PROFUNDICEMOS SOBRE EL TEMA

Riesgos de privacidad en el inicio de sesión con cuentas de redes sociales o Google

> ***OAuth: inicio de sesión único en varias plataformas***[1]
> *En nuestro día a día, visitamos muchos sitios web y utilizamos diferentes programas y aplicaciones móviles para hacer que nuestra vida personal y profesional sea más sencilla y agradable. Al existir tal cantidad de herramientas a nuestra disposición, cada vez es más normal utilizar el contenido de una aplicación web (como Instagram) en otro sitio web (como Facebook). En resumen, el contenido se utiliza en varias plataformas al mismo tiempo. Sin embargo, para que estos procesos puedan llevarse a cabo, es necesario ceder muchos datos personales y, en este punto, surge la cuestión relativa a la seguridad de la privacidad. El protocolo de autenticación OAuth ha sido diseñado precisamente para reducir los riesgos asociados al uso no autorizado de nuestros datos. La pregunta es: ¿está realmente a la altura de su cometido?*

¿Cuántas contraseñas utilizas a lo largo del día? ¿10? ¿20? Y se supone que todas ellas tienen que ser diferentes, largas, suficientemente complejas, no estar relacionadas con su vida, etc. Todo esto para que sean seguras y un atacante no las pueda adivinar o reutilizar si las averigua o roba.

Para ahorrarles trabajo, en los últimos años se está trabajando mucho en ofrecer a los usuarios soluciones que les permitan autenticarse (demostrar que son quienes dicen ser) cuando necesitan utilizar un recurso, aplicación o servicio web, normalmente desde su PC o móvil.

Una de estas soluciones son los **esquemas federados** para la gestión de accesos. Se llaman esquemas federados porque se basan en construir federaciones de confianza: los usuarios finales y los proveedores de los recursos, aplicaciones o servicios a los que quieren acceder (una tienda de comercio electrónico, el banco, la web) confían en proveedores de identidades.

De esta manera, para acceder a cualquier servicio (ajeno a esas compañías), basta con que el usuario se autentique, normalmente con una contraseña, en el proveedor de identidades. Es decir, puede registrarse o iniciar sesión a través de Google, Apple o alguna red social para no tener que crear una nueva cuenta y su clave correspondiente.Es rápido. Es fácil. ¿Pero es seguro? Iniciar sesión en sitios web con Facebook y Google tiene sus riesgos, pero también ventajas.

---

[1] Extraìdo de: https://www.ionos.es/digitalguide/servidores/seguridad/oauth-y-su-version-oauth2/

Riesgos	Ventajas
• Pérdida de control sobre los datos personales, cuando el servicio accede a determinados datos del perfil social del usuario. • Utilización de los datos obtenidos de la red social para finalidades distintas de las consentidas por el usuario. • Acceso de las redes sociales a una mayor información sobre nuestro uso de las aplicaciones o comportamiento por Internet, lo que facilita el seguimiento y perfilado. • Ante una brecha de seguridad del servicio no se verá afectada la contraseña del usuario porque al ingresar de esa forma no estamos brindando una contraseña, pero si puede verse afectada mucha información del perfil social de usuarios, incluidos datos sobre sus intereses y perfilado para publicidad comportamental. • En caso de perder el control sobre la cuenta de la red social (robo de credenciales), se pierde también el control del resto de servicios donde nos hemos registrado con esa cuenta, que podrían también verse comprometidos.	• Nos ayuda a reducir el número de contraseñas que usamos. • Los procesos de registro son más rápidos porque muchos de los detalles de registro, si no todos, son automáticamente proporcionados por el servicio de autenticación federada. • Existe menos riesgo de que nuestras contraseñas de acceso acaben viéndose afectadas por una brecha de seguridad en el servicio concreto al que accedemos, porque todas esas aplicaciones y servicios no guardarán de ninguna forma nuestras contraseñas. Y en caso de verse afectada sólo sería necesario cambiar una contraseña. • Las redes sociales pueden llegar a tener datos muy completos sobre nosotros, nuestra vida, nuestros gustos, nuestras aficiones, nuestros intereses, etc., tanto por la información que hemos facilitado en nuestros perfiles de usuario como por los datos obtenidos o inferidos directamente a través del uso que hacemos de las aplicaciones de Internet en las que nos autenticamos haciendo uso de esta técnica.

Para realizar un ***USO SEGURO*** de esta tecnología sigue las siguientes recomendaciones:

- Antes de iniciar sesión con tu cuenta de una red social en una aplicación, infórmate sobre esa aplicación y sobre los datos a los que tendrá acceso, valora también el uso que vas a hacer de la misma.

- Si se trata de una aplicación que desconoces, que únicamente vas a utilizar puntualmente, o simplemente quieres conocerla y experimentar, evita iniciar sesión con tus credenciales de tu red social habitual.

- No guardes contraseñas en el navegador ni las reutilices en diferentes servicios.

- Utiliza únicamente aquellos servicios de identidad federada que te ofrezcan mejores garantías respecto al uso de tus datos personales, mayor control sobre los datos personales que compartirán con la aplicación en la que te registras y medidas de seguridad adecuadas, como un segundo factor de autenticación.

- Cuando utilices tus credenciales de una red social para acceder a una aplicación asegúrate de gestionar adecuadamente los permisos de acceso a tus datos personales que concedes a la aplicación, tanto en el momento del registro como posteriormente. Evita obtener más datos de ti de los que consideres necesarios.

- Gestiona y revisa en los ajustes de privacidad de tu cuenta en redes sociales, las aplicaciones en las que has iniciado sesión o permites que se inicie sesión, eliminado o revocando el permiso para aquellas que hayas dejado de utilizar.

Link de referencias:

- https://www.avg.com/es/signal/is-it-safe-to-log-in-with-facebook-or-google

- https://skynet-sys.es/iniciar-sesion-con-tus-cuentas-de-redes-sociales-supone-un-riesgo-de-privacidad/

- https://www.aepd.es/es/prensa-y-comunicacion/blog/riesgos-privacidad-iniciar-sesion-cuentas-rrss-otras-aplicaciones