كبسولة المراسلات الآمنة

متون
matoon

كبســـــــــولة
المراسلات الآمنة

جدول المحتويات

مقدمة	3
البريد الإلكتروني	3
أجهزة الموبايل	5
إعدادات الخصوصية في سيجنال	6
تأكيد الهوية	8
نقائص وأوجه قصور	10
ختام	11

مقدمة

عممت التقنية اليوم استخدام المراسلات بشكل واسع في العمل وبين الأصدقاء وفي أماكن الدراسة وحتى للأمور الترفيهية، ويعتمد الكثير من المستخدمين على تطبيقات الشات والإيميل والمراسلات المختلفة يوميًا بما فيهم من موظفون وصحفيون ونشطاء أو مستخدمين عاديين لديهم بيانات حساسة وقد يشمل هذا كل البشر الذين يعتبرون الخصوصية من الأشياء التي يجب الحفاظ عليها وصونها حتى وإن لم يعرف الجميع هذا إلى أن يصل الأمر إلى انتهاك خصوصيتهم/ن، في هذه الكبسولة نقدم المعلومات الأساسية للحصول على مراسلات آمنة على جميع الأجهزة الرقمية

البريد الإلكتروني

الإيميل ليس مشفرًا!

معظم خدمات الإيميل الشهيرة ليست مشفرة افتراضيًا بشكل كافي، على عكس ما يعتقد البعض، فإن أردت الحصول على إيميل مشفر عليك استخدام تطبيق لتشفير الملفات والرسائل في أي مكان مثل PGP الذي يشفر كافة الملفات والرسائل على أي خدمة إيميل، أو حتى تشفير الملفات على الأجهزة بشكل محلي -داخل الجهاز نفسه- والذي يقدم خدمة تشفير لا تعتمد على مقدم الخدمة أو المنصة platform-agnostic ولهذا ينصح الكثير بتشفير PGP لاستخدامه على خدمات الإيميل، لأنه قديم ومجرب بشكل كبير ولهذا يقدم موثوقية عالية بالإضافة لأنه مستخدم بشكل واسع.

لاستخدام بروتوكول تشفير PGP على خدمة البريد الإلكتروني توجد العديد من الخيارات، منها اختيار منصة تدعم PGP بشكل افتراضي أو استخدام البروتوكول بشكل يدوي عن طريق برنامج على الجهاز المستخدم.

من البرامج التي تدعم بروتوكول PGP برنامج Kleopatra المتوفر على ويندوز ولينكس بالإضافة إلى توفره على سطر الأوامر في ويندوز ولينكس أيضًا، وعن طريقه يمكن تشفير الملفات والايميلات وغيرها من النصوص، كما أن بروتوكول PGP يمكننا من التأكد من هوية المراسل فيه حال عدم التأكد من الهوية أو التأكد من الهوية بشكل عام على الإنترنت بما فيها الحسابات (للمزيد قراءة جزء تأكيد الهوية لاحقًا).

يمكنكم الرجوع إلى فيديوهات متون عن PGP عن كيفية إنشاء مفاتيح تشفير PGP (ويندوز ولينكس وماك) وعن كيفية إنشاء مفاتيح تشفيرمع تطبيق ثندربيرد

بالإضافة إلى مقال متون عن بروتوكولات التعمية (التشفير)

أما في حالة أردتم الحصول على خدمات إيميل مشفرة، توجد بعض الخيارات مثل: **بروتون ميل، توتانوتا، سكيف**

قد تقدم خدمات الإيميل المشفرة بديلًا أسهل في الاستخدام من PGP حتى وإن كانت لا تقدم نفس الخيارات الكاملة التي يقدمها PGP مثل تشفير الملفات على أي منصة أو جهاز أو نظام تشغيل ولكنها قد تكون مناسبة بشكل كبير بالنسبة للأفراد، أو للمؤسسات التي تحتاج إلى تشفير واسع بالنسبة للعاملين بها أو المستفيدين منها كما أنها تقدم خدمات أخرى مثل تطبيقات التقويم ونقل الملفات بشكل مشفر بدلًا من استخدام خدمات غير صديقة للخصوصية مثل تطبيقات جوجل كالندر وغيرها من التطبيقات المعروف عنها جمع المعلومات بشكل كبير.

أجهزة الموبايل

أشهر تطبيقات التراسل الحديثة إما مشفرة إفتراضيًا أو تقدم خدمة التشفير من إعداداتها، مثل تطبيقي واتساب وسيجنال الشهيرين، واللذان يقدمان تشفير افتراضي باستخدام نفس البروتوكول (بروتوكول سيجنال) والذي تمت إضافته لتطبيق واتساب منذ عدة سنوات.

واتساب هو التطبيق الأشهر للمراسلات في العالم ويقدم تشفير **من طرف إلى طرف** بما يعني أنه لا يمكن معرفة ما تحتويه أيًا من رسائل الطرفين، ولكن عليك الحذر إذا تغيَّر كود الأمان الخاص بالطرف الآخر لأن هذا قد يعني أن واتساب الطرف الأخر تغيَّر وربما تغيرت هويته -تم سرقة حسابه أو تغيير رقم الهاتف الخاص به- ويجب التأكد من هوية الشخص الذي نقوم بمراسلته في هذا الحالة عن طريق آخر غير واتساب، ويفضَّل بطريقة لا تحمل شكًا كالمقابلة الشخصية أو مكالمة شخصية، وليس استخدام تطبيق آخر.
*للمستخدمين المتقدمين من الممكن استخدام طريقة للتأكد من هوية الغير مثل **بروتوكول بي جي بي** أو أحد خدمات التأكد من الهوية مثل **كي بيز** (سنوضح في قسم تأكيد الهوية أدناه).

في المقابل يقدم سيجنال نفس التشفير المستخدم في واتساب ولكن مع إعدادات خصوصية أعلى نسبيًا من تطبيق واتساب بما فيها إمكانية إخفاء الرقم أو حتى تمويه التطبيق نفسه على الجهاز، كما أنه مفيد في حالات الرقابة على بعض التطبيقات في بعض الدول التي تقوم بمنع تطبيقات التراسل مثل إيران، لأن سيجنال يستخدم شبكة واسعة من خدمات كسر الحجب ومنها شبكة Proxy خاصة ومتقدمة وغير مركزية بشكلٍ كبير، حيث يقوم عدد من المستخدمين بتشغيلها بأنفسهم بالإضافة إلى خوادم الشركة نفسها.

ولكن هذا لا يعني عدم وجود تطبيقات أخرى كثيرة، لأنه توجد الآن تطبيقات كثيرة تدعم التشفير والخصوصية مثل: **وايرـ سيشن، سمبلكس تشات** وتقدم كل البرامج مزايا مختلفة عن غيرها قد تكون مناسبة لبعض المستخدمين عن غيرهم.

يقدم سيشن نظام لا مركزي للتراسل ولا يحتاج لرقم هاتف، والتطبيق نفسه على أندرويد مبني على أساس تطبيق سيجنال ولكن من غير المعروف إلى أين يتجه تطوير التطبيق والشبكة في المستقبل.

بينما يقدم سيبملكس تشات أول تطبيق بدون أي نظام تعريفي ولا حتى عنوان ثابت للتواصل! وبرغم أن التطبيق ما زال في مرحلة التجريب لكنه مشروع واعد للغاية لتقديم الخصوصية ويقدم التطبيق إمكانيات مختلفة من اختيارات الشبكات من بينها شبكات شخصية أو خاصة بما يقدم ميزة مهمة للغاية من ناحية الخصوصية وتعدد الخيارات للمستخدمين.

*يمكنكم الرجوع إلى ويكي السلامة الرقمية للقراءة عن المراسلات سواء الفورية أو عبر البريد الالكتروني.

إعدادات الخصوصية في سيجنال

1. **تخصيص اسم مستخدم**

الضغط على رقم المستخدم > اختيار اسم للمستخدم عن علامة @

2. **إخفاء رقم الهاتف**

يمكنك التحكم بمن يمكنه رؤية رقم هاتفك عند التحدث إليك على سيجنال

الإعدادات > الخصوصية > رقم الهاتف

3. **إرسال صورة قابلة للعرض مرة واحدة**

يمكنك إرسال صورة يمكن مشاهدتها لمرة واحدة فقط، ومن ثم تختفي

فتح المحادثة > ثم النقر أيقونة (+) > اختر الصورة من المعرض > بعد ذلك انقر على أيقونة الدائرة بالرمز (∞) > لتبديلها إلى دائرة برمز (1x)
بمجرد الانتهاء قم بارسال الصورة، وسيتم حذفها تلقائيًا بمجرد مشاهدتها لمرة واحدة فقط.

4. رسائل التدمير الذاتي

وهي ميزة تعمل اختفاء الرسائل في المحادثات بعد قراءة المستلم للرسالة بوقت معين من تحديد المستخدم

افتح محادثة > ثم انقر على القائمة ثلاثية النقاط في الأعلى > من قائمة الخيارات انقر على "الرسائل المخفية" > من هنا حدد وقت اختفاء الرسائل.

5. الرقم التعريفي الشخصي

يتطلب رمز PIN الخاص بك عند تسجيل رقم هاتفك مرة أخرى باستخدام سيجنال

الإعدادات > الخصوصية > قم بالنقر على "الرقم التعريفي الشخصي لحماية التسجيل" > ثم انقر على "تشغيل".

6. تأمين الشاشة

تمنع التقاط الآخرين لقطات الشاشة للمحادثات التي تجريها معهم

الإعدادات > الخصوصية > قم بتشغيل مفتاح التبديل بجوار "تأمين الشاشة".

7. **قفل الشاشة**

ميزة تجعل التطبيق أكثر أمانًا، بحيث لا يمكن لأحد عند استخدام هاتفك من الوصول إلى قائمة محادثاتك

الإعدادات > الخصوصية > تبديل مفتاح "قفل الشاشة" إلى تشغيل.

8. **وضع التخفّي في لوحة مفاتيح**

هذه الميزة تمنع لوحة المفاتيح من إرسال الكتابة في محادثات سيجنال إلى جهة خارجية، مما قد يسمح بتسريب البيانات الحساسة.

انتقل إلى الخصوصية > ثم فعل مفتاح التبديل بجوال "وضع التخفّي للوحة مفاتيح"

9. **تمويه تطبيق سيجنال على الهاتف**

يمكن تغيير شكل أيقونة التطبيق على الهاتف، قد يحتاج هذا إلى صلاحية من نظام التشغيل

اختيار المظهر > أيقونة التطبيق > تغيير الأيقونة

تأكيد الهوية

للتراسل الآمن على الإنترنت يجب تأكيد هوية المراسلين ببعضهم البعض، لأنه رغم استخدام تطبيقات مشفرة قد لا يكون كافيًا في حالة أن الشخص المراسل هو شخص منتحل للشخصية الحقيقية التي نريد التواصل معها أو انتحال شخصياتنا على الإنترنت مع أشخاص نتراسل معهم بانتظام.

وكما أسلفنا يمكن تأكيد الهوية عن طريق خدمات مختلفة منها بروتوكول PGP الشهير أو خدمات مثل Keybase وغيرها من الخدمات ولكن هنا سنحاول الحديث عنها باستفاضة أكبر.

1. بروتوكول بي جي بي PGP لتأكيد الهوية

ارتبط في أحيان كثيرة بروتوكول التشفير PGP بما يسمى بخادم PGP لحفظ الهويات المستخدمة عن طريق الأفراد المختلفين في تشفير ملفاتهم / نصوصهم ويستخدم الخادم لحفظ اسم المستخدم ومفتاح التشفير العلني الخاص به وبالتالي يمكن تأكيد هوية الشخص عن طريق هذا الخادم الذي يرتبط بإيميل أو بحساب معين يستخدمه الشخص المراد التأكد من هويته.

على سبيل مثال يستخدم يوسف إيميل بعنوان test@test.com ومفتاح PGP معين، نحن نعلم الإيميل الذي يستخدمه يوسف فيمكننا البحث عنه على الخادم والتأكد من مفتاحه العلني لتأكيد هويته، حيث يأكد الخادم مسبقًا ترابط المفتاحين العلني والسري ليوسف.

بالتالي عندما نراسل يوسف مرة أخرى يمكننا التأكد بشكل كبير من هويته ما لم تتم سرقة مفتاحه السري.

2. تطبيق كي بيز Keybase لتأكيد الهويات

يستخدم تطبيق Keybase والموجود على رابط https://keybase.io تقنية تشبه كثيرًا المستخدمه في خوادم PGP ولكنها توسع طريقة التأكيد من الهوية لربطها بالهواتف المحمولة للمستخدم وحسابات السوشيال ميديا خاصته أيضًا.

يقوم الموقع في البداية بتأكيد هوية الشخص عن طريق تأكيد هويته على حسابات السوشيال ميديا المختلفة إما عن طريق رسالة أو حتى عن طريق صفحة ويب يقوم بإنشائها على موقعه الخاص أو عن طريق PGP كذلك، بالتالي يقوم الموقع يجمع معظم أنواع التأكيد في موقع واحد مركزي.

يسمح تطبيق وموقع Keybase بالتراسل على الموقع نفسه بدلًا من استخدام مواقع أو تطبيقات أخرى إلا أنه محدود الإمكانيات لكنه قد يكون مفيدًا فيه حالات معينة عند عدم التأكد من هوية الشخص على أي تطبيق أو موقع آخر.

توجد بدائل أخرى لتطبيق كي بيز كذلك مثل تطبيق كي أوكسايد Keoxide مفتوح المصدر ولكن المشروع ما زال في بداياته بشكل كبير.

نقائص وأوجه قصور

يعتمد التراسل الآمن على أن الأجهزة التي تستخدم في التراسل مؤمنة بشكل كبير ولا يحتوي نظام التشغيل أو الجهاز على فيروسات قد تؤثر على التراسل نفسه، وهذا يمكن بشكل ما التأكد منه عبر استخدام مضادات الفيروسات التي تحمي من عدد كبير من الفيروسات المعروفة ولكنها ليست فعالة بنسبة 100%

فيه حالات أخرى يمكن استخدام أجهزة افتراضية Virtual machines للتراسل من خلالها حيث أنها تقدم تأمين كبير حتى في حالة أن الجهاز المستخدم ليس مؤمنًا بشكل كامل أو مشكوك في أمنه، ولكن من الأفضل أن يكون استخدام الأجهزة الافتراضية من الطرفين لان اختراق طرف واحد قد يعني اختراق الطرف التاني حتى إن كان الطرف الثاني مؤمنًا بشكل كبير.

وفيه الحالات القصوى يمكن استخدام أجهزة مخصصة فقط لمهمة واحدة، سواء كانت التراسل مع مجموعة من الأشخاص أو حتى لمراسلة واحدة فقط في الحالات الأكثر حساسية.

ختام

التراسل الآمن اليوم لم يعد رفاهية في ظل الجمع الكبير للمعلومات من على معظم المنصات والحكومات ولكنه صار أسهل بفضل المشاريع الواعدة المتعددة والعديد من التحولات في المشاريع القائمة بالفعل والمستخدمة عن طريق ملايين من المستخدمين ولكن ربط التراسل الآمن بزيادة الخصوصية ما زال غير معروفًا للكثير من مستخدمي الإنترنت ولكن عن طريق قدر صغير من المعرفة يمكننا تحقيق قدر كبير من الأمن والخصوصية كذلك.