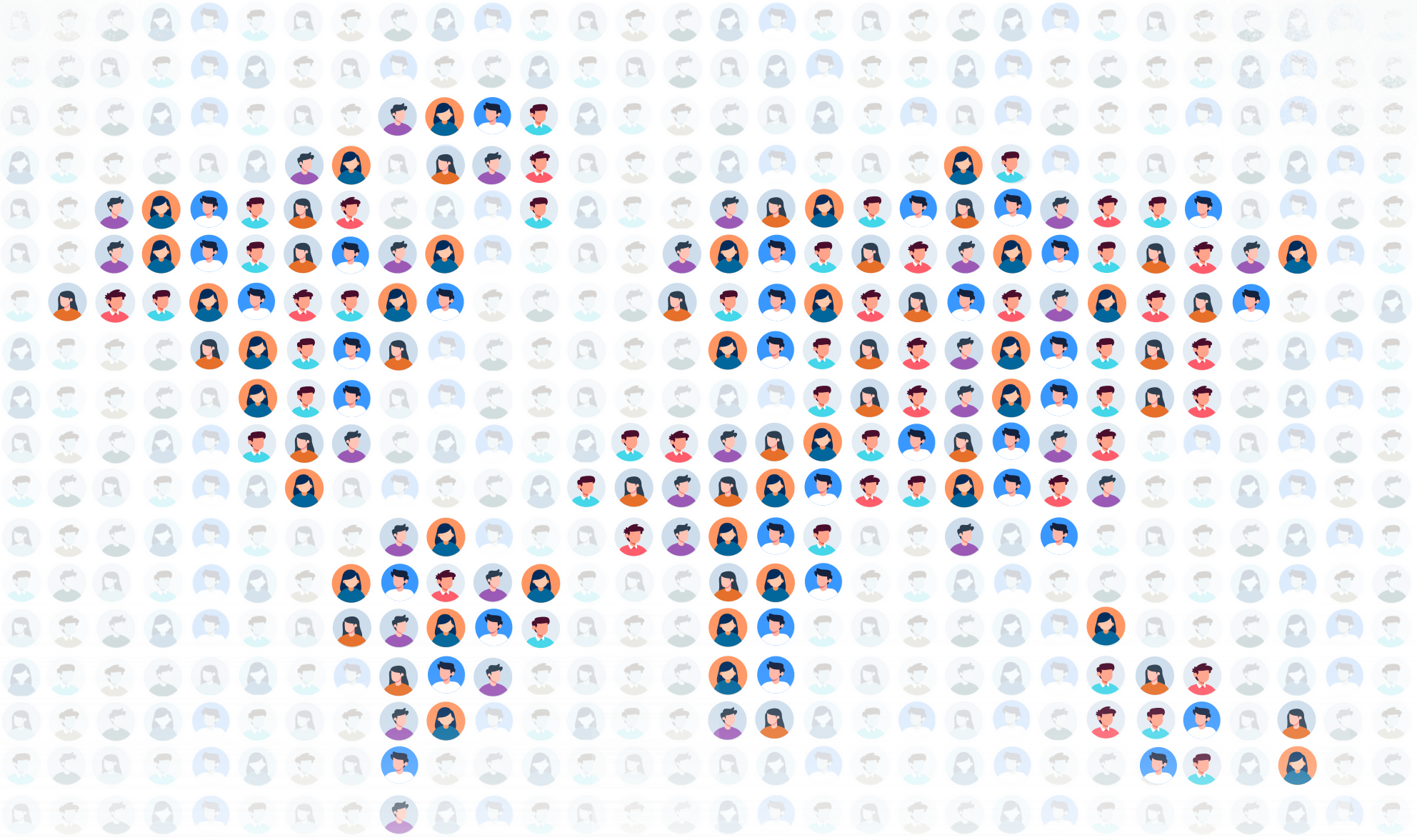


دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

مهارات
Maharat

دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

تم إعداد هذا الدليل من قبل مؤسسة مهارات، بدعم من هيئة الأمم المتحدة للمرأة والسفارة الفرنسية في بيروت.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

الجزء ٢

أدوات تواصل رقمية آمنة: توصيات لتطبيقات المراسلة المشفرة وخدمات البريد الإلكتروني الآمن.

إعداد:
خبير في الأمن الرقمي بهاء نصر

SOURCE : © 2024 - THE NEW ARAB / GETTY

التواصل الآمن

في عالم اليوم، أصبحت الإتصالات الرقمية **الأداة الأكثر شيوعًا التي نستخدمها للتواصل مع بعضنا البعض**، من المحادثات الشخصية إلى الإتصالات التجارية الحساسة. أدى تزايد التهديدات السيبرانية إلى تسليط الضوء على **الحاجة إلى أدوات تواصل رقمية آمنة.** يُعتبر التشفير أحد أكثر الطرق الفعالة لضمان أن الأطراف المعنية فقط هي التي تستطيع الوصول إلى المعلومات المتبادلة.

التشفير هو المفتاح

عند اختيار تطبيق مراسلة أو خدمة إتصال، يُعد **التشفير العامل الأكثر أهمية** الذي يجب مراعاته. يضمن التشفير **تحويل الرسائل إلى رموز غير مقروءة أثناء عملية الإرسال،** مما يجعل من شبه المستحيل على الأطراف الثالثة قراءة الاتصالات.

يوجد نوعان رئيسيان من التشفير:

التشفير من طرف لطرف (E2EE)

يضمن أن **المرسل والمستلم فقط هما من يستطيعان تشفير الرسالة وفك تشفيرها وقراءتها.** حتى مزود الخدمة المستخدم لإرسال الرسالة لا يستطيع قراءة محتواها. هذا يعني أن الرسالة نفسها تُشفر في التطبيق على جهازكم وتُرسل مُشفرة إلى المستلم أو المستلمين، حيث يفك تشفيرها لتتم قراءتها. حتى إذا **تمكن شخص ما من اعتراض الرسالة، فلن يستطيع قراءتها بسبب التشفير.**

تشفير طبقة النقل

يحمي البيانات أثناء ارسالها، لكن يمكن **لمزود الخدمة فك تشفير الرسالة**. هذا يعني أن الرسالة نفسها ليست مشفرة، بل تُنقل من جهازكم إلى مزود الخدمة عبر قناة مشفرة ثم تُنقل إلى المستلم أو المستلمين مرة أخرى عبر قناة مشفرة. **وهذا يعني أن مزود الخدمة، وأحيانًا القراصنة، يمكنهم قراءة هذه الرسائل.**

تطبيقات وخدمات تركز على الخصوصية والأمان:

سيجنال (Signal) يُعتبر "سيجنال" واحدًا من أكثر تطبيقات المراسلة أمانًا المتاحة حاليًا. **يعتمد التطبيق على التشفير القوي من طرف إلى طرف بشكل افتراضي**، مما يضمن أن يكون الوصول إلى الرسائل مقتصرًا فقط على المرسل والمتلقي. إن "سيجنال" أيضًا **مفتوح المصدر**، مما يعني أن الشيفرة المصدرية للتطبيق متاحة للجمهور ليتمكن المبرمجون الآخرون من التحقق من مستوى الأمان، مما **يعزز مصداقيته وشفافيته**. وإلى جانب الرسائل الفردية والجماعية، **يدعم "سيجنال" المكالمات الصوتية والمرئية المشفرة.**

الخصائص الرئيسية:

- التشفير من طرف لطرف لجميع الرسائل والمكالمات.
- يدعم المراسلات الجماعية، والمكالمات الصوتية والمرئية.
- خاصية الرسائل التي تختفي من أجل تعزيز الخصوصية.
- مفتوح المصدر ويتم مراجعته بانتظام للكشف عن أي ثغرات أمنية.
- جمع بيانات وصفية محدودة
- تحتاجون الى رقم هاتف لإنشاء حساب، لكن بعد ذلك يمكنكم إضافة اسم المستخدم ومشاركة الإسم فقط، مما يحافظ على خصوصية رقم الهاتف.

تتوفر العديد من الميزات الإضافية لتعزيز خصوصيتكم وأمانكم داخل التطبيق. ننصحكم بالتحقق من الإعدادات وضبطها وفقًا لإحتياجاتكم ونوعية المخاطر الخاصة بكم.

تطبيقات وخدمات تركز على الخصوصية والأمان:

واتساب هو **تطبيق شائع للمراسلة** يقدم تشفيرًا من **طرف لطرف للرسائل والمكالمات والوسائط التي يتم تبادلها بين المستخدمين.** على الرغم من أنه يوفر تشفيرًا قويًا، فإن **واتساب مملوك لشركة ميتا (المعروفة سابقًا بفيسبوك)، وهو ما أثار قلق الناشطين في مجال أمن المعلومات بشأن إدارة البيانات** (والمخاطر المحتملة المتمثلة في تسليم ميتا البيانات إلى الحكومات أو الأطراف الأخرى). كما أن واتساب **ليس مفتوح المصدر، مما يعني أنه لا يمكن لأحد الاطلاع على كيفية نقل البيانات** وتخزينها وإدارتها، مما يجعل من الصعب التحقق من ادعاءات الخصوصية والأمان المقدمة من ميتا.

الخصائص الرئيسية:

- تشفير من طرف لطرف لجميع الاتصالات.
- واجهة سهلة الاستخدام وانتشار واسع.
- يدعم المراسلات الجماعية، والمكالمات الصوتية والمرئية.
- خاصية الرسائل التي تختفي من أجل تعزيز الخصوصية.
- سهولة مشاركة الملفات.

تطبيقات وخدمات تركز على الخصوصية والأمان:

واير هو تطبيق إتصالات يقدم تشفيرًا من طرف إلى طرف للرسائل والمكالمات الصوتية والمرئية. كما **يتضمن أدوات تعاون مثل مشاركة الملفات والدردشات الجماعية. واير مملوك لشركة سويسرية**، ويمتثل ل**قوانين صارمة لحماية البيانات، بما في ذلك اللائحة العامة لحماية البيانات (GDPR)**، مما يجعله مناسبًا للشركات والمنظمات التي تتطلب قنوات اتصال آمنة وخاصة

الخصائص الرئيسية:

- تشفير من طرف إلى طرف لجميع الاتصالات.
- أدوات التعاون ومشاركة الملفات للمجموعات.
- امتثال لـ GDPR وجاهز لاستخدام للمؤسسات.
- مفتوح المصدر وخضع للمراجعة.
- يمكنكم إنشاء حساب دون الحاجة إلى رقم هاتف محمول.

تطبيقات وخدمات تركز على الخصوصية والأمان:

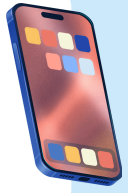
يوفر تطبيق **"تليغرام" التشفير من طرف إلى طرف فقط في "المراسلات السرية"**، في حين أن **المراسلات العادية تكون مشفرة فقط أثناء عملية الإرسال** مما يعني أن القيمين على التطبيق يمكنهم قراءة الرسائل. ويحتاج المستخدمون إلى تفعيل هذه الخاصية يدويًا لبدء "المراسلات السرية" في كل مرة.

الخصائص الرئيسية:

- التشفير من طرف لطرف متاح فقط في "المراسلات السرية".
- يدعم المراسلات الجماعية والقنوات.
- خاصية الحذف التلقائي للرسائل من أجل تعزيز الخصوصية.

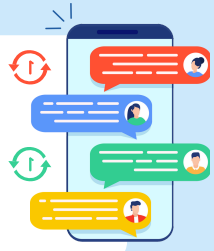
٣ التوصيات

إستخدام تطبيق تواصل آمن هو خطوة أولى أساسية نحو حماية محادثاتكم الحساسة، ولكن من المهم أن تتذكروا أن الأمان يتجاوز مجرد الأدوات التي تستخدمونها؛ فهو يتطلب **ممارسات ثابتة ويقظة مستمرة**. الاعتماد فقط على تطبيق آمن لبعض المحادثات بينما يتم **استخدام منصات أقل أمانًا لمحادثات مرتبطة يمكن أن يكشف عن ثغرات.** القيام بذلك قد يهدد الأمان الذي تهدفون إلى حمايته، حيث يمكن للمهاجمين تجميع المعلومات من مصادر مختلفة لبناء صورة أكبر.

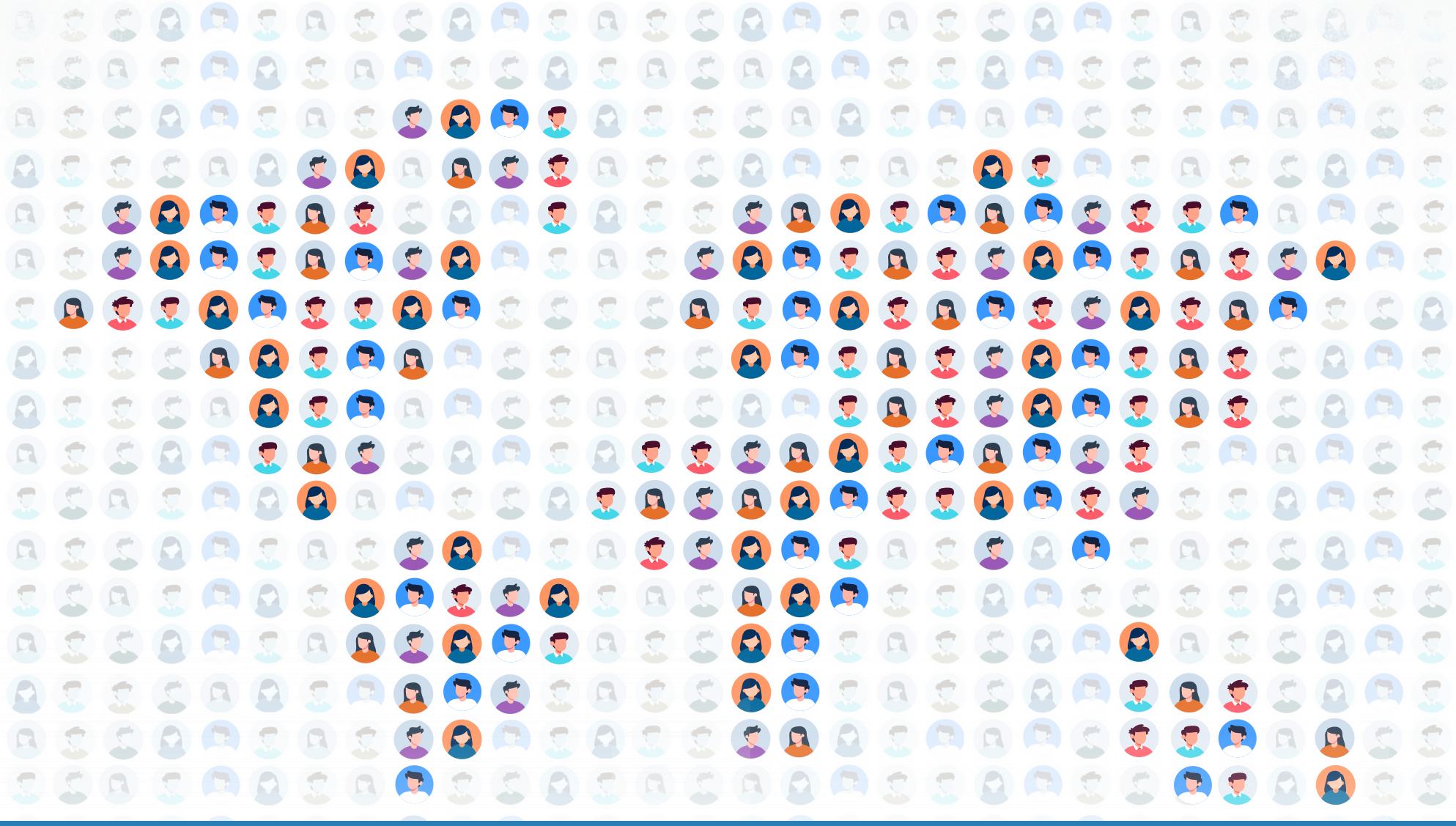


تأكدوا من أن جميع أجهزتكم، سواء كانت هاتفًا ذكيًا، أو جهازًا لوحيًا، أو حاسوبًا، **يتم تحديثها بانتظام بأحدث التحديثات البرمجية وتصحيحات الأمان.** قد تحتوي البرمجيات القديمة على ثغرات يمكن للمهاجمين استغلالها.

تجنبوا مشاركة أجهزتكم مع الآخرين. حتى لو كنتم تثقون بمن حولكم، فإن **مشاركة جهازكم تفتح المجال لاحتمال حدوث ثغرات أمنية غير مقصودة.** على سبيل المثال، قد يقوم شخص **ما دون قصد بتنزيل برمجيات خبيثة، أو تغيير إعدادات الأمان، أو الوصول إلى معلومات حساسة.**



فعّلوا خاصية الرسائل التي تختفي تلقائيًا أو خاصية الحذف التلقائي للرسائل. هذه الخيارات تزيل المحادثات تلقائيًا بعد فترة زمنية محددة، **مما يقلل من خطر تخزين المعلومات الحساسة أو استعادتها إذا وقع جهازكم في الأيدي الخاطئة.** هذا **لا يقلل فقط من بصمتكم الرقمية، بل يحدّ أيضًا من كمية البيانات التي قد تُعرض في حالة خرق الأمان أو مصادرة الجهاز أو فقدانه.**



مؤسسة مهارات

العنوان:
جديدة، المتن
بيروت، لبنان

معلومات التواصل:
الموقع الإلكتروني: maharatfoundation.org
البريد الإلكتروني: info@maharatfoundation.org

مهارات
Maharat