



نشرة الوعي الأمني الإخبارية الشهرية للجميع

## أجهزة المنزل الذكية

### أجهزة المنازل الذكية أو ما يعرف بإترنت الأشياء (IoT)

إن عدد الأجهزة المتصلة بالإنترنت سابقا كان محصوراً على أجهزة الكمبيوتر المحمول، الهواتف الذكية أو أجهزة التحكم بالألعاب. ولكن اليوم فإن كل أجهزة المنزل أصبحت متصلة بالإنترنت على سبيل المثال لا الحصر بدءاً من المصابيح، مكبرات الصوت، التلفاز، أقفال الأبواب الذكية، وأيضاً السيارات. يطلق على الأجهزة المتصلة بالإنترنت مسمى إنترنت الأشياء (IoT) أو أجهزة المنزل الذي. بقدر ما توفره هذه الأجهزة المتصلة من الراحة، فإنها تجلب أيضاً مخاطر أمنية جديدة.

### اذن ما المشكلة؟!

كلما زاد عدد الأجهزة المتصلة بشبكة الإنترنت، زادت المخاطر الأمنية. بحيث يستطيع الهاكر (قراصنة الإنترنت) استخدام هذه الأجهزة إما في مساعدته باختراق أجهزة أخرى، أو أن يتم اختراقها وتعطيلها عن الخدمة، كما يستطيع منتج هذه الأجهزة جمع معلومات تفصيلية عن الأنشطة التي تقوم بها. ونظراً لأن العديد من الشركات المصنعة لأجهزة إنترنت الأشياء لا تمتلك خبره في مجال أمن الفضاء الإلكتروني (cyber security) ونظرتها المادية تجاه توفير الاحتياجات الأمنية لهذه الأجهزة تتج عن ذلك توفر القليل من الاحتياطات الأمنية أو عدم توفرها أصلاً. وعلى سبيل المثال فإن بعض الأجهزة تحتوي على كلمات مرور افتراضية معروفة جيداً أو لا يمكنك تغيير الإعدادات الافتراضية لها لتصبح سهلة الاختراق.

### كيف احمي نفسي

إذاً ما الذي يمكنك فعله؟ بالتأكيد نحن نريدك ان تستفيد من الأجهزة المتصلة بالإنترنت الاشياء بصورة آمنه ومحميه، فاستخدام هذه الأجهزة سيوفر لنا مزايا رائعة الامر الذي يجعل حياتنا أسهل. أضف الى ذلك ان هذه التقنية تتطور سريعاً الامر الذي سيجعلنا بمرور الوقت لا نملك خياراً إلا أن نتعامل مع الأجهزة الذكية المتصلة بالإنترنت الاشياء. اليك بعض الخطوات الأساسية التي يمكنك اتباعها لتحمي نفسك:

**اربط الأجهزة التي تحتاج فقط، بالشبكة:** ان أسهل الطرق لحماية الأجهزة هي عدم ربطها بالإنترنت. فما دمت لست بحاجة لأن يكون جهازك على الإنترنت، فببساطه تجنب ربطه بالشبكة اللاسلكية Wi-Fi في بيتك. ترى هل يهيك حقيقة ان يقوم جهاز تجميع الخبز ان يرسل لك تنبيهها على جوالك؟!

**كن على دراية بالأجهزة المتصلة:** اي الأجهزة في البيت قمت بربطها بشبكتك المنزلية؟ لست متأكداً او لا تتذكر؟ حسناً، قم بفصل نقطه الاتصال بالشبكة اللاسلكية وتفقد الأجهزة التي ما عادت تعمل. قد لا تضمن هذه الطريقة كشف كل الأجهزة المتصلة لكنك في النهاية ستفاجئ بعدد الأجهزة التي قمت بربطها ونسيت ذلك بمرور الوقت.

**ابقها محدثة على الدوام:** كأي جهاز حاسوب أو جوال، إنه من الضروري جدا ابقاء انظمته التشغيل المدمجة في اجهزتك محدثة باخر الاصدارات. لذلك ان كانت اجهزتك تتيح تحديث انظمتها اوتوماتيكياً فندعوك للتأكد من تفعيل هذه الخاصية.



**كلمات المرور:** لا تتوانى أبدا عن تغيير كلمة المرور الافتراضية على أجهزتك، قم باستبدالها بكلمة مرور فريدة وقوية لا يعلمها غيرك. عادة هذه العملية لن تحتاج للقيام بها أكثر من مره واحده. لكن هناك مشكله! ألا تستطيع تذكر كلمات المرور الكثيرة لكل هذه الأجهزة؟ معك حق، ولا حتى نحن!، لذا نقترح عليك استخدام أحد برمجيات ادارة وحفظ كلمات المرور لتسهيل هذه المهمة.



**خيارات الخصوصية:** ان كانت الأجهزة تتيح لك اعداد خيارات الخصوصية، فقم بتحديد كم البيانات التي تقوم بجمعها ومشاركتها من المستخدمين. نقترح عليك ان تقوم بتعطيل الخيار الذي يسمح بإتاحة او مشاركة المعلومات.



**المصنّعين والباعه:** احرص دوما على شراء المنتج من شركات تثق بها وتعرفها. ابحث دائما عن المنتج الذي يدعم خصائص الامان والتحديث المستمر للمنتج. كأن يتيح نظام تشغيل الجهاز ميزه التحديثات الآلية علاوة على امكانيه تعديل كلمات المرور وتخصيص اعدادات الخصوصية.



**التصنت الدائم:** ان كان الجهاز يتحسس صوتك بصوره دائمة كجهاز اليكسا او جوجل هوم، اللذان يمكنهما تسجيل محادثاتك الحساسة في اي وقت. فعليك ان تقرر بناء على ذلك مكان تواجد هذا النوع من الأجهزة في بيتك مع مراجعه خيارات الخصوصية فيها.



**الشبكات المعزولة (شبكة الضيوف):** حاول استضافه وربط اجهزه المنزل الذكية على شبكات معزولة عن الشبكة الأصلية في بيتك او في مكان العمل والتي تربط عليها عادة اجهزه الكمبيوتر والجوالات المحمولة. بهذه الطريقة تكون قد عزلتها تماما في حال اخترق اي منها او اصابه فايروس فلن يؤثر على الشبكة الأصلية مما يضمن ابقائها آمنة.



ليس هناك من سبب يجعلك تخشى من التقنيات الحديثة لكن يتعين عليك ان تتفهم المخاطر التي قد تشكلها. هذه الخطوات القليلة والبسيطة سابقه الذكر يمكنها ان تساهم في بناء بيت ذي أكثر أمانا.



## الضيف المحرر

روبرت لي Robert M. Lee (@RobertMLee) هو الرئيس التنفيذي ومؤسس لشركة دراجوس لأمن الفضاء الالكتروني والصناعي كما يعمل أيضا مدرس معتمد لمؤسسة SANS و مؤلف لمحتوي دورة تدريبية بعنوان FOR578 متخصصة في تهديدات الفضاء الالكتروني إضافة لدورة تدريبية بعنوان ICS - ICS515 متخصصة في مجال الدفاع والاستجابة للحوادث.

## مصادر إضافية

[https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704\\_aa.pdf](https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_aa.pdf)

[https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709\\_aa.pdf](https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_aa.pdf)

[https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201602\\_aa.pdf](https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201602_aa.pdf)

عبارات المرور (باللغة العربية):

تطبيقات إدارة كلمات المرور (باللغة العربية):

حماية شبكة المنزل الخاص بك (باللغة العربية):

OUCH! من قبل فريق الوعي الأمني في SANS وتُوَزَع بموجب Creative Commons BY-NC-ND 4.0. يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو إستخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter) | المجلس التحريري: والت سكريفنز، فل هوفمان، كاثي كليك، شيريل كوني | ترجمها إلى العربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكردي