لماذا يجب عليك التوقف عن استخدام فيسبوك ماسنجر؟

ترجمة وتحرير: نون بوست

إذا كنت من مئات الملايين من مستخدمي فيسبوك ماسنجر، قد يكون الآن الوقت مناسبًا للتفكير في بدائل أخرى لهذه المنصة. فرغم إعلان المنصة تحديثًا أمنيًا كبيرًا الأسبوع المنصرم بإضافة أقفال الأجهزة البيومترية على نظام تشغيل آي أو إس، إلا أن الجوانب الأمنية لماسنجر تشوبها العديد من الثغرات. وتستمر هذه المشكلة في التفاقم، ولا يمكن لفيسبوك حلها بسهولة.

عند إعلان ميزات التحديث الجديد، أخبرت فيسبوك المستخدمين بأن "الخصوصية محور اهتمام تطبيق ماسنجر، حيث تستطيع أن تكون على سجيتك مع أحبتك". وقالت الشركة أيضا إن قفل التطبيق "سيضيف طبقة أخرى من الحماية لرسائلك لمنع اختراقها".

لكن هذا التحديث يشبه إضافة أقفال على باب البنك، بينما باب الخزنة مفتوح على مصراعيه، ليكون بذلك مجرد إجراء هامشي. تتوفر العديد من البدائل التي تتميز بخصائص مشابهة في حين أن استخدامها ينطوي على خطورة أقل. لذلك، حان الوقت للتغيير.

إذًا ما هي المشكلة؟ الجواب في كلمة واحد فقط: التشفير. لست أنا مصدر هذه المعلومة، وإنما فيسبوك ذاته الذي حذر مستخدمي ماسنجر من أن رسائلهم ليست مشفرة بين الطرفيات. ففي سنة 2017، عند تقديمها "المحادثات السرية"، اعترفت الشركة أن ذاك بأن هذا الإجراء الأمني قد يقلل من احتمال اختراق البنية التحتية للخادم والشبكات المستخدمة في ماسنجر، إضافة إلى فيسبوك.

تتيح المحادثات السرية إمكانية تشفير المحادثات الثنائية في ماسنجر التي تكون بين الأشخاص، وليس بين المجموعات، وهذا ليس خيارا تلقائيًا. وتقول فيسبوك: "المحادثة السرية في ماسنجر مشفرة ومخصصة لك والشخص الذي تتحدث معه فقط"، مشيرة إلى أن جميع الرسائل غير "السرية" معرضة للاختراق.

خلقت فيسبوك لنفسها مشكلة حقيقية بسبب الثغرات الأمنية التي تشوب ماسنجر. فقد أصبحت

الشركة المؤيد الأول للتشفير بين الطرفيات، حتى أن مارك زوكربيرغ نادى شخصيًا بفوائدها. ولكن الشركة اعترفت أيضًا بأن التعقيدات التقنية لإضافة هذا النوع من الحماية إلى ماسنجر قد يتطلب سنين. بعبارة أخرى، أنتم لستم في أمان كاف، ولكن إن انتظرتم بضع سنين سنحل مشكلتكم هذه.

ما عليك سوى النظر إلى توضيح واتسآب لإدراك مدى أهمية التشفير: "إحدى أكثر ذكرياتكم خصوصية محفوظة ومنشورة عبر واتسآب، لذا فقد طبقنا التشفير بين الطرفيات في تطبيقنا. يحمي هذا التشفير من وقوع رسائلكم، وصوركم، ومقاطع الفيديو، ورسائلكم الصوتية، وملفاتكم، ومكالماتكم في الأيادي الخاطئة".

لا تقتصر هذه المشاكل على فيسبوك ماسنجر، بل إن نظام الرسائل القصيرة "الإس إم إس" في حال أسوأ. وهذا الأمر بات معلوما للعيان. إن النصيحة التي تقدم في هذه الحالة هي وقف استخدام الرسائل القصيرة إذا أمكن ذلك. توفر كل من خدمة آي مسج من أبل وآر سي أس من غوغل بديلا مشفرًا لنظام الإرساليات القصيرة، الذي ما زال من أكثر أنظمة الرسائل انتشارًا في العالم.

لاينبغي أن يتفاجأ أحد باعتراف تويتر بأن الاختراق الأخير لحساب أكثر من 100 مستخدم قد ساهم في الاطلاع على الرسائل الخاصة بـ 36 حسابا

يمتلك ماسنجر أكثر من مليار مستخدم، وعلى عكس نظام الرسائل القصيرة، فإنه يُعرف كبديل مُحدث ومليء بالخصائص المميزة لأنظمة الرسائل القديمة. ويحذر خبير الأمن السيبراني جيك مور من أنه "على من يختار التواصل عن طريق ماسنجر فهم التهديد الحقيقي الذي يتربص بمعلوماته في هذا النوع من التطبيقات. وعلى الرغم من أن الكثيرين قد يظنون أن محتوى رسائلهم ليس خصوصيًا، إلا أن المشكلة الحقيقة تكمن في أن أي معلومات عنك ستكون عرضة لإساءة الاستخدام إذا وقعت بين أيدي أناس آخرين".

إن كانت تساورك الشكوك، فما عليك سوى إلقاء نظرة على حملات التشهير التي طالت تويتر. لا ينبغي أن يتفاجأ أحد باعتراف تويتر بأن الاختراق الأخير لحساب أكثر من 100 مستخدم قد ساهم في الاطلاع على الرسائل الخاصة بـ 36 حسابا. وذلك لأن الرسائل المباشرة في تويتر غير مشفرة، تمامًا كماسنجر، وهي عالقة في النقطة ذاتها منذ سنوات.

لكن تويتر ليس منصة للرسائل الخاصة، ذلك أن حجم رسائله مقارنة بالرسائل على ماسنجر بسيط للغاية. ولكن خذ ذلك كتحذير. وأضاف مور أن "التعقيدات الأخيرة مع تويتر توضح مجددًا مدى أهمية التشفير بين الطرفيات في الرسائل وتركيز منصات المراسلة على الأمن والخصوصية".

بيّن الهجوم الذي استهدف تويتر مدى ضعف منصة معينة بحوزتها المفاتيح لفك تشفير محادثاتك الخاصة. قد تستخدم المنصة تلك المفاتيح في حالة المساءلة القانونية، ولكن احتمال استغلال الموظفين الفاسدين أو قراصنة الإنترنت لهذه المفاتيح يظل قائما أيضًا. يقول فيسبوك إن "خوادمنا موجودة فقط في البلدان ذات القوانين المشددة. ولدينا إجراءات حماية وضمانات قوية للبيانات التي تضع المعلومات تحت الحماية، بحيث لا يستطيع الموظفون الوصول إلى محتوى الرسائل".

لكن كما تشير خدمة البريد الإلكتروني المشفرة "بروتون مايل" فإن "أفضل طريقة لحماية البيانات هي عدم إتاحة الوصول إليها من قبل الشركة على الإطلاق. وتتمثل فائدة استخدام الخدمات المشفرة في أنه يصبح بالإمكان الحفاظ على البيانات آمنة حتى في حالات الاختراق الحتمية، لأن مزود الخدمة نفسه ليس لديه القدرة على فك تشفير بيانات المستخدم. فمن المستحيل أن يستطيع المتسللون سرقة شيء لا تمتلكه الخدمة في حد ذاتها".

في ذلك تحذير حتى لتطبيقات المراسلة ذات أعلى درجات الأمان نسبيًا. فلا يتم تشفير النسخ

الاحتياطية للرسائل من أبل وغوغل، بل يقومان فقط بتخزين نسخة من بيانات الهاتف غير المشفرة. وعندما تستخدم ميزة واتسآب للنسخ الاحتياطية السحابية الحالية، فإنك تواجه نفس المخاطر، إلا أن هذه الميزة يتم إصلاحها حاليًا.

يناشد كل من مور والكاتب جون أودناكر باستعمال سيغنال، وهي المنصة المفضلة لخبراء الإنترنت، وذلك لتبنيها نهج الأمان أوّلا وعدم امتلاكها أي شكل من أشكال الرسائل الاحتياطية. وقد أخبرني أوديناكر أنه "يجب على الناس التفكير في أن كل ما يقولونه على الرسائل الخاصة بتويتر أو فيسبوك ماسنجر سينشر علنًا، عاجلًا أم آجلًا. فإذا كنت تريد مراسلة خاصة، فاستخدم تطبيقات مثل سيجنال التي تعمل على التشفير الكلي".

ينصح مور أيضًا بتطبيق تلغرام، وهو خيار أكثر تعقيدًا بعض الشيء. لا يقوم تلغرام بالتشفير من طرف إلى طرف بشكل تلقائي. وقد أوضحت الشركة أن المشكلة تكمن في أنه يصبح من المستحيل على المستخدمين الوصول إلى الرسائل بسهولة على أجهزتهم المختلفة أو استعادة سجلهم عند فقدان الجهاز أو استبداله. وعلى الرغم من اعتماد تلغرام على نهج الأمان أولاً، إلا أنه يمتلك القدرة على توزيع مفاتيح التشفير التي يمتلكها للسلطات القضائية المختلفة لإحباط أي محاولات داخلية، سواء كانت خبيثة أو بناء على طلب وكالات الأمن، للوصول إلى المحتوى.

ينصح محترفو الأمن بسيغنال وأمثالها دائمًا، حيث تُقدم التحديثات فقط عند التأكد من أنها لا تُعرّض أمن المنصة للخطر. ولكنك في الحقيقة لا تحتاج للبحث أبعد من تطبيق واتسآب، وهو أكثر المنصات التي تعمل على التشفير شيوعًا، حيث يوفر التشفير للمحادثات والمجموعات الفردية وكذلك لمكالمات الصوت والفيديو بشكل تلقائي تمامًا.

يجب أن يكون الناس قادرين على التواصل بشكل آمن وخاص مع الأحباء والأصدقاء دون استماع أو مراقبة من قبل أي أحد

واجه تطبيق واتسآب مشاكل عبر السنين، ولكن لم يتم اختراق تشفيرها قط. فالقراصنة يستهدفون الأجهزة، لا المنصات الأساسية، ذلك أنه عند كل نهاية طرف محادثة مشفرة، ثغرة أمنية غير مشفرة. حتى تلغرام يحذر من أنه: "لا يمكننا حمايتك من أمك إذا أخذت هاتفك غير المقفل، أو من قسم تكنولوجيا المعلومات إن كان لديهم القدرة على الوصول إلى حاسوبك في مكان عملك، أو من أي أحد استطاع الوصول الفعلي إلى هاتفك أو جهاز الكمبيوتر الخاص بك".

عندما يتعلق الأمر بسهولة الاستخدام والميزات المتاحة، فإن ماسنجر يتفوق على واتسآب. لكن هذا المعطى على وشك أن يتغير. يخطط واتسآب لتوفير وصول حقيقي متعدد للأنظمة مع الأجهزة المرتبطة، ويبدو أيضًا أنه يسعى لإضافة نسخ احتياطية مشفرة على السحابة التي ستوفر مركز رسائل محفوظة على غرار ما يقدمه ماسنجر. قد يصبح واتسآب قابلاً للتشغيل المتبادل مع ماسنجر في وقت قريب. لذلك يمكنك الانتقال إلى التشفير من طرف إلى طرف حسب النظام الأساسي الافتراضي مع البقاء على اتصال مع من لا يريد التغيير.

إن أي تحديثات رئيسية للميزات تسعى من خلالها الأنظمة الآمنة لمزيد تسهيل استخدام ماسنجر ستزيد في الواقع من المخاطر. وحسب باحث المعلومات الأمنية شون رايت فإن "العديد من هذه التطبيقات، لا يستخدم التشفير من الطرفيات بمعناه الحقيقي. أقول هذا نظرًا لأنه يمكنك تلقي الرسائل وسجل الرسائل عند تسجيل الدخول إلى جهاز آخر". ومع ذلك، فإن هذه المخاطر بعيدة كل البعد عن المشكلات الموجودة في ماسنجر، وتويتر، ونظام الرسائل القصيرة، حيث لا وجود للتشفير الافتراضي على الإطلاق.

بالنسبة لجميع أولئك الذين لا يزالون يستخدمون ماسنجر لأنه سهل ومألوف، لديك الآن خياران: إما أن تعيش مع الاختلال الأمني للسنوات القليلة القادمة، أو تقوم بالانتقال إلى نظام يوفر كل المزايا تقريبًا مع إصلاحه للمشكلة الأكثر خطورة. ويقول مور إن: "منصات الرسائل غير المشفرة معرضة للهجوم كليًا، وتصبح معرضة للخطر بمجرد اكتشاف الثغرات. يجب أن نبدأ في توعية الناس بشأن المخاطر والبدء في الانتقال إلى التطبيقات التي تركز على الخصوصية".

من جهته، لا يزال فيسبوك "ملتزما بتشفير ماسنجر من طرف إلى طرف بشكل افتراضي" مما يشير إلى أنه لم يكن هناك أي تأخير حتى الآن، وأن التوقيت "يتوافق مع ما قلناه منذ إطلاق المنصة، أي أنه سيستغرق بعض الوقت ونحن ملتزمون بالقيام به بشكل صحيح". كما وجهتني الشركة إلى دفاعها عن هذا الإجراء الأمني في أعقاب ضغوط الحكومة الأمريكية.

في تصريح أدلى به العام الماضي، صرّح جاي سوليفان، أحد أعضاء لجنة مجلس الشيوخ، بأنه "يجب أن يكون الناس قادرين على التواصل بشكل آمن وخاص مع الأحباء والأصدقاء دون استماع أو مراقبة من قبل أي أحد، بما في ذلك فيسبوك، إلى محادثاتهم. ويجب أن يكون الأشخاص قادرين على إرسال معلومات طبية وتفاصيل مالية أو تفاصيل دفع ومحتويات حساسة أخرى، مع كامل الثقة في أنها لن تقع في أيدي لصوص الهوية أو أي مترصد آخر... ويصر فيسبوك على جعل هذه الاتصالات الخاصة متاحة على نطاق واسع".

لكن هذا الأمان الافتراضي غير متاح اليوم ولن يكون متاحًا في أي وقت قريب. عندما يقوم ماسنجر بالتشفير الكامل، ستتغير هذه النصيحة. ولكن حتى ذلك الحين، فإن نصيحتي هي البحث عن بديل آمن. يحتاج فيسبوك إلى تجاوز عقباته الفنية، ولكن بينما يستمر الكثيرون في استخدام التطبيق، فلن تسير هذه العملية على محمل السرعة أبدًا. أفضل ما نستطيع القيام به هو مكافأة تلك التطبيقات، بما في ذلك واتسآب، التي تضع أمننا وخصوصيتنا أولاً، وتجنب استخدام تلك التي لا تفعل ذلك

المصدر: فوربس