خمس طرق يراقبك بها الإنترنت دون علمك

كتبه أميرة جمال | 7 يناير ,2018

كلما استخدمت الإنترنت أكثر، يجب أن تعرف أنك تمنح معلوماتك الشخصية بشكل تطوعي غير مباشر لجميع المواقع والمنصات التي تستخدمها، وكلما قضيت وقتًا أكثر وأدخلت الكثير من المعلومات الخاصة بك مثل معلومات حساباتك البنكية أو تاريخ التسوق الإلكتروني، فهذا يعني أن للإنترنت فرصة أكبر لمراقبتك، وهذا ما يحدث بالفعل دون علمك.

هناك طرق مختلفة للمراقبة، البعض منها يوافق عليها المستخدم أو المتصفح بنفسه، والبعض الآخر يتم بشكل غير مباشر ودون علمك، ويتحكم فيها بشكل كبير مواقع التواصل الاجتماعي ومواقع التسوق الإلكتروني وتطبيقات للتواصل أو تطبيقات الخدمات مثل أوبر على سبيل المثال، سنعرض لك هنا أهم سبع طرق يراقبك بها الإنترنت.

1- الكوكيز (Cookies)

هل قمت بزيارة أحد المواقع من قبل ولم تستطع قراءة أو مشاهدة ما كنت تنوي تصفحه على الموقع بسبب رسالة ظهرت لك مفادها أن هذا الموقع يستخدم "كوكيز" أو ما يعرف باللغة العربية "ملفات التعريف بالارتباط"، فإن كنت توافق على ذلك يمكنك متابعة عملك على هذا الموقع، أما إن رفضت ربما لن يظهر لك المحتوى الذي نويت زيارته، وحينها يقرر المتصفح إما الموافقة أو محاولة الوصول إلى موقع آخر لا يستخدم "كوكيز".

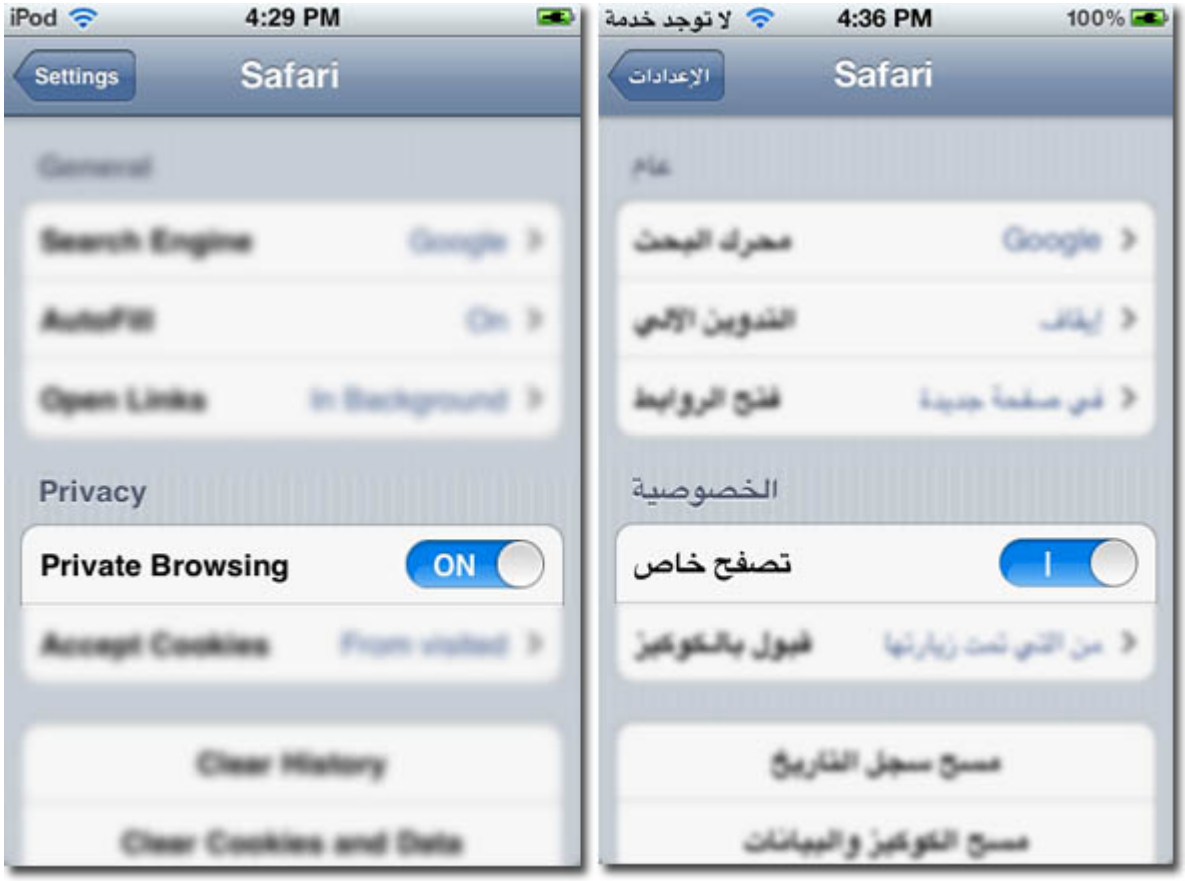
> لا تتذكر الكوكيز معلوماتك الشخصية مثل كلمة المرور أو عنوان البريد الإلكتروني فحسب، بل يمكنها تتبع حركتك على الإنترنت، حينها تدرك تلك المواقع نوعية المواقع التي يزورها المستخدم من خلال تاريخ زياراته

كلما استخدمت موقعًا يمكنه أن يحفظ معلومات الدخول مثل عنوان البريد الإلكتروني وكلمة السر، فيجب أن تعرف أن الموقع يستخدم الكوكيز، وهي ملفات نصية ترسل من المتصفح إلى المستخدم، هدفها جمع المعلومات عنه، حينها تسمح للموقع باسترجاع تلك المعلومات عنك عند الحاجة، مثل كلمة المرور الخاصة بك للدخول إلى موقع ما، باستخدام الكوكيز لن تحتاج لكتابة كلمة المرور في كل مرة تزور الموقع، فسوف تسترجعها الكوكيز من أجلك.

لا تتذكر الكوكيز معلوماتك الشخصية مثل كلمة المرور أو عنوان البريد الإلكتروني فحسب، بل يمكنها تتبع حركتك على الإنترنت، حينها تدرك تلك المواقع نوعية المواقع التي يزورها المستخدم من خلال تاريخ زياراته على المتصفح، فمثلًا إن كان في تاريخ الزيارات الحديث زيارة إلى موقع شركة الخطوط التركية للطيران، ومن ثم قمت بفتح منصة فيسبوك الذي يستخدم كوكيز هو الآخر، حينها إن كان

موجودًا على فيسبوك إعلان للخطوط التركية للطيران، ستظهر لك على الفور وقتما تستخدم فيسبوك.

يثبت ذلك خاصية "عدم التتبع" الموجودة في أغلب المتصفحات مثل فايرفوكس وكروم كما هو واضح في الصورة أسفل، إلا أنها ليست ذات فائدة كبيرة، حيث إن برمجة أغلب المواقع التي يزورها المستخدم مصممة لتتجاهل هذه الخاصية، بالإضافة إلى أنها غير معقدة بشكل كافٍ، إذ إنها ستطلب من المستخدم تحديد أي من المواقع التي لا يود أن تتعقب تاريخ زياراته على الإنترنت، ولهذا يجب على المستخدم أن يتبع إجراءات أكثر تعقيدًا من ذلك، بما فيها التصفح بشكل سري أو خاص "Incognito" الذي لن يتبادل أي معلومات عنك.



2- مواقع التواصل الاجتماعي

واجهت شركة أوبر عدة مشاكل قبل سنتين من الآن أقحمتها في عدة دعاوى قضائية مرفوعة من بعض الأيقونات المعروفة في عالم التجارة في الولايات المتحدة، حيث كان سبب تلك الدعاوى أن أوبر تستغل معلومات المستخدمين، وبالأخص المشهورين منهم، من خلال نشر مواقعهم على الخريطة من خلال سيارات أوبر التي تقلهم للدعاية للشركة وخدماتها.

على الرغم من أن أوبر أفادت أن معلومات المستخدمين في كل مدينة وكل بلد معلومات خاصة لا يمكن الوصول إليها من كل من يعملون في الشركة، ربما كان جزء من ذلك صحيحًا، حيث لا يمكن لكل سائقي أوبر الوصول لمعلومات المستخدمين الشخصية، إلا أن كل ما عداهم يمكنه ذلك، فيمكن لأوبر التعرف عليك وعلى هويتك من خلال موقعك والسيارة التي تقلك.

كان هذا جزء بسيط مما تفعله مواقع التواصل الاجتماعي والخدمات الاجتماعية بمعلوماتنا، ناهيك أن أغلبها إن لم يكن كلها يستخدم الكوكيز المشار إليها سابقًا، التي تساعدهم في جلب مزيد من الإعلانات بناءً على ما تزوره أنت على المتصفح الخاص بك.

> أوبر تستغل معلومات المستخدمين، وبالأخص المشهورين منهم، من خلال نشر مواقعهم على الخريطة من خلال سيارات أوبر التي تقلهم للدعاية للشركة وخدماتها

ذلك بالإضافة إلى موافقة أغلب المستخدمين في شروط استخدام كل من فيسبوك وجوجل على أن يصل كل منهما لميكروفون الهاتف أو جهاز الحاسوب، وعليه فإن الشركتين تتنصتان على كل ما يدور حول الميكروفون لأغراض إعلانية ولتعزيز خدماتها على حسب احتياجات المستخدمين كما تزعم، بينما تزعم جوجل التي يستخدمها الكل في أغلب نشاطاته اليومية أنها تسجل المحادثات التي تدور

حول الميكروفون، من أجل تحديث خدماتها اللغوية والصوتية.

3- التسوق عبر الإنترنت

يمكن للمواقع أن "تقتنصك" من مواقع التواصل الاجتماعي، من خلال خاصية "Look like"، وهي تحديد خصائص أكثر المستخدمين ولاءً للموقع ومن خلاله يتم اقتناص كل من يتشارك معه في تلك الخصائص

هناك طرق عديدة تستخدمها مواقع التسوق الإلكتروني لكي تجني أكبر نسبة من الأرباح من المتسوقين إلكترونيًا، من بينها قدرة تلك المواقع على التعرف ما إن كان المشتري يشتري لنفسه أم يشتري هدايا لآخرين، المتسوقون الذين يستخدمون التسوق الإلكتروني من أجل الهدايا لا تعتبرهم المواقع متسوقين لديهم ولاء ولهذا لا تستثمر فيهم، بينما يعد الآخرون كنزًا لهم، ولهذا يقدمون لهم الخصومات والعروض من أجل كسب مزيد من الولاء.

يمكن للمواقع أن "تقتنصك" من مواقع التواصل الاجتماعي، من خلال خاصية "Look like"، وهي تحديد خصائص أكثر المستخدمين ولاءً للموقع ومن خلاله يتم اقتناص كل من يتشارك معه في تلك الخصائص على مواقع التواصل الاجتماعي وبالأخص فيسبوك، حينها يقوم الموقع بالدعاية له على تلك المنصات.

استخدام مربع البحث على مواقع التسوق الإلكتروني شديد الأهمية بالنسبة إليهم، إذ إن الزبائن الباحثين عن علامات تجارية بعينها مثل "Nike" أو "Zara" تعتبرهم المواقع زبائن ذوات قيمة أكبر

من غيرهم، إذ إنهم يبحثون عن الجودة أكثر من السعر، وعليه فهم معرضون للاستهداف أكثر لإعلانات مواقع التسوق الإلكتروني من خلال الكلمات التي يبحثون عنها.

ربما سيبدو هذا شديد اللامنطقية، إلا أن باستخدام الكوكيز المشار إليها هنا سابقًا، يمكن لمواقع التسوق الإلكتروني أن تميز نوع جاهز الحاسوب أو الهاتف الذي تستخدمه في أثناء التسوق عبر تلك المواقع، وكلما كان ذلك الجهاز أعلى قيمة وأغلى في سعره، كنت زبونًا قيمًا بالنسبة لها وكنت أكثر عرضة لإعلاناتهم.

4- الأجهزة المنزلية الذكية

باعت شركة جوجل في عام 2017 وحده أكثر من 6 ملايين أجهزة منزلية ذكية (Smart Home Devices)، وإن كنت لا تجد سببًا يجعلك مرتعبًا من المستقبل، فهذا وحده يكفي، إذ إن هناك جدلًا عن أجهزة المنازل الذكية، وبالأخص أجهزة جوجل الذكية التي تثير الشكوك بشأن قدرتها على التجسس على المواطنين داخل منازلهم من خلال تلك الأجهزة.

كل جهاز من تلك الأجهزة لديه كاميرا ومايكروفون واتصال جيد بالإنترنت قادر على أن يكون فرصة ذهبية للتجسس عليك داخل منزلك، فهذا كل ما يحتاجه المتجسس لكي يراك ويسمعك وأنت في منزلك، لا سيما إن كان ذلك الجهاز متصلًا بنفس بريدك الإلكتروني الذي تستعمله لهاتفك ولحاسوبك أيضًا، حينها يجب أن تعرف أنك داخل سحابة تحيط بك من جميع الجهات.

ربما يجب عليك أن تعيد النظر في كل ما تنوي إدخاله إلى منزلك من الأجهزة الذكية، فهذه الأجهزة

ليست معرضة للاختراق من المتجسسين أو اللصوص فحسب، بل معرضة للاختراق من الحكومات أيضًا ومن الشركات التجارية.

5- جهاز الواي فاي

ربما جلست طويلًا تبحث بين المواقع المختلفة عن حل لحماية أجهزتك الإلكترونية من الاختراق، أو حماية حساباتك على مواقع التواصل الاجتماعي أو حتى بريدك الإلكتروني، إلا أنك لم تفكر أن الشبكة التي تتصل بها يمكن اختراقها أيضًا، من خلال اختراق جهاز الواي فاي الذي تتصل عن طريقه بالإنترنت.

> كل جهاز من تلك الأجهزة لديه كاميرا ومايكروفون واتصال جيد بالإنترنت قادر على أن يكون فرصة ذهبية للتجسس عليك داخل منزلك

يمكن للمخترقين قضاء بضعة ساعات من وقتهم ليخترقوا جهاز واي فاي WIFI واحد، إلا أن اختراقه ليس أمرًا مستحيلًا، وبمجرد اختراقه يمتلك المتجسس القدرة على الوصول إلى الأجهزة الإلكترونية المتصلة به ونقل بعض من المعلومات من عليها إلى جهازه هو، ذلك لأنه سيكون له القدرة على فتح جهازك من على بعد وكأنه يستخدم الجهاز نفسه.

لا تنتهي طرق المراقبة عن طريق الإنترنت عند هذه القائمة فحسب، بل هناك العديد من الأساليب والطرق التي من الممكن الوصول إلى معلوماتك واستخدامها في مراقبتك لخدمة مصالح جهات أو شركات بعينها، ربما يجب عليك التفكير مرتين قبل زيارة أي موقع أو شراء جهاز ذكي جديد، فمن الممكن أن يكون السبيل لوضعك تحت المراقبة.

رابط المقال : https://www.noonpost.com/21519/