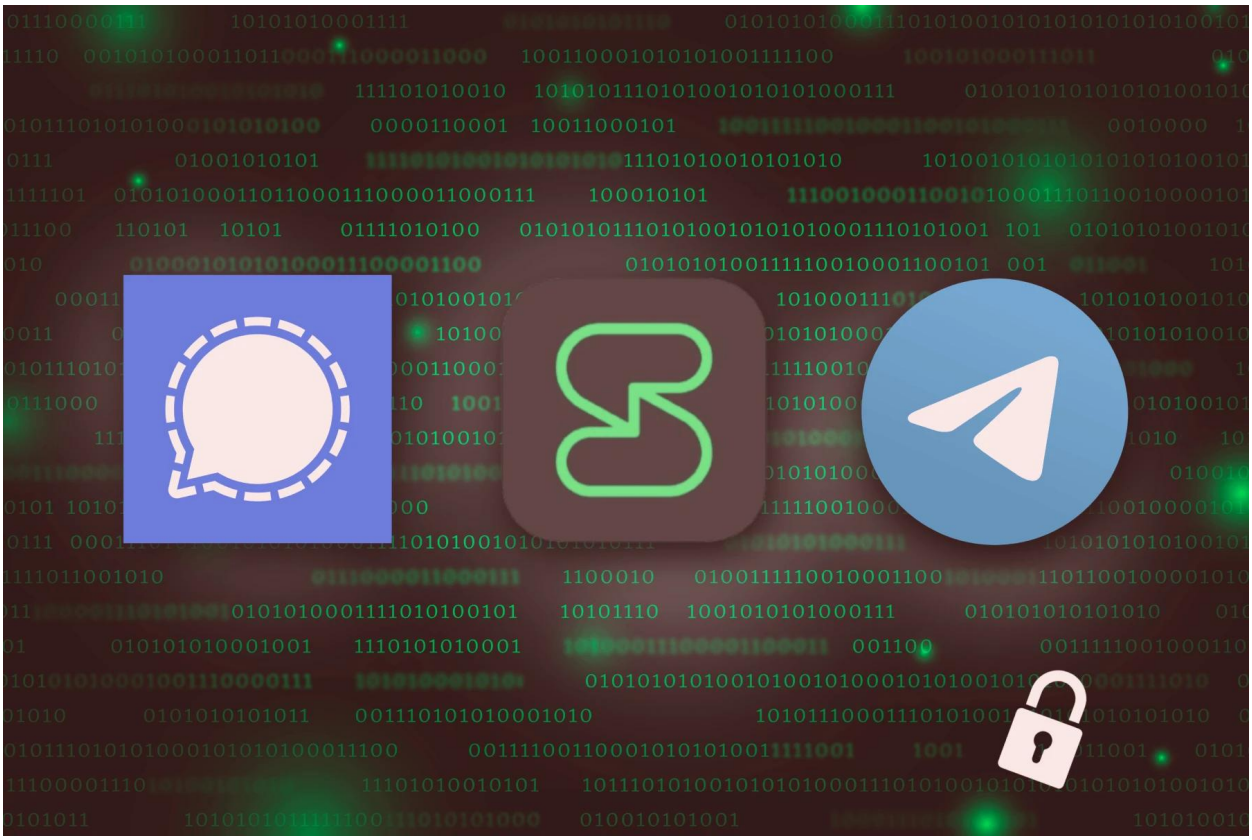
هل تطبيق Session آمن فعلاً؟ تحليل لخصائص الحماية ومشاكل الخصوصية

حمزة حسن | August 26, 2025



في البيئات السياسية الخانقة كما هو الحال في الشرق الأوسط، قد يكون التحدي الأكبر الذي يواجه الناشط أو الصحفي أو حتى المتعاون السلمي هو الهاتف الذي يحمله في جيبه. فرسالة واحدة غير محمية قد تتحول إلى خيط يقود أجهزة الأمن إلى شبكة كاملة من الأصدقاء والزملاء أو حتى الشخص نفسه بشكل قد يهدد حياته أو عمله في ظل وجود أنظمة مقيدة للحريات كما هو الحال الآن.

لذلك يعد الأمن الرقمي في هذا الوقت ضرورة أساسية وليست رفاهية. لكن السؤال الذي يواجهه كل ناشط يوميا هو: كيف أرسل رسالة حساسة لشخص ما، مرة واحدة فقط، ثم أختفي دون أن أترك أثرا؟

نحاول في هذا المقال أن نقدم إطارًا عمليًا ولكن لا نعدك بحل سحري، حيث سنتوقف عند أشهر التطبيقات المستخدمة حاليا في التواصل مثل Telegram و Signal، ثم نركز على Session كأداة غير مشهورة قد تمنح النشطاء خيارا جديدا ومختلفا خصوصا في الحالة التي نتكلم هنا وهي رسائل المرة الواحدة.

الرقابة لم تعد ترفًا تقنيًا

في معظم الأنظمة المقيدة للحريات اليوم لم تعد المراقبة الرقمية خيارا لها، بل أصبحت سياسة تمارسها بشكل يومي، فالأجهزة الأمنية لهذه الدول لم تعد بحاجة إلى قراءة نصوص رسائلك لتعرف الكثير عنك، بل يكفيها جمع ما يسمى بـ الميتاداتا.

ماهي الميتاداتا ؟

الميتاداتا لا تعني محتوى الرسالة نفسه، وإنما المعلومات المحيطة بها وفي حالتنا هي: من الذي تواصلت معه، في أي ساعة تم هذا التواصل، من أي مكان، وكم مرة تكرر هذا التواصل. والمفارقة أن هذه البيانات قد تكون أحيانًا أخطر من نص الرسالة نفسها، لأنها تكشف "شبكة العلاقات" بدلًا من مجرد جملة واحدة.

و لتوضيح المسألة دعنا نضرب مثالا : تخيل صحفيًا تواصل مع منظمة حقوقية دولية عبر تطبيق مشفّر. ورغم أن السلطات لم تستطع قراءة الرسائل نفسها، لكنهم لاحظوا أن هاتفه تواصل أكثر من مرة مع رقم دولي محدد في ساعات الليل. هذه المعلومة وحدها كافية لإثارة الشك وربط هذا الصحفي بتسريب أو تعاون "غير مرغوب فيه".

الخطير أن هذا كله لم يعد يحتاج إلى جندي يتنصت على المكالمات أو يتتبع الرسائل الصادرة والواردة، فاليوم أصبحت برامج التحليل الآلية قادرة على ابتلاع ملايين السجلات يوميا ومعالجتها بضغطة زر، فترسم خريطة اجتماعية تحدد بها من هو "المركز"، ومن يتواصل مع من، ومن يظهر فجأة على الخط ومن يختفي.

ولهذا السبب، لم يعد يكفي الناشط أن يقول "أنا أستخدم تطبيقا مشفرا". حتى أن أقوى التطبيقات قد تترك أثرا من الميتاداتا إذا استخدمت بشكل متكرر أو من نفس الجهاز والهوية لتحديد مكانك و هويتك وشخصيتك وشخصك. ما يحتاجه الناشط فعلا هو وسيلة تسمح له بإرسال رسالة واحدة ثم محو هويته الرقمية فورا من أجل تقليل الأثر ومنع أي طرف آخر من رسم شبكة حوله.

لماذا لا تكفي الأدوات الشائعة؟

كثير من النشطاء حتى اليوم يعتمدون على التطبيقات الشهيرة والمنتشرة في التواصل لسهولة استخدامها، لكن عندما نتحدث عن رسائل حساسة لمرة واحدة تظهر لنا بعض القيود التي تجعل من هذه البرامج وسائل غير مناسبة:

- Telegram: لا يفعّل التشفير الطرفي بشكل مباشر إلا في المحادثات السرية فقط "Secret Chats"، ومعظم المستخدمين لا يستعملونها أصلا بل أن الكثير يجهل تواجدها. هذا يعني أن أغلب المحادثات تبقى محفوظة على خوادم مركزية يمكن الوصول إليها قانونيًا أو بالضغط. فوق ذلك، يحتاج Telegram إلى رقم هاتف للتسجيل، ما يجعل الهوية دائمًا مرتبطة بخط SIM.

• Signal: يعتبر الأكثر قوة وموثوقية في التشفير المفتوح المصدر، وموصى به عالميا للتواصل طويل المدى. لكن مشكلته الأساسية أنه لا يعمل إلا برقم هاتف.

حتى لو حاول الناشط الالتفاف على مشكلة الرقم عن طريق شراء بطاقة SIM غير مسجلة باسمه، فإن تشغيلها على أي هاتف قد يكشف لمزود الخدمة (شركة الإتصالات) رقم الجهاز (IMEI) وبذلك يربط البطاقة بالجهاز الذي فُعّل الحساب من خلال، كما أن عملية التفعيل تسجل أيضا الموقع الجغرافي التقريبي عبر أبراج الشبكة، مما يمنح السلطات "بصمة مكانية وزمنية" لوقت التفعيل.

ولتوضيح ذلك سنقوم بضرب مثال واقعي:

لنتخيل أن هناك ناشط حقوقي يريد إرسال ملف حساس لمرة واحدة عبر تطبيق سيجنال Signal، يقوم الناشط بشراء بطاقة سيم كارد (خط) SIM جديدة ويظن أنها ستبقى مجهولة، لكنه ومن أجل أن يستقبل رمز التفعيل يضعها في هاتفه الشخصي لدقيقة واحدة، في هذه اللحظة، تسجل شركة الاتصالات هذه المعلومات:

1. رقم البطاقة (SIM).
2. رقم الجهاز (IMEI).
3. الموقع الجغرافي للأبراج التي اتصل بها الهاتف.

بهذه البيانات، يمكن للسلطات تضييق النطاق بسرعة: "الرقم تم تشغيله في الحي الفلاني الساعة 9 مساء، وعلى جهاز من نوع سامسونج برقم ايمي كذا"، وبالتالي حتى لو لم يكن الرقم مسجلا باسمه، فإن هذا الربط الزمني–المكاني قد يكفي للإشارة إليه ومعرفة من هو.

ولهذا السبب، ورغم قوة تطبيقي سيجنال وتليجرام في التشفير، إلا أن اعتمادهما على رقم الهاتف يجعل استخدامهما لرسائل "مرة واحدة" محفوفًا بالمخاطر التقنية، ويترك أثرًا قد يُستخدم ضد الناشط، كما أنه يأتي بتكلفة عالية وهي سعر الخطوط كل مرة يحتاج لإرسال رسالة لمرة واحدة فقط.

كل هذه القيود هي ما دفعت بعض النشطاء للبحث عن بدائل لا تعتمد على رقم هاتف، وفي هذه الحالة يظهر لنا تطبيق سيشن (جلسات) Session كخيار مختلف.

Session: ما المختلف هنا؟

بعكس سيجنال وتليجرام التي تشترط رقم هاتف وبالتالي تكشف نفسك منذ لحظة التفعيل عبر الـSMS والـIMEI والموقع الجغرافي، تم تصميم تطبيق سيشن ليعالج هذه المشكلة من الأساس فهو:

- لا يطلب رقم هاتف، ما يعني أن حسابك غير مرتبط بخط SIM أو بجهازك الشخصي.

- ينشئ لك Session ID عشوائي، مع إمكانية التخلص منه فور انتهاء المهمة.
- يعتمد على شبكة موزعة من "العقد" (تشبه Tor) والتي تقلل من إمكانية تتبع المصدر.
- وبمجرد حذف الـ Session ID، تنقطع الصلة بينك وبين الرسائل السابقة.

لكن وعلى الرغم هذه المزايا،دائما هناك قيود مهمة وعيوب منها:

- بطء الأداء: وهذا يحدث بسبب مرور الرسائل عبر عدة عقد مما يجعل التواصل أبطأ، كما أنه يؤخر الرسائل العاجلة لبعض الوقت.
- تخزين الرسائل غير المستلمة: تبقى في الشبكة 14 يوما، ما يمثل نافذة محتملة للهجوم إذا تم استهداف الجهاز أو العقد الوسيطة.
- لا يحمي من اختراق الجهاز: إذا كان هاتفك مخترقا فأن كل محاولاتك للحماية ستكون فاشلة مهما كانت قوة التشفير لأن المخترق يرى ما تفعله على هاتفك ويسجل كل تحركاتك عليه.
- الأخطاء البشرية: مثل إعادة استخدام نفس Session ID لأكثر من غرض، أو لأكثر من مرة، إبقاء التطبيق مثبتا على هاتفك لفترة طويلة، كل هذه الأمور أو احدها قد تترك أثرا على جهازك يمكن ربطه بك.
- الاعتماد على شبكة متطوعة: لأن التطبيق يعتمد على شبكة يديرها متطوعون بدلًا من خادم مركزي واحد، قد تتأخر الرسائل أحيانًا أو يتذبذب الأداء، وبعض نقاط الشبكة قد تكون أضعف أمام الاستهداف.

ولنضرب مثالا واقعيا حول المخاطر التي يمكن أن تحدث نتيجة ما سبق:

لنفترض أن هناك ناشطا يريد إرسال موقع اجتماع حساس لشخص واحد. أنشأ Session ID جديدًا وقام بإرسال الرسالة. لكنه وبدلا من حذف السيشن أي دي أو التطبيق فورا بعد استلام الرسالة من قبل الطرف الآخر، أبقى التطبيق على هاتفه واستعمل نفس الهوية لاحقا مع شخص مختلف. هنا أصبح هناك خيط تقني واحد يربط محادثتين منفصلتين، فلو تمت مصادرة هاتفه أو جهازه، يمكن للسلطات حينها ربط الرسالتين ببعضهما البعض وبناء شبكة علاقات رغم أن التشفير الخاص بالتطبيق لم يُتم اختراقه وإنما الخلل جاء عبر المستخدم.

نستنتج مما سبق أن :

سيشن يقدّم حلا حقيقيًا لمشكلة رقم الهاتف والـ IMEI الذي من خلاله يتم تحديد الجهاز والموقع المحدد عبر بطاقة السيم كارد، وهي تلك المشاكل التي تجعل تيليجرام وسيجنال غير مناسبين للرسائل "ذات المرة الواحدة".

لكنه ومع ذلك ليس حصنا مطلقا منيعا: فالبطء والتخزين المؤقت والأخطاء البشرية كلها نقاط ضعف قد تحوله من أداة حماية إلى خطر إضافي إذا تم استخدامه بطريقة خاطئة.

صحيح أن سيشن يتجاوز مشكلة SIM/IMEI التي تعاني منها التطبيقات الأخرى لكنه لا يمنع تماما من ملاحظة

أن جهازا ما استخدم تطبيق سيشن أو في أي وقت تم ذلك، وهذه المعلومة قد تظهر لدى مزود خدمة الإنترنت الخاص بك (ISP) أو عبر أنظمة المراقبة الشاملة، ومع أن المحتوى يبقى مشفّرا، إلا أن مجرد معرفة وقت الاستخدام قد يضيق مجال البحث إذا تم جمعها مع بيانات أخرى.

أمنك الشخصي أهم من أي شيء

بالنسبة لناشط يعيش في بلد يمنع ويجرّم التواصل مع المنظمة الحقوقية أو وسائل الإعلام المستقلة، فهذه التفاصيل التي ذكرناها ليست مجرد اعتبارات تقنية، بل قد تكون مسألة بالغة الخطورة بالنسبة له، لأن خطأ بسيط واحد أو أثر رقمي ضئيل قد يكون كافيا لأن يعرضه لمساءلة قانونية أو مخاطر شخصية.

كيف يمكن للنشطاء أن يستخدموا سيشن على الهواتف؟

لأن الهاتف هو الأداة الأولى للنشطاء والأسهل بالطبع، فإن طريقة استخدام شيشن عليها قد تحدد الفارق بين رسالة آمنة ورسالة تتحول إلى خيط يكشف شبكة كاملة أو يعرض حياته للخطر، لذلك يجب الإنتباه الى تلك الخطوات الأساسية:

1. التثبيت الآمن

ـ دائما نزل التطبيق من متاجر الأجهزة المعتمدة مثل Google Play أو App Store.

ـ إذا كان المتجر محجوبا أو مراقبا،يمكنك استخدم الموقع الرسمي (getsession.org) مع VPN موثوق.

ـ تحقق من الرابط دائمًا لتفادي أي نسخ مزيفة قد تحتوي على برمجيات تجسس أو تتبع.

2. إنشاء الهوية

● عند فتح التطبيق ولأول مرة تم توليد رقم فريد للجلسة Session ID بشكل تلقائي، هذا الرقم هو الرقم الذي تستخدمه من أجل استقبال الرسائل من الأطراف الأخرى.

● إذا كانت رسالتك لمرة واحدة، أرسلها وانتظر حتى تظهر إشارة "تم التسليم".

● تذكّر أن أي رسالة غير مُستلمة تبقى في الشبكة حتى 14 يومًا، وهو ما يمثل نافذة خطر إذا استُهدف الجهاز أو العقد الوسيطة.

● بمجرد وصول الرسالة، احذف الهوية القديمة مباشرة. وإذا انتهت مهمتك، يفضل أن تقوم بحذف التطبيق نفسه لتقليل أي أثر.

3. إعدادات الخصوصية

- عطل الإشعارات، لأنها تمر عبر خدمات جوجل أو أبل وحينها قد تسرب بيانات خاصة بك لتحديد هويتك.
- أوقف النسخ الاحتياطي للهاتف أو السحابة.
- قم بتفعيل قفل التطبيق بكلمة مرور أو بصمة.
- قم بتعطيل أذونات الكاميرا، الميكروفون، والموقع من إعدادات الهاتف.
- استعمل VPN أثناء الاستخدام، وليس فقط وقت التثبيت.

4. أثناء الاستخدام

- لا ترسل صورك أو بيانات شخصية أبدا كما لا ترسل أي ملف تم التقاطه بهاتفك إلا بعد أن تتأكد من إزالة الـ exif أو الميتاداتا الخاصة بالملف.
- يفضل ألا تستخدم تطبيق سيشن على نفس الهاتف الذي يحوي حساباتك المكشوفة (WhatsApp، Gmail...).
- اعتبر تطبيق سيشن أداة لمهمة محددة، ولا تستخدمه كبرنامج دردشة دائم.

5. بعد الاستخدام

- بمجرد وصول الرسالة للطرف الآخر، احذف الرقم التعريفي الخاص بالجلسة Session ID مباشرة.
- إذا لم تعد بحاجة للتطبيق، من الأفضل حذفه بالكامل.

الأخطاء القاتلة

في معظم الحالات الأداة لا تخونك، لكن طريقة استخدامك لها قد تفعل لذلك تجنب:

- إعادة استخدام نفس Session ID لغرضين مختلفين.
- ترك نسخ للرسائل او لقطات شاشة.
- استخدام شبكات Wi-Fi عامة دون VPN.
- الاعتماد على جهاز مخترق مسبقا أو جهاز تظن أنه مخترق.
- افتراض أن Session يحميك مهما كان سلوكك.
- وفي الحالات شديدة الخطورة قد يكون من الخطر مشاركة نفس الجهاز بين أكثر من ناشط.

طبقة إضافية من الحماية

أحيانًا لا يكفي أن تكون الرسالة مشفرة أو مجهولة المصدر، بل يجب أن تختفي تمامًا بعد قراءتها. هنا تأتي خدمات مثل Privnote أو BurnerNote، التي تعمل بطريقة بسيطة: تكتب الرسالة، تحصل على رابط خاص، ترسله للطرف الآخر، وبمجرد أن يفتحه تختفي الرسالة نهائيًا.

هذه الفكرة قد تبدو مثالية، لكنها إذا استُخدمت بشكل مباشر دون احتياطات قد تتحول إلى خطر :

- بمجرد دخولك للموقع عبر متصفح عادي، يسجل مزوّد الخدمة زيارتك، فيعرف أنك استخدمت هذه الأداة حتى لو لم يطّلع على محتوى الرسالة.
- مجرد سجل الوقت والمكان الذي دخلت فيه يكفي في بعض البيئات القمعية لربطك بحدث أو اجتماع حساس.
- بعض المواقع المزيفة تقلّد Privnote لخداع النشطاء وسرقة رسائلهم.
- حتى الرسائل ذاتية التدمير لا تمنع الطرف الآخر من أخذ لقطة شاشة أو إعادة كتابة ما وصله.
- إضافة لذلك،يجب الانتباه إلى أن بعض الأجهزة قد تحتفظ بآثار غير مباشرة، مثل سجل النسخ.

ولهذا قد تكون دمج تلك الخدمات مع سيشن وسيلة أكثر من جيدة لضمان الحماية عبر طبقات متعددة.

الحل الأفضل: الدمج مع Session

لتقليل الأثر الذي تتركه خلفك خلال إرسال الرسائل، لا تفتح تلك المواقع التي تشفر الرسائل من متصفحك العادي، بل قم باستخدامها من خلال متصفح آمن مثل تور، بحيث يمر الاتصال عبر قناة مجهولة ومشفرة.

بعد ذلك قم بكتابة رسالتك واستخدم الرابط وأرسله عبر سيشن للطرف الآخر وفور التأكد من وصول الرسالة قم بحذف رقم الجلسة التعريفي ولا تنس أن تقوم أيضا بتنظيف سجل النسخ في هاتفك.

بهذا الشكل لن يرى مزود الخدمة أنك قمت بالدخول إلى هذه المواقع لأنها مخفية داخل قناة تطبيق السيشن نفسه أو المتصفح المحمي، كما أن الرسالة تختفي مباشرة بعد قرائتها، كل هذه الأمور تصعب من ترك الأثر الرقمي وبالتالي تقدم لك المزيد من الحماية.

ومع ذلك يجب الانتباه إلى أن:

الرسائل ذاتية التدمير مفيدة، لكن خطورتها تكمن في طريقة استخدامها. فلو تم استخدامها بشكل مباشر، قد تصبح نقطة ضعف. أما إذا استُخدمت عبر متصفح آمن ثم داخل سيشن، فهي تمنح النشطاء أداة عملية لإرسال رسالة لمرة واحدة تختفي بعد قراءتها، مع تقليل الأثر الرقمي إلى الحد الأدنى الممكن.

ما الذي لا يحميك منه تطبيق سيشن؟

قد يغريك الشعور بأنك "محمي" لمجرد أنك تستخدم تطبيقًا مشفرًا مثل سيشن. لكن في الحقيقة تم تصميم سيشن ليحل مشكلة محددة وهي التخلص من الحاجة إلى رقم هاتف والآثار المرتبطة به (SIM، IMEI، الموقع الجغرافي). أما بقية المخاطر فهي موجودة، وقد تكون أشد فتكا ومنها كما ذكرنا سابقا الاختراق المباشر للجهاز وبالتالي المخترق يقرأ ويرى كل ما يحدث على جهازك حتى قبل ارسالك الرسالة، أو أن الطرف الآخر المستلم لرسالتك قد قام بأخذ لقطة شاشة أو غيرها، كما أن الاستخدام الخاطئ للتطبيق أو اهمال الأمور المتعلقة بالتواصل نفسه وحمايته قد تؤدي إلى تسريب ميتاداتا تؤدي إليك.

باختصار:

سيشن يقلل الأثر الرقمي الخاص بك، لكنه لا يزيل الخطر، يحمي رسالتك، لكنه لا يحميك من جهاز مخترق، أو من صديق غير حذر، أو من نظام قادر على تحليل أنماط السلوك، أو من كاميرا تصورك في العلن، كما لا يحميك من سوء الاستخدام.

نحو استراتيجية أوسع للأمان

سيشن قد يساعدك في مهمة محددة، لكنه مجرد طبقة واحدة في جدار الحماية. الأمن الرقمي الحقيقي لا يعتمد على تطبيق بعينه بل على ممارسات أوسع:

- جهاز ثانوي للمهام الحساسة: لا تخلط بين هاتفك اليومي والهاتف المخصص للتواصل السري.
- اتصال محمي دائمًا: استخدم VPN أو Tor مع أي شبكة عامة.
- وعي جماعي: أمان الفريق لا يتجاوز أضعف أفراده، لذلك التدريب المشترك ضروري.
- خطة للطوارئ: ضع دائمًا سيناريو بديل في حال صودرت أجهزتك أو انكشف أحد أفراد الشبكة.

باختصار: الأمن الرقمي ثقافة متكاملة—جهاز نظيف، اتصال محمي، فريق واعٍ، وخطة بديلة. سيشن جزء من الصورة وليس الصورة كلها.

الخلاصة: التقنية أداة، وليست ضمانة

لا يوجد تطبيق واحد يضمن لك الأمان الكامل. في البيئات القمعية، أي أثر رقمي قد يكون كافيًا لاعتقالك أو تعريضك للمساءلة وتعطيل عملك الحقوقي أو الصحفي أنت وشبكتك. لكن سيشن يقدّم ميزة نادرة: إمكانية إرسال رسالة مجهولة قصيرة المدى، ثم التخلص من الهوية بسرعة وكأنك لم تكن موجودًا.

لكن تذكر: سيشن ليس حصنًا مطلقًا، بل مجرد أداة ضمن استراتيجية أوسع. هو ليس بديلًا عن سيغنال الذي يظل الأفضل للتواصل الطويل المدى مع مراجعات أمنية مستقلة. وهو بالتأكيد ليس حصنًا ضد برمجيات التجسس، ولا ضد خطأ بشري بسيط مثل إعادة استخدام الهوية أو نسيان حذف التطبيق.

القانون الذهبي الذي يجب أن يبقى في ذهن كل ناشط وصحفي ومحامٍ:

- سيشن للرسائل القصيرة المجهولة، لمرة واحدة فقط.
- سيغنال للتواصل المستمر والموثوق طويل المدى.
- لا تمنح أي أداة ثقة مطلقة، فالأمن الرقمي ثقافة وممارسات قبل أن يكون تطبيقات.

باختصار:

التقنية تستطيع أن تخفي رسالتك، لكنها لا تستطيع أن تخفيك أنت. النجاة لا تأتي من أداة واحدة، بل من وعيك، من تدريب فريقك، ومن خططك لما بعد الطوارئ.

إخلاء مسؤولية :

هذا المقال لأغراض التوعية العامة فقط. لا نشجع على خرق القوانين المحلية أو تجاوزها. الهدف هو تعزيز فهم الأمان الرقمي بشكل عام.

هذه الأدوات مستخدمة أيضًا من قبل الصحفيين الأوروبيين والمنظمات الإعلامية الكبرى لحماية مصادرهم، وهو حق مشروع تضمنه المواثيق الدولية مثل المادة 19 من الإعلان العالمي لحقوق الإنسان.

تنويه قانوني:

هذا المقال يُقدَّم لأغراض إعلامية وتثقيفية بحتة في مجال الأمن الرقمي. لا يتضمن أي دعوة أو تشجيع على خرق القوانين المحلية أو الانخراط في أنشطة غير مشروعة. الكاتب والموقع يقدمان هذه المعلومات في إطار الحق في حرية التعبير والحق في الوصول إلى المعرفة،وفقًا للتشريعات الأوروبية، وخصوصًا الميثاق الأوروبي لحقوق الإنسان والمواثيق الدولية ذات الصلة.