واتساب مخترق

واتساب WhatsApp هو تطبيق مراسلات Messenger مجاني للهواتف الذكية، وهو يستخدم الإنترنت لإرسال الرسائل والصور والصوت والفيديو والوثائق والموقع والمكالمات الصوتية. ولعل هذه الخدمة مشابهة جدًا لخدمات الرسائل النصية إلاّ أن واتساب يستخدم الإنترنت لإرسال الرسائل، ولذلك فإن تكلفة استخدامه أقل بكثير، كما يمكن أيضًا استخدام واتساب على أجهزة الكمبيوتر العادية المرتبطة بالإنترنت.

من يملك واتس آب، ولماذا هو مجاني؟

انضمت شركة واتساب إلى فيسبوك Facebook عام ٢٠١٤، لكنها استمرت في العمل كتطبيق مستقل، حث وصل عدد مستخدمي واتساب إلى أكثر من مليار شخص في أكثر من 180 دولة. لا يعتمد التطبيق على نشر الإعلانات وهو مجاني، وبالرغم للمحاولات الكثيرة لوضع رسوم اشتراك سنوية منخفضة على استخدامه إلاّ أنه استمر مجاناً حتى الآن. نعم، هناك رسوم على بعض خدمات تطبيق واتساب للأعمال WhatsApp for Business الذي يمكّن الشركات من التواصل مع عملاءها عن طريق برامج API.

أصلاً .. كيف يعمل واتس آب؟

بعد تثبيت تطبيق WhatsApp يقوم بالمرور على جميع أرقام الهواتف المسجلة لديك في قائمة الاتصال، ويقوم بمقارنتها مع الأرقام المسجلة في قاعدة بيانات ضخمة بالمسجلين لدى واتساب، لكي يقوم التطبيق تلقائياً بإضافة الأشخاص المسجلين لديك ممن يستخدمون تطبيق واتساب، إلى قائمة جهات اتصال واتساب في هاتفك. ولا يمكنك إضافة جهات اتصال أو حذفها يدويًا لأن التطبيق يرتبط مباشرة مع قائمة جهات الاتصال في هاتفك، ويقوم بالتعرّف عليهم عند طريق بأرقام الهواتف (وليس عن طريق الاسم أو البريد الالكتروني مثلاً). بعد اكتمال عملية إضافة الأرقام في قائمة اتصال واتساب، يمكنك البدء في التواصل عن طريق المحادثات.

زين.. من يحتفظ برسائل واتساب؟

الرسالة تبدأ من هاتفك، فهي موجودة لديك إلى أن تقوم بحذفها. تنتقل الرسالة مشفرة إلى خوادم واتساب، ويحتفظ بها مشفرة كما هي، فقط إلى أن يتم تسليمها إلى الطرف الآخر، وتبقى لدى الطرف الآخر حتى يقوم بحذفها. ولا يمكن لأي طرف ثالث بما في ذلك واتساب قراءة الرسائل على أي حال لأنها مشفرة.

ممم.. هل واتس آمن؟

إذا كنا نتكلم عن التشفير، فإن واتساب يخضع للتشفير التام، وهو ما يعرف بـ end-to-end encryption (أي التشفير من الطرف الأول إلى الطرف الثاني). بعض برامج المراسلات الأخرى تقوم بالتشفير بينها وبين المستخدم فقط، أي إنها تستطيع قراءة الرسائل كما هي، لكن التشفير التام في واتساب يحمي معلوماتك فلا يمكن لأحد، بما في ذلك واتساب، قراءة محتوى محادثات سواك أنت والطرف الآخر الذي تتواصل معه.

السبب في ذلك هو أن رسائلك محمية بواسطة قفل التشفير، ومن يملك المفتاح الخاص لفتح هذا القفل ويمكنه قراءة الرسائل هو أنت والطرف الذي تتحادث معه فقط. وللمزيد من الحماية فإن كل رسالة ترسلها لها قفل جديد (وفريد) ومفتاح جديد (وفريد). يتم التشفير التام تلقائياً، وليس هنالك أي إعدادات يجب ضبطها لحماية رسائلك.

ينطبق ذلك على المكالمات التي تجريها عبر واتساب، فهي مشفرة تماماً فلا يمكن لأي طرف ثالث بما في ذلك واتساب التنصت عليها.

طيب.. كيف يخترق واتساب؟

هناك العديد من الطرق لاختراق واتساب، وتتفاوت درجة التعقيد والمهارات التقنية المطلوبة لذلك. ولعل أسهل طريقة هي انتحال شخصيتك ونقل تطبيق واتساب من هاتفك الحالي إلى هاتف آخر، كأنك تقوم باستبدال هاتفك بآخر جديد.

يستغل المهاجم ميل الكثير من المستخدمين إلى عدم تغيير كلمة السر الافتراضية للبريد الصوتي للهاتف الجوال. يقوم المهاجم بتسجيل رقم هاتفك في تطبيق واتساب على هاتفه. وحسب الإعدادات الافتراضية، فسيقوم واتساب بإرسال رمز التحقق المكون من ستة أرقام عبر رسالة نصية قصيرة SMS إلى رقم هاتفك، للتحقق من أن الشخص الذي يقوم بتسجيل الرقم يمتلك ذلك الهاتف فعلاً.

الآن تأتي الحركة المهمة في الحصول على رقم التحقق. قد يقوم المهاجم بالاتصال عليك واختلاق قصة ما كفوزك بجائزة من إحدى الشركات المتحالفة مع واتساب، وللتأكد من شخصيتك

فقد تم ارسال رمز التحقق على هاتفك من برنامج واتساب لزيادة الموثوقية، ويطلب منك هذا الرقم لإتمام إجراءات حصولك على الجائزة.

طبعاً في الأحوال العادية، وعند وصول رسالة برمز التحقق إلى جوالك، فإنك ستنتبه أن هناك شيء غير طبيعي. لذلك يقوم المهاجم بطريقة أخرى أكثر دهاءً، فيتجنب ذلك عن طريق شن الهجوم في وقت لا ترد فيه أنت على الهاتف، عندما تكون نائماً بعد منتصف الليل، أو أثناء سفرك بالطائرة، حيث يقوم الكثير من الناس إلى ضبط هواتفهم على خاصية "عدم الإزعاج" خلال هذا الوقت.

إذا لم يقم المهاجم بإدخال رمز التحقق، (طبعاً لأنه لم يستلم الرسالة)، فسيفترض واتساب أن الرسالة لم تصل لأي سبب تقني، عندها سيعرض على المهاجم أن يقوم واتساب بأرسال رمز التحقق عن طريق الاتصال بك صوتياً. وبهذا ينتقل المهاجم للمرحلة التالية، ومرة أخرى عندما يتصل واتساب صوتياً فلن تقوم أنت بالرد أيضاً لأنك لا تزال نائماً. وعندما لا ترد فسيتم تحويل المكالمة إلى البريد الصوتي كرسالة مسجلة تحتوي على رمز التحقق.

حتى الآن لم يستطع المهاجم الوصول إلى رمز التحقق، وسينتقل للمرحلة التالية وهي الوصول إلى البريد الصوتي لهاتفك. هذه المرة سيستغل ثغرة أمنية بسيطة وهي أن شركات الاتصالات عادة ما تقوم بتعيين مرور افتراضية للوصول إلى البريد الصوتي، مثل 0000 أو 1234، أو الأرقام السهلة التي عادة ما يستخدمها الناس مثل 1111 أو 9999 أو غيرها، وذلك هو كل ما يحتاجه المهاجم للوصول بريدك الصوتي والاستماع إلى الرسالة التي وصلت من واتساب والتي تحتوي على رمز التحقق.

الآن، هاتف المهاجم أصبح لديه كامل السيطرة على واتساب الخاص بك، كأنه أنت، في حين أنه تم طردك من واتساب في هاتفك الحقيقي!!

خير.. أيش يقدر يسوي؟

يستطيع المهاجم انتحال شخصيتك، ولديه كل ما يحتاج. قائمة الاتصال، الرسائل والمحادثات السابقة، الصور والفيديو والوثائق ورسائل تحديد الموقع. أحدى الطرق المستخدمة أن يقوم المهاجم بمراجعة الرسائل والتعرّف على اسلوبك في الحديث من أصدقائك بحيث يستطيع التواصل معهم كأنه أنت. عادة ما يختلق المهاجم قصة أنك مسافر لدولة بعيدة وقد سرق جوازك ومحفظتك، وإنك محتاج لمساعدة عاجلة للخروج من هذه الورطة بإرسال مبلغ لشراء تذكرة العودة. وبما أن بطاقة البنك قد سرقت منك فليس هناك فائدة من التحويل إلى حسابك البنكي في بلدك بل إلى حساب أحد الأشخاص في تلك البلدة البعيدة ليقوم مشكوراً بتسليمه لك نقداً أو أن يشتري لك تذكرة العودة ويدفع حساب الفندق.

يستطيع المهاجم ابتزازك أنت شخصياً، بالمساومة على الصور ومقاطع الفيديو الشخصية والعائلية، أو بالتهديد بتشويه سمعتك بإرسال رسائل وصور غير أخلاقية إلى جميع من هم في قائمة اتصالك.

يستطيع المهاجم الاطلاع على كثير من أسرار العمل والعملاء والزملاء، وربما يكون مدفوعاً من شركات منافسة تريد اخراجكم من السوق بأي ثمن.

الاحتمالات لا تنتهي.

هل يمكنني استرجاع حسابي؟

لكي يزيد المهاجم الأمور سوءً، فيمكنه بعد الاستيلاء على حسابك أن يقوم بتفعيل ميزة التحقق من خطوتين two-step verification، حيث يطلب واتساب من المستخدم وضع رقم سري يجب عليه إعادة إدخاله إذا كان يريد إعادة التحقق من رقم هاتفه وبذلك يقوم المهاجم بإبعادك ومنعك من استعادة السيطرة على رقم هاتفك.

وعلى كل حال، فحين تعرض تطبيق واتساب في هاتفك للاختراق، فقم بالتواصل مباشرة مع شركة واتساب لمحاولة استرجاع الحساب.

أخيراً.. كيف أحمي واتساب من الاختراق؟

إذا كنت تستخدم خدمة تعتمد على الرسائل الصوتية الآلية فاحرص على البحث عن كيفية تغيير الرقم السري الافتراضي الذي تضعه شبكة الاتصالات لبريدك الصوتي. قم باختيار رقم قوي يصعب تخمينه. سيساعد ذلك في الحفاظ على سرية رسائلك ومنع هذا النوع من عمليات القرصنة على واتساب.

أيضا، يمكنك القيام بتمكين ميزة التحقق من خطوتين على حساب واتساب. اذهب إلى الإعدادات> الحساب> التحقق من خطوتين> تفعيل.