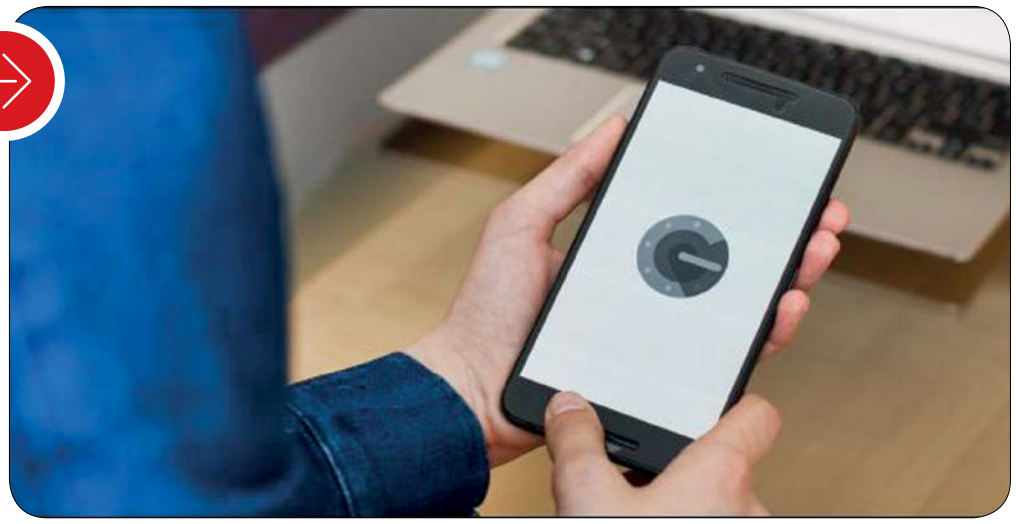
سال‌هاست هکرها به کمک حفره امنیتی SS7 سیستم سیگنالینگ شماره ۷ و تنها با داشتن شماره تلفن همراه فرد توانسته‌اند به متن پیامک‌ها و تماس‌های تلفنی و موقعیت مکانی صاحب گوشی دسترسی داشته باشند



Google Authenticator از تمام شبکه‌های اجتماعی و سایت‌های بزرگ و مطرح مثل فیس‌بوک، توییتر، اینستاگرام و جیمیل و حساب‌های رمزارز پشتیبانی می‌کند

هر آنچه درباره نرم‌افزار Google Authenticator لازم است بدانید

# دنیای رمزهای لحظه‌ای

عارف چراغی
روزنامه‌نگار فناوری

**تصور کنید هر هکر تازه‌کاری بتواند به‌راحتی تمام فعالیت‌های شما را در تلفن همراه‌تان زیر نظر بگیرد. از شنود تلفن‌هایتان گرفته تا پیامک‌هایتان. حساب‌های بانکی‌تان را ظرف چند ثانیه خالی کند و اکانت‌های شبکه‌های اجتماعی‌تان را به کنترل خود درآورد. همه این اقدامات را انجام بدهد بدون این‌که نیاز باشد از خانه خارج شود و حتی شاید یک قاره آن‌طرف‌تر باشد. همه اینها موجب شده در سال‌های اخیر، رمزی کوتاه‌مدت و پویا فعال شود. ولی واقعیت این است حتی رمزهای کوتاه‌مدت هم از چنگال هکرها در امان نیستند. اینجاست که رمزهای دومرحله‌ای اهمیت پیدا می‌کنند. در این گزارش به بررسی ویژه‌ترین اپلیکیشن در این زمینه می‌پردازیم.**

سال‌هاست هکرها به کمک حفره امنیتی SS7 سیستم سیگنالینگ شماره ۷ و تنها با داشتن شماره تلفن همراه فرد توانسته‌اند به متن پیامک‌ها، تماس‌های تلفنی و موقعیت مکانی صاحب گوشی دسترسی داشته باشند.

پیشتر تصور می‌شد استفاده از رمزهای پویا و یکبارمصرف که از طریق پیامک فرستاده می‌شوند، از بیشترین درجه امنیت برخوردار هستند، اما هکرها به‌کمک حفره امنیتی در پروتکل SS7 یا روش‌های دیگر می‌توانند به این رمز دسترسی پیدا کنند.

همه اینها باعث شد متخصصان حوزه امنیت سایبری به فکر راه‌حلی برای محافظت از کدهای احرازهویت دومرحله‌ای (two-factor authentication) یا همان 2FA بیفتند.

در این روش، رمز پویا دیگر به کاربر پیامک نمی‌شود، بلکه ازطریق اپلیکیشن روی گوشی نمایش داده می‌شود و این یعنی تنها راه دسترسی هکر به این کد، دسترسی فیزیکی به گوشی است.

اپلیکیشن‌های زیادی در سال‌های اخیر در این حوزه توسعه یافته‌اند؛ اما یکی از مطمئن‌ترین آنها Google Authenticator است. با استفاده از Google Authenticator در صورت ورود یک کاربر به حساب خود با استفاده از یک دستگاه ناآشنا برای استفاده از حساب لازم است رمزی که گوگل در اختیارتان قرار می‌دهد را وارد کنید.

در واقع گوگل با توجه به پل ارتباطی امنی که بین خود و صاحب حساب وجود دارد اقدام به ارسال کد می‌کند تا کاربر بتواند وارد حساب خود شود.

در واقع احراز هویت دو مرحله‌ای به این صورت است که در آن کاربر برای ورود به اپلیکیشن یا حساب آنلاینش، علاوه بر رمز عبور همیشگی، باید کد دیگری هم برای تأیید هویت خود وارد کند.

خوشبختانه این اپلیکیشن از تمام شبکه‌های اجتماعی و سایت‌های بزرگ و مطرح مثل فیس‌بوک، توییتر، اینستاگرام و جیمیل و شماری از حساب‌های رمزارز پشتیبانی می‌کند. اپلیکیشن Google Authenticator رمز عبور یکبار مصرف شش‌رقمی تولید می‌کند که هر ۳۰ ثانیه یکبار تجدید می‌شود.

محدودیت زمانی این کد به این‌معنی است که اگر یک هکر سایبری موفق شد به طریقی به کد یکبار مصرف شما دسترسی پیدا کند، این کد تنها ۳۰ ثانیه اعتبار داشته باشد و بعد از گذشت این زمان دیگر اثری نخواهد داشت. این پلتفرم هیچ‌گونه دسترسی به حساب‌هایتان ندارد و بعد از انتقال اولیه کد، ارتباطی با سایت مدنظر برقرار نمی‌کند.

کار این اپلیکیشن فقط تولید کد است و برای این کار به خدمات مخابرات یا حتی اینترنت نیازی ندارد. اپلیکیشن Google Authenticator در مقایسه با پلتفرم‌هایی با کارکرد مشابه، تنها از دو قابلیت، یعنی همان تولید کد 2AF و اکسپورت اطلاعات اکانت‌ها به گوشی دیگر پشتیبانی می‌کند، به‌همین‌دلیل کار با آن بسیار ساده است.

**پس از نصب این برنامه، هر بار اپلیکیشنی را باز کنید، با کد شش‌رقمی روبه‌رو می‌شوید که برای تکمیل مرحله لاگین به اکانت متصل شده لازم است. توجه کنید این کد هر ۳۰ ثانیه یکبار عوض می‌شود**

## چطور آن را برای اکانت‌هایمان فعال کنیم؟

برای متصل کردن Google Authenticator به حساب‌هایتان کافی است با نام کاربری و رمز عبور خود طبق معمول وارد اکانت دلخواه‌تان شوید. سپس به بخش مربوط به فعال‌کردن قابلیت 2AF بروید و کد QR نمایش داده شده را با این اپلیکیشن اسکن کنید. با این کار، اکانت شما به اپلیکیشن متصل می‌شود و از این پس برای ورود به اکانت‌تان لازم است کدی را وارد کنید که در اپلیکیشن ظاهر می‌شود.

## مراحل نصب اپلیکیشن

شاید به جرات بتوان گفت این اپلیکیشن از ساده‌ترین محصولات شرکت گوگل است. حتی بعد از اتمام دانلود و نصب اپلیکیشن روی گوشی هوشمندتان نیازی نیست اپلیکیشن را باز کنید.

۱ ابتدا از طریق کامپیوتر یا گوشی یا تبلت دیگری، وارد صفحه مربوط به فعال‌کردن احرازهویت دوعاملی یا احراز هویت دومرحله‌ای وب‌سایت مدنظر شوید و این قابلیت را فعال کنید. این قابلیت معمولا در بخش Security اکانت قرار دارد.

۲ بعد از این مرحله، دنبال گزینه استفاده از اپلیکیشن احراز هویت authenticator app بگردید و روی آن کلیک کنید.

۳ هنگام راه‌اندازی 2FA، معمولا از شما خواسته می‌شود کد QR را اسکن کنید؛ به‌همین خاطر به کامپیوتر یا گوشی یا تبلت دیگری نیاز دارید تا بتوانید این قابلیت را روی اکانتتان فعال کنید. اگر به دستگاه دیگری دسترسی ندارید یا دوربین گوشی‌تان کار نمی‌کند، می‌توانید گزینه نمایش کلید راه‌اندازی را به‌جای کد QR انتخاب کنید.

۴ حالا اپلیکیشن را باز کنید. گزینه Get Started را لمس کنید تا به صفحه اولیه هدایت شوید.

۵ روش راه‌اندازی را انتخاب کنید. این مرحله به وب‌سایتی بستگی دارد که قصد دارید 2FA را برای آن فعال کنید. گزینه اسکن کد QR متداول‌ترین روش راه‌اندازی است. اگر هنگام فعال‌سازی روش 2FA در وب‌سایتی با کد QR روبه‌رو شدید، روی اپلیکیشن گزینه Scan a QR code را انتخاب کنید.

۶ اگر با رشته‌ای از حروف موسوم به کلید راه‌اندازی روبه‌رو شدید، از اپلیکیشن گزینه Enter a setup key را انتخاب کنید.

۷ حالا کد QR نمایش‌داده شده روی وب‌سایت را با گوشی‌تان اسکن کنید.

۸ برای گزینه Enter a setup key، ابتدا برای اکانت‌تان نامی به‌دلخواه انتخاب و در نوار زیرین، کلید را به‌طور دستی وارد کنید. سپس، دکمه add را فشار دهید.

۹ بعد از تأیید، اکانت مدنظر به اپلیکیشن Google Authenticator متصل می‌شود.

۱۰ از این پس هر بار اپلیکیشنی را باز کنید، با کد شش‌رقمی روبه‌رو می‌شوید. این کد برای تکمیل مرحله لاگین به اکانت متصل‌شده لازم است. توجه کنید این کد هر ۳۰ ثانیه یکبار عوض می‌شود. اگر هنگام تایپ کد ارقام نمایش‌داده شده روی اپلیکیشن تغییر کرد، کد نوشته‌شده را پاک و از کد جدید استفاده کنید.

۱۱ برای اضافه‌کردن اکانت‌های جدید به اپلیکیشن، دکمه «+» در انتهای صفحه را فشار دهید و گزینه Scan a QR code برای اسکن کد QR یا Enter a setup key را انتخاب کنید.