Signal يمنع مساعدات الذكاء الاصطناعي في أنظمة التشغيل من قراءة المحادثات الخاصة



يمنع Signal مساعدات الذكاء الاصطناعي مثل Siri AI على iOS 27 وGeminig على أندرويد من التقاط محتوى المحادثات. تبقى ثغرات، أبرزها على macOS والملفات المحلية، لذا ينبغي للمؤسسات مراجعة تعرضها.

- يحجب Signal لقطات الشاشة داخل التطبيق على iOS 27 لمنع Siri AI من قراءة محتوى الرسائل، عبر إعداد باسم Block Siri AI.
- على أندرويد يكتشف التطبيق محاولة مساعد ذكاء اصطناعي قراءة الشاشة ويفعّل إعداد Screen security تلقائياً.
- تبقى قيود: يمكن لوكيل ذكاء اصطناعي الوصول إلى المحتوى المخزّن على الجهاز، ولا توجد حماية مماثلة على macOS.
- يُنصح مستخدمو macOS 27 بإضافة Signal إلى قائمة Excluded Apps ضمن System Settings

> Siri.

- تطالب Signal شركات Apple وGoogle وMicrosoft بآلية موثقة لاستثناء التطبيقات من وصول الذكاء الاصطناعي إلى الشاشة والملفات والإشعارات وواجهات البرمجة.

أطلق Signal حمايات تمنع مساعدات الذكاء الاصطناعي المدمجة في أنظمة تشغيل الهواتف من التقاط محتوى المحادثات. وتشمل Siri AI على iOS 27 والمساعدات على أجهزة أندرويد المدعومة، ومنها Gemini من Google.

أهمية الموضوع

تستطيع هذه المساعدات قراءة ما يظهر على شاشة الهاتف للإجابة عن الأسئلة وتنفيذ المهام. وبحسب Signal، قد يؤدي ذلك إلى نسخ نص الرسائل إلى قاعدة بيانات محلية أو خادم بعيد تستخدمه المساعدات، فيخرج المحتوى عن سيطرة التطبيق ويعرّض خصوصية جميع أطراف المحادثة، لا صاحب الجهاز وحده.

آلية الحماية

على iOS 27 يحجب Signal لقطات الشاشة داخل التطبيق كي لا تتمكن Siri AI من قراءة الرسائل عبر الشاشة، ويتحكم بذلك إعداد Block Siri AI. وعلى أندرويد يكتشف التطبيق محاولة المساعد قراءة الشاشة فيفعّل إعداد Screen security تلقائياً، إذ لا توفر كثير من الشركات المصنعة وسيلة موثوقة لاكتشاف محاولات التقاط الشاشة.

وتوضح Signal حدود هذه الحماية. فما زال بإمكان وكيل ذكاء اصطناعي استرجاع المحتوى المخزّن على الجهاز عبر نظام الملفات. وعلى macOS لا يستطيع Signal حجب لقطات الشاشة بشكل موثوق، لذلك يوصي مستخدمي macOS 27 بإضافته إلى قائمة Excluded Apps ضمن Siri > System Settings. ويمكن للمستخدم تعطيل الحماية، لكن ذلك قد يعرّض رسائله ورسائل جهات اتصاله للمساعدات.

وتطالب Signal شركات Apple وGoogle وMicrosoft بآلية موثقة تتيح للتطبيقات استثناء نفسها من وصول الذكاء الاصطناعي إلى محتوى الشاشة والملفات والإشعارات وواجهات البرمجة، مع توثيق أوضح لكيفية تعامل الوكلاء مع البيانات.

الخطوات المقترحة

بالنسبة للمؤسسات المنظمة، الخلاصة العملية أن مساعدات نظام التشغيل قد تصل إلى المحتوى الحساس المعروض في أي تطبيق. وتساعد الإجراءات التالية على إدراج ذلك ضمن ضوابط الأجهزة المحمولة وحماية البيانات القائمة.

ما يجب فعله الآن

1. حصر الموظفين الذين يستخدمون Signal أو تطبيقات مراسلة مشابهة في العمل، وتحديد مساعدات الذكاء الاصطناعي المفعّلة على أجهزتهم.
2. تحديث سياسات إدارة الأجهزة المحمولة والاستخدام المقبول لتشمل مساعدات الذكاء الاصطناعي التي تملك صلاحية قراءة الشاشة.
3. توجيه الموظفين إلى إبقاء إعدادي Block Siri AI وScreen security مفعّلين، وإضافة Signal إلى

Excluded Apps على macOS 27.

4. تقييم احتمال وصول بيانات مصنفة أو شخصية متداولة في تطبيقات المراسلة إلى قواعد بيانات المساعدات، وإدراج ذلك في تقييمات المخاطر وفق نظام حماية البيانات الشخصية PDPL وضوابط NCA ECC.
5. مخاطبة مزودي الأجهزة وأنظمة التشغيل بشأن نقص التوثيق وطلب تفاصيل واضحة عن كيفية معالجة المساعدات لبيانات التطبيقات.