روش های جلوگیری از هک واتساپ

در دنیای امروز که واتساپ به یکی از اصلی‌ترین ابزارهای ارتباطی تبدیل شده است، محافظت از حساب کاربری در برابر هک اهمیت ویژه‌ای دارد. در این مقاله به روش‌های عملی و به روز پیشگیری از هک واتساپ می‌پردازیم تا امنیت حریم خصوصی و داده‌های شما تضمین شود.

۱ .فعال‌سازی تأیید هویت دو مرحله‌ای

برای افزودن لایه امنیتی اضافی، حتماً قابلیت تأیید هویت دو مرحله‌ای را در واتساپ فعال کنید. این ویژگی از شما یک پین شش‌رقمی می خواهد که در هنگام نصب واتساپ روی دستگاه جدید باید وارد شود.
در صورتی که PIN را فراموش کنید، می‌توانید آدرس ایمیل بازیابی را وارد کنید تا لینک بازنشانی برای‌تان ارسال شود. هر کاربر باید مطمئن شود که این PIN را با دیگری به اشتراک نمی‌گذارد، چرا که فاش شدن آن می‌تواند مهاجم را قادر سازد قفل دومرحله‌ای را دور بزند.

۲ .مدیریت و نظارت بر دستگاه‌های متصل

واتساپ وب و دسکتاپ به شما امکان اتصال همزمان تا چهار دستگاه را می‌دهد، اما همواره بهتر است فهرست نشست‌های فعال را بازبینی کنید. از مسیر Settings > Linked Devices می‌توانید دستگاه‌های متصل را مشاهده و جلسات ناشناس را بلافاصله با Log out قطع نمایید.

این اقدام جلوی دسترسی مهاجمان به حساب شما از طریق سشن‌های بدون اجازه را می‌گیرد.

۳ .به‌روزرسانی منظم اپلیکیشن

نسخه‌های قدیمی واتساپ ممکن است حاوی آسیب‌پذیری‌هایی باشند که مهاجمان از آن سوءاستفاده می‌کنند. برای مثال، آسیب‌پذیری CVE-2025-30401 در نسخه دسکتاپ ویندوز پیش از 2.2450.6 امکان اجرای کد از راه دور را می‌داد که به‌تازگی وصله شده است؛ بنابراین همواره اپلیکیشن را از کانال‌های رسمی به‌روز نگه دارید.

(PCWorld)

۴ .حفاظت در برابر حملات SIM Swap

حملات تعویض سیم‌کارت (SIM Swap) موجب می‌شود مهاجم با دسترسی به شماره تلفن شما، کدهای تأیید SMS واتساپ را دریافت کند. برای پیشگیری:

- پین یا سؤال امنیتی برای حساب کاربری اپراتور خود تنظیم کنید.
- اگر ممکن است، از احراز هویت چندعاملی مبتنی بر اپلیکیشن (Authenticator) به جای SMS استفاده کنید.

۵ .احتیاط در اسکن QR Code و کلیک روی لینک‌ها

حمله‌های QRLJacking و فیشینگ QR Code همچنان یکی از آسان‌ترین راه‌ها برای هک واتساپ وب هستند.

- هیچ‌گاه QR دریافتی از منابع ناشناس را اسکن نکنید و پیش از اسکن از صحت مبدأ اطمینان حاصل کنید.

- لینک‌های ارسالی در پیام‌ها را بدون بررسی نشانی و گواهی SSL کلیک نکنید، زیرا ممکن است به صفحات فیشینگ هدایت شوید.

۶ .استفاده از نسخه رسمی واتساپ و اجتناب نصب نسخه های مود شده

اپلیکیشن‌های جعلی یا مودشده FMWhatsApp، GBWhatsApp و.. ممکن است به تروجان‌ها و جاسوس‌افزارها آلوده باشند. همیشه واتساپ را تنها از فروشگاه‌های Google Play یا App Store و وب‌سایت رسمی دانلود کنید.

۷ .بهره‌گیری از «حریم خصوصی پیشرفته» جدید واتساپ

WhatsApp اخیراً قابلیت «Advanced Chat Privacy» را معرفی کرده که از خروج محتوای چت‌ها جلوگیری می‌کند و امکان دانلود خودکار رسانه‌ها توسط دیگران را محدود می‌سازد؛ فعال کردن این گزینه، لایه‌ای اضافی برای محافظت از داده‌های شما ایجاد می‌کند.

۸ .تنظیم رمز عبور یا قفل برنامه

علاوه بر FA2، می‌توانید برای دسترسی به اپلیکیشن واتساپ روی گوشی خود، از رمز عبور یا حسگر بیومتریک (اثر انگشت/چهره) استفاده کنید تا در صورت دستیابی فیزیکی، مهاجم نتواند بدون اجازه وارد اپ شود.

۹ .فعال‌سازی اعلانات امنیتی

واتساپ قابلیت هشدار به کاربر را دارد که در صورت تغییر کلیدهای رمزگذاری انتهابه‌انتها، شما را مطلع می‌کند. این ویژگی را در Settings > Account > Security فعال کنید تا اگر کسی قصد سرقت مکالمه را داشته باشد، سریعاً مطلع شوید.

۱۰ .آموزش و آگاهی‌بخشی

آگاهی از روش‌های مهندسی اجتماعی و فیشینگ، کلید اصلی پیشگیری است.

- کاربران و خانواده را با نشانه‌های پیام‌های فیشینگ (مانند لحن اضطراری یا ادعای فوری بودن) آشنا کنید.
- در گروه‌های کاری یا دوستانه، نکات امنیتی را منتشر و به‌روزرسانی‌های جدید را اطلاع‌رسانی نمایید.

با اجرای منظم این توصیه‌ها و حفظ هوشیاری، می‌توانید از حساب واتساپ خود در برابر انواع حملات سایبری محافظت کنید و حریم خصوصی‌تان را امن نگه دارید.