راهنمای گام به گام برای رمزنگاری نامه‌های‌تان در جی‌میل

چگونه یک ایمیل امن ارسال کنیم؟

هر زمان سخن از رمزنگاری داده‌ها به میان می‌آید، برخی از کاربران تصور می‌کنند رمزنگاری داده‌ها علمی است که هکرها به آن علاقه داشته و بیش از اندازه تخصصی و فنی است. اما واقعیت چیز دیگری است. رمزنگاری داده‌ها نقش کلیدی در زندگی امروزی ما دارد. فرقی نمی‌کند یک کاربر عادی یا کارمند سازمان بزرگی باشید، برای حفظ حریم خصوصی و محافظت از داده‌های شخصی خود مجبور هستید حداقل اطلاعات لازم را در حوزه رمزگذاری کسب کنید. پست الکترونیک یا همان ایمیل، یکی از مهم‌ترین سرویس‌هایی است که با زندگی همه ما عجین شده و با علم رمزنگاری داده‌ها تعامل مستقیمی دارد. اگر برای انجام کارهای شخصی یا تجاری خود از پست الکترونیک جی‌میل استفاده می‌کنید، پیشنهاد می‌کنم چند دقیقه وقت صرف کرده و تا انتها این مقاله را مطالعه کنید تا آگاه شوید این سرویس چگونه از اطلاعات شخصی شما محافظت کرده و بر مبنای چه راهکارهایی قادر هستید سطح ایمنی این سرویس را بهبود بخشید. این راهنمای گام‌به‌گام نشان می‌دهد، رمزنگاری جی‌میل چگونه کار کرده و برای بهبود سطح محرمانگی ایمیل‌های خود چه کارهایی باید انجام دهید.

رمزنگاری جی‌میل: چگونه گوگل از پیام‌های ما محافظت می‌کند؟

گوگل برای پیاده‌سازی **رمزنگاری** در جی‌میل از پروتکل TLS (سرنام Transport Layer Security) استفاده می‌کند. اگر گیرنده ایمیل شما از پست الکترونیک مبتنی بر TLS استفاده کند، همه ایمیل‌های ارسالی از جی‌میل برای مخاطب به شکل رمزنگاری‌شده ارسال خواهد شد. این حرف به معنای آن است که ایمیل از مبدا تا مقصد به شکل ایمنی ارسال خواهد شد و احتمال این‌که شخصی بتواند محتوای ایمیل شما را خوانده یا یک حمله مرد میانی با موفقیت به سرانجام برساند، خیلی ضعیف است. اما زمانی‌که پیغام به میل سرور می‌رسد، دیگر هیچ‌گونه ضمانتی وجود ندارد که اصل محرمانگی حفظ شود، زیرا خود گوگل اگر تصمیم بگیرد این توانایی را دارد تا پیغام‌های شما را مشاهده کرده و به همین دلیل می‌تواند ایمیل‌های شما را پویش کرده و مانع از آن شود تا هرزنامه‌ها و حمله‌های فیشینگ به سمت صندوق‌پستی شما گسیل‌شده و مهم‌تر از آن قابلیت‌های پیشرفته‌ای همچون پاسخ هوشمند (Smart Reply) را ارائه می‌کند. قابلیتی که بر مبنای محتوای ایمیل‌های دریافتی پاسخ‌های آماده به ارسالی به شما پیشنهاد می‌دهد. گوگل برای نشان دادن آگهی‌های هدفمند محتوای ایمیل‌های کاربران جی‌میل را اسکن می‌کرد که پس از حرف‌وحدیث‌های بسیاری که پیرامون این قضیه به وجود آمد، در نهایت سال 2017 این‌کار را متوقف کرد.

اگر میل سرور شخصی که برای او ایمیل ارسال می‌کنید، از استاندارد TLS پشتیبانی نکند، ایمیل‌های ارسالی شما رمزنگاری نمی‌شود. البته، گوگل برای این گروه از کاربران سرویس ویژه G Suite را در نظر گرفته که رایگان نیست. مدیران شبکه می‌توانند برای برقراری امنیت تنها اجازه ارسال و دریافت پیام‌هایی را بدهند که با پروتکل TLS رمزنگاری شده‌اند. البته، چنین راهکاری محدودیت‌های خاص خود را داشته و برای مثال ممکن است ایمیل مهمی از مدیر سازمان برای شما ارسال‌شده، اما به دلیل این‌که از پروتکل TLS استفاده نکرده‌اید، جی‌سویت اجازه نداده پیغام به صندوق پستی شما وارد شود.

رمزنگاری جی‌میل؛ راهکار پیشرفته‌تر

جی‌میل در کنار پروتکل TLS، از استانداردهای دیگری نیز پشتیبانی می‌کند که S/MIME (سرنام Secure/Multipurpose Internet Mail Extensions) یکی از این موارد است. البته استاندارد فوق فقط برای حساب‌های کاربری پولی G Suite Enterprise و G SuiteEducation ارائه‌شده و در اختیار کاربران سرویس رایگان جی‌میل قرار ندارد. استاندارد S/MIME در بسته G Suite، ایمیل‌ها را بر مبنای کلیدهای تخصیص‌یافته به هر کاربر **رمزنگاری** کرده تا اصل محرمانگی ایمیل‌ها از مبدا تا مقصد حفظ‌شده و فقط گیرنده ایمیل بتواند ایمیل‌ها را رمزگشایی کند. این استاندارد همانند TLS تنها زمانی کارایی اصلی خود را دارد که هر دو طرف از سرویسی مبتنی بر این استاندارد استفاده کنند. در این استاندارد ارسال‌کننده و دریافت‌کننده، پیش از آن‌که ایمیلی را ارسال کنند؛ کلیدها را مبادله می‌کنند تا **رمزنگاری** به شکل درستی انجام شود. مشابه با استاندارد TLS در این تکنیک نیز زمانی‌که ایمیل به میل سرور رسید، محتوا دیگر محرمانه نبوده و گوگل قادر است متن پیغام‌های جی‌میل را به شکل خودکار پویش کند.

مطلب پیشنهادی

گوگل قصد دارد با Adiantum امنیت و حفظ حریم خصوصی را به همه عرضه کند
Adiantum سیستم امنیتی رمزگذاری جدید گوگل

رمزنگاری جی‌میل: رمزنگاری نقطه پایانی/سراسری (End-To-End Encryption)

گوگل از سال 2014 میلادی تا به امروز (ژانویه 2019 میلادی) بارها و بارها درباره اضافه کردن فناوری **رمزنگاری** نقطه‌به‌نقطه (End-to-End encryption) به جی‌میل پست‌های مختلفی منتشر کرده، اما هنوز این حرف‌ها به واقعیت تبدیل نشده‌اند و به اعتقاد برخی از تحلیلگران ممکن است هیچ‌گاه در عمل شاهد چنین موضوعی نباشیم. در مقطع فعلی بهترین راهکاری که برای دسترسی به چنین سطح بالایی از امنیت در جی‌میل در اختیار ما قرار دارد، به‌کارگیری سرویس‌های ثالثی مانند FlowCrypt است. FlowCrypt یک افزونه جانبی است که برای نسخه دسکتاپی مرورگر کروم یا فایرفاکس ارائه‌شده است. البته نسخه بتای این افزونه برای اندروید نیز منتشرشده است. زمانی‌که افزونه فوق به صفحه عادی جی‌میل اضافه می‌شود، دکمه‌ای به نام Secure Compose در اختیارتان قرار می‌دهد. با فعال کردن این دکمه افزونه از استاندارد PGP سرنام (Pretty Good Party) برای **رمزنگاری** ایمیل‌ها و ارسال آن‌ها استفاده می‌کند. البته دریافت‌کننده پیام باید افزونه فوق یا هر سرویسی را که از PGP استفاده می‌کند، روی مرورگر خود نصب کرده باشد. البته کلید اختصاصی PGP باید برای دریافت‌کننده ایمیل ارسال شود تا بتواند ایمیل شما را رمزگشایی کرده و محتوای ایمیل را مشاهده کند. البته راهکار دیگری نیز وجود دارد؛ از افزونه‌هایی استفاده کنید که برای **رمزنگاری** یک پیام از گذرواژه استفاده می‌کنند. البته در این روش باید گذرواژه را به شکلی برای دریافت‌کننده ارسال کنید تا بتواند پیام شما را باز کند. بله همان‌گونه که مشاهده کردید، این روش خیلی ساده نیست و مهم‌تر از آن به‌کارگیری افزونه‌های ثالث راهکار چندان شاخصی نیست، ولی به هر ترتیب مشکل دسترسی غیرمجاز به محتوا را برطرف می‌کنند و مهم‌تر از آن رایگان هستند.

ویژگی Confidential Mode جی‌میل چیست و چه کاری انجام می‌دهد؟

Confidential Mode یا همان حالت محرمانگی از جمله قابلیت‌های جدید جی‌میل است که گوگل در سال 2018 از آن رونمایی کرد. این قابلیت به شما اجازه می‌دهد، مانع از آن شوید تا گیرنده، ایمیل را کپی، فوروارد، چاپ یا هرگونه محتوای ضمیمه ایمیل را دانلود کند. با استفاده از این قابلیت می‌توانید ایمیل‌هایی ارسال کنید که تاریخ انقضا داشته باشید و پس از سپری شدن زمان مدنظر دیگر در دسترس گیرنده نباشد. قابلیت فوق به شما اجازه می‌دهد گذرواژه‌ای ایجاد کنید که از طریق ایمیل یا پیام متنی به دست گیرنده رسیده و باز کردن ایمیل تنها از طریق این گذرواژه امکان‌پذیر باشد. قابلیت‌هایی که به آن‌ها اشاره شد، ایده‌آل هستند، اما اگر به دنبال امنیت به شکل واقعی آن هستید، مواردی که به آن‌ها اشاره شد، زیاد جوابگو نیستند، زیرا مادامی که الگوی **رمزنگاری** نقطه‌به‌نقطه روی پیام‌ها اعمال نشود، گوگل قادر است محتوای ایمیل‌های شما را خوانده و آن‌ها را ذخیره‌سازی کند. حالت محرمانگی راهکارهای جالب‌توجهی در اختیارتان قرار می‌دهد، اما اگر گیرنده ایمیل از صفحه خود یک اسکرین‌شات بگیرد، این

قابلیت‌ها چندان کاربردی نخواهند بود. البته گوگل به این حقیقت اذعان دارد که حالت محرمانگی قرار نیست بالاترین سطح از امنیت را ارائه کند، بلکه هدفش این است که اجازه ندهد مردم به شکل پنهانی اطلاعات دیگران را به اشتراک قرار داده و اطلاعات در اختیار افراد مختلفی قرار گیرد. تعیین بازه زمانی برای غیرقابل‌دسترس کردن ایمیل‌ها چنین وضعیتی دارد، زیرا اصل ایمیلی که ارسال‌شده پس از سپری شدن زمان موردنظر در پوشه پیام‌های ارسالی قرار خواهد گرفت. در مجموع، ویژگی حالت محرمانگی برای اعمال یکسری محدودیت‌ها کاربرد داشته و نباید برای **رمزنگاری** یا پیاده‌سازی بالاترین سطح از محرمانگی روی آن حساب زیادی باز کنید. راهکار پیشنهادی گوگل باعث شده تا بنیاد Electronic Frontier Foundation به آن واکنش نشان داده و اعلام کند حالت محرمانگی بیشتر یک حس امنیت کاذب به وجود می‌آورد و مانع از آن می‌شود تا کاربران تمهیدات امنیتی لازم را اتخاذ کنند.

مطلب پیشنهادی

جادوگری با ایمیل‌ها
۵ ترفند کوتاه و کاربردی جی‌میل

چه راهکارهای پیشنهادی دیگری پیش روی ما قرار دارد؟

اگر تمایل دارید رمزنگاری نقطه‌به‌نقطه را به شکلی بومی روی سرویس ایمیل خود پیاده‌سازی کرده و محرمانگی در بهترین سطح ممکن در اختیارتان قرار گیرد، پیشنهاد می‌کنیم از دایره قابلیت‌های ارائه‌شده از سوی جی‌میل خارج‌شده و به سراغ برنامه کاربردی ProtonMail بروید. نسخه اندرویدی ProtonMail بهترین برنامه کاربردی در حوزه امنیت و حفاظت از حریم شخصی است که برای اکوسیستم اندروید ارائه‌شده است. این برنامه تعهد خاصی در قبال محرمانگی داشته و خیلی بهتر و دقیق‌تر از **رمزنگاری** استاندارد جی‌میل قادر است از پیام‌های شما محافظت کند. Protonmail برای پیاده‌سازی **رمزنگاری** نقطه‌به‌نقطه‌ای یک الگو متن‌باز استفاده می‌کند. متن‌باز بودن این ضمانت را می‌دهد که هیچ شخص ثالثی به جز دریافت‌کننده ایمیل نتواند محتوای ایمیل‌های شما را مشاهده کند. ProtonMail برای انجام کارهای خود از شما اطلاعات شخصی دریافت نکرده و شرکت ارائه‌دهنده هیچ‌گونه آدرس آی‌پی یا اطلاعاتی را که ارتباطی میان شما و حساب‌کاربری‌تان به وجود آورد، ذخیره‌سازی نمی‌کند.
اگر کنجکاو شده‌اید درباره سرورهای این شرکت اطلاعاتی به دست آورید، باید به شما بگوییم سرورهای این برنامه در کشور سوییس و در عمق 1000 متری کوه قرار گرفته‌اند که خود یک برتری طبیعی را برای سرورهای این شرکت به وجود آورده‌اند. عملکرد برنامه ProtonMail به این شکل است که پس از دریافت و نصب برنامه، باید در آن ثبت‌نام کنید. در ادامه ProtonMail تحت دامنه خود، یک آدرس ایمیل سفارشی در اختیار شما قرار می‌دهد. شما می‌توانید از این آدرس برای ارسال پیام‌های ایمن درون برنامه‌ای استفاده کنید. این برنامه روی پلتفرم iOS قابل‌استفاده بوده و نسخه تحت وب آن نیز ارائه‌شده است. هر زمان با آدرس ارائه‌شده از سوی برنامه ایمیلی برای فردی ارسال کنید، پیام شما به شکل خودکار **رمزنگاری** می‌شود. هر زمان برای فردی ایمیل ارسال کردید که از ProtonMail استفاده نمی‌کند، به‌راحتی می‌توانید گزینه ارسال بدون **رمزنگاری** را انتخاب کرده یا دکمه ویژه ارائه‌شده از سوی این برنامه را انتخاب کنید تا گذرواژه‌ای برای ایمیل شما ایجاد شود. در ادامه گذرواژه را به شکلی ایمن برای گیرنده ارسال کنید تا بتواند پیام شما را رمزگشایی کرده و محتوای آن را مطالعه کند. این برنامه به شکل رایگان و پولی قابل‌استفاده است. در نسخه رایگان یک آدرس ایمیل ویژه با 500 مگابایت فضای ذخیره‌سازی و امکان ارسال 150 پیام در روز در اختیارتان قرار می‌گیرد. افرادی که به دنبال فضای ذخیره‌سازی بیشتری هستند و پیام‌های متعددی در یک روز ارسال می‌کنند و به قابلیت‌های پیشرفته‌ای همچون فیلتر ایمیل‌ها، سامانه پاسخ‌گویی خودکار و پشتیبانی از دامنه‌های سفارشی نیاز دارند باید از نسخه پولی این برنامه استفاده کنند. شما می‌توانید این راهکار را با سرویس جی‌میل ترکیب کرده و جی‌میل را به شکلی تنظیم کنید تا پیام‌ها را برای پروتون ارسال کنید یا از برنامه ProtonMail در قالب یک نسخه مکمل برای جی‌میل استفاده کرده و پیام‌های حساس خود را با این برنامه ارسال کنید. اگر حوزه کاری شما حساس بوده و نگرانید اطلاعات‌تان فاش شوند، ProtonMail یک راهکار کم‌نظیر و جالب‌توجه در اختیارتان قرار می‌دهد.

تاریخ انتشار:

27 اسفند 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/14820/%DA%86%DA%AF%D9%88%D9%86%D9%87-%DB%8C%DA%A9-%D8%A7%DB%8C%D9%85%DB%8C%D9%84-%D8%A7%D9%85%D9%86-%D8%A7%D8%B1%D8%B3%D8%A7%D9%84-%DA%A9%D9%86%DB%8C%D9%85%D8%9F