الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

التلفزيون الذكي.. الرفاهية مقابل الخصوصية

انتشرت في الآونة الأخيرة التلفزيونات الذكية التي منحت المشاهد الكثير من المزايا فلم يعد التلفاز مجرّد الشاشة الكبيرة وجهاز التحكم عن بعد فقد أصبح هناك الكثير من أوجه التشابه بينها وبين الحواسيب فنظام التشغيل ربما يكون «Windows» أو «MAC» في الحاسبات، بينما في التلفزيونات الذكية «Android» أو «IOS»، وأيضاً المعالج الدقيق الذي ربما يكون من الفئة والجيل نفسيهما في الحالتين، إلى جانب شرائح الذاكرة الالكترونية (RAM) التي تتطابق أيضاً في الحالتين (من حيث الفئة والبنية الهيكلية لكن تختلف من حيث الطراز) وهناك وحدة التخزين وهي عامل مشترك كامل بين الجهازين، وكذلك خط اتصال بالإنترنت ربما يكون مباشرة عبر «كابلات» النطاق العريض مثل «DSL» وغيرها، أو من خلال شبكات «Fi-Wi» منزلية ومكتبية.

هذا الوضع يجعل الهجمات الأمنية على أجهزة التلفزيونات الذكية أمراً منطقياً ومتوقعاً وجديّاً للغاية، وعليه حذّر خبراء في أمن المعلومات من هجمة أمنية وشيكة يُحتمل أن تتعرّض لها أجهزة التلفزيونات الذكية، حيث أكّدت كلا شركتي

Samsung & KasperSky بأنّ الفيروسات بدأت تشق طريقها الآن إلى التلفزيونات الذكية، بعدما اجتاحت الحاسبات المكتبية والمحمولة والهواتف الذكية خصوصاً في أعقاب التطوّر السريع في صناعة أجهزة التلفزيون، وزيادة اندماجها مع الإنترنت والتي كانت من أبرزها:

- ❖ فيروسات الفدية « Ransomware» التي تعمل على تشفير الجهاز وتمنع تشغيله إلا بعد دفع فدية مالية للمهاجمين.
- ❖ الفيروسات من فئة الديدان « worms » التي باتت تنتقل من شبكات الحاسب الى التلفزيون الذكي.
- ❖ أحصنة طروادة «Trojan Horse» التي تخفي نفسها داخل البرامج المشروعة.

- ❖ تقنية تُعرف باسم «التعرّف الأوتوماتيكي على المحتوى» أوACR ، والتي تُعتبر من أكثر العوامل المزعزعة للثقة في التلفزيونات الذكية الحديثة حيث تعمل كمحقق يجمع البصمات من خلال التقاط الجهاز صورة لما تضمّه الشاشة من بيكسلات ثمّ يطابقها مع قاعدة بيانات للبرامج المتلفَزة لمعرفة ما تشاهدونه ومعظم أجهزة التلفاز المتوفرة اليوم في الأسواق تستخدم هذه التقنية القادرة على التعامل مع أي شيء يُعرض على الشاشة، ومن بينها الفيديوهات المستورَدة من أجهزة بث كابلات خارجية غير متصلة بالإنترنت.

- ❖ الخطر الأكبر الناجم عن البرامج المصمّمة للتجسس فحالما يتصل التلفاز بالإنترنت سيُطلب منك إدخال معلومات تسجيل الدخول من قبل مزود خدمة الإنترنت ISP، وسيعرض التلفاز قائمة تشغيل الشاشة التي تتضمّن عدداً من قنوات الإنترنت المتاحة على شكل تطبيقات، بعضها محمّلٌ تلقائياً بينما ستتمكّن من تحميل المزيد وإضافتها إلى التطبيقات الموجودة على التلفاز الذكي مما قد ينجم مشاكل تتعلّق بالخصوصيّة، فعادةً ما يتتبع كلٌ من التلفاز ومزودي تطبيقات المحتوى نشاطك على الإنترنت لتقديم الاقتراحات المناسبة لك، هذا التتبع لنشاطك قد يتضمّن مخاطر إضافية، فمثلاً إن كان مزوّداً بكاميرا ويب أو ميكروفون هذا يعني إمكانية التنصت عليك ورؤيتك من قبل بعض قراصنة الإنترنت، ونوّهت شركة Samsung في تحذيرٍ لها عن الخطورة المترتبة عن التحكم في جهاز تلفاز سامسونغ الذكي باستخدام خاصيّة تفعيل الصوت التي تمكّن أجهزة التلفاز الذكي "الاستماع" لكلّ محادثة تجرى أمامها، وقد تشارك أي تفاصيل تلتقطها مع سامسونغ أو أطرافٍ ثالثة.

للوقاية من ذلك :

✓ **تشغيل برنامج فحص فيروسات منتظم على أجهزة التلفاز على أن يتمّ المسح كل بضعة أسابيع**

الخطوات المتبّعة لفحص أجهزة تلفاز سامسونغ الذكية:
تحميل القائمة، ثم الانتقال الى «عام»، ومن ثم «إدارة النظام»، وبعدها «التأمين الذكي»، ثم مفتاح «مسح»، وبالضغط على هذا المفتاح، تبدأ عملية مسح التلفزيون بحثاً عن الفيروسات، التي تستغرق وقتاً أطول من وقت إجراء الفحص .
أما بالنسبة لمعظم العلامات التجارية الأخرى التي تعمل بنظام تشغيل «تلفاز أندرويد» الرسمي من Google أو تعتمد على نظام تشغيل أندرويد والذي يدعم التحميل المتوازي لتطبيقات أندرويد حيث لا يوجد تطبيق مخصص للعمل على أجهزة تلفاز أندرويد لذا سوف يضطّر المستخدمون إلى الاعتماد على التحميل المتوازي لأي ملف APK لتطبيق مكافحة الفيروسات على أجهزة التلفاز الذكية والذي يتمّ بالخطوات التالية:

- نزّل أي تطبيق مكافحة فيروسات جيّد من مصدرٍ موثوق.
- انقله إلى جهاز التلفزيون باستخدام محرك USB وقم بتثبيته.
- بمجرد التثبيت، شغّل التطبيق واضغط على زر الفحص لبدء عملية فحص الجهاز من الفيروسات.

نذكّر أنّ تلك التطبيقات مصمّمة للعمل على المنصّات الهاتفية لذا سوف تحتاج إلى توصيل Mouse وkeyboard للتنقل داخل التطبيق.

ويمكننا تعطيل خواص التجسس في التلفاز الذكي ولكنّ الطرق تختلف من جهاز لآخر وذلك حسب الشركة المصنّعة ولمعرفة تفاصيل أكثر عن هذه الطرق يرجى الاطّلاع على الرابط التالي:
https://www.samma3a.com/tech/ar/turn-off-smart-tvs-spying-features

- ✓ **إيقاف عرض ملفات تعريف الارتباط cookies**

يمكنك من خلال إعدادات متصفح الويب الخاصة بأيّ من أجهزة التلفاز الذكية تعطيل ملفات الـ cookies ومنها ملفات الطرف الثالث، إضافةً لإمكانيّة تفعيل ميزة التصفح الخاص، وهذا من شأنه الحد من تتبّع نشاطك على الويب، وتقييد تصفحك لبعض مواقع الويب.

- ✓ **تأمين الشبكة**

احرص على ضمان أمن شبكة Fi-Wi لتقليل التهديدات الممكنة قدر الإمكان وذلك بالدخول إلى الإعدادات اللاسلكية للراوتر وضبطها على خيار WPA2 الذي يُعتبر الخيار الأكثر أماناً لمعظم الأجهزة.

- ✓ **اختيار كلمة مرور قوية**

استخدم كلمة مرور قوية للراوتر ولكافة الحسابات الخاصة بك التي قد تستخدمها في التلفاز.

- ✓ **فصل التلفزيون عن شبكة الإنترنت في المنزل عندما لا تكون ميزات التلفزيون الذكي قيد الاستخدام**

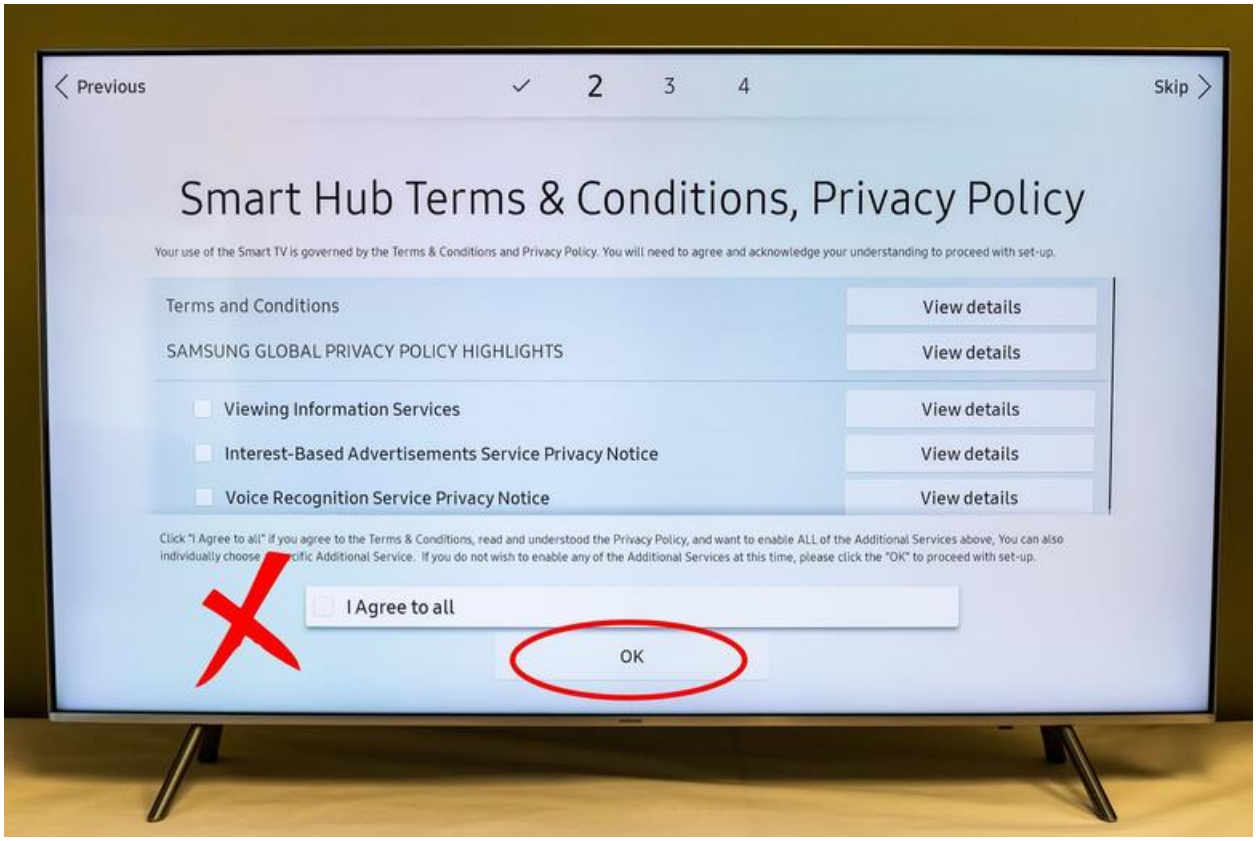
وبذلك نكون قد منعنا فرصة الوصول إلى جميع الوظائف التي يتحكم بها الإنترنت في جهاز التلفزيون، ولزيادة الأمان عند وجود الكاميرا يفضل تغطية العدسة أو تعطيلها في حال عدم استخدامها .

- ✓ **إرجاع التلفاز إلى وضع ضبط المصنع في حال رغبة المستخدم ببيعه**

وذلك لكي يتمّ حذف بيانات الوصول المخزّنة عليه.

- ✓ **قراءة الشروط والأحكام العامة للخدمات بعناية وتجنّب الموافقة العمياء في أي موضع**

يتعيّن على المستخدم أن يدرك أنّه مع أجهزة التلفاز الذكية يتمّ تسجيل كثير من التفاصيل الخاصّة بسلوكيّات المستخدم على الإنترنت ويرتبط ذلك بالشركات المنتجة لأجهزة التلفاز والتطبيقات المستخدمة، ولذلك يجب على المستخدم التأني في قراءة الشروط ورفض الإتفاقيات التي تتيح الوصول للبيانات الشخصية مثل :
خواص التعرف التلقائي – Automatic Content Recognition (ACR)
والموافقة بوعي عند استخدام التلفاز لأول مرة، وعدم إفشاء البيانات بسهولة، وفي حالة الرفض قد لا تعمل بعض الخدمات عندها يمكن للمستخدم تغيير بعض القرارات عن طريق قائمة التلفاز والتي تمّ اتّخاذها سابقاً.



و بِكُلِّ تأكيد _عزيزي القارئ _ لا تصل خُطورة البيانات التي يتمّ جمعها عبر التلفزيون الذكي إلى تلك التي يتمّ جمعها عبر شبكات التواصل الإجتماعي والتي لا تُهدّد خُصوصيّتك فقط بل تُهدّد أمنك أيضاً، إلا أنّه من حقك كمُستخدم على أقلّ تقدير أن تعرف ما هي البيانات التي يتمّ جمعها عنك بالإضافة إلى أن تُمنح خياراً لإيقاف هذا الأمر.

وفي نهاية المطاف لا يمكن إنكار أنّ التكنولوجيا الرقمية لم يعد من الممكن الاستغناء عنها ولا لأي سببٍ كان، وخاصّةً بعد أن اتّخذت تلك الأجهزة صفة "الضرورية" وأصبحت تشكّل جزءاً مهمّا من حياة الناس اليومية ووجدت معظم أحلام الرفاهية طريقها إلى التحقق على أرض الواقع لذلك يجب التعامل بحذر مع تلك الأجهزة لكي لا نفتح المجال للتطفل على خصوصياتنا وأسرارنا.

إعداد :ماري بركات

بإشراف رئيس مركز أمن المعلومات

م. سلمان سليمان

هاتف: 3937078 11 963+، فاكس 3937079 11 963+، ص.ب: الصبورة-60، بريد إلكتروني info@nans.gov.sy

هاتف: 3937078 11 963+، فاكس 3937079 11 963+، ص.ب: الصبورة–60، بريد إلكتروني info@nans.gov.sy