Google sumará cuentas verificadas en Gmail para evitar casos de suplantación de identidad

22/07/2020

Google anunció la incorporación de una nueva función de seguridad en Gmail que incluye el uso del logotipo de una marca como avatar junto al correo, para que el usuario sepa que recibió un correo electrónico genuino, y que no se trata de un caso de suplantación de identidad, **también conocido como phishing**.

La funcionalidad utiliza el estándar de indicadores de marca para la identificación de mensajes (BIMI), a cuyo grupo de trabajo se unió a Google el año pasado. **Esta herramienta se comenzará a probar con un número limitado de usuarios en las próximas semanas.**

"Nuestro piloto BIMI permitirá a las organizaciones, que autentican sus correos electrónicos utilizando DMARC, validar la propiedad de sus logotipos corporativos y transmitirlos de forma segura a Google. **Una vez que estos correos electrónicos autenticados pasen todas nuestras otras comprobaciones contra el uso abusivo, Gmail comenzará a mostrar el logotipo en las ranuras de avatar existentes en la interfaz de usuario de Gmail**", explicó la compañía en su blog oficial.

Es una lógica similar a la verificación (tilde azul) que se ve en las cuentas de algunos usuarios en Twitter o Instagram, por ejemplo. De este modo se busca dar cuenta de que el usuario en cuestión es quien dice ser y no alguien más. **En el caso de Gmail esa verificación no llegará de la mano de un tilde azul sino de la imagen de un logo.**

“Para las organizaciones que desean crear una presencia de marca confiable por correo electrónico, BIMI es una gran oportunidad, incentivándolos a implementar una autenticación sólida, lo que a su vez conducirá a un ecosistema de correo electrónico más seguro y confiable para todos”, dijo, el comunicado difudido, Seth Blank, presidente de el Grupo de Trabajo de Authindicators, y vicepresidente de Estándares y Tecnologías, Valimail.

Además de esta novedad, la compañía anunció otras actualizaciones que incorporarán en sus servicios con el objetivo de mejorar la seguridad.

Nuevos controles en Meet

1. Una vez que se expulsa a un asistente de una videoconferencia, ese usuario no podrá unirse a la misma reunión nuevamente, a menos que el anfitrión los vuelva a invitar.

2. Si una solicitud de llamada de un usuario se ha denegado varias veces, se bloqueará automáticamente al usuario para que no envíe más solicitudes para unirse a la reunión.

Se sumaron nuevas herramientas de seguridad a Google Meet.

3. **Los anfitriones accederán a bloqueos de seguridad avanzados para que puedan proteger mejor las reuniones con unos pocos clics.** Con los bloqueos de seguridad, los anfitriones pueden decidir qué métodos utilizar para que se unan los invitados. Puede ser, por ejemplo, por invitación de calendario o por teléfono. Y en el marco de estas opciones de seguridad, también se requiere que los usuarios obtengan una aprobación explícita por parte de los anfitriones para unirse a una videollamada.

4. Al activar los bloqueos de seguridad se bloquearán los intentos de todos los usuarios anónimos (usuarios que no han iniciado sesión en una cuenta de Google) de unirse a una

reunión, y se aplicará el requisito de que el anfitrión se una primero al encuentro.

5. **Los bloqueos de seguridad específicos permiten al anfitrión controlar el nivel de interacción de los participantes en la reunión**. El bloqueo de chat y el bloqueo actual permitirán a los anfitriones controlar qué asistentes pueden chatear o hacer presentaciones dentro de una reunión.

Nuevas funciones de seguridad en el chat

1. Cuando se envía un enlace a través del chat, se verificarán los datos en tiempo real y se indicará si se descubre que es un link malicioso.

2. En las próximas semanas, se podrá informar y bloquear salas de chat si se sospecha de actividad maliciosa en alguna de ellas.

Si se le envía un enlace a través de Chat, se verificará con los datos en tiempo real de Navegación segura y se marcará si se descubre que es malicioso.

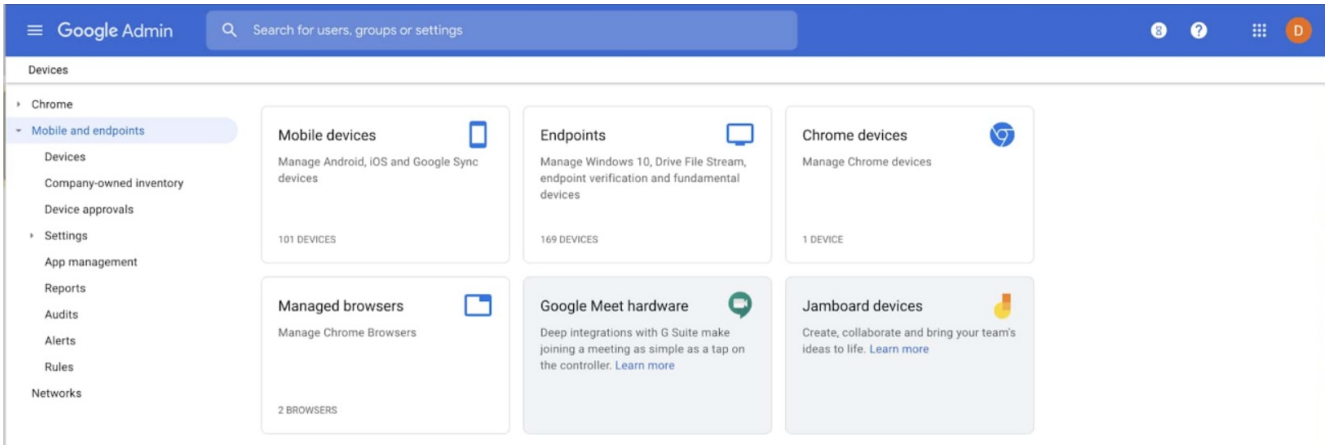
Controles de seguridad adicionales para los administradores

1. **Se rediseñó la página de dispositivos en la consola de administración de G Suite para incluir una navegación más intuitiva.** El objetivo es facilitar la administración de dispositivos y para mostrar rápidamente la cantidad de equipos administrados por cada servicio.

2. Se lanzó una integración con Apple Business Manager (anteriormente DEP) para proporcionar a los administradores de G Suite Enterprise, G Suite Enterprise Essentials, Cloud Identity Premium y G Suite Enterprise for Education la capacidad de distribuir y administrar de manera simple y segura dispositivos iOS.

3. Ahora los administradores pueden usar **controles**

automatizados de gestión de derechos de información (IRM) para evitar la filtración de datos al impedir que los usuarios finales descarguen, impriman o copien documentos, hojas y diapositivas de Google Drive que contengan contenido confidencial.



Se rediseñó la página de dispositivos en la consola de administración de G Suite (Google).

Estos controles se relacionan con las reglas de Prevención de pérdida de datos que se han establecido para la organización, y los administradores pueden ejecutar un análisis completo de todos los archivos dentro de Google Drive y **habilitar automáticamente estos controles para todos los usuarios.** Todas estas funciones ahora **están disponibles en Beta para G Suite Enterprise, G Suite Enterprise Essentials y G Suite Enterprise for Education.**

4. Además, los administradores ya pueden decidir **qué aplicaciones de terceros pueden acceder a los datos de G Suite de los usuarios con OAuth 2.0**. Ahora, con el control de acceso a la aplicación, pueden bloquear el acceso de las aplicaciones a los servicios de G Suite a través de la API sin crear una lista de permisos para cada aplicación que requiere acceso a los datos de G Suite.

Fuente: Infobae