چگونه ارتباطات ایمیلی امن داشته باشیم؟

By noshabe

سرویس هایی مانند ایمیل برای کاربران شخصی و حتی شرکت ها بسیار با ارزش هستند. استفاده راحت، هزینه کم و انعطاف پذیری این سرویس ها باعث محبوبیت شان شده است. همچنین سرعت و اتصال مطمئن که در سرویس هایی همچون اسکایپ) سرویس انتقال صوت از طریق اینترنت) ارائه می گردد، از دیگر عوامل موثر در این محبوبیت هستند. اما متاسفانه چه بخواهیم و چه نخواهیم این سرویس های دیجیتالی هم همانند سرویس های قدیمی و سنتی نمی توانند به طور کامل از اطلاعات و ارتباطات ما محافظت کنند. سرویس های ایمیل، تلفن و اس ام اس همواره از لحاظ امنیتی آسیب پذیر هستند، مخصوصاً اگر توسط سرویس دهنده آن یا هکر یا و افراد فضول مورد بررسی و کنترل قرار گیرند.

تفاوت مهم سرویس های دیجیتال که مبتنی بر اینترنت هستند، با سرویس های سنتی در این است که در بسیاری از مواقع این شما هستید که سطح امنیت را در این سرویس ها برای خودتان تعیین می کنید. اگر بدون استفاده از راه های امن ایمیلی بفرستید، یا به صورت صوتی یا متنی با کسی صحبت (چت) کنید، به جرات می توان سطح امنیتی این کار شما را با یک تلفن غیر امن یا ارسال یک نامه با پست عادی مقایسه کرد.

البته چون کامپیوترهای کمی وجود دارند که توانایی جستجو و ردیابی موردی خاص از بین انبوهی از اطلاعات (عبارات مورد نظر، فرستنده، گیرنده و ...) را داشته باشند، دلیل نمی شود که امنیت را دست کم بگیریم؛ باید بدانیم در صورت لزوم نیروی لازم برای تجسس در آن حجم از اطلاعات هم همانند سرویس های سنتی فراهم می شود و ارتباط امنی نخواهیم داشت. با این حال با رعایت برخی نکات احتیاطی، می‌توان تا حد زیادی از بروز مشکل و ناامنی جلوگیری کرد .هکرها ممکن است هر جایی در میان ارتباطات اینترنتی شما در کمین باشند تا از کارهای شما سر دربیاورند. بنابراین همیشه باید مراقب امنیت ارتباطات خود باشید. در این مطلب نگهبان خواهید آموخت که چگونه از حداقل امنیت برای ارسال و دریافت ایمیل هنگام استفاده از سرویس های Webmail برخوردار شوید.

امنیت ارتباطات ایمیلی وقتی که از Webmail استفاده می کنید

درکل تنها چند قدم ساده اما مهم برای افزایش امنیت ارتباطات ایمیلی وجود دارد که انجام آنها اکیدا توصیه می شود.

چگونه ایمیل مان را محرمانه نگه داریم:

درواقع اینترنت از شبکه به هم پیوسته ای از اطلاعات تشکیل شده است. آن هم اطلاعاتی قابل خواندن که دائماً در حال جابجایی هستند. اگر ایمیلی معمولی که در راه رسیدن به گیرنده است در میانه راه دزدیده یا باز شود، به راحتی می توان اطلاعات و نوشته های آن را بازخوانی کرد. اینترنت شبکه ای عظیم و جهانی است که اتصال واسط بین این همه کامپیوتر و دستگاه های مختلف را برقرار کرده و در هر لحظه افراد زیادی هم در حال جا به جا کردن پیام بین هم هستند که این پیام ها باید از واسط های مختلفی عبور کنند تا به مقصد برسند؛ پس ممکن است افراد زیادی هم در میان این همه تقاطع و اتصال بعضی از این تبادل ها را زیر نظر بگیرند.

اولین دریافت کننده ایمیل شما، همان ISP یا سرویس دهنده اینترنت شما است و مسلماً سرویس دهنده ی اینترنتی گیرنده ی اصلی پیام هم یکی دیگر از نقاط توقف ایمیل است؛ که البته آخرین توقف گاه، قبل از گیرنده واقعی است. باید بدانید که پیام های شما می توانند در این ایستگاه های اجتناب ناپذیر و سایر ایستگاه های احتمالی توسط هر کسی خوانده شوند و این در صورتی اتفاق می افتد که شما از حریم ایمیلی خود محافظت نکنید.

البته امکان برقراری اینگونه ارتباطات امن مدت‌های مدیدی است که ایجاد گردیده است. اغلب اوقات در زمان وارد کردن رمز عبور یا اطلاعات کارت اعتباری، رد و بدل اطلاعات بصورتی امن انجام می شود. تکنولوژی مورد استفاده در این مواقع، SSL Encryption (Secure Sockets Layer – لایه رمزگذاری شده امن) نام دارد. معمولاً همه شما با این سایت ها و صفحات برخورد کرده اید و می توانید رد پای این سطح امنیتی را در محل آدرس بار در مرورگر خود مشاهده کنید.

همه آدرس های معمولی مانند شکل زیر با HTTP شروع می شوند:

و وقتیکه شما با آدرسی شبیه زیر روبرو می شوید که با HTTPS شروع شده است، درواقع از شیوه رمزگذاری SSL استفاده می کنید.

این "S" اضافه شده به انتهایHTTP ، نشان دهنده اتصال امن از نوع SSL Encryption است. همچنین ممکن است شما شکل یک قفل را هم در بالا یا پایین مرورگر خود مشاهده کنید. این قفل هم نشانه دهنده آن است که در واقع هیچ کس به جز شما و سایت هدف، اطلاعات صفحه مورد نظر را بازبینی و یا مشاهده نمی کند.

این شیوه علاوه اینکه برای ارتباط امن هنگام کار با رمزهای عبور و اطلاعات مالی به کار می رود، در بعضی سرویس های ایمیل هم استفاده می گردد، که تا حد زیادی هم موثر و کارآمد است. به هر ترتیب متأسفانه بسیاری از سرویس دهنده های ایمیل برای دسترسی امن کاربران به ایمیل شان اهمیتی قائل نیستند، اما بعضی هم یا بصورت پیش فرض و یا بصورت سفارشی، امکان استفاده از این قابلیت را برای کاربران خود فراهم می کنند.

در هر صورت شما باید هنگام وارد کردن رمز عبور و همچنین باز کردن، خواندن و ارسال ایمیل، از امنیت اتصال به سرویس ایمیل خود اطمینان حاصل کنید.

همچنین در زمان ورود باید مراقب اخطارهای احتمالی مرورگر، در خصوص صفحات امن نامعتبر هم باشید. چرا که ممکن است کسی با مداخله در ارتباط کامپیوتر شما و سرور مربوطه، قصد نفوذ به سیستم و دسترسی به پیام های شما را داشته باشد. شدیدا توصیه می کنیم که اگر اطلاعات مهم و حساسی را با ایمیل مبادله می کنید، از سرویس های امن استفاده کنید. همچنین استفاده از مرورگر فایرفاکس به همراه افزونه های امنیتی آن هم توصیه می شود.

مهاجرت به یک سرویس ایمیل امن تر
وب میل های کمی هستند که برای سرویس ایمیل شان از پروتکل امنیتی SSL استفاده می کنند. به عنوان مثال یاهو و هات میل فقط در پنجره ورودی از SSL استفاده می کنند، که برای حفظ امنیت رمز ورود شما است؛ اما این دو سرویس دهنده برای ارسال و دریافت ایمیل های شما از این تکنولوژی استفاده نمی کنند. ضمن اینکه یاهو و هات میل حتی آدرس IPکامپیوتری را که از آن برای ارسال ایمیل استفاده کرده‌اید نیز ضمیمه ایمیل می کنند. بنابراین این دو سرویس برای کسانی که به دنبال ایمیل امن هستند واقعاً مناسب نیستند.

سرویس جیمیل، از اتصال امن برای دسترسی کاربران به ایمیل هایشان استفاده می کند. البته در حالت پیش فرض فقط هنگام ورود به جیمیل آدرس صفحه را اینگونه (https://www.mail.google.com) و با HTTPS می بینید و این آدرس بعد از ورود به ایمیل به HTTP بر می گردد. شما می توانید از طریق بخش تنظیمات جیمیل استفاده از آن را به طور دائمی بر روی HTTPS و تحت یک اتصال امن قرار دهید.
بنابراین تا وقتی که این تنظیم را روی جیمیل فعال نکرده باشید جیمیل هم مانند یاهو و هات میل یک سرویس غیرامن محسوب می شود.

برای این کار در جیمیل روی Settings کلیک کنید و در قسمت General روی بخش Browser connection گزینه Always use https را فعال کنید. و دکمه Save را بزنید. حالا یک بار از جیمیل خارج شوید و دوباره وارد اکانت ایمیل خود بشوید. از این به بعد جیمیل همیشه روی حالت https باز خواهد شد و تمام ایمیل‌های شما در مسیر به صورت رمزنگاری منتقل می شود.

همچنین برخلاف یاهو و هات میل، در جیمیل آدرس IP شما ضمیمه ایمیل های ارسالی تان نمی شود. بنابراین امکان ردیابی شما وجود نخواهد داشت. البته همین موارد نباید منجر به اعتماد کامل شما به گوگل و ارسال ایمیل های حساس و محرمانه توسط جیمیل شود. جیمیل مطالب کاربران را اسکن و ذخیره می کند و در صورت انجام تخلفات اینترنتی توسط یک کاربر، اطلاعات ایمیل او را پس از طی مراحل قانونی به دولت مربوطه تحویل می دهد.

راه حل دوم استفاده از سرویسRiseUp
در صورتیکه بتوانید از سرویس ایمیل RiseUp بهره مند شوید، یک وب میل امن دارید که به بهترین نحوه و با بهترین سیستم های رمزگذاری از ایمیل های شما محافظت می کند. این سوریس دهنده از بهترین و امن ترین راه های ایمن سازی ایمیل استفاده می کند. بر خلاف سیاست گوگل در ارائه اطلاعات ایمیل افراد بخاطر مسائل امنیتی کشورها، RiseUpاز سیاست امنیت مطلق برای کاربران استفاده می کند. (استفاده از این سرویس علیرغم رایگان بودن نیازمند پاسخ این سرویس دهنده به شما از طریق ارسال درخواست در سایت آن است. همچنین از طریق دعوت کاربران این سرویس -با دریافت دعوتنامه از طرف دو کاربر -می‌توان به عضویت آن در آمد. بنابراین متأسفانه دریافت حساب ایمیل در این سرویس کار آسانی نیست.

آدرس سایتhttps://mail.riseup.net :

به هر شکل سریعترین و بهترین راه برای دسترسی به این سرویس رایگان، پیدا کردن دو کاربر و درخواست دعوت نامه از طرف آنها است.

جیمیل، RiseUpو بسیاری از سرویس های ایمیل، از برنامه‌های (کلاینت (دریافت ایمیلی هم که بر روی کامپیوتر کاربر نصب می شود، پشتیبانی می کنند .یکی از این برنامه ها Mozilla Thunderbird است که بسیاری از تکنیک ها و سیستم های امنیت ایمیلی را پشتیبانی می کند. تضمین رمزگذاری اتصال اینترنتی برای یک کلاینت همانند دسترسی به سرویس ایمیل در وب از طریقHTTPS ، از اهمیت ویژه ای برخوردار است. در صورتی که شما به صورت مستقیم از وب میل خودتان استفاده نمی‌کنید و از یک کلاینت واسط مانند تاندربرد برای دریافت و ارسال ایمیل استفاده می‌کنید باید قبل از کار با آن، از برقرار بودن اتصال تحتSSL ، مطمئن باشید.

سوال: پس در این صورت بهتر است که من از RiseUp استفاده کنم. یا کار با جیمیل را با اعمال تغییر در تنظیمات جیمیل برای استفاده از HTTPS ادامه دهم؟
جواب: تصمیم با تو است، اما نکته هایی ظریف وجود داد که باید قبل از این تغییر بدانی. اول اینکه اگر تو فقط به یک ارتباط امن نیاز داری، جیمیل این قابلیت را دارد و می توانی از آن استفاده کنی. دوم اینکه آیا امنیت کامل ایمیل های تو برایت خیلی مهم است و دوست نداری تحت هیچ شرایطی به دست هیچ کس بیافتد؟ خب در این صورت بهتر است که از دومی استفاده کنی، البته اگر بتوانی یک حساب ایمیل در آن بدست بیاوری. اما داشتن جیمیل نیازی به درخواست دادن یا دعوت نامه ندارد.

با توجه به اهمیت تصمیم گیری در انتخاب یک سرویس ایمیل، به یاد داشته باشید که هر پیامی یک فرستنده و یک یا چند گیرنده دارد. حتی اگر شما در امن ترین حالت به ایمیل خود دسترسی داشته باشید، ممکن است گیرنده ایمیل در زمان دریافت، باز کردن، خواندن و یا حتی ارسال آن به دیگری بی دقتی کند .توجه داشته باشید که اگر می خواهید از امنیت ایمیل های ارسالی خود مطمئن باشید، باید ابتدا از وضعیت امنیتی دوستان و همکارانی که با آنها تبادل ایمیل دارید مطمئن شوید.

ضمناً باید به نکات دیگری هم توجه داشته باشید چرا که امکان دارد شما از جاهای دیگری که بسیار ساده هم به نظر می رسند، لطمه بخورید. مواردی مانند یک *Keylogger مخفی که روی سیستم شما نصب شده است، یا فردی که ممکن است از طریق یک دوربین مخفی رمز عبور شما را هنگام تایپ کردن ببیند و یا عدم رعایت اصول اولیه ایمنی از طرف فردی که با وی مکاتبه می کنید. یک راه خوب برای حل مشکلات امنیتی طرف مقابلتان این است که نگهبان را به او معرفی کنید تا بخواند!

Keylogger*یکی از برنامه های جاسوسی است که کلیدهای فشرده شده توسط کاربر را مانیتور و ذخیره کرده، برای شخص ثالثی می فرستد. این برنامه ها عموماً برای یافتن نام کاربری و رمز عبور حساب های اینترنتی و ایمیل ها بکار برده می شوند.

نکات تکمیلی برای بالا بردن سطح امنیت ایمیل
-۱همیشه در زمان باز کردن ایمیل های ناشناس و حاوی فایل ضمیمه، به اخطارهای احتمالی مرورگر و یا نرم افزار ایمیل خود توجه کنید و بدانید که کامپیوتر شما باید مجهز به یک آنتی ویروس قوی و به روز باشد.
-۲از نرم افزارهایی مانند (TOR (http://www.torproject.org ، برای مخفی کردن هویت استفاده کنید.
-۳در زمانیکه شما در یک سایت مانند تالار اینترنتی یا شبکه اجتماعی و غیره ثبت نام می کنید، که ممکن است بعداً از طریق سرویس ایمیل خود پیامی را برای این سایت ها ارسال کنید، توجه داشته باشید که بهتر است از نام واقعی خود و نام هایی که شناسایی شما را آسان می کنند، استفاده نکنید .مخصوصاً در سرویس های ایمیلی مانند یاهو و هات میل که آی پی شما را هم برای گیرنده به نمایش می گذارند، رعایت این نکته بسیار مهم است.
-۴در صورتی که افراد دیگری هم از کامپیوتر شما استفاده می کنند، باید در دوره های زمانی مشخص فایل های TemporarySیستم خود را پاک کنید. توصیه می کنیم از نرم افزار CCleaner برای این کار استفاده کنید.

" چگونه ردپا ها را با CCleaner پاک کنیم؟
-۵به هیچ عنوان روی لینک هایی که توسط ایمیل برای شما ارسال شده‌اند کلیک نکنید و حتماً افزونه NoScript را بر روی مرورگرتان نصب کنید.

NoScript "افزونه ای برای وبگردی ای امن

منبع: نگهبان