دليل تأمين سيجنال

EUROPEAN ENDOWMENT FOR DEMOCRACY

دَلِيلُ تَأمِينِ سيجنال

جدول المحتويات

مقدمة

أليس سيجنال آمنا بالفعل؟ لماذا نحتاج لتأمينه إذن؟ بلى، سيجنال أحد أكثر منصات التراسل موثوقية لدى خبراء الأمان الرقمي بسبب بروتوكول تشفيره الذي أصبح أشهر بروتوكولات تشفير المراسلات حاليا، وهو المعروف ببروتوكول end-to-end encryption (واختصارا e2ee) أو التشفير من طرف لطرف. وهذا البروتوكول هو الميزة الأساسية في سيجنال بالإضافة إلى جعل تشفيره مقاوما لحواسيب الكم وكونه مفتوح المصدر واحتوائه عدة مزايا أمنية أخرى، كل تلك الأشياء تجعل سيجنال خيارا آمنا، لكن بغض النظر عن قوة بروتوكول تشفيره، فقد تأتي التهديدات من جوانب أخرى تماما، كأن يقع الهاتف في يد شخص غير مرغوب، أو أن يكون الجهاز الذي نستخدم سيجنال من خلاله مصابا ببرمجية خبيثة تسجل محتوى الشاشة، وقد فكر مطورو سيجنال بهذه الأمور ووضعوا لها بعض الحلول، لكن ليست كل تلك

الحلول مفعلة تلقائيا، فلتحقيق أكبر قدر من الحماية سيتعين علينا التخلي عن بعض الرفاهية، لهذا يجب علينا التفكير قليلا في بعض جوانب ومزايا التطبيق واتخاذ قرارات بخصوص المزايا التي نريد تفعيلها لزيادة الأمان أو إلغاءها لتسهيل الاستخدام. ليس الهدف من هذا الدليل حث جميع المستخدمين على تفعيل جميع الخيارات الأمنية، إنما يهدف إلى توضيح الهدف من كل خيار حتى يتمكن كل شخص من تحديد ما يناسبه منها. سنبدأ بتحديد المزايا الأساسية لسيجنال والتي يتمتع بها جميع مستخدميه، ثم سننتقل إلى المزايا الاختيارية التي قد يود بعض المستخدمين تفعيلها لكنها ليست إلزامية.

المزايا الأساسية

هذه المزايا أساسية في خدمة سيجنال، أي أنها ليست اختيارية بحيث يمكن تفعيلها أو إلغاء تفعيلها، وهي ما تميز سيجنال بالأساس وتعطيه سمعته وموثوقيته كمنصة تراسل آمنة.

التشفير من طرف لطرف

بروتوكول تشفير المراسلات الذي ابتكرته سيجنال يعتبر أكثر بروتوكولات تشفير الرسائل موثوقية وحيث أنه ليس احتكاريا فإن العديد من منصات التراسل الأخرى تعتمد عليه أيضا، وهو يضمن أن الرسائل بين طرفين لا يمكن اعتراضها ومعرفة فحواها بواسطة أي طرف ثالث يتمكن من اعتراض الرسائل؛ حيث أن الرسائل يتم تشفيرها على جهاز الراسل وتنتقل بصورة مشفرة عبر الإنترنت ثم يتم فك تشفيرها على جهاز المرسل إليه، وهذا ما يؤمن عملية نقل آمنة للرسائل ويحميها من المتلصصين المحتملين.

التشفير المقاوم لحواسيب الكم

قام سيجنال مؤخرا بتطوير بروتوكول التشفير الشهير حتى يصبح منيعا أمام حواسيب الكم التي يمكن تطويرها في المستقبل والتي قد تكتسب فيما بعد

قدرة على كسر تشفير بعض المراسلات. لم تتمكن حواسيب الكم الحالية من كسر التشفير حتى الآن، لكن هذا التطوير لمقاومة حواسيب الكم يحمي المراسلات من إمكانية كسر تشفيرها في المستقبل إذا تطورت حواسيب الكم بعد ذلك.

المصدر المفتوح

يعتمد سيجنال على الشفافية في عمله بحيث يتيح الكود المصدري لتطبيقاته وخوادمه للعامة فيمكن لأي شخص يمتلك المعرفة التقنية اللازمة فحصها والتأكد من خلوها من الوظائف الخبيثة، وكذلك يمكن للمبرجمين الآخرين المساهمة في تطويره وتقديم الاقتراحات.

المزايا الاختيارية

هذه المزايا اختيارية في تطبيق سيجنال، يمكن تفعيلها وتعطيلها حسب الحاجة، والعديد منها لا يتوفر على نسخة سطح المكتب من التطبيق.

الرسائل المؤقتة

يمنحنا تشفير الرسائل أمانا من قدرة أطراف أخرى على اعتراض هذه الرسائل وقراءتها أثناء إرسالها، لكن ماذا إذا وقع جهازنا أو جهاز الشخص الذي نراسله في الأيدي الخطأ؟ أحد الحلول لتجنب وصول رسائلنا الحساسة إلى طرف غير مرغوب فيه هو جعلها مؤقتة، أي أن يتم حذف الرسائل تلقائيا بعد قراءتها بوقت محدد. ويمكن القيام بهذا إما لكل محادثة بشكل منفرد، أو ضبط هذا الخيار ليجعل الرسائل في جميع المحادثات مؤقتة. لضبط هذا الخيار للمحادثات بشكل منفرد، نفتح المحادثة ثم نحدد مدة بقاء الرسائل قبل حذفها. يجب أن ننبه مجددا أن توقيت حذف الرسائل المؤقتة لا يُحتسب منذ وقت إرسالها إنما منذ وقت قراءتها، أي أنني إذا ضبطت الرسائل المؤقتة إلى ساعة واحدة ثم أرسلت رسالة يوم الخميس في الساعة الثامنة، ورآها المرسل إليه يوم الجمعة في الساعة الخامسة، فإن سيجنال سيحذف الرسالة يوم الجمعة في الساعة السادسة دون اعتبار لوقت إرسالها، إنما لوقت قراءتها.

تغيير أيقونة التطبيق

(أندرويد فقط)

يسمح تطبيق سيجال على نظام تشغيل أندرويد بتغيير شكل الأيقونة إلى شكل آخر قد لا يثير الشك مثل أيقونة لتطبيق أخبار أو تطبيق ملاحظات أو تطبيق طقس أو أيقونة أمواج، ويجب الانتباه إلى أن هذا التغيير لا ينطبق سوى على قائمة التطبيقات في الشاشة الرئيسة فحسب، بينما ستظل أيقونة سيجنال كما هي في باقي الأماكن كإعدادات التطبيقات وأحيانا كذلك قائمة الإشعارات، لهذا لا يجب الاعتماد عليها كوسيلة أساسية لإخفاء التطبيق، وللمزيد حول إخفاء التطبيقات، اقرأوا دليلنا حول إخفاء التطبيقات (**هنا**). وهذا الخيار موجود في خيارات المظهر في إعدادات سيجنال.

معاينة الروابط

عند إرسال رابط من خلال رسائل سيجنال فإن سيجنال يتصل بذلك الرابط من أجل إظهار معاينة لهذا الرابط تظهر في الرسالة، وهذا يتضمن أن يقول سيجنال بإرسال طلب إلى هذا الموقع، ولهذا فإن من المفيد إلغاء معاينات الروابط من سيجنال، ويمكن التحكم في ذلك من خلال إعدادات المحادثات في سيجنال.

قفل الشاشة

إذا تمكن أحد من الاستيلاء على هاتفك وهو مفتوح، فبوسعه الوصول إلى معظم محتويات هاتفك بما في ذلك تطبيق سيجنال والمحادثات بداخله، لكن تفعيل خيار قفل الشاشة يجعل سيجنال يطلب تأكيد قفل الشاشة مجددا عند فتحه للتأكد من أن صاحب الهاتف هو من يحاول فتحه بالفعل وليس شخصا استولى على الهاتف بينما كان مفتوحا، وهذا الخيار موجود ضمن خيارات الخصوصية في التطبيق.

الإشعارات

الكثير من الهواتف تُظهر الإشعارات حتى قبل فك قفل الهاتف، وفي هذه الحالة ننصح بتعديل إعدادات خصوصية الإشعارات في هاتفك، لكن قد نود التحكم بهذه الإشعارات حتى عندما يكون الهاتف مفتوحا، وفي هذه الحالة فإن سيجنال يوفر تحكما في المحتوى الذي يظهر في الإشعارات، ويمنح سيجنال المستخدم خيار إظهار اسم الراسل ومحتوى الرسالة في الإشعار، أو إظهار اسم الراسل فقط وإخفاء محتوى الرسالة، أو إخفاء اسم الراسل ومحتوى الرسالة كليهما. ويمكن الوصول إلى إعدادات الإشعارات في خيار الإشعارات في إعدادات سيجنال.

منع لقطات الشاشة

يعطي سيجنال مستخدمه خيار منع ظهور لقطة شاشة من سيجنال في قائمة التطبيقات المفتوحة، وهذا مفيد أيضا في أشياء أخرى، فمثلا في حال قيام أي مهاجم باختراق الجهاز وتنصيب برمجية خبيثة تقوم بالتقاط الشاشة وإرسال محتوياتها لهذا المهاجم فإن محتويات شاشة سيجنال لن تظهر مطلقا، وكذلك فإن الشاشة لن تظهر بالخطأ عند بث محتوى شاشة الهاتف إلى التلفاز مثلا، لذلك يجب إيقاف هذا الخيار إذا كان المستخدم يود أخذ لقطات للشاشة من التطبيق، أو يود بث محتواه على شاشات التلفاز مثلا. ويمكن التحكم في هذا الخيار عن طريق إعدادات الخصوصية.

تحويل المكالمات

لجعل المكالمات الصوتية ومكالمات الفيديو أسرع يقوم سيجنال بربط المتصلين ببعضهما باستخدام بروتوكول يسمح للطرف الذي يملك معرفة تقنية كاملة بمعرفة عنوان الـ IP للطرف الآخر، ولتجنب هذا الأمر يمكن تحويل المكالمات إلى سيرفر سيجنال، وهذا سيحمي عنوان الـ IP من الطرف الآخر لكنه سيقلل من جودة الاتصال. ويمكن إيجاد هذا الخيار ضمن خيارات الخصوصية المتقدمة تحت اسم "دعم المكالمات دوما".

إخفاء الرقم

يمنح سيجنال المستخدم القدرة على التحكم في مدى مجهولية رقم الهاتف، وبشكل افتراضي لا يسمح سيجنال للمستخدمين الآخرين برؤية رقم هاتفك، لكنه يسمح لمن يملكون رقم هاتفك بالعثور على حسابك ويمكن للمستخدم التحكم إذا كان بوسع الآخرين رؤية رقم الهاتف أو لا، وإذا كان بوسع من يملكون رقم الهاتف العثور على الحساب أو لا، وتعطيل هذين الخيارين مفيد في حال أراد المستخدم إنكار امتلاكه حسابا على سيجنال من الأساس، حتى إذا كان الشخص أو الجهة الذين يحاولون معرفة حقيقة امتلاك المستخدم حسابا على سيجنال لديهم بالفعل رقم هاتفه، وبدلا عن تبادل أرقام الهواتف يمكن للمستخدمين تبادل أسماء المستخدم فقط. وهذه الخيارات موجودة في إعدادات سيجنال، في إعدادات الخصوصية، ثم إعدادات رقم الهاتف.

لوحة المفاتيح الخاصة

عند الكتابة على الهاتف، فإن الكثير من لوحات المفاتيح تسجل ما يكتبه المستخدم لتقديم اقتراحات إكمال النص أثناء كتابة نصوص جديدة عن طريق الاحتفاظ بالنصوص القديمة، وهذا ما قد يمثل خطرا إذا كانت لوحة المفاتيح غير موثوقة أو تعرضت للاختراق، ونوصي عموما باستخدام لوحات المفاتيح الموثوقة فقط وإلغاء تفعيل خيار الإكمال التلقائي، لكن سيجنال

يوفر خيارا خاصا به يمكنه من أن يطلب من لوحة المفاتيح عدم الاحتفاظ بالنصوص التي يكتبها المستخدم داخل تطبيق سيجنال حصرا، لكن يجب أيضا التنويه على أن لوحات المفاتيح غير الآمنة قد تتجاهل هذا الطلب، ويمكن تفعيل هذا الخيار داخل سيجنال من خيارات الخصوصية تحت اسم "لوحة مفاتيح في وضع متخفي".

تجاوز الرقابة

إذا كان المستخدم يعيش في دولة تقوم بحجب سيجنال فإن التطبيق يوفر إمكانية تجاوز هذا الحجب عبر جعل الاتصال بسيجنال يبدو كأنه اتصال بمواقع عامة أخرى، وتفيد هذه الخاصية أيضا حتى عندما لا يكون سيجنال محجوبا في بلد المستخدم عندما يرغب المستخدم في إخفاء حقيقة استخدامه لسيجنال عن أي جهة قد تتمكن من اعتراض اتصاله، وفي هذه الحالة، فإننا نوصي باستخدام شبكة خاصة افتراضية (VPN)، وقد تناولنا هذا بالتفصيل في **دليلنا لتأمين الاتصال بالإنترنت**. ويمكن العثور على هذا الخيار ضمن خيارات الخصوصية المتقدمة.