تطبيقات الانترنت وبياناتنا الشخصية، من يتعقبها؟



www.nasainarabic.net
@NasaInArabic NasaInArabic NasaInArabic NasaInArabic NasaInArabic

إن كنت من المولعين بالإنترنت، فلا بد أنك تعرف المقولة الشهيرة "إن لم تدفع شيئًا، فأنت هو المُنتَج". وفي واقع الحال لا تُعد هذه المقولة دقيقةً بما يكفي. ففي عالم الإنترنت، غالبًا ما تكون أنت المنتَج. وعلى الرغم من معرفة غالبية المستخدمين بجمع بياناتهم واستثمارها، إلا أن قليلًا منهم يعي حجم مشكلة جمع واستثمار البيانات، لاسيما عندما تقوم التطبيقات بذلك.

هذا وقد تَبيّن من خلال أبحاثنا على أكثر مئة تطبيق مجانية ومدفوعة في متجر غوغل بلاي في أستراليا والبرازيل وألمانيا والولايات المتحدة أن أغلبها يحتوي متعقبًا واحدًا على الأقل، وبالتالي فإن البيانات يجري جمعُها لصالح الشبكات الإعلانية وخدمات الدفع المالي. وليس هذا سوى البداية فقط، فوجود برامج المساعد الصوتي الذكي مثل سيري **Siri** وغوغل ناو **Google Now** والتي تتطور وتحدّ من احتياجنا لباقي التطبيقات، يجعل السؤال المطروح بخصوص ما يتم عمله في بياناتنا أكثر تعقيدًا.

لا شيء بالمجان

إن باستطاعة التطبيقات المجانية والمدفوعة الأجر على حد سواء تعقب بياناتنا الشخصية. وعلى الرغم من أن التطبيقات التي تراها في الصورة لا تقوم بتعقب البيانات في غالب الأمر، إلا أنه يصعب تحديد أيها سيقوم بذلك أم لا. المصدر: Flickr/Blake Patterson, CC BY-SA

وفي فضيحة موقع أنرول دوت مي **Unroll.Me** الأخيرة بدا الفرق واضحًا بين توقعات المستخدمين حول استخدام بياناتهم وبين ما تقوم به التطبيقات فعليًا بهذه البيانات. حيث يوفر هذا الموقع خدمة تنظيف صندوق البريد الالكتروني وذلك بإلغاء اشتراك المستخدم بالرسائل غير المرغوبة من المواقع المختلفة، إلا أن الكثير قد صُدموا عندما تبين أن الموقع استخدم محتوى البريد الالكتروني لجمع البيانات واستثمارها. فعلى سبيل المثال، قام هذا الموقع بالبحث في البريد الالكتروني عن الإيصالات العائدة لشركة ليفت **Lyft** للركوب التشاركي **ridesharing** وبيعها للشركة المنافسة أوبر **Uber**.

وقال الرئيس التنفيذي لأنرول دوت مي معتذرًا: "كان على الشركة القيام بعمل أفضل وذلك بالإفصاح عن مسألة استخدام البيانات". والسؤال المطروح؛ من المخطئ هنا؟ هل هم المستهلكون باعتقادهم أن هذه الخدمات مجانية؟ أم مقدمو الخدمات الذين يتوجب عليهم إخبار المستخدمين بالبيانات التي تُجمَع؟

ويصبح السؤال أكثر إلحاحًا عندما يتعلق الأمر بتطبيقات الهاتف. ففي الحقيقة ومقارنة بخدمات الانترنت التي تقوم بجمع بيانات شخصية محدودة، فإن تطبيقات الهاتف تصل إلى الكثير من المعلومات الشخصية الدقيقة للمستخدمين، كالموقع والرسائل وسجل التصفح وسجل التطبيقات المثبتة. ويقوم المبرمجون بهذا عن طريق تضمين مكتبات الطرف الثالث البرمجية **third-party libraries** في التطبيقات. وهي عادةً ما تكون تطفلية جدًا، حيث تقوم بالبحث عن أدق البيانات الشخصية.



ملخص الدراسة لأكثر مائة تطبيق مجاني ومدفوع الأجر في متجر غوغل. المصدر: NICTA.

كيف تعمل المكتبات البرمجية؟

المكتبات البرمجية هي عبارة عن طرف ثالث تعمل كمتعقبات، يستخدمها مطورو التطبيقات للتواصل والتفاعل مع خدمات لا علاقة لها بالتطبيق، والتي قد تكون شبكات إعلانية أو منصات تواصل اجتماعي أو حتى منافذ للدفع المالي مثل بايبال **Paypal**، فضلًا عن إمكانية استخدامها لتعقب مشاكل التطبيق والأخطاء البرمجية.

وفي عام 2015 قمنا بدراسة تضمنت تحليل هذه المكتبات التعقبية في أكثر مئة تطبيق مجاني وأكثر مئة تطبيق مدفوع الأجر تحميلًا في كل من أستراليا والبرازيل وألمانيا والولايات المتحدة، وكانت النتائج مقلقة حقًا. فقد تبين أن ما يقرب من 90% من البرامج المجانية و60% من البرامج المدفوعة الأجر في متجر غوغل تحتوي على متعقبات برمجية ضمنها.

وقد تبين أن غوغل آدز **Google Ads** وفلوري **Flurry** هي المتعقبات الأكثر انتشارًا في التطبيقات المجانية والمدفوعة الأجر على حدٍ سواء. فقد وُجدت فيما يزيد عن 25% من التطبيقات.

ومن الأمثلة الأخرى على المتعقبات واسعة الانتشار في التطبيقات هي تابجوي **Tapjoy** وغوغل انالاتيكس **Google Analytics** وماليينال ميديا **Millennial Media** وتشارت بوست **Chartboost**. وغالبا ما تتواجد هذه المتعقبات في أكثر من تطبيق في آن واحد، مما يعني استقبالها لبيانات كثيرة ومتنوعة لنفس المستخدم.

وبما أن هذه الدراسة أُجريت منذ سنتين، فمن المؤكد أن هذه الأرقام قد تغيرت، حيث إن الدراسات الحديثة تُبين أن هذه الأرقام ما زالت متجهةً للتوسع بشكل أكبر.

ومن الممكن تواجد هذه المكتبات البرمجية دون القيام بجمع البيانات، ومع ذلك فمن المزعج تواجد الكثير من هذه المتعقبات في التطبيقات المدفوعة والتي يتبين أن لها طرقًا تجاريًة جانبية أخرى.

ماذا بعد ذلك؟

كيف يمكنك اجتناب التعقب؟

أولاً، عندما يَطلب منك تطبيق ما صلاحياتٍ معينةً مثل الموقع أو الوصول للأسماء، يجب أن تسأل نفسك: هل يحتاج هذا التطبيق بالفعل لتلك الصلاحيات كي يعمل؟ كرقم الهاتف مثلاً.

ثانياً، يجب الاهتمام بتحميل تطبيقات الحماية من الفيروسات وتطبيقات الأمان مثل **Lookout Security & Antivirus** وكذلك تطبيق **Mobile Security and Antivirus** وتطبيق **PrivMetrics**. وعلى أي حال، تبقى هذه الحلول سطحيةً بالنسبة لعمق وحجم المشكلة.

وقد تأتي هذه التطبيقات في المستقبل القريب كخدمات مضمنة في أنظمة تشغيل الهواتف الذكية. فعلى سبيل المثال، إن تطبيقات المساعد الصوتي الذكي مثل غوغل ناو قد يُنهي الحاجة لتطبيقات مختلفة مثل تطبيقات الملاحة والجو وتطبيقات الرسائل والأخبار والطقس وكذلك بعض التطبيقات المالية.

يمكن لهذه الخدمات والتي تعرف بـ مجمع منصة الخدمات **aggregator platform services** أن تُنشئ محتوى شخصيًا واسعًا يغطّي جوانبَ عدة عن سلوكنا على الانترنت وخارج الانترنت. ويمكن لهذه الخدمات عند استعمالها معرفة الكثير عن أنشطتنا، ناهيك عن تحديد موقعنا كذلك. ومع هذا يقوم المستخدمون بتبادل بياناتهم مع التطبيقات لضمان عملها، ويبدو أن هناك أسبابًا قليلةً للاعتقاد بأن

هذا الاتجاه لن يستمر.

- التاريخ: 2017-08-17
- التصنيف: تكنولوجيا

#الانترنت #الهواتف الذكية #تطبيقات الانترنت #تطبيقات الهاتف

المصادر

- phys.org
- الصورة

المساهمون

- ترجمة
  - حمدان زياد
- مُراجعة
  - حسن شوفان
- تحرير
  - محمد نور الدين يسري
- تصميم
  - مكي حسين
- نشر
  - مي الشاهد