد أوتش "إدارة كلمات المرور" باللغة الانجليزية:

عدد أوتش "تأمين الجهاز اللوحي الجديد" باللغة الانجليزية:

عدد أوتش "حماية شبكة المنزل الخاصة بك":

أوتش! تنشر من قبل برنامج «سانس» لحماية الإنسان ويتم توزيعها بموجب الرخصة [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو استخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الاتصال على: ouch@securingthehuman.org

مجلس التحرير: بيل وإيمان، والت سكرين، فيل هوفمان، لانس سيستسر، كارمن رويل هاردي، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين، محمد سرور، زياد الشهري.



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](https://www.securingthehuman.org/gplus)