

IEEE G-Suite and Recent Report of Google Allowing App Developers to Access Your Email

IEEE became aware of an investigative report published by the Wall Street Journal headlined, “Tech’s Dirty Secret: The App Developers Sifting Through Your Gmail.” This article and other media reports raised privacy concerns for many people as well as some of our IEEE volunteers since Google G-Suite is used by staff in addition to members through the GoogleApps@IEEE service.

IEEE has determined that Google is not providing access to application developers to read your email regardless of whether you are using the free version of Gmail or one of their G-Suite versions. Google does provide a mechanism and ability for application developers to create applications (a.k.a. plugins or extensions) that provide extended functionality for Gmail users. This extended functionality may provide enhanced email and calendaring tasks such as, but not limited to; sorting email, automatically converting messages to follow-up tasks, re-prioritizing messages or setting up automatic reminders.

Before using any of these applications, Google presents the user with an authorization request, which specifies what the application will have access to. The user decides whether to allow the application to have access or not. This is very similar to installing an application on a mobile device, where the user is prompted to grant access to the application if it needs to access a hardware component (such as the camera or microphone), data or other applications on the device. According to the media reports it was determined some application developers have used the access granted by end users to gather samples of their email which was used to improve their products without their knowledge.

Google published a post on its Keyword blog to explain and defend its privacy practices (<https://slate.com/technology/2018/07/why-we-suddenly-care-that-google-let-app-developers-read-our-gmail.html>). Google has indicated that they enforce a multi-step review process that includes automated and manual review of the third-party developer applications. This includes assessing the applications homepage, privacy policy as well as testing to ensure they works as claimed. Google references a feature called Security Checkup that can be used by end users to periodically check their privacy settings, including the access they’ve granted to third-party applications.

Use of Google G-Suite at IEEE

IEEE is using Google G-Suite for Business for both members and staff. G-Suite for Business allows an enterprise to control and manage the use of G-Suite core services such as Email, Calendar, Google Drive and; provides security mechanisms to restrict access to third party applications and enforce security policies.

There are some differences in the way we support staff and members. There are a set of policies that control how staff has access to Google, we enforce retention policies for the staff. Currently, while we have the capability to control access to third-party applications, this is not enforced.

For IEEE members, we provide access to core G-Suite services similar to the ones used by staff with some exceptions. The core services available to members are defined by MGA. There are few restrictions applied to the applications that members are allowed to use. For example, we restrict the ability for members to create their own Google Site or create Google Groups.

Google encrypts all data stored in the G-Suite environment. Any 3rd party application that may interact with this data requires permission from the end user to do so. This applies to applications used by members and staff. This can be controlled, if needed, by denying access to all applications, and creating a whitelisted subset of approved applications. In this case, IEEE will need to review requested application(s) and approve their use prior to making them available to end users.

While there are retention policies applied to IEEE staff email, as required to maintain compliance with established legal, operations and financial processes; there are no retention policies applied to IEEE members using G-Suite and, as a result, the email stays in the member's mailbox until is removed by the member. Not all members keep their email in G-Suite, some have chosen to forward their email to external accounts – this may include anything that Google may consider spam since this is controlled by the member.

Staff data is backed up and legal-hold mechanisms are in place that enables the retention of data in the event of legal litigation. While this is not the case for our members, in some special cases the retention mechanism may be applied to members holding leadership positions at the IEEE as requested by the IEEE Legal and Compliance Department.