

خصوصية مستخدمي المكتبات: ست خطوات لحماية بياناتهم

جينى غيهارت، كيري شيهان



المخلص:

يدعو المقال المكتبات إلى تعزيز حماية الخصوصية الفكرية للمستخدمين، انطلاقاً من حساسية سجلات القراءة والبحث واستخدام الشبكات، ويعرض ستة محاور تشمل تقليل جمع البيانات والاحتفاظ بها، ووضع إجراءات للطلبات الحكومية والإخطار، ونشر سياسات دقيقة، وتشفير الاتصال، وتأمين المتصفحات، ومراجعة ممارسات الموردين. ويؤكد أن مسؤولية المكتبة تمتد إلى الخدمات الخارجية التي تجمع معلومات أو تحلل سلوك المستخدمين، مع أهمية الموافقة والشفافية والإعدادات المناسبة. كما يربط الحماية برسالة المكتبات في حرية الاستقصاء وخدمة الفئات المعرضة للخطر. ويظل العرض متعلقاً بالسياق الأمريكي والقانوني والتقني لعام 2016، مع الحفاظ على نسب توصياته إلى المصدر. ويركز على الحوكمة وتقليل البيانات وفهم التهديدات بدل افتراض أن إجراء واحد يكفي لحماية المستخدمين.

الكلمات المفتاحية: خصوصية المستخدمين، المكتبات، حماية البيانات، الخصوصية الفكرية، الموردون

مقدمة:

قد تكشف الكتب المستعارة والكلمات المبحوث عنها على حواسيب المكتبة أسئلة مراهق عن ميوله الجنسية، أو توجهات جار دينية، أو اهتمامات طالب سياسية. وتعدّ المكتبات الأمريكية، وخاصة العامة، خدمة الفئات الأشد هشاشة والأقل حصولاً على الخدمات جزءاً من رسالتها، ومنهم المشردون والعاطلون والمهاجرون الجدد واللاجئون. وحين يأتي موظفو الحكومة للسؤال، يحتاج هؤلاء إلى مكتبيين يساندونهم.

ظلت المكتبات والمكتبيون حراساً لحرية التعبير والاستقصاء. ومن واجبهم حماية قدرة المستخدم على الوصول إلى أكثر الأفكار والمعلومات إثارة للجدل دون رقابة حكومية. ومنذ إقرار قانون باتريوت خصوصاً، محوا سجلات عند الضرورة لمواجهة المطالب الحكومية غير الدستورية، وقاوموا خطابات الأمن القومي غير الدستورية (NSLs). ووقفوا مع (EFF) والاتحاد الأمريكي للحريات المدنية عند العمل على إقرار قانون خصوصية القارئ في كاليفورنيا عام 2011.

ومع انتخاب دونالد ترامب رئيسًا مؤخرًا، تخشى مكتبات كثيرة بحق تجدد تهديد خصوصية مستخدميها. فإذا التزمت الإدارة المقبلة بوعود تحديد ملايين الأشخاص وترحيلهم، ومراقبة الأفراد بحسب معتقداتهم الديني، وتوسيع قوانين التشهير مثلًا، فقد تتلقى المكتبات طلبات حكومية غير مسبقة عن مستخدميها.

لذلك نوصي بالتأكد سريعًا من الخطوات التالية لحماية الخصوصية الفكرية. وعلى المكتبات أن تتجاوز عملها الداخلي لتضمن مستوى الحماية نفسه لدى جميع موردي الخدمات الخارجيين.

الخطوات العملية:

1. تقليل جمع معلومات المستخدمين والاحتفاظ بها:

كلما قل ما تجمع من معلومات، قل ما قد تضطر إلى تسليمه. والأفضل جمع الحد الأدنى اللازم للخدمة وعدم إبقائه أكثر من الضرورة؛ فاحذف بيانات الإعارة بمجرد إرجاع الكتاب مثلًا. واجعل حذف السجلات عادة منتظمة باستخدام أداة حذف آمن، بما فيها الإعارة وحضور الأنشطة واستخدام الحواسيب ونشاطها والبحث واتصالات (Wi-Fi) واستعلامات قواعد البيانات. وإن لزم الاحتفاظ بسجلات للتخطيط للموارد أو المطالبة بالتمويل، فاتبع أفضل ممارسات نزع الهوية وإخفائها إلى أقصى حد.

وعند الجمع أخطر المستخدمين وأتح لهم الموافقة الصريحة. وقلل البيانات بإتاحة استخدام مجهول الهوية أو باسم مستعار حيث يمكن؛ اسمح مثلًا باستخدام الحاسوب دون تسجيل دخول شخصي، ولا تلزم بتسجيل الدخول إلى خدمات الويب إلا للوصول إلى حساب المستخدم. ويقترح الأصل كذلك ترك (Wi-Fi) المكتبة مفتوحة، وعدم حفظ عناوين (IP)، وحذف سجلات الاتصال فور الخروج.

وتأكد من أن المواقع والخدمات التي تديرها المكتبة لا تسجل عناوين (IP) للمستخدمين، وإلا فاحذفها سريعًا وبانتظام. وشرح الفروق بين الوصول من المكتبة وعن بُعد؛ فالخدمة عبر حاسوب المكتبة ترى عنوان المكتبة، بينما قد يكشف الوصول البعيد عنوان المستخدم نفسه.

2. سياسات وإجراءات للاستجابة لطلبات الحكومة وإخطار المستخدمين بها:

وضح للمستخدمين كيفية الاستجابة لطلبات معلوماتهم. وتتراوح الطلبات بين سؤال بسيط دون إذن أو أمر قضائي، واستدعاء قضائي، وإذن تفتيش، وخطاب أمن قومي. ويجب أن تحدد السياسة بوضوح تصرف العاملين في كل حالة وأن يعرفوه.

ويذكر الأصل أن المكتبات الأمريكية، في غياب إذن أو أمر قضائي أو خطاب أمن قومي، غير ملزمة عمومًا بتقديم المعلومات ويمكنها الرفض. وقد تنفذ أذون التفتيش فورًا، لكن يستطيع مستشار المكتبة القانوني فحص جميع الطلبات بحثًا عن عيوب قانونية. وعند طلب معلومات المستخدمين ينبغي الاتصال بمحامٍ و(EFF) مستعدة لمساعدة المكتبات على تقييم الخيارات عند تلقي إجراء قانوني مشتبه فيه.

وتحدد السياسات أيضًا متى وكيف يُخطر المستخدم بطلبات الحكومة. وقد واجهت مكتبات مثل (Internet Archive) و(Library Connection) أوامر منع الإفصاح الملحقة بالطلبات وسعت لرفعها، و(EFF) مستعدة للمساعدة هنا أيضًا.

3. سياسات خصوصية دقيقة ومتاحة، وإخطار المستخدمين بتغيرها:

توضح السياسة على الأقل أنواع المعلومات التي تُجمع ومدة تخزينها واستخداماتها ومن يصل إليها وبأي شروط. ويُخطر المستفيد فور تغير السياسة مع فرصة الموافقة الصريحة على استمرار استخدام الخدمات المتأثرة.

وقد لا تغطي سياسة المكتبة كل الفهارس والقواعد والكتب الإلكترونية وأنظمة الإعارة وخدمات الأطراف الأخرى. فيجب على الأقل تنبيه المستفيد إلى تعامله مع مورد خارجي وسياسة خصوصيته، وإتاحة موافقة صريحة على الخدمات الأقل حماية. والأفضل، حيث يمكن، إلزام المورد بمضاهاة حماية المكتبة. ويمكن الرجوع إلى سياسة (EFF) مثلاً.

4. استخدام (HTTPS) للموقع كله طوال الوقت، وحث الموردين على ذلك:

تستخدم مكتبات كثيرة (HTTPS) في أجزاء من الموقع، لكن ذلك لا يؤمن المعلومات بفاعلية. ويمكن استخدام (Certbot) لنقل الموقع كاملاً، وحث موردي الخدمات والكتب الإلكترونية على فعل الشيء نفسه. وبدون الحماية تتعرض المعلومات أثناء النقل لمن يتصل بالشبكة نفسها.

وقل كذلك ملفات الارتباط التي تتبع التفضيلات والأنشطة. وإن استُخدمت، فلتكن بموافقة صريحة؛ ولا تجعل قبولها شرطاً للدخول.

5. تأمين متصفحات حواسيب المكتبة:

قد تسرب المتصفحات غير المؤمنة عمليات البحث والمواقع التي يزورها المستخدم، فترسم صورة تفصيلية للنشاط. ويوصي المقال بجعل المتصفح الافتراضي ذا حماية مدمجة، مثل (Mozilla Firefox) أو (Google Chrome)، وتفعيل إضافات الخصوصية مثل (Privacy Badger) و(HTTPS Everywhere) وتحديث المتصفح والإضافات كلما توافر تحديث.

6. إلزام الموردين بممارسات المكتبة لحماية بيانات المستخدم:

تعتمد المكتبات أكثر فأكثر على أطراف خارجية تصل إلى البيانات؛ وعليها ضمان تبنيتها ممارسات وسياسات منسجمة مع سياستها. فقد تتبع الخدمات السلوك وتجمع بياناته وتحللها، ثم تطلب جهات إنفاذ القانون هذه البيانات. ويشمل ذلك الاسم ومعرفات الحساب و(IP) والبيانات السكانية وسجلات البحث والقراءة، وهي شديدة الحساسية.

ويستطيع المكتبيون التحكم في استخدام الخدمات وعرضها، وضبط الإعدادات الافتراضية لأقصى حماية، ومراجعة الممارسات والخيارات دورياً.

وقد تشكل خدمات التحليل والتنميط السلوكي خطراً خاصاً، إذ تنتج سجلات تفصيلية للهويات وعادات القراءة والسلوك. فلا تسمح بوصولها دون موافقة صريحة ومباشرة من المستفيد.

التطلع إلى المكتبات:

مع تولي الإدارة الجديدة في يناير نحتاج إلى المكتبيين أكثر من أي وقت؛ لحماية الوصول إلى المعلومات والخصوصية الفكرية، وتقليل مقدار البيانات المتاحة وتفصيلها، ومقاومة طلبات الحكومة عن المستخدمين.

وعلى الجميع تجاوز هذه الخطوات الأساسية إلى النظر في طيف التهديدات الكامل وحماية الخصوصية في بيئة متغيرة. ونحیی عمل المكتبات القائم، ونحث المجتمع المكتبي كله على خطوات إضافية قبل فوات الأوان.

المراجع:

روابط الإحالات الواردة في الأصل

- <https://www.theguardian.com/books/2016/nov/30/library-user-data-government-surveillance-donald-trump>
- <https://www.thenation.com/article/librarians-versus-nsa/>
- <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>
- <https://www.theguardian.com/us-news/2016/jan/13/us-library-records-purged-data-privacy>
- <https://www.eff.org/press/releases/internet-archive-received-national-security-letter-fbi-misinformation-about>
- <https://www.eff.org/press/archives/2011/10/03>
- <http://www.npr.org/sections/thetwo-way/2016/11/13/501921177/donald-trump-says-hell-deport-2-3-million-people-once-in-office>
- <http://www.nytimes.com/politics/first-draft/2015/11/20/donald-trump-says-hed-absolutely-require-muslims-to-register/>
- <http://www.politico.com/blogs/on-media/2016/02/donald-trump-libel-laws-219866>
- <https://ssd.eff.org/en/module/how-delete-your-data-securely-mac-os-x>
- <https://ssd.eff.org/en/module/how-delete-your-data-securely-windows>
- <https://www.eff.org/cases/2016-internet-archive-nsa>
- <https://www.eff.org/policy>
- <https://www.eff.org/deeplinks/2015/05/what-every-librarian-needs-know-about-https>
- <https://certbot.eff.org/>
- http://www.slate.com/articles/technology/future_tense/2016/07/the_fbi_should_need_a_warrant_to_access_your_browser_history.html
- <https://www.eff.org/privacybadger>
- <https://www.eff.org/https-everywhere%20>