[redacted]

[redacted]

[redacted]

[redacted]

[redacted] (Transport Layer Security [redacted]) TLS [redacted]

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 رمزنگاری 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

PGP .

Confidential Mode

2018 Confidential Mode Electronic Frontier Foundation

ProtonMail .

ProtonMail ProtonMail .

Protonmail .

ProtonMail .

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.

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
07:15 - 27/12/1397
برچسب:
رمزنگاری جی میل - رمزنگاری داده ها - راهنمای ساخت ایمیل امن - امنیت ایمیل - رمزنگاری

نشانی
□□□□: 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