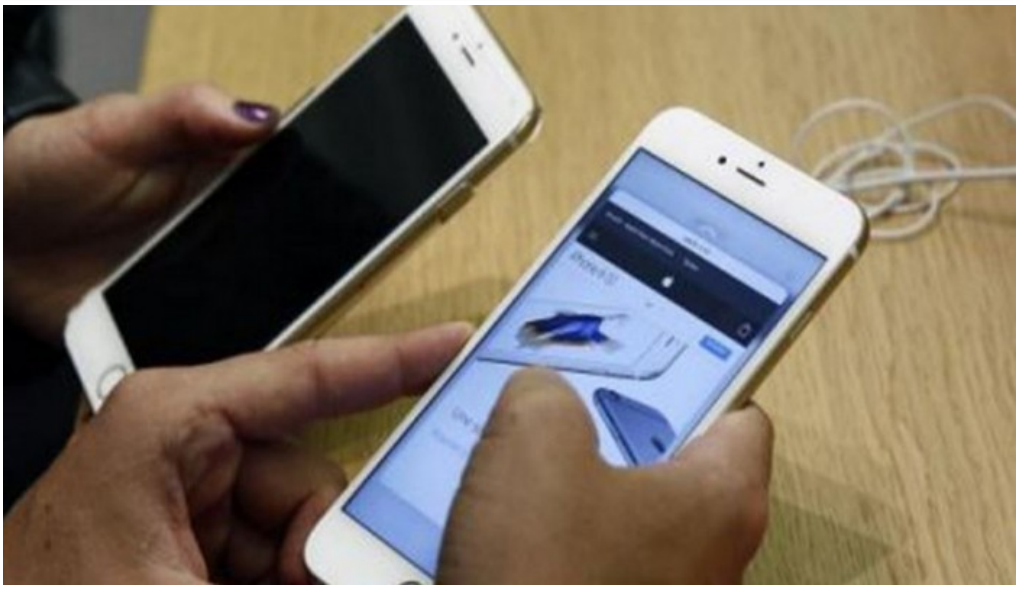
7 طرق لمنع أجهزتك الذكية من التجسس عليك



الخميس 30 مارس 2017 08:03 م

تتلاحق الخطى لتحقيق كل سبل الراحة والرفاهية بتوظيف التكنولوجيا والإنترنت وتطبيقاتها لتكون على اتصال بكل ما يستخدمه الإنسان من أجهزة بدءا من أجهزة التلفزيون إلى أجهزة تحميص الخبز، وصولاً إلى أنظمة تكييف الهواء التي يمكن تفعيلها عن بعد، بينما تكون في طريق العودة من العمل إلى البيت لكن هذا يجلب أيضا مخاوف جديدة تتعلق بالخصوصية؛ حيث إن أي شيء متصل بالإنترنت يثير شهية الهاكرز وقراصنة الإنترنت، ويحفزهم على الولوج من خلاله للتلصّص أو التجسّس، بحسب مجلة "تايم" الأميركية

وفي هذا السياق تشير الوثائق، التي نشرها مؤخرا موقع "ويكيليكس"، على سبيل المثال، إلى أن وكالة الاستخبارات المركزية "سي أي إيه" يمكنها استخدام أجهزة التلفزيون المستهدفة، وتحويلها إلى ميكروفونات تستمع دائما

كما ادعت مؤخراً كيليان كونواي، مستشارة الرئيس دونالد ترمب، أن أفران المايكروويف يمكن أن تستخدم كأجهزة للتجسس، على الرغم من أنها نفت لاحقا تلك التعليقات

في الوقت نفسه، كشف أن الأجهزة "الذكية" الأخرى تتابع سرًّا سلوكيات مستخدميها، وتبلغ تلك المعلومات إلى الشركة التي صنعتها

أمام كل تلك التحذيرات أو حتى الشكوك، لا بد من أخذ مسألة الخصوصية الشخصية على محمل الجد

لذا نورد عدة خطوات يمكن القيام بها؛ لحماية خصوصية كل فرد في عالمنا الذي يتشابك بشكل متزايد يوما بعد يوم:

1 - كلمات سر قوية:

إن أفضل كلمات السر هي تلك التي يكون من الصعب تخمينها، ويمكن أن تتضمن مزيجا من الحروف والأرقام، والأشكال الخاصة ولكن الأهم من ذلك، ألا تعيد أبدا استخدام نفس كلمة السر مرور لحسابات متعددة، لأن اللجوء إلى ذلك يجعل الأمر أكثر سهولة على المتسللين في الوصول إلى كل تلك الخدمات والأجهزة

2 - شريط لاصق على كاميرا الكمبيوتر المحمول:

قد لا تمنع تغطية كاميرا الكمبيوتر الـ"هاكرز" من الاستيلاء عليها، ولكنها ستساعد على ضمان عدم حصولهم على أية لقطات ذات خصوصية يمكنهم استخدامها ضدك إذ يمكن للقراصنة الوصول إلى كاميرا الويب وغيرها من خلال نوع من البرامج المعروفة باسم "ريموت أدمنيستريشن تووول" (أداة الإدارة عن بعد)، أو اختصارا "أر إيه تي". لا تنزعج من مظهر الشريط اللاصق على كاميرا كمبيوترك المحمول، فقد سبق أن نشرت لقطات للرئيس التنفيذي لشركة "فيسبوك" مارك زوكربيرغ، وهو يضع شريطا لاصقا على كاميرا الكمبيوتر المحمول الخاص به

3 - تطبيقات الهواتف الذكية:

إن العديد من التطبيقات تطلب استخدام موقعك من أجل تقديم خدمات أفضل على سبيل المثال فإن "فيسبوك" سوف يستخدم موقعك للسماح لك بالدخول إلى مكان بعينه أو تحديد مكان التقاط صورة ما، ولكنك قد لا تريد أن يعرف كل تطبيق أين أنت في جميع الأوقات

إذا كنت تستخدم أجهزة آيفون، يمكنك أن تختار بشكل فردي ما إذا كانت تطبيقات معينة يمكنها رصد موقعك طوال الوقت، فقط أثناء

استخدامك للتطبيق، أو عدم استخدامه مطلقا عبر التحكم بوضعية الخصوصية في قائمة الإعدادات، كما أنه يمكن إلغاء تلك الخاصية على "غوغل بيكسيل" وبالطبع الأجهزة التي تعمل بنظام آندرويد.

4 - تحديث برامجك:

ينطبق ذلك الإجراء على جميع أجهزتك سواء كان ذلك لهاتفك أو جهاز الكمبيوتر أو أي شيء آخر، يجب أن تتأكد دائما من أنك تستخدم أحدث إصدار ممكن من البرامج. إن تحديثات البرامج عادة ما تجلب إصلاحات أمن حرجة، وتلك الهفوات في الإصلاح هي التي يحب الـ"هاكرز" استغلالها. وهناك خيار للتحقق من وجود تحديثات البرامج عادة ما يكون موجودا في قائمة إعدادات جهازك.

5 - وقف ميزات تتبع التلفزيون:

تسجل بعض أجهزة التلفزيون الذكية المزيد من المعلومات حول عاداتك في المشاهدة بأكثر مما تتخيل، فعلى سبيل المثال، دفعت شركة فيزيو لإنتاج التلفزيونات مؤخرا مبلغ 2.2 مليون دولار إلى لجنة التجارة الفيدرالية لتسوية غرامات عليها؛ لأنها كانت ترصد المحتويات التي يهتم بها المشاهدون دون موافقة منهم، ثم باعت تلك البيانات للمعلنين.

إن فصل جهازك التلفزيوني الذكي عن الإنترنت تماما هو أفضل وسيلة لضمان أن البيانات الحساسة لن تنتقل، ولكن اللجوء إلى تلك الطريقة يمكن أن يحد بشكل ملحوظ من وظيفة التلفزيون، لذا فإن بعض الشركات المصنعة للتلفزيونات تسمح لك بتعطيل خاصية معينة لجمع البيانات، وفقا لما نشره موقع "وايرد".

6 - تعرف هاتفك على صوتك:

في حين أن بعض أجهزة التلفزيون الذكية لديها قدرات التعرف على الصوت، فإن هناك فرصة أكبر بكثير من أن يكون هاتفك الذكي مزودا بهذه الخاصية. وتتضمن أحدث إصدارات من الأجهزة التي تعمل بنظام آندرويد، مساعد غوغل، وهناك أيضا نظام أبل "هيي سيري" على إصدارات "آيفون"، وتدعم هذه الأنظمة ميزة الاستماع لعبارة افتتاحية من أجل الإجابة عن الأسئلة وتلبية الطلبات والأوامر دون الحاجة إلى الضغط على أي زر.

7 - تسجيلات أمازون إيكو:

إذا كنت تمتلك حساب "أمازون إيكو"، فإن هناك احتمالات بأنه استمع إلى المحادثات الخاصة بك بواسطة "آمازون ستورز" من أجل التكيف بشكل أفضل مع تفضيلاتك. ومع ذلك، يمكنك حذف تاريخ تسجيلات صوتك من خلال تطبيق "أليكسا" بفتح الإعدادات ثم التاريخ. من هناك، يمكنك النقر على اختيار تسجيل لتقوم بحذفه، كما يمكنك أيضا القيام بذلك من خلال زيارة موقع "أمازون كونيكت أند ديفايسز"، وإلغاء اختيار "إدارة تسجيلاتك الصوتية".