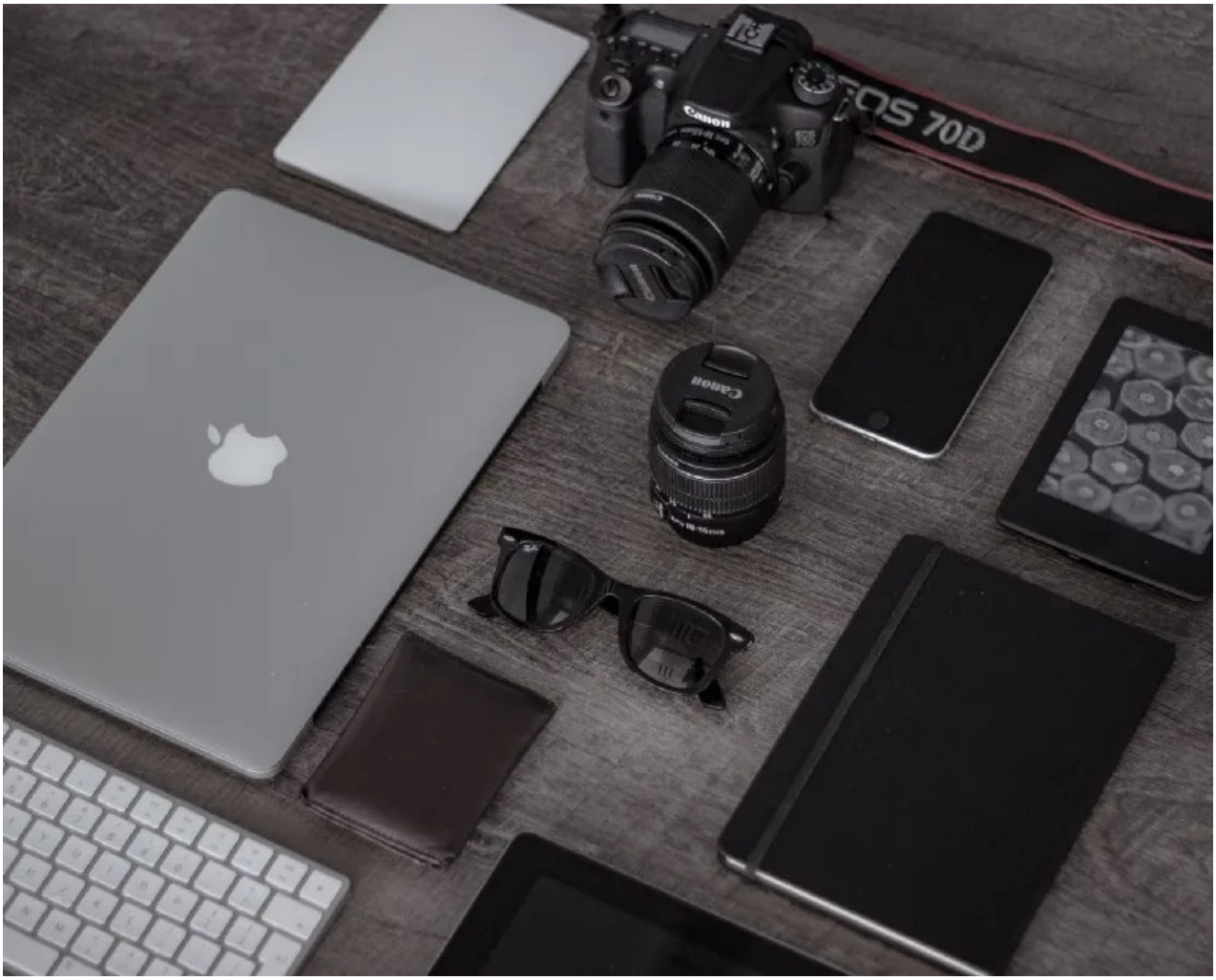
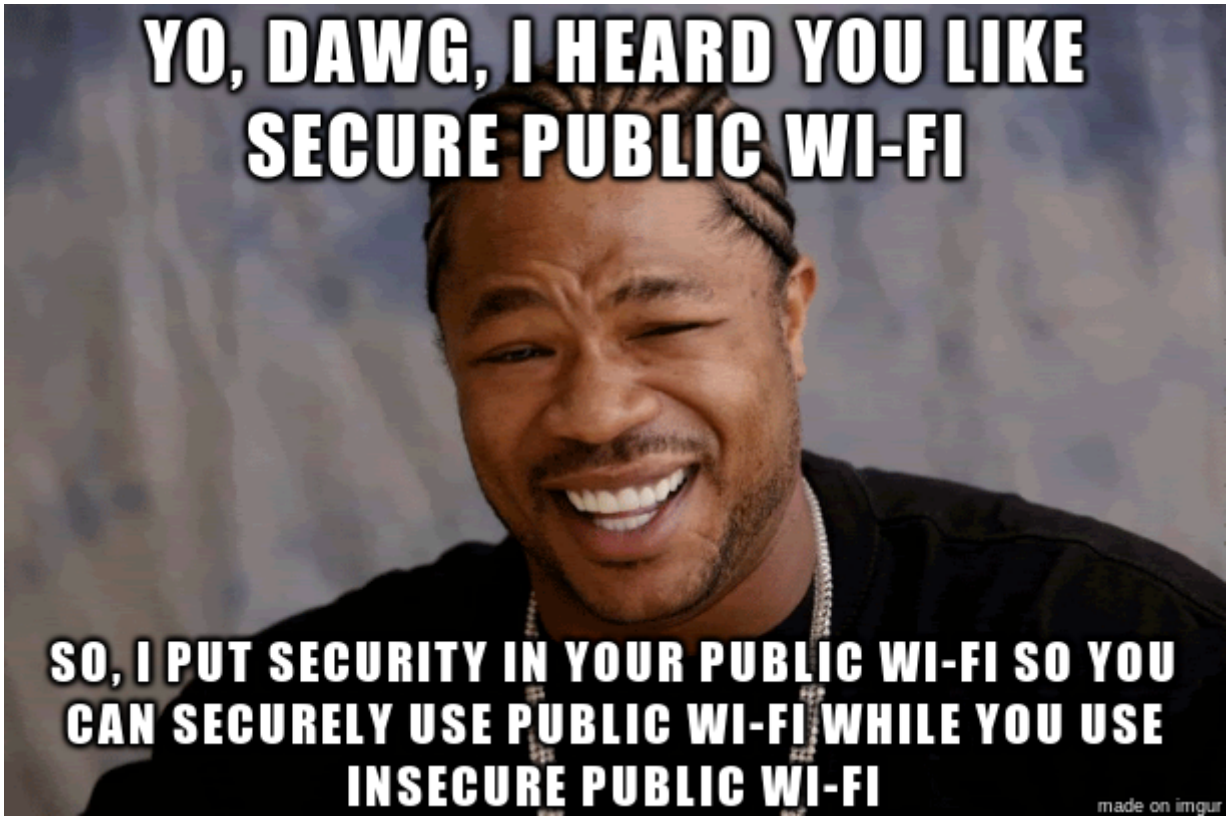
هكذا تحمي خصوصيتك عند الاتصال بشبكات الواي فاي العامة!



ترجمة وتحرير نون بوست

إنّ شبكات الواي فاي التي نتصل بها والمواقع التي نزورها بالإضافة إلى البروتوكولات التي نستخدمها قد تفشل أحيانًا في حماية بياناتنا على الإنترنت. ونتيجة لذلك، ينبغي على كل فرد اتخاذ إجراءات وقائية لاستخدام الإنترنت بشكل آمن.



هذا هو الجزء الثالث من سلسلتي حول انعدام الأمن على شبكات الواي فاي العامة.

وقد تطرّق الجزء الأول إلى مخاطر الاختراق المرتبطة بشبكة الواي فاي العامة، في حين مثل الجزء الثاني نظرة عميقة لما وصلنا إليه اليوم.

ابدأ بحالة أمن معروفة:

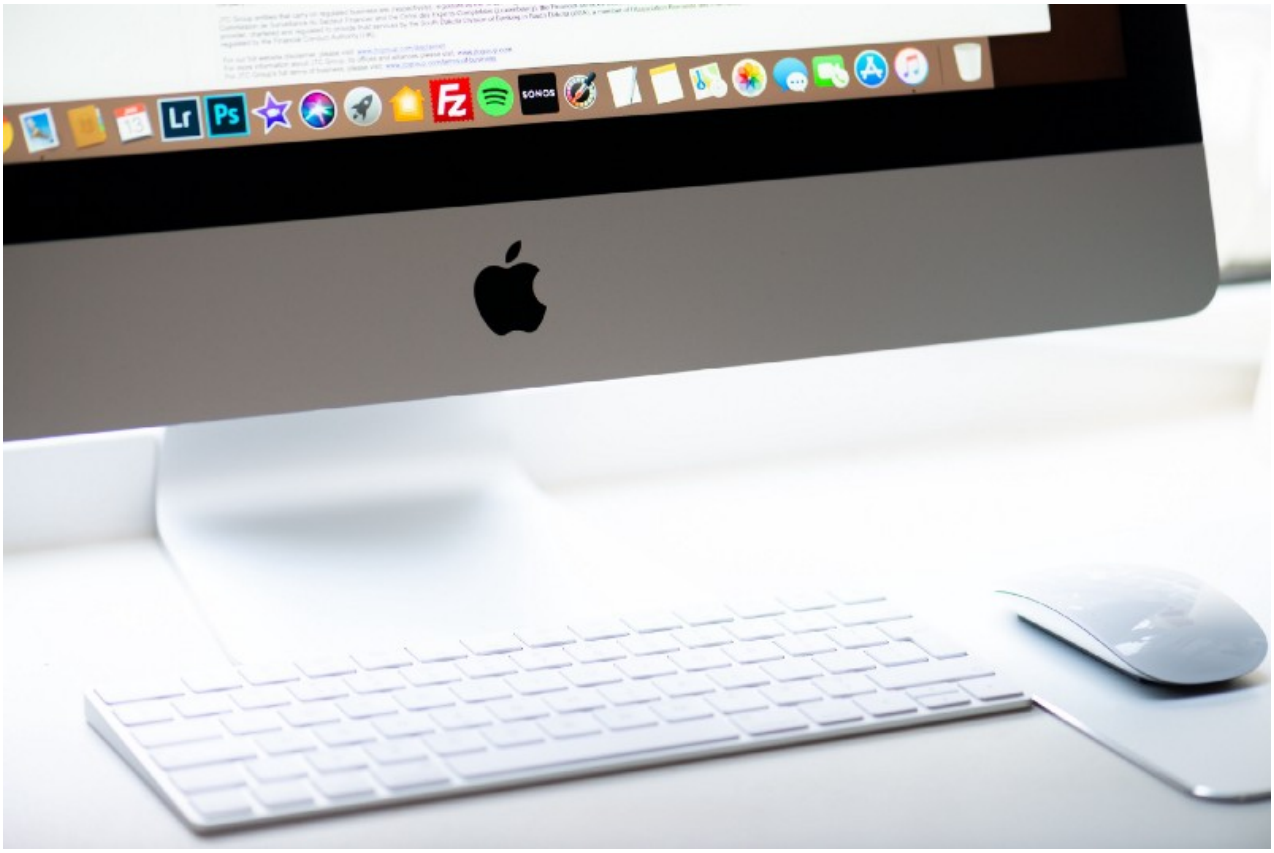
ينبغي أن يكون النفاذ إلى الإنترنت آمنا بشكل عام حتى يكون استخدامك لشبكة الواي فاي العامة آمنًا أيضًا. لذلك، فأنت تحتاج على الأقل إلى:

استخدام حسابات على شبكة الإنترنت تكون متأكدًا من أنها لم تتعرّض للاختراق.

استعمال كلمات مرور قوية وعدم استخدامها لأكثر من مرة.

تطبيق خاصية التحقق المزدوج في جميع حساباتك.

نظرًا لسهولة إعادة تحويل مسار الرسائل النصية بسهولة نحو هاتف المخترق، فإنه لا ينبغي في هذه الحالة استخدام هذه الخاصية في الرسائل النصية القصيرة. ولن يكون هناك ضرر في اتخاذ احتياطات إضافية، على غرار تمكين إنذار تسجيل الدخول لحساباتك المالية أيضًا.



في ظل وجود العديد من التطبيقات المثبتة، يزيد احتمال المخاطر في الوقت الذي تمنح فيه ثقتك للمطورين وممارسات البرمجة.

ابق دائما على اطلاع

يجب إصلاح المشاكل المتعلقة بأيقونات متصفحات الويب، ومواطن الضعف الموجودة في تي إل إس/إس إس إل، مع ضرورة الاطلاع على بروتوكول استيثاق شبكة الواي فاي، ونقاط الضعف في التطبيق ونظام التشغيل قبل الاتصال بشبكات إنترنت أخرى.

هذا يؤكد مدى أهمية تحديث أنظمة التشغيل ومختلف التطبيقات الموجودة في جهازك، ناهيك عن تحديث جميع الأجهزة الإلكترونية الأخرى، على غرار أجهزة التوجيه وآلات الطباعة والأجهزة الذكية، حيث يمكن أن تكون متجهات هجوم للأجهزة الأخرى و/ أو الحسابات الإلكترونية. وبعد تثبيت التحديثات اللازمة، من الضروري إعادة تشغيل التطبيقات على غرار متصفح الويب. وقد يتطلّب الأمر في بعض الأحيان إعادة تشغيل جهاز الكمبيوتر بالكامل في حال قمت بتحديث نظام التشغيل لتطبيق هذه التحديثات.

يمكن أن يشكّل سطح الهجوم المكشوف بشكل غير ضروري خطرا محدقا على الأجهزة والتطبيقات.

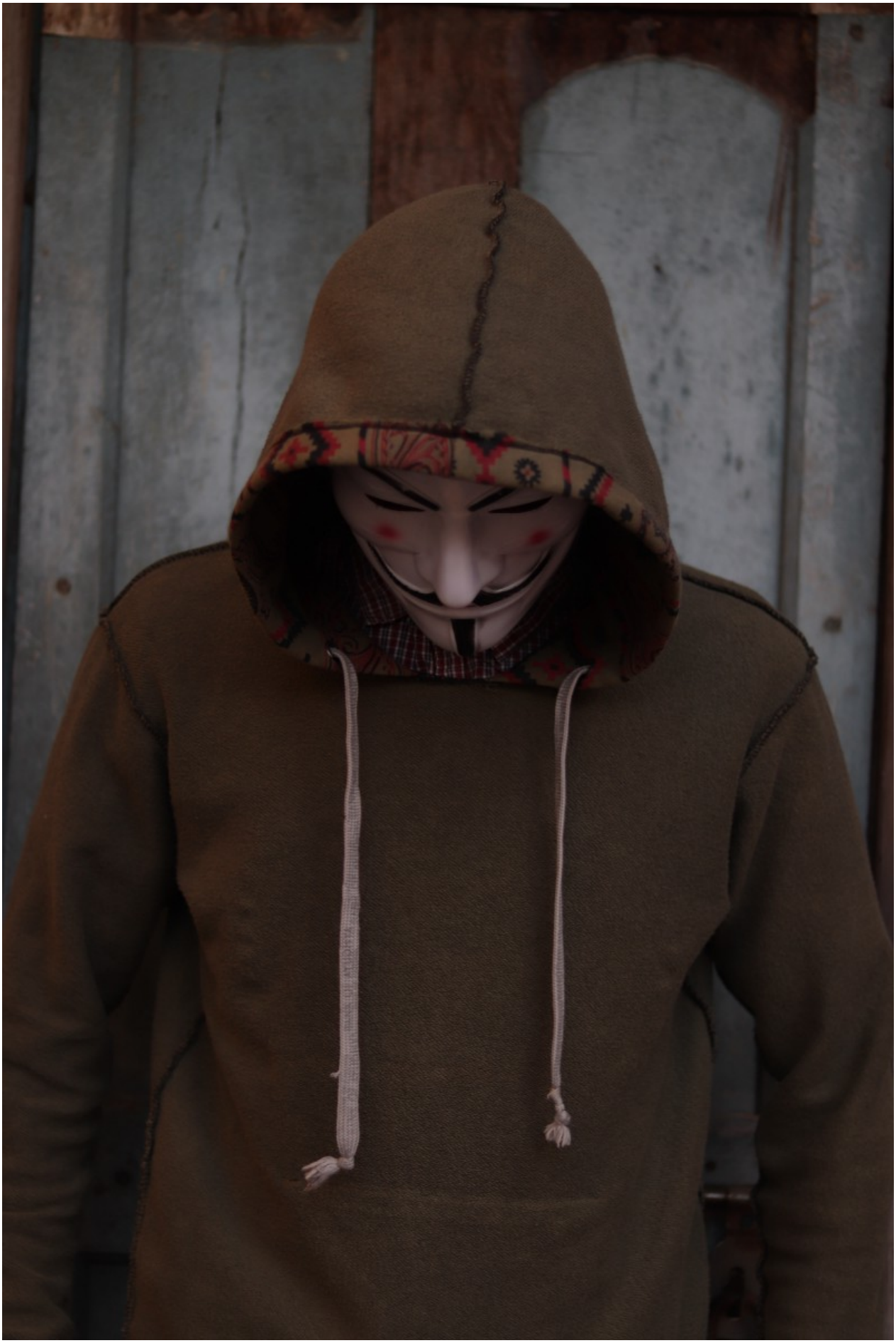
احتو سطح الهجوم في جهازك

قبل الاتصال بشبكة إنترنت عامة، يجدر بك في البداية التفكير في كيفية حماية الكمبيوتر من الهجمات، حيث ينبغي عليك التأكّد من عدم استخدام خدمات زائفة أو مشاركة ملفات على جهاز الكمبيوتر، إلى جانب التأكّد من تثبيت جدار الحماية وضبطه بشكل صحيح.

يعد الحدّ من عدد التطبيقات المثبتة وإلغاء تثبيت التطبيقات غير المستخدمة خطوة إضافية من شأنها التقليل من احتمال ترك ثغرة أمنية، تُعرف باسم سطح الهجوم. ومن الأفضل الاحتفاظ بقائمة غير متصلة بالإنترنت تحتوي على جميع حساباتك تفاديا لنسيانها أو نسيان المعلومات المرتبطة بها، ومراجعة قائمة الحسابات التي لم تعد تستخدمها وإلغاء تنشيط الحسابات غير الضرورية.

هكذا تحمي خصوصيتك عند الاتصال بشبكات الواي فاي العامة!

باتريك ف. | نشر في ٧ يونيو ٢٠١٩,



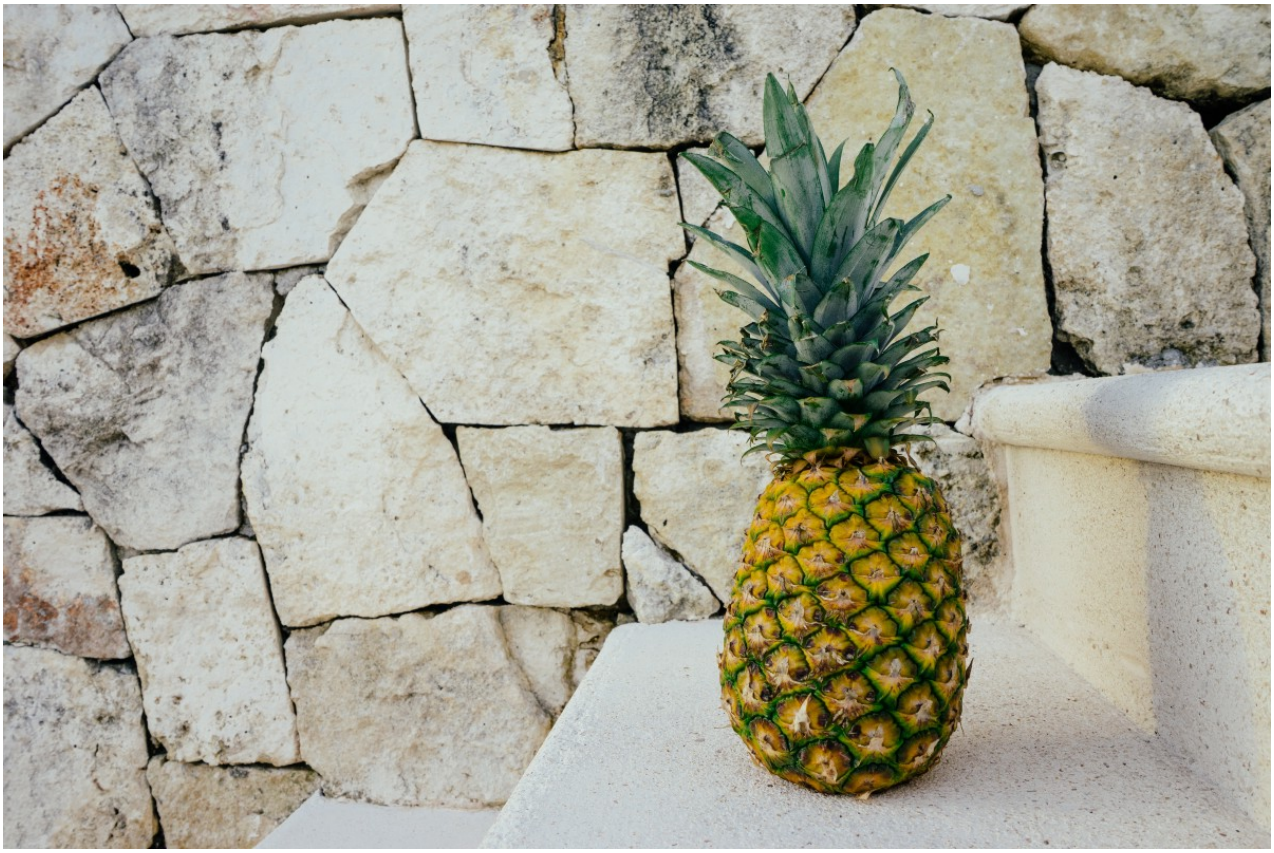
لا أحد يعلم من وراء هذا القناع، هل هو مخترق أم مدافع عن الخصوصية، أو كلاهما، أو لا أحد منهما.

منع الاعتراض

قبل الاتصال بشبكة عامة، يجب عليك اتخاذ إجراءات مضادة لمنع اعتراض بيانات التطبيق، وذلك عن طريق العثور على شبكة خاصة افتراضية موثوقة وتثبيتها وتهيئتها بشكل صحيح بحيث يمكن تشغيلها على الفور دون تسريب أي حزم خاصة بالبروتوكولات (على غرار طلبات نظام أسماء النطاقات). علاوة على ذلك، لا بد من تحميل الشبكة الخاصة الافتراضية قبل الاتصال بشبكة واي فاي عامة باعتبار أنه لا يمكن الوثوق بها لتنزيل برمجيات لا تحتوي على برامج ضارة.

الاتصال بشبكة مناسبة

تستخدم العديد من الشبكات العامة بوابة إلكترونية التي إما تحتوي على شروط الاستخدام أو تُجمّع المعلومات حول مستخدميها. ولسوء الحظ، إذا اختار عدد كبير من المستخدمين استعمال إحدى الشبكات الخاصة الافتراضية، فينبغي حينها تعطيلها حتى تكون قادرا على اختراق البوابة والاتصال بالإنترنت. وبإمكان هذه البوابات إبطال فوائد الشبكة الخاصة الافتراضية، ناهيك عن وجود آثار تتبع محتملة في حال تم تعيين ملفات تعريف الارتباط خلال هذه العملية.



يمكنك الاتصال بموجّهات واي فاي أناناس لكن مع مشكلة تتمثل في وجود مخاطر تتعلق بالأمان والخصوصية.

تجنب الاتصال بشبكة واي فاي أناناس

على الرغم من أن شبكة واي فاي أناناس تعد بمثابة موجّهات يمكن الاتصال بها بسهولة، إلا أنها تُستخدم كوسائل اختراق خبيثة تتوارى خلف ستار شبكات إنترنت حميدة. وفي حال كان جدار الحماية والشبكة الخاصة الافتراضية يعملان بشكل مثالي، فلن تكون شبكة واي فاي أناناس قادرة على اختراق

جهازك. في المقابل، لا بد من توخي الحذر إذ يمكن أن تأخذ إحدى الشبكات الضارة بسهولة شكل شبكة شرعية، التي من الممكن أن تحتوي بدورها على عناصر ضارة مرتبطة بها.

استخدام البرامج المساعدة في المتصفح لإصلاح ثغرات أمان الويب

يتم زيارة 25 بالمئة من المواقع الإلكترونية، التي تتعقب عائلتك، دون استخدام التشفير. فضلا عن ذلك، توجد امتدادات خاصة بالمتصفح على غرار "إتش تي تي بي إس في كل مكان" التي من شأنها أن تساعدك على تصفح شبكة الإنترنت. بالإضافة إلى ذلك، من الممكن أن تساهم هذه الامتدادات بشكل أفضل في عزل المواقع وبياناتها عن بعضها البعض، فضلا عن منع بعض أجهزة التتبع عبر الإنترنت.

لا أوصي بشدة باستخدام هذه الامتدادات لجميع مواقع الويب التي تقوم بزيارتها. وفي حال كنت عضوا في مجموعة معرضة للخطر، على غرار أن تكون ناشطا أو مراسلا أو رجل أعمال غني، فيمكنك الاستفادة من الفصل بين مختلف الأنشطة على الإنترنت باستخدام أجهزة منفصلة ومخصصة للأنشطة الحساسة، خاصة وأنه لا وجود لاحتواء افتراضي من شأنه أن يكون أفضل من الفصل المادي.

فهم وتحسين نموذج التهديد الخاص بك

لكل شخص نموذج تهديد مختلف تُحدده ظروف مختلفة:

ما هي الأعمال الأكثر قيمة بالنسبة لي؟

ما هي الأماكن التي قد أكون فيها أكثر عرضة للهجوم؟

ما هي التهديدات التي من المرجّح أن تواجهني؟

اسأل نفسك باستمرار: ما الذي يمكنني فعله للحد من التهديدات وعيش حياتي وأنا أكثر وعيًا بالأمان والخصوصية؟

إلى جانب ذلك، عليك أن تسأل نفسك: هل لدي ظروف خاصة (في حال كنت مراسلًا يحتاج إلى عدم الكشف عن هويته، أو مديرا تنفيذيا ملياردير لديه حق الوصول إلى بعض الحسابات المصرفية الضخمة)؟ إذا كان الأمر كذلك، فاحرص على الاطلاع على إجراءات المراقبة والدفاع عن النفس التي توفرها مؤسّسة الجبهة الإلكترونيّة، وكذلك وسائل إخفاء الهوية إذا لزم الأمر. ففي الواقع، يتطلب البقاء في مأمن على الشبكات العامة وشبكات الإنترنت توفير التوعية واتخاذ الإجراءات اللازمة.

خلاصة

يجب عليك، كحدّ أدنى، استخدام الشبكة الخاصة الإفتراضيّة الموثوقة، واستخدام خاصيّة الاستيثاق بعاملين في كل مكان (ولكن ليس عبر الرسائل القصيرة)، إلى جانب تثبيت الامتداد الإضافي للتصفّح، "إتش تي تي بي إس في كل مكان"، وتحديث نظامك باستمرار. وفي حال لم تكن تتبع هذه الإجراءات، فربما يجب عليك إعادة النظر في وضعك الأمني. وإذا بدا هذا الوضع وكأنه مخصص وصعب ومن غير المرجح أن يحميك تمامًا عبر الإنترنت، ولا حتى يمنحك تجربة مستخدم جيدة بشكل معقول، فأنت على حقّ تماما لسوء الحظ.

في وظيفتي اليومية في "ماجيك"، نعمل بنشاط على حل هذه المشكلات من خلال تطبيق وظائف وقدرات تختصّ في أمن الإنترنت بشكل افتراضي، مع إيلاء أهميّة لتجربة المستهلك. ولكن في الوقت الحالي، لا يمكنك الوثوق بشبكات الإنترنت المشتركة وشبكة الواي فاي العامة. كما أخفقت المواقع والبروتوكولات الشعبية في أداء دورها في حمايتنا بشكل كاف، وبالتالي يتعين على المستهلكين البحث بمفردهم في مجالات أمن الإنترنت إلى حدّ كبير.

المصدر: هاكر نون

رابط المقال: https://www.noonpost.com/27987/