June 26, 2009

Dear Signatories:

Thank you for your letter dated June 16, 2009 concerning our use of HTTPS encryption technology in Google services, such as Gmail, Google Docs, and Google Calendar. As we mentioned in our blog post published on June 16 on the Google Online Security Blog, we're always looking at ways to help make the web more secure and more useful. We understand that you were pleased with our response, and we join you in your hope that other companies will also take steps to provide HTTPS options to their users.

Google has long demonstrated a focus on strong security in web applications, and we have been an industry leader in the HTTPS offerings we present to our users. As you mention in your letter, most providers of major web services — including Yahoo! Mail, Microsoft Hotmail, Facebook, and MySpace — offer less consistent or no HTTPS support for the whole time their users are accessing the service despite serving the majority of webmail users. By contrast, Gmail has provided free HTTPS since we launched the service in 2004. Typing https:// into the browser address bar or setting a bookmark instructs Gmail — or Google Docs or Google Calendar — to use HTTPS. In 2008 we improved our HTTPS support for Gmail users by adding a feature to the Gmail Settings page to give users a choice to keep HTTPS always on for their Gmail account. We are not aware of any other major provider of free webmail that has given all of their users the option of turning on HTTPS by default.

One of the key recommendations of your letter was that we should turn on HTTPS by default for all users of Gmail and other Google services. HTTPS is a subject that we have given a lot of thought, as evidenced by the atypically robust level of HTTPS support we already offer. While we think we've made good progress with our HTTPS options in Gmail, we know there is room to possibly offer more for some of our other products. Ideally, we'd like to provide HTTPS by default for all connections, but for now we need to investigate the ways to reduce performance impact for users since HTTPS can in some cases make web applications slower. At this stage, we stress the value of giving users the choice to enable HTTPS.

We agree it's important to continue to push for more adoption of HTTPS. Since long before we received your letter we have been considering the possibility of offering an HTTPS default setting as an option for users of some of our other services. As we mentioned in our blog post, we're planning a trial in which we'll move small samples of different types of Gmail users to HTTPS to see what their experience is, and whether it affects the performance of their email. We feel we need to more completely understand the impact of HTTPS on our users' experience, analyze the data from trials and experiments, and make sure we aren't introducing negative effects. In the absence of such negative effects or other complications, we intend to turn on HTTPS by default more broadly — hopefully for all Gmail users, and possibly for users of other applications like Google Docs and Google Calendar.

We'd like to clarify a point that was characterized incorrectly in your letter. Contrary to your claims, a cookie from Docs or Calendar doesn't give access to a Gmail session. The master authentication cookie is always sent over HTTPS — whether or not the user specified "always use HTTPS" for their Gmail account. Ultimately, we feel it's important to keep in mind that HTTPS is not a silver bullet for web security. No single company can make email across the Internet secure. While HTTPS can provide good protection for communication between a user and their mail provider, it cannot guarantee the security of the rest of the path the email travels during delivery. We want to enable users to take advantage of HTTPS for their email, but we are concerned that an overemphasis on HTTPS may lead people to believe that use of HTTPS means zero risk of emails being intercepted as they travel to other parts of the Internet.

At Google, we are always looking for ways to improve the services we provide our users and to help make the web more secure. We appreciate the interest and feedback from the research community, and we welcome helpful discussion of issues that will further these goals. We can all agree that HTTPS can provide real benefits. As we push to determine how we can best support HTTPS in our individual products and services, we will continue to encourage the broad use of HTTPS in web services across the industry.

Sincerely,

Alma Whitten
Software Engineer, Security and Privacy
Google Inc.