تكنولوجيا

احذر حيلة خطيرة.. تسمح للقراصنة بسرقة رسائلك على واتساب

الثلاثاء 1 ديسمبر 2020 08:09 م

حذر الباحثون الأمنيون من حيلة خطيرة تسمح للقراصنة بالوصول إلى جميع رسائل المستخدمين عبر "واتساب"، ثم استخدام حساباتهم لسرقة المحادثات الخاصة لأشخاص آخرين أيضا.

ويسمح الهجوم للقراصنة بالتظاهر بأنهم أصدقاء والوصول إلى حساب الشخص. وفي حالة فقد حساب بهذه الطريقة، يمكن للقرصان استخدام ذلك لمهاجمة أشخاص آخرين؛ مما يعني أن الوقوع ضحية للهجوم لن يؤذيك وحدك، وإنما أيضا الأشخاص الآخرين في جهات الاتصال الخاصة بك.

ويعتمد الهجوم على طريقة بسيطة، لكنها قوية للوصول إلى حسابات مختلفة.

ومع ذلك، تعتبر الحماية من ذلك بسيطة إلى حد ما: لا تعطِ أحدا أبدا "رمز التحقق" المكون من 6 أرقام، والذي سيرسله لك "واتساب" عندما يحاول شخص ما الدخول إلى حسابك، ويمكنك إعداد مصادقة ثنائية لتؤمن نفسك أكثر.

يبدأ الاختراق عندما يتمكن المهاجم من الوصول إلى حساب "واتساب" آخر؛ مما يجعلك مدرجا كجهة اتصال، ثم يرسل إليك بعد ذلك رسائل تبدو وكأنها قادمة من هذا الشخص، وقد تبدو طبيعية.

وفي نفس الوقت تقريبا، تتلقى رسالة نصية تحتوي على رمز مكون من 6 أرقام يطلب منك "واتساب" إدخاله كلما حاولت تسجيل الدخول أو إجراء تغييرات على حساب.

يحدث هذا لأن المهاجم يحاول سرا تحويل جميع الأشخاص الموجودين في قائمة جهات اتصال الشخص الأصلي إلى حساب "واتساب بيزنس".

بعدها سيقول القرصان الذي يتظاهر بأنه صديقك بأنه أرسل الرمز المكون من 6 أرقام إلى الحساب الخطأ، ويطلب منك مساعدته بإرسال الرمز.

إذا قمت بذلك، سيصل القرصان لحسابك وتفقده، ثم سيصبح حسابك طريقة أخرى لوصول المخترق إلى المزيد من الحسابات؛ حيث يتلقى أصدقاؤك رسائل يبدو أنها منك.

إن أبسط طريقة للحماية من هذه المشكلة هي عدم تمرير الرمز المكون من 6 أرقام، ويُنصح أيضا بتشغيل التحقق من خطوتين، والذي يوفر حماية إضافية للحساب.

وحاولت هجمات أخرى في الماضي أن تفعل الشيء نفسه، لكن كانت الرسائل التي تطلب الرمز عادة ما تأتي من شخص يتظاهر بأنه "الفريق الفني لواتساب" أو ما شابه. أما ما يجعل هذا الهجوم ضارًا للغاية فهو أن الرسالة قد تبدو وكأنها من صديق لك.